Topics in Number Theory
Lecture Notes for MTH 417
Spring 2010

Ulrich Meierfrankenfeld

April 30, 2010

Preface

These are the Lecture Notes for the class MTH 417 in Spring 10 at Michigan State University. The notes are based on Jones and Jones, Elementary Number Theory [Text Book].

Contents

Chapter 1

Set Theory

1.1 Induction and the Well Ordering Principal

Let $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, \ldots\}$. So $\mathbb{N}$ is the natural numbers, that is the set of all non-negative integers.

Just for fun, let us define what we mean with the symbols, $0, 1, 2, 3$ and so on.

We define 0 the empty set: $0 := \{\}$. 1 is the set whose only element is the empty set, so $1 := \{\{\}\} = \{0\}$. 2 is the set whose elements are 0 and 1: $2 := \{0, 1\} = \{\{\}, \{\{\}\}\}$. Observe that 2 is the unions of the set $\{0\}$ and $\{1\}$. Since $1 = \{0\}$ we have $2 = 1 \cup \{1\}$. Suppose we already define a natural number n. Then we define

$$n + 1 := n \cup \{n\}$$

So $n + 1$ has all the elements of n, plus one more: $\{n\}$. It follows that

$$n + 1 = \{0, 1, 2, 3, \ldots, n\}$$

The natural numbers will be the main object of interest in the class. The most of important tool to prove statement about the natural numbers

Axiom 1 (Principal of Induction)**.** [**pi**] *Let $P(n)$ be a statement involving the variable n. Suppose that*

(I1) [**1**] *$P(1)$ is true.*

(I2) [**2**] *If $P(n)$ is true for a natural number n, then also $P(n + 1)$ is true.*

Then $P(n)$ is true for all n.

Since this is not a logic class, we will not define what we really mean with '$P(n)$ be a statement involving the variable n' and '$P(n)$' is true. Instead, here is an equivalent version of a the Principal of induction, purely in set theoretic terms:

Axiom 2 (Principal of Induction, Set Theoretic Version)**.** [**pis**] *Let A be a set of natural numbers. Suppose that*

(I1S) [**1**] *$1 \in A$.*

(I2S) [**2**] *If $n \in A$ then $n + 1 \in A$. true.*

Then $n \in A$ for all $n \in N$ (that is $A = \mathbb{N}$.).

Lets us prove that the two version are equivalent. Indeed if $P(n)$ is statement, then define

$$A = \{n \in \mathbb{N} \mid P(n)\}$$

Conversely if A is a set of natural number, define $P(n)$ to be statement

$$P(n): \qquad n \in A$$

In both cases we see that

$$P(n) \text{ is true } \iff n \in A$$

and so

$$P(1)\text{true} \iff 1 \in A,$$

$$\begin{gathered} P(n) \text{ is true for a natural number } n \text{, then also } P(n+1) \text{ is true .} \\ \iff \\ \text{If } n \in A \text{ then } n+1 \in A. \end{gathered}$$

and

$$\begin{gathered} P(n) \text{ is true for all natural numbers.} \\ \iff \\ n \in A \text{ for all } n \in N \end{gathered}$$

This shows what the two versions of the principal of inductions are indeed equivalent.
Often we will use the following more powerful version of the principal of inductions:

Axiom 3 (Principal of Strong Induction)**.** [**psi**] *Let $P(n)$ be a statement involving the variable n. Suppose that for all $n \in \mathbb{N}$,*

(SI) [**2**] *If $P(k)$ is true for a natural number k with $k < n$, then also $P(n)$ is true.*

Then $P(n)$ is true for all positive integers n.

Also the Principal Strong Induction has a set theoretic version:

Axiom 4 (Principal of Strong Induction, Set Theoretic Version)**.** [**psis**] *Let A be a set of natural numbers. Suppose that for all $n \in \mathbb{N}$,*

(SIS) [**sis**] *If $k \in A$ for all $k \in \mathbb{N}$ with $k < n$, then $n \in A$.*

Then $n \in A$ for all $n \in \mathbb{N}$ (that is $A = \mathbb{N}$.).

The same argument as above, shows that Principal of Strong Induction is equivalent to its set theoretic version,
As we will prove below, all of the above principal of inductions are equivalent to

Axiom 5 (Well Ordering Principal)**.** [**L**]*et A be a non-empty set of natural numbers. Then A has a least element, that is there exists $m \in A$ with $m \leq a$ for all $m \in A$.*

Theorem 1.1.1. [**equivalence of induction**] *The following are equivalent:*

(a) [**a**] *The Principal of Induction.*

(b) [**b**] *The Principal of Strong Induction.*

(c) [**c**] *The Principal of Induction, Set Theoretic version.*

(d) [**d**] *The Principal of Strong Induction,Set Theoretic version.*

(e) [**e**] *The Well Ordering Principal.*

Proof. We already have seen that (a) and (c) are equivalent, and that (b) and (d) are equivalent. So it suffices to show that the last three statements are equivalent.

(c) $\Longrightarrow$ (d): Let A be set such that $n \in A$ whenever $n \in N$ with $k \in A$ for all $k \in \mathbb{N}$ with $k < n$. But

$$B = \{n \in \mathbb{N} \mid k \in A \text{ for all } k \in \mathbb{N} \text{ with } k < n\}$$

The clearly $1 \in B$ and if $n \in B$, then $n \in A$ by assumptions. If $k < n+1$. then $k < n$ or $k = n$ and so $n+1 \in B$. The Principal of induction implies $n \in B$ for all $n \in \mathbb{N}$ and since $n < n = 1$, $n \in A$ for all $n \in A$.

(d) $\Longrightarrow$ (e): Let A be a set and A has no least element. Put $B = N \setminus A$. Let $n \in B$ such that $k \in B$ for all $k \in \mathbb{N}$ with $k < n$. Then $k \notin A$ for all k with $k < n$ and so $n \leq a$ for all $a \in A$. Since A has no least element $n \notin A$ and so $n \in B$. The Principal of Strong Induction now implies that $B = \mathbb{N}$ and so $A = \mathbb{N} \setminus B = \emptyset$.

(e) $\Longrightarrow$ (c): Let A be set with $1 \in A$ and $n+1 \in A$ whenever $n \in A$. Let $B = \mathbb{N} \setminus A$. Suppose that B has a least element m. Since $1 \in A$, $m \neq 1$. Thus $m > 1$, $m-1 \in \mathbb{N}$ and $m-1 < m$. Since m is minimal elements of B, $m-1 \notin B$ and so $m-1 \in A$. Hence $m = (m-1)+1 \in A$, a contradiction to $m \in B$. Thus B has no least element and the Well Ordering Principal shows that $B = \emptyset$. Thus $A = \mathbb{N} \setminus B = \mathbb{N}$. □

1.2 Equivalence Relations

Definition 1.2.1. [**def:relation**] *Let A be a set.*

(a) [**a**] *A* relation *on A is a subset R of $A \times A$. Let $a, b \in A$ we will write aRb if $(a, b) \in R$.*

(b) [**b**] *A relation R in A is called*

- *(a)* [**a**] reflexive *if aRa for all $a \in R$.*
- *(b)* [**b**] symmetric *if bRa for all $a, b \in R$ with aRb.*
- *(c)* [**c**] transitive *if aRc for all $a, b, c \in R$ with aRb and bRc.*
- *(d)* [**d**] *an* equivalence relation *if R is reflexive, symmetric and transitive.*

(c) [**c**] *Let R be relation on A and $a \in A$. Then $[a]_R := \{b \in R \mid aRb\}$. if there is no doubt about the relation in mind. We just write $[a]$ for $[a]_R$,*

(d) [**d**] *Let R be an equivalence relation on A and $a \in A$. Then $[a]_R$ is called an equivalence class of R. $A/R := \{[a]_R \mid a \in A\}$. So A/R is the set of equivalence classes of R.*

Lemma 1.2.2. [**basic equivalence**] *Let R be an equivalence relation on A and $a, b \in R$. Then the following statements are equivalent* *(a)* [**a**] aRb

(b) [**b**] $b \in [a]$.

(c) [**c**] $[a] \cap [b] \neq \emptyset$.

(d) [**d**] $[a] \subseteq [b]$

(e) [**e**] $a \in [b]$

(f) [**f**] $[b] \subseteq [a]$

(g) [**g**] $[a] = [b]$.

(h) [**h**] bRa.

In particular, a lies in a unique equivalence class of R, namely $[a]$.

Proof. (a) $\Longrightarrow$ (b): If aRb, then by definition of $[a]$, $b \in [a]$.

(b) $\Longrightarrow$ (c): Since R is reflexive, bRb and so $b \in [b]$. Thus $b \in [a] \cap [b]$ and $[a] \cap [b] \neq \emptyset$.

(c) $\Longrightarrow$ (d): Let $c \in [a] \cap [b]$ and $d \in [b]$. Then aRd, aRc and bRc. Since R is symmetric, we get dRa, aRc and cRb. Since R is transitive, this gives dRc and then dRb and bRd. Hence $d \in [b]$ and so $[a] \subseteq [b]$.

(d) $\Longrightarrow$ (e): Since R is reflexive, aRa and $a \in [a]$. Since $[a] \subseteq [b]$, $a \in [b]$.

(e) $\Longrightarrow$ (f): Apply Steps '(b) $\Longrightarrow$ (c): ' and '(c) $\Longrightarrow$ (d): ' with to (b, a) in place of (a, b).

(f) $\Longrightarrow$ (g): We have $b \in [b] \subseteq [a]$ and so $[a] \cap [b] \neq \emptyset$. Step '(c) $\Longrightarrow$ (d): ' implies $[b] \subseteq [a]$. So $[a] = [b]$.

(g) $\Longrightarrow$ (h): $a \in [a] = [b]$ and so bRa.

(h) $\Longrightarrow$ (a): This hold since R is symmetric.

Since (c) and (g) are equivalent, $a \in [b]$ if and only if $[b] = [a]$. So $[a]$ is the unique equivalence class containing a. $\square$

Chapter 2

Divisibility

2.1 The Division Algorithm

Theorem 2.1.1 (Division Algorithm)**.** [**division algorithm**] *Let a and b be integers with $b \neq 0$. Then there exists unique integers q and r with*

$$a = qb + r \text{ and } 0 \leq r < |b|$$

Proof. Let $A = \{a - kb \mid k \in \mathbb{Z}\}$. Put $k = -\frac{|b|}{b}|a|$. Then $k = \pm a$ and so $k \in \mathbb{Z}$. Since $b \neq 0$, $|b| \geq 1$ and so

$$a - kb = a - (-\frac{|b|}{b}|a|)b = a + |a||b| \geq a + |a| \geq 0$$

If follows that $A \cap \mathbb{N} \neq \emptyset$ and so by the Well Ordering Principal, $A \cap \mathbb{N}$ has a least element r. Then $r \geq 0$ and $r = a - qb$ for some $a \in \mathbb{Z}$. Suppose that $|b| \leq r$. Then

$$0 \leq r - |b| = a - qb - |b| = a - (q + \frac{|b|}{b})b$$

Thus $r - |b| \in A \cap \mathbb{N}$, a contradiction since $r - |b| < r$ and r is the least element of $A \cap \mathbb{N}$.

This show the existence of q and r. To show uniqueness, let $q, \tilde{q}, r, \tilde{r} \in \mathbb{Z}$ with

$$a = qb + r, 0 \leq r < |b|, a = \tilde{q}b + r \text{ and } 0 \leq \tilde{r} < |b|$$

Thus $qb + r = a = \tilde{q}b + \tilde{r}$ and so

$$(*) \qquad (q - \tilde{q})b = \tilde{r} - r$$

Since $0 \leq \tilde{r}$ and $r < |b|$ we have $-|b| = 0 - |b| < \tilde{r} - r$ and and since $\tilde{r} < |b|$ and $0 \leq r$, $r - \tilde{r} < |b| - 0 = |b|$. Hence $-|b\langle \tilde{r} - r < |b|$ and by (*) $-|b| < (q - \tilde{q})b < |b|$. Therefore $|q - \tilde{q}||b| < |b|$ and dividing by $|b|$ gives $|q - \tilde{q}| \leq 1$. Since $q - \tilde{q}$ is an integer, this implies $q - \tilde{q} = 0$. (*) $\tilde{r} - r = 0$ and thus $q = \tilde{q}$ and $r = \tilde{r}$. So q and r are indeed unique. ☐

q is called the *integer quotient* and r the *remainder* of a when divided by b.

Lemma 2.1.2. [**n2mod4**] *Let n be an integer. Then the remainder of n^2 when divided by 4 is 0 or 1.*

Proof. By the division algorithm $n = 2q+r$ with $0 \leq r < 1$. The $r = 0$ or 1 and so $r = r^2$. Moreover,

$$n^2 = (2q + r)^2 = 4q^2 + 4qr + r^2 = 4(q^2 + qr) + r$$

Since $0 \leq r < 4$, we see that r is the remainder of n^2, when divided by 4. $\square$

Definition 2.1.3. [**def:divide**] *Let a and b be integers. Then we say that a* divides *b and write $a|b$ if there exists an integer n with $b = am$.*

Instead of saying that a divides b, we will often use the expression a is a factor of b or b is a multiple of a.

Let a be any integer. Then $a|a$, $a|-a$, $a|0$ and $1|a$. But $0|a$ if and only if $a = 0$.

Lemma 2.1.4. [**basic divide**] *Let a, b and c be integers.*

(a) [**a**] *If $a|b$ and $b|c$, then $a|c$.*

(b) [**b**] *If $a|b$ and $a|c$, then $a|b + c$.*

(c) [**c**] *If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*

Proof. (a) By definition of dividing we have $b = ka$ and $c = lb$ for some integers k and l. Thus

$$c = lb = l(ka) = (lk)a$$

Since l and k are integers also lk is an integer and thus $a \mid c$, by the definition of divide.

(b) By definition of dividing we have $b = ka$ and $c = la$ for some integers k and l. Thus

$$b + c = ka + la = (k + l)a$$

Since l and k are integers also $k + l$ are integers and thus $a|b + c$, by the definition of divide.

(c) I By definition of dividing we have $b = ka$ for some integer k. Since $0a = 0$ and $b \neq 0$, $k \neq 0$. Since k is an integer this gives $|k| \geq 1$ and so $|b| = |ka| = |k||a| \geq 1|a| = |a|$. $\square$

Corollary 2.1.5. [**divide linear comb**] *Let $a, b_1, b_2, \ldots b_k, l_1, l_2, \ldots l_k$ be integers with $a|b_i$ for all $1 \leq i \leq k$. Then*

$$a|l_1b_1 + l_2b_2 + \ldots + l_kb_k$$

Proof. Since $a|a_k$ and $a_k|l_kb_k$, 2.1.4(a), shows that $a|a_kb_k$. In particular, the statement holds for $k = 1$. Assume inductively that the statements holds for $k-1$. Then $a|l_1b_1 + l_2b_2 \ldots l_{k-1}b_{k-1}$. Since also $a \mid a_kb_k$, 2.1.4(b) shows

$$a|(l_1b_1 + l_2b_2 \ldots l_{k-1}b_{k-1}) + l_kb_k$$

and so the statements also hold for k. $\square$

Lemma 2.1.6. [**greatest element**] *Let A be a set of non-empty set of integers numbers and suppose there exists $k \in \mathbb{Z}$ with $a \leq k$ for all $a \in A$. Then A has a greatest element, that is there exists $d \in A$ with $a \leq d$ for all $a \in A$.*

Proof. Let $B = \{k-a \mid a \in A\}$. Since $a \leq k$, $k-a \in \mathbb{N}$. Thus B is non-empty set of natural number and so by the Well ordering principal has a least element b. Then $b = k - d$ for some $d \in A$. The $k - d \leq k - a$ for all $a \in A$ and so $a \leq d$. $\square$

Definition 2.1.7. [**def:gcd**] *Let A be a set of integers and d an integer.*

(a) [**a**] *We say that d is a* common divisor *if A and write $d|A$, if $d|a$ for all $d \in A$.*

(b) [**b**] $\mathrm{Div}(A) = \{d \in \mathbb{Z} \mid d \mid A\}$ *is the set of common divisor of A.*

(c) [**c**] *We say that d is a* greatest common divisor *of A, if d is a greatest element of* $\mathrm{Div}(A)$*, that is if*

  (i) [**i**] *$d \mid a$ for all $a \in A$, and*

  (ii) [**ii**] *If $e \in A$ with $e \mid a$ for all $a \in A$, then $e \leq d$*

If d and e are greatest common divisors of a set of integers A, then $d \leq e$ and $e \leq d$. So $e = d$. This shows that A has at most one greatest common divisor.

Lemma 2.1.8. [**gcd**] *Let A be a set of integers. Then A has a greatest common divisor if and only if $A \nsubseteq \{0\}$.*

Proof. Suppose first that $A \subseteq \{0\}$. Since $n|0$ for all $n \in \mathbb{Z}$ we conclude that $\mathrm{Div}(A) = \mathbb{Z}$ and so $\mathrm{Div}(A)$ does not have a greatest element.

Suppose next that $A \nsubseteq \{0\}$. Then there exists $a \in A$ with $a \neq 0$. Since $n \mid a$ for all $n \in \mathrm{Div}(A)$ we get $n \leq |a|$ for all $n \in \mathrm{Div}(A)$ and so be 2.1.6, $\mathrm{Div}(A)$ has a greatest element. □

Notation 2.1.9. [**not:gcd**] *Let A be a set of integers. If $A \subseteq \{0\}$ then* $\gcd(A) = 0$ *and if $A \nsubseteq \{0\}$ then* $\gcd(A)$ *is the greatest common divisor of A.*

Lemma 2.1.10. [**equal gcd**] *Let a, b, q and r be integers with $a = qb + r$. Then* $\mathrm{Div}(a, b) = \mathrm{Div}(b, r)$ *and* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $m \in \mathrm{Div}(a, b)$. The m divides a and b and also $r = a - rb$. Thus $\mathrm{Div}(a, b) \subseteq \mathrm{Div}(b, r)$.

Now let $m \in \mathrm{Div}(b, r)$. The m divides b and r and also $a = qb + r$. Thus $\mathrm{Div}(b, r) \subseteq \mathrm{Div}(a, b)$. This proves the first statement. The second follows from the first. □

Lemma 2.1.11. [**gcd a0**] *Let $a \in \mathbb{Z}$. Then* $\gcd(a, 0) = |a|$.

Proof. Note that $\mathrm{Div}(a, 0) = \mathrm{Div}(a) = \mathrm{Div}(|a|)$. If $a \neq 0$, then $b \leq |a|$ for all $b \in \mathrm{Div}(|a|)$ and so $\gcd(a, 0) = |a|$. If $a = 0$, then $\mathrm{Div}(|a|) = \mathbb{Z}$ and $\gcd(a, 0) = 0 = |a|$. □

Theorem 2.1.12 (Bezout)**.** [**bezout**] *Let a and b be integers and let E_{-1} and E_0 be the equations*

$$\begin{array}{rccccccc} E_{-1}: & a & = & 1 & a & + & 0 & b \\ E_0: & b & = & 0 & a & + & 1 & a \end{array}$$

and suppose inductively we defined equation $E_k, -1 \leq k \leq i$ of the form

$$\begin{array}{rccccccc} E_k: & r_k & = & x_k & a & + & y_k & b \end{array}$$

If $r_i \neq 0$, let E_{i+1} be equation obtained by subtracting q_{i+1} times equation E_i from E_{i-1} where q_{i+1} is the integer quotient of r_{i-1} when divided by r_i. Let $m \in \mathbb{N}$ be minimal with $r_m = 0$ and put $d = r_{m-1}$, $x = x_{m-1}$ and $y = y_{m-1}$.

(a) [**a**] $\gcd(a, b) = |d|$

(b) [**b**] $x, y \in \mathbb{Z}$ *and* $d = xa + yb$,

Proof. Observe that $r_{i+1} = r_{i-1} - q_{i+1}r_i$, $x_{i+1} = x_{i-1} - q_{i+1}x_i$ and $y_{i+1} = y_{i-1} - q_{i+1}x_i$. So inductively $r_{i+1}, x_{i+1}, y_{i+1}$ are integers and r_{i+1} is the remainder of r_{i-1} the divided by r_i. So $r_{i+1} < |r_i|$ and the algortithm will terminate in finitely many steps.

From $r_{i-1} = q_{i+1}r_i + r_{i+1}$ and 2.1.10 we have $\gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1})$ and so

$$\gcd(a, b) = \gcd(r_{-1}, r_0) = \gcd(r_0, r_1) = \ldots = \gcd(r_{m-1}, r_m) = \gcd(d, 0) = |d|$$

So (a) holds. Since each x_i and y_i are integers, x and y are integers. $d = xa + yb$ is just the equation E_{m-1}. □

Example 2.1.13. [**ex:bezout**] *Let* $a = 1492$ *and* $b = 1066$. *Then*

$$\begin{array}{rcrcl}
1492 & = & 1 \cdot 1492 & + & 0 \cdot 1066 \\
1066 & = & 0 \cdot 1492 & + & 1 \cdot 1066 \\
426 & = & 1 \cdot 1492 & - & 1 \cdot 1066 \\
214 & = & -2 \cdot 1492 & + & 3 \cdot 1066 \\
212 & = & 3 \cdot 1492 & - & 4 \cdot 1066 \\
2 & = & -5 \cdot 1492 & + & 7 \cdot 1066 \\
0 & & & &
\end{array}$$

So $\gcd(1492, 1066) = 2$ *and* $2 = -5 \cdot 1492 + 7 \cdot 1066$

Corollary 2.1.14. [**linear eq**] *Let* a, b, c *be integers. Then the equation*

$$xa + yb = c$$

has integral solution if and only if $\gcd(a, b)\,|c$.

Proof. Suppose first that $c = ax + by$ for some $x, y \in \mathbb{Z}$. Since $\gcd(a, b)$ divides a and v, we conclude from 2.1.5 that $\gcd(a, b)$ divides c.

Suppose next that $\gcd(a, b)\,|c$. then $c = k\gcd(a, b)$ for some $k \in \mathbb{Z}$. By 2.1.12, $\gcd(a, b) = ua + vb$ for some $u, v \in \mathbb{Z}$ and hence $c(ku)a + (kv)b$. □

Definition 2.1.15. [**def:lcm**] *Let* A *be a set of integers and* $m \in \mathbb{Z}$.

(a) [**a**] *We say that* m *is a* common multiple *of* A *and write* $A|m$ *if* $a|m$ *for all* $a \in A$.

(b) [**b**] $\mathrm{Mult}(A) = \{m \in \mathbb{Z} \mid A|m\}$ *is the set of common multiples if* A.

(c) [**c**] *If* $\mathrm{Mult}(A) \cap \mathbb{Z}^+ \neq \emptyset$ *then* $\mathrm{lcm}(A)$ *is the least element of* $\mathrm{Mult}(A) \cap \mathbb{Z}^+$. *If* $\mathrm{Mult}(A) \cap \mathbb{Z}^+ = \emptyset$, *then* $\mathrm{lcm}(A) = 0$. $\mathrm{lcm}(A)$ *is called the* least common multiple *of* A.

If $A = \emptyset$ then $\mathrm{Mult}(\emptyset) = \mathbb{Z}$ and so $\mathrm{lcm}(A) = 1$. If $A = \{a_1, a_2, \ldots, a_n\}$ is a non-empty of non-zero integers, then $|a_1a_2\ldots a_n| \in \mathrm{Mult}(A) \cap \mathbb{Z}^+$ and so $\mathrm{lcm}(A) \in \mathbb{Z}^+$. If A is infinite or A contains 0, then $\mathrm{Mult}(A) = \{0\}$ and so $\mathrm{lcm}(A) = 0$.

Lemma 2.1.16. [**gcd lcm**] *Let* a *and* b *be integers.*

(a) [**a**] $\gcd(a,b)\,\mathrm{lcm}(a,b) = |ab|$.

(b) [**b**] *Let $m \in \mathbb{Z}$. Then $a|m$ and $b|m$ if an only if $\mathrm{lcm}(a,b)|m$.*

Proof. If $a = 0$ and $b = 0$ this is readily verified. So assume that $(a,b) \neq 0$. Replacing a and b by $|a|$ and $|b|$ we may assume that $a \geq 0$ and $b \geq 0$. $d = \gcd(a,b)$ and $l = \frac{ab}{d}$. We first prove

1°. [**1**] *$l \in \mathbb{Z}^+$ and l divides a and b.*

Note that $l = \frac{b}{d}a = \frac{a}{d}b$. Since $d|a$ and $d|b$, (1°) holds.

2°. [**2**] *If $m \in \mathbb{Z}$ with $a|m$ and $b|m$, then $l|m$.*

By 2.1.12, $d = xa + yb$ for some integers x and y. Thus

$$\frac{m}{l} = \frac{m}{\frac{ab}{d}} = \frac{md}{ab} = \frac{m(xa+yb)}{ab} = \frac{m}{b}x + \frac{m}{a}y$$

Since $a|m$ and $b|m$, both $\frac{m}{b}$ and $\frac{m}{a}$ are integers. Hence also $\frac{m}{l} = \frac{m}{b}x + \frac{m}{a}y$ is an integer and so $l|m$.

3°. [**3**] *$l = \mathrm{lcm}(a,b)$ and so (a) holds.*

By (1°), l is a common multiple of a and b. If m is any common multiple of a and b, then by (2°), $l \mid m$. so by 2.1.4(c), $l = |l| \leq |m|$. Thus l is the least element of $\mathrm{Mult}(a,b) \cap Z^+$ and so $l = \gcd(a,b)$.

It remains to prove (b). By (3°) and (2°), $\mathrm{lcm}(a,b)$ divides any common multiple of a and b. Conversely suppose that $\mathrm{lcm}(a,b) \mid m$ for some $m \in \mathbb{Z}$. Since a and b divide m we conclude (see 2.1.4(a)) that a and b divide m. Thus (b) holds. □

Corollary 2.1.17. [**lcm and mult**] *Let A be a finite set of integers.*

(a) [**a**] *If $A = B \cup C$ for some subsets B and C, then*

$$\mathrm{lcm}(A) = \mathrm{lcm}(\mathrm{lcm}(B), \mathrm{lcm}(C))$$

(b) [**b**] *Let $m \in \mathbb{Z}$. Then $A|m$ if and only if $\mathrm{lcm}(A)|m$.*

Proof. We will prove (a) and (b) simultaneously by induction on $|A|$. If $|A| = 0$, the $A = \emptyset = B = C$, $A|m$ for all $m \in \mathbb{Z}$ and $\mathrm{lcm}(A) = 1$. So both (a) and (b) hold.

So suppose $|A| > 0$ and let $A = B \cup C$ for subsets B and C of A. If $A = B = C$, then clearly (a) holds. So we may assume that $B \neq A$. and so by induction $\mathrm{lcm}(B)|m$ for all $m \in \mathrm{Mult}(B)$. In particular, $\mathrm{lcm}(B)|\,\mathrm{lcm}(A)$. Assume that $C = A$. It follows that $\mathrm{lcm}(\mathrm{lcm}(B), \mathrm{lcm}(C)) = \mathrm{lcm}(C) = \mathrm{lcm}(A)$ and again (b) holds. Assume $C \neq A$, then by induction also $\mathrm{lcm}(C)|m$ for all $m \in \mathrm{Mult}(C)$ Hence

$$\mathrm{Mult}(A) = \mathrm{Mult}(B \cup C) = \mathrm{Mult}(B) \cap \mathrm{Mult}(C) = \mathrm{Mult}(\mathrm{lcm}(B)) \cap \mathrm{Mult}(\mathrm{lcm}(C))$$

and so by 2.1.16

$$\mathrm{Mult}(A) = \mathrm{Mult}(\mathrm{lcm}(\mathrm{lcm}(B), \mathrm{lcm}(C))$$

It follows that $\mathrm{lcm}(\mathrm{lcm}(B), \mathrm{lcm}(C))$ is the smallest possible integer in $\mathrm{Mult}(A)$. Hence $\mathrm{lcm}(A) = \mathrm{lcm}(\mathrm{lcm}(B), \mathrm{lcm}(C))$ and

$$(*) \qquad \mathrm{Mult}A = \mathrm{Mult}(\mathrm{lcm}(A))$$

If $|A| = 1$, then $A = \{a\}$ for some $a \in A$ and $\mathrm{lcm}(A) = |a|$. So (b) holds in this case. If $|A| > 1$, then $A = B \cup C$ for some subsets B, C with $B \neq A \neq C$. Thus (*) implies that (b) holds. □

Definition 2.1.18. [**defc:coprime**] *Let $a, b \in \mathbb{Z}$ then a and b are called* coprime *if* $\gcd(a, b) = 1$.

Corollary 2.1.19. [**coprime**] *Let a, b, c be integers with a and b coprime. Then*

(a) [**a**] *If $a|c$ and $b|c$, then $ab|c$.*

(b) [**b**] *If $a|bc$, then $a|c$.*

Proof. (a) Since a and b are coprime, we have $\gcd(a, b) = 1$. So by 2.1.16(a), $\mathrm{lcm}(a, b) = |ab|$ and by 2.1.16(b), $\mathrm{lcm}(a, b) \mid c$. So $|ab||c$ and $ab|c$.

(b) By 2.1.12 there exists $x, y \in \mathbb{Z}$ with $xa + yb = \gcd(a, b) = 1$. Hence

$$c = c1 = c(ax + by) = (cx)a + y(bc)$$

Since a divides a and bc, 2.1.5 shows that $a|c$. □

Lemma 2.1.20. [**ax+by=c**] *Let a, b, c be integers with $(a, b) \neq (0, 0)$ and put $d = \gcd(a, b)$. Then the equation $ax + by = c$ has an integral solution, if and only if $d|c$. In this case, if (x_0, y_0) is a particular solution , thene (x, y) is an solution if and only if*

$$x = x_0 + n\frac{b}{d} \text{ and } y = y_0 - n\frac{a}{d}$$

for some $n \in \mathbb{Z}$.

Proof. The first statement we already proved, see 2.1.14. So suppose (x_0, y_0) is a solution. Then

$$a\left(x_0 + n\frac{b}{d}\right) + b\left(y_0 - n\frac{a}{d}\right) = ax_0 + by_0 + \frac{anb}{a} - \frac{bna}{d} = ax_0 + by_0 = c$$

So $x = x_0 + n\frac{b}{d}$ and $y = y_0 - n\frac{a}{d}$ is indeed a solution. Conversely suppose that (x, y) is integral solution. Then

$$ax + by = c = ax_0 + by_0$$

and so

$$a(x - x_0) = -b(y - y_0)$$

and

$$(*) \qquad (x - x_0)\frac{a}{d} = -(y - y_0)\frac{b}{d}$$

Since $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ we conclude from 2.1.19(b), that $\frac{b}{d}\big|(x - x_0)$. Thus

$$x - x_0 = n\frac{b}{d}$$

for some $n \in \mathbb{Z}$. Substituting into (*) gives $n\frac{b}{d}\frac{a}{d} = -(y - y_0)\frac{b}{d}$ and so

$$y - y_0 = -n\frac{a}{d}$$

So

$$x = x_0 + n\frac{b}{d} \text{ and } y = y_0 - n\frac{a}{d}$$

for some $n \in \mathbb{Z}$.

$\square$

Example 2.1.21. [**ex:ax+by=c**] *Consider the equation* $1492x + 1066y = 6$.

By 2.1.13 $\gcd(1492, 1066) = 2$ and $-5 \cdot 1492 + 7 \cdot 1066 = 2$. Since $\frac{6}{2} = 3 \in \mathbb{Z}$, we get

$$-15 \cdot 1492 + 21 \cdot 1066 = 6.$$

So $x_0 = -15$ and $y_0 = 21$ is a particular solution. Also $\frac{1492}{2} = 746$ and $\frac{1066}{2} = 533$. Hence

$$x = -15 + 533n \text{ and } y = 21 - 746n$$

is the general solution.

Chapter 3

Primes

3.1 Prime decompositions

Definition 3.1.1. [**def:prime**] *An integer p is called a* prime *if $p > 1$ and 1 and p are the only positive divisors of p.*

Lemma 3.1.2. [**basic prime**] *Let p be a prime and $a, b \in \mathbb{Z}$. Then*

(a) [**a**] $p|a$ *or* $\gcd(a,p) = 1$.

(b) [**b**] *If $p|ab$, then $p|a$ or $p|b$.*

Proof. (a) Let $d = \gcd(a,p)$. Then $d|p$ and since p is a prime, $d = p$ or $d = 1$. If $d = 1$ we have $\gcd(a,p) = 1$. If $d = p$, then $p \mid a$.

(b) We may assume that $p \nmid a$. Thus by (a), $\gcd(a,p) = 1$ and so by 2.1.19(b), $p \mid b$. □

Corollary 3.1.3. [**p divide product**] *Let p be a prime and $a_1, \ldots a_k$ integers. If p divides $a_1 a_2 \ldots a_k$, then p divides a_i for some $1 \leq i \leq k$.*

Proof. By induction on k. If $k = 1$, the statement is obvious. Suppose now that $k > 1$. Then p divides $(a_1 \ldots a_{k-1})a_k$ and so by 3.1.2(b), $p|a_1 \ldots a_{k-1}$ or $a_1 \mid a_k$. In the first case, by induction, $p \mid a_i$ for some $1 \leq i \leq k-1$. □

Theorem 3.1.4. [**prime decomposition**] *Let n be an integer with $n > 1$. Then there exists uniquely determined positive integers $k, p_1, p_2, \ldots p_k, e_1, \ldots e_k$ such that*

(a) [**a**] *p_i is a prime for all $1 \leq i \leq k$.*

(b) [**b**] $p_1 < p_2 < \ldots < p_k$.

(c) [**c**] $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$

Proof. We will first show the existence. If n is a prime, choose $k = 1$, $p_1 = n$ and $e_1 = 1$. So suppose n is not a prime. Then $n = ab$ for some integers, $1 < a, b < n$. By induction the theorem holds for a and b in place of n and it so also for n.

To prove uniqueness, suppose $n = p_1^{e_1} \ldots p_k^{e_k} = q_1^{f_1} \ldots q_l^{f_l}$, where $k, l, e_1, \ldots e_k, f_1, \ldots, f_l$ are positive integers and $p_1, \ldots, p_k, q_1, \ldots q_l$ are primes. Then $q_1 | n = p_1^{e_1} \ldots p_k^{e_k}$ and so by 3.1.3, $q_1 \mid p_i$

for some $1 \leq i \leq p_k$. Since p_i is a prime and $q_1 > 1$ this gives $q_1 = p_i$. hence $p_1 \leq p_i \leq q_i$ and by symmetry, $q_1 \leq p_1$. Hence $p_1 = q_1$. Thus

$p_1^{e_1-1} p_2^{e_2} \dots p_k^{e_k} = \frac{n}{p_1} = \frac{n}{q_1} = q_1^{f_1-1} q_2^{e_2} \dots q_l^{f_l}$.

By induction we conclude that $k = l$, $e_1 - 1 = f_1 - 1$, $q_i = p_i$ and $e_i = f_i$ for all $2 \leq i \leq k$. ☐

Corollary 3.1.5. [**prime divisor**] *Let $n \in \mathbb{Z}$ with $n > 1$. Then there exist a prime p with $p \mid n$.*

Proof. Just choose $p = p_1$ in 3.1.4 ☐

Corollary 3.1.6. [**prime and divide**] *Let $p_1, \dots p_k$ be pairwise distinct primes and $e_1, \dots e_k$, $f_1 \dots f_k$ be non-negative integers. Put*

$$a = p_1^{e_1} \dots p_l^{e_k} \text{ and } b = p_1^{f_e} \dots p_k^{f_k}$$

(a) [**a**] *$a \mid b$ of if and only if $e_i \leq f_i$ for all $1 \leq i \leq k$.*

(b) [**b**] $\gcd(a, b) = p_1^{g_1} \dots p_k^{g_k}$, *where $g_i = \min(e_i, f_i)$.*

Proof. (a): Suppose first that $e_i \leq f_i$ and put $d = p_1^{f_1 - e_1} \dots p_k^{f_k - e_k}$. Then $d \in \mathbb{Z}$ and $ad = b$. So $a \mid b$.

Suppose next that $a \mid b$. Then $b = ad$ for some $d \in \mathbb{Z}^+$.By 3.1.4 $d = p_1^{s_1} \dots p_k^{s_k} q_1^{t_1} \dots q_l^{t_l}$, where $p_1, \dots p_k, q_1 \dots q_l$ are pairwise distinct primes $s_i \in \mathbb{N}$, $t_j \in \mathbb{Z}^+$ and $l \in \mathbb{N}$. Thus

$$p_1^{f_1} \dots p_k^{f_k} = b = ad = p_1 e_1 + s_1 \dots p_k^{e_k + s_k} q_1^{t_1} \dots q_l^{t_l}$$

The uniqueness of prime factorizations now shows that $f_i = e_i + s_i$ and so $e_i \leq s_i$.

(b) Let $c = p_1^{s_1} \dots p_k^{s_k}$ with $s_i \in \mathbb{N}$. By (a), c divides a and b iff $s_i \leq e_i$ and $s_i \leq f_i$, iff $s_i \leq g_i$ iff $c \mid p_1^{g_1} \dots p_k^{g_k}$. Thus (b) holds. ☐

Lemma 3.1.7. [**powers and primes**] *Let $a = a_1 \dots a_k$ where $a_1, a_1 \dots a_k$ are pairwise coprime positive integers and let $m \in \mathbb{Z}^+$.*

(a) [**a**] *Let p be a prime with $p^m \mid a$. Then $p^m | a_i$ for some $1 \leq i \leq k$.*

(b) [**b**] *There exists $b \in \mathbb{Z}^+$ with $a = b^m$ if and only if there exist $b_i \in \mathbb{Z}^+$, $1 \leq i \leq k$, with $a_i = b_i^k$.*

Proof. (a) By 3.1.3 there exists $1 \leq i \leq k$ with $p \mid a_i$. If $m = 1$, we are done. So suppose $m > 1$. Since the a_j's are pairwise coprime $p \nmid a_j$ for all $j \neq i$. Note that

$$p^{m-1} | a_1 a_2 \dots a_{i-1} \frac{a_i}{p} a_{i+1} \dots a_k$$

Since $p^{m-1} \nmid a_j$ for $j \neq i$ we conclude by induction on m that $p^{m-1} \mid \frac{a_i}{p}$ and so $p^m | a_i$.

(b) The backwars directions is obvious. So suppose $a = b^m$ for some $b \in \mathbb{Z}^+$. If $b = 1$, then $a = 1$ and $a_i = 1$ for all $1 \leq i \leq k$. So (a) holds with $b_i = 1$. Thus we may assume that $b > 1$ and so there exists a prime p with $p \mid b$. Then $p^m \mid b^m = a$ and so by (a), $p^m \mid a_i$ for some i. Then

$$\left(\frac{b}{p}\right)^p = a_1 a_2 \dots a_{i-1} \frac{a_i}{p^i} a_{i+1} \dots a_l$$

By induction in a we conclude that there exists $c_j \in \mathbb{Z}^+$ with

$$a_1 = c_1^m, \dots a_{i-1} = c_{i-1}^m, \frac{a_i}{p} = c_i^p, a_{i+1} = c_{i+1}^p, \dots a_k = c_k$$

Put $b_j = c_j$ for $j \neq i$ and $b_i = pc_j$. Then (b) holds. ☐

Corollary 3.1.8. [**m root**] *Let $n, m \in \mathbb{Z}^+$. Then $\sqrt[m]{n} \in \mathbb{Q}$ if and only if $\sqrt[m]{n} \in \mathbb{Z}$.*

Proof. The backwards direction is obvious. So suppose that $\sqrt[m]{n} \in \mathbb{Q}$. Then $\sqrt[m]{n} = \frac{a}{b}$ with $a, b \in \mathbb{Z}^+$ and $\gcd(a, b) = 1$. Thus $\left(\frac{a}{b}\right)^m = n$ and so

$$a^m = b^m n$$

Since $n \mid a^m$ and a and b are coprime we conclude that b and n. Hence also b^m and n are coprime, and by 3.1.7(b) $n = c^m$ for some $c \in \mathbb{Z}^+$. This $\sqrt[m]{n} = c \in \mathbb{Z}$. □

3.2 On the number of primes

Lemma 3.2.1. [**infinitely many primes**]

(a) [**a**] *Let $p_1, p_2, \ldots, p_n$ be primes. Then there exists a prime p with $p \mid p_1 p_2 \ldots p_n + 1$ and $p \neq p_i$ for all $1 \leq i \leq n$.*

(b) [**b**] *Let $n \in \mathbb{Z}^+$. Then there exists at least n primes less or equal to $2^{2^{n-1}}$.*

(c) [**c**] *There are infinitely may primes.*

Proof. (a): By 3.1.5 there exists a prime dividing p dividing $p_1 p_2 \ldots p_n + 1$. If $p = p_i$ for some i, then p would divide, $p_1 \ldots p_n$ and so also $1 = (p_1 \ldots p_n + 1) - (p_1 \ldots p_n)$, a contradiction. Thus $p \neq p_i$ for all $1 \leq i \leq n$ and (a) is proved.

(b) Note that 2 is a prime less or equal to $2 = 2^{2^{1-1}}$. So (b) holds for $n = 1$. Suppose inductively that (b) holds for all $1 \leq i \leq n$. Then there exists n pairwise distinct primes primes $p_1, p_2, \ldots p_n$ with $p_i \leq 2^{2^{i-1}}$. Let p be as in (a). Then

$$\begin{aligned} p &\leq p_1 p_2 \ldots p_n + 1 \\ &\leq 2^{2^0} 2^{2^1} 2^{2^2} \ldots 2^{2^{n-1}} + 1 \\ &= 2^{2^0 + 2^1 + 2^2 + \ldots 2^{n-1}} + 1 \\ &= 2^{2^n - 1} + 1 \\ &\leq 2^{2^{n+1}} \end{aligned}$$

So (b) also holds for $n + 1$ and (b) is proved.

(c) follows immediately from (b). □

Lemma 3.2.2. [**primes 3 mod 4**] *There exists infinitely many primes of the form $4q + 3$, $q \in \mathbb{N}$.*

Proof. Observe first that 3 is such a prime. Now suppose $p_1, p_2 \ldots, p_n$ are distinct primes with $p_i = 4q_i + 3$ for some $q_i \in \mathbb{N}$. By 3.1.4

$$4p_1 p_2 \ldots p_n - 1 = t_1 \ldots t_2 \ldots t_k$$

for some primes $t_1, t_2 \ldots t_k$. By the remainder theorem $t_i = 4m_i + r_i$ for some $m_i, r_i \in Z$ with $0 \leq r_i \leq 3$. Since $4p_1 p_2 \ldots p_n + 2$ is odd also each t_i and r_i is odd. Thus $r_i \in \{1, 3\}$. Suppose for a contratiction that $r_i = 1$ for all $1 \leq i \leq k$. Then

$$t_1 t_2 \ldots t_k = (4m_1 + 1)(4m_2 + 1) \ldots (4m_k + 1)$$

and so by the distributative law, $t_1 \dots t_l = 4m + 1$ for some $m \in \mathbb{Z}$. But this contradicts

$$4m + 1 = t_1 t_2 \dots t_k = 3p_1 p_2 \dots p_n + 2 - 1$$

and so $4 \mid 1 - (-1) = 2$, a contradiction.

Hence $r_i = 3$ for some $1 \le i \le t_i$. Since t_i divides $4p_1 \dots p_k$ and $t_i \nmid -1$, $t_i \neq p_j$ for all $1 \le j \le n$. Therefore t_i is another prime of the form $4q + 3$ and the Lemma is proved. □

3.3 Fermat and Mersenne Primes

Definition 3.3.1. [**def:fermat**]

(a) [**a**] *A prime p is called a* Fermat prime *if $p = 2^n + 1$ for some $n \in \mathbb{N}$.*

(b) [**b**] *A prime p is called a* Mersenne prime *if $p = 2^n - 1$ for some $n \in N$.*

(c) [**c**] *Let $n \in N$. Then $F_n = 2^{2^n} + 11$. F_n is called a* Fermat number.

(d) [**d**] *Let p be a prime. Then $M_p = 2^{p-1}$. M_p is called a* Mersenne number.

Lemma 3.3.2. [**binom**] *Let a and b be integers and $m \in \mathbb{Z}^+$. Then $a - b$ divides $a^m - b^m$.*

Proof.

$$\begin{array}{rrl} & (a-b) & (a^{m-1} + a^{m-2}b + \ldots + ab^{m-2} + b^{m-1}) \\ = & a^m & +a^{m-1}b + \ldots + ab^{m-1} \\ & & -a^{m-1}b - \ldots - ab^{m-1} - b^m \\ = & a^m - b^m & \end{array}$$

□

Lemma 3.3.3. [**fermat primes**] *All odd Fermat primes are Fermat numbers. That is if $n \in \mathbb{Z}^+$ such that $2^n + 1$ is a prime, then $n = 2^m$ for some $m \in \mathbb{N}$ and $2^n + 1 = F_m$.*

Proof. Let $n = 2^m k$ with $m \in \mathbb{N}$, $k \in \mathbb{Z}^+$ and k odd. Put $a = 2^{2^m}$.

$$2^n + 1 = 2^{2^m k} + 1 = a^k + 1 = a^k - (-1)^k$$

By 3.3.2 $a + 1 = (a - (-1)$ divides $a^k - (-1)^k = 2^n + 1$. Note that $a \ge 2$ and so $a + 1 > 1$. Since $2^n + 1$ is a prime, $a + 1 = 2^n + 1 = a^k + 1$. Hence $a = a^k$ and since $a \ge 2$, $k = 1$ Thus $n = 2^m$ and $2^n + 1 = 2^{2^n+1} = F_m$. □

The first five Fermat numbers all are Fermat primes:
$F_0 = 2^1 + 1 = 3$
$F_1 = 2^2 + 1 = 5$
$F_2 = 2^4 + 1 = 17$
$F_3 = 2^8 + 1 = 257$,
$F_4 = 2^{16} + 1 = 65,537$.
But no other odd Fermat primes are known.
We will show that F_5 is not a prime, by proving that 641 divides $F_5 = 2^{32} + 1$.
Observe that

$$641 = 16 + 625 = 2^4 + 5^4$$

and

$$641 = 5 \cdot 128 + 1 = 4 \cdot 2^7 + 1$$

Thus

$$\begin{aligned} 2^{32} &= 2^4 \cdot 2^{28} &&= (641 - 5^4) \cdot 2^{28} \\ &= (641 \cdot 2^{28}) - (5 \cdot 2^7)^4 &&= (641 \cdot 2^{28}) - (641 - 1)^4 \\ &= 641 \cdot 2^{28} - 641^4 + 4 \cdot 641^3 - 6 \cdot 641^2 + 4 \cdot 641 - 1 \end{aligned}$$

Hence $2^{32} = 641m - 1$ for some $m \in \mathbb{Z}$ and so $641m = 2^{32} + 1$.
So F_5 indeed is not a prime.

Lemma 3.3.4. [**fn relation**] *Let $n \in \mathbb{Z}^+$.*

(a) [**a**] $F_n - 2 = (F_{n-1} - 2)F_{n-1}$.

(b) [**b**] $F_n - 2 = F_0 F_1 F_2 \ldots F_{n-1}$.

(c) [**c**] *Let $m \in \mathbb{N}$ with $m < n$. Then* $\gcd(F_n, F_m) = 1$.

Proof. Observe first that $F_n - 2 = (2^{2^n} + 1) - 2 = 2^{2^n} - 1$. We compute

$$(F_{n-1} - 2)F_{n-1} = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) = (2^{2^{n-1}})^2 - 1 = 2^{2^n} - 1 = F_n - 2$$

and so (b) holds.

We have $F_1 - 2 = 5 - 2 = 3 = F_0$ and so (b) holds for $n = 1$. Thus (b) follows from (a) and induction on n

Let $d = \gcd(F_n, F_m)$. Since F_n is odd, d is odd. As $m < n$ and $d \mid F_m$ we conlcude from (b), that $d \mid F_n - 2$. Since also $d \mid F_n$, d divides $F_n - (F_n - 2) = 2$. Since d is odd this gives $d = 1$ and (c) is proved. □

Proposition 3.3.5. [**mersenne**] *Let a, n be integers such that $a > 1$, $n > 1$ and $a^n - 1$ is a prime. Then $a = 2$ and n is a prime. So $a^n - 1 = 2^n - 1 = M_n$ is a Mersenne prime and a Mersenne number.*

Proof. Since $n > 1$ there exist a prime p with $p \mid n$. Put $b = a^{\frac{n}{p}}$. Then $b^p - 1 = a^n - 1$ is a prime By 3.3.2, $b - 1$ divides $b^p - 1$. Since $b > 1$ and $p > 1$, $b^p - 1 > b - 1$ and since $b^p - 1$ is a prime, $b - 1 = 1$. Thus $b = 2$. Since $b = a^{\frac{n}{p}}$ we conlude that $a = 2$, $\frac{n}{p} = 1$ and $n = p$ is a prime. □

Lemma 3.3.6. [**check prime**] *Let n be an integer with $n > 1$. Then n is not a prime if and only of the exits a prime p with $p \mid n$ and $p \leq \sqrt{n}$.*

Proof. The backwards direction is obvious. So suppose n is not a prime. Then there exists $a \in \mathbb{Z}$ with $1 < a < n$ and $a \mid n$. Thus $n = ab$ for some $b \in Z$. Note that also $1 < b < n$ and interchaning a and b if necessary, we may assume that $a \leq b$. Then $a^2 \leq ab = n$ and so $a \leq \sqrt{n}$. By 3.1.5 there exists a prime p with $p \mid a$. Then $p \mid n$ and $p \leq a \leq \sqrt{n}$. □

Chapter 4

Congruences

4.1 The Ring $\mathbb{Z}_n$

Definition 4.1.1. [**modulo n**] *Let $n \in \mathbb{Z}$. Define the relation $\equiv_n$ on $\mathbb{Z}$ by*

$$\equiv_n := \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \,\big|\, n|b-a\}$$

If $a \equiv_n b$ we say that a and b are congruent modulo n *and write*

$$a \equiv b \pmod{n}$$

Note that $a \equiv_n b$ iff $a \equiv b \pmod{n}$ and iff n divides $b - a$.

Lemma 4.1.2. [**mod equiv**] *Let $n \in \mathbb{Z}$. Then $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Note that $0n = 0 = a - a$. So $n \mid a - a$, $a \equiv a \pmod{n}$ and $\equiv_n$ is reflexive.

Suppose $a \equiv b \pmod{n}$. Then $n \mid (b - a)$ and so also $n \mid (-1)(b - a) = a - b$. Thus $b \equiv a \pmod{n}$ and $\equiv_n$ is symmetric.

Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n \mid (b - a)$ and $n \mid (c - b)$. Hence also $n \mid (b - a) + (c - b) = (c - a)$ and $a \equiv c \pmod{n}$. Thus $\equiv_n$ is reflexive. $\square$

Definition 4.1.3. [**def:congruence class**] *Let $n \in \mathbb{Z}$.*

(a) [**a**] $[a]_n := \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$. *$[a]_n$ is called the* congruence class *of a modulo n.*

(b) [**b**] $\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$.

Note that $[a]_n$ is the equivalence class of $\equiv_n$ containing a.

If $n = 0$, then $n \mid b - a$ if and only if $b - a = 0$, that is $b = a$. So $[a]_0 = \{a\}$ and $\mathbb{Z}_0$ is essentially the same as $\mathbb{Z}$.

If $n = 1$, then $n \mid b - a$ for all $a, b \in \mathbb{Z}$. So $[a] = \mathbb{Z}$ and $\mathbb{Z}_1$ has just one element, namely $\mathbb{Z}$.

Observe that $n \mid b - a$ if and only if $-n \mid b - a$. Hence $\equiv_n = \equiv_{-n}$.

Lemma 4.1.4. [**modulo and remainder**] *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then the following are equivalent.*

(a) [**a**] $[a]_n = [b]_n$

(b) [**b**] $a \equiv b \pmod{n}$

(c) [**c**] $b = a + kn$ *for some* $k \in \mathbb{Z}$.

(d) [**d**] a *and* b *have the same remainder when divided by* n.

Proof. By 1.2.2 (a) and (b) are equivalent.
(b) $\Longrightarrow$ (c): If $a \equiv b \mod n$, then $n \mid b-a$, $b-a = kn$ for some $k \in \mathbb{Z}$ and $b = a + kn$. So (c) holds.
(c) $\Longrightarrow$ (d): Let $a = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < |n|$. Then $b = a + kn = (q+k)n + r$ and so r is also the remainder of b when divided by n.
(d) $\Longrightarrow$ (b): Let r be the (same) remainder of a and b divided by n. Then $a = qn + r$ and $b = \tilde{q}n + r$ for some $q, \tilde{q} \in \mathbb{Z}$. Thus $b - a = (\tilde{q} - q)n$ and so $n \mid b - a$ and $a \equiv b \pmod{n}$. □

Corollary 4.1.5. [**zn**] *Let* $n \in \mathbb{Z}$ *with* $n \geq 1$. *Then*

(a) [**a**] $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots [n-1]_n\}$.

(b) [**b**] *Let* $[r]_n \neq [s]_n$ *for all* $0 \leq r < s < n$.

(c) [**c**] $|\mathbb{Z}_n| = n$.

Proof. (a): Let $a \in \mathbb{Z}$ and r the remainder of a when divided by n. Then $[a]_n = [r]_n$ and so (a) holds. (b): Follows from 4.1.4.
(c) follows from (a) and (b). □

Lemma 4.1.6. [**ring zn**] *Let* $a, b, a', b', n \in \mathbb{Z}$ *with*

$$a \equiv a' \pmod{n} \text{ and } b \equiv b' \pmod{n}$$

Then

$$\begin{aligned} a' + b' &\equiv a + b \pmod{n} \\ a' - b' &\equiv a - b \pmod{n} \\ a'b' &\equiv ab \pmod{n} \end{aligned}$$

Proof. Since $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ there exist $k, l \in \mathbb{Z}$ with $a' = a + kn$ and $b' = b + ln$. Thus

$$\begin{aligned} a' + b' &= a + b + (k + l)n \\ a' - b' &= a - b + (k - l)n \\ a'b' &= ab + (al + kb + kln)n \end{aligned}$$

and so the Lemma holds. □

Definition 4.1.7. [**def:ring zn**] *Let* n *be an integers. The binary operations "+","-" and "·" on* $\mathbb{Z}_n$ *are defined by*

$$\begin{aligned} [a]_n + [b]_n &= [a+b]_n \\ [a]_n - [b]_n &= [a-b]_n \\ [a]_n [b]_n &= [ab]_n \end{aligned}$$

Note that by 4.1.6 these binary operation are well defined.

Lemma 4.1.8. [**polynomials modulo n**] *Let $f \in \mathbb{Z}[x]$ and $a,b \in \mathbb{Z}$. If $a \equiv b \pmod{n}$, then also $f(a) \equiv f(b) \pmod{n}$.*

Proof. Let $f = \sum_{i=0}^{n} c_n x^n$ with $c_i \in \mathbb{Z}$. If $n = 0$, then $f(a) = c_0 = f(b)$ and the lemma holds. So suppose $n \geq 1$ and put $g = \sum_{i=0}^{n-1} c_{i+1} x^i$. Then $f = c_0 + xg$. By induction on n, $g(a) \equiv g(b) \equiv p$ mod n. Also $c_0 \equiv c_0 \pmod{n}$ and $a \equiv b \pmod{n}$. Hence by 4.1.6

$$f(a) \equiv c_0 + ag(a) \equiv c_0 + bg(b) \equiv f(b) \pmod{n}$$

□

Example 4.1.9. [**ex:no root**] *The polynomial $f = x^5 - x^2 + x - 3$ has no root in $\mathbb{Z}$.*

We compute modulo 4

$$\begin{aligned}
f(-1) &\equiv & -1-1-1-3 && \equiv -6 \not\equiv 0 \pmod{4} \\
f(0) &\equiv & && -3 \not\equiv 0 \pmod{4} \\
f(1) &\equiv & 1-1+1-3 && \equiv -2 \not\equiv 0 \pmod{4} \\
f(2) &\equiv & 32-4+2-3 && \equiv 27 \not\equiv 0 \pmod{4}
\end{aligned}$$

Now let n be any integer. Then n is congruent to one of $-1, 0, 1$, or 2 modulo 4. Hence 4.1.8 and the above calculation, $f(n) \not\equiv 0 \pmod{4}$. Thus $f(n)$ is not a multiple of 4 and in particular, $f(n) \neq 0$.

4.2 Solving One Congruence

Lemma 4.2.1. [**divide congruence**] *Let $a, b, n, t \in \mathbb{Z}$ such that t divides a, b and n and $t \neq 0$. Then*

$$\begin{aligned}
& a \equiv b && \pmod{n} \\
\iff & \tfrac{a}{t} \equiv \tfrac{b}{t} && \left(\bmod \frac{n}{t}\right)
\end{aligned}$$

Proof. We have

$$\begin{aligned}
& a \equiv b \pmod{n} && \\
\iff & b - a = kn && \text{for some } k \in \mathbb{Z} \\
\iff & \tfrac{b}{t} - \tfrac{a}{t} = k\tfrac{n}{t} && \text{for some } k \in \mathbb{Z} \\
\iff & \tfrac{a}{t} \equiv \tfrac{b}{t} \pmod{\tfrac{n}{t}} &&
\end{aligned}$$

□

Lemma 4.2.2. [**cancel modulo n**] *Let $a, b, n, t \in \mathbb{Z}$ and suppose that $\gcd(n,t) = 1$. Then*

$$\begin{aligned}
& a \equiv b && \pmod{n} \\
\iff & at \equiv bt && \pmod{n}
\end{aligned}$$

Proof. We have

$$\begin{aligned} & a \equiv b \pmod n \\ \iff \quad & n \mid b-a \\ \iff \quad & n \mid (b-a)t \qquad \text{since}\,\gcd(n,t)=1(2.1.19(\text{b})) \\ \iff \quad & n \mid bt-at \\ \iff \quad & at \equiv bt \pmod n \end{aligned}$$

□

Lemma 4.2.3. [**congruence**] *Let a, b and n be integers with $n \neq 0$ and put $d = \gcd(a, n)$. Then the linear congruence*

$$ax \equiv b \pmod n$$

has a solution if and only if $d|b$. If $d|b$ and x_0 is a solution, then x is a solution if and only if $x = x_0 + t\frac{n}{d}$ for some $t \in \mathbb{Z}$. In particular, the solutions form exactly d congruence classes modulo n, namely $[x_0 + t\frac{n}{d}]_n, 0 \leq t < d$.

Proof.

$$\begin{aligned} & xa \equiv b \pmod n \qquad \text{for some } x \in \mathbb{Z} \\ \iff \quad & ax = b - ny \qquad \text{for some } x, y \in \mathbb{Z} \\ \iff \quad & ax + ny = b \qquad \text{for some } x, y \in \mathbb{Z} \end{aligned}$$

So by 2.1.20 $ax + ny = b$ has a solution if and only if $d \mid b$. Hence also $xa \equiv b \pmod n$ has solution if and only if $d \mid b$. Also if (x_0, y_0) is a particular solution of $ax + ny = b$, the (x, y) is a solution of $ax + ny = b$ if and only if

$$x = x_0 + t\frac{n}{d} \text{ and } y = y_0 - t\frac{a}{d}$$

for some $t \in \mathbb{Z}$. Thus then x is a solution of $xa \equiv b \pmod n$if and only if $x = x_0 + t\frac{n}{d}$ for some $t \in \mathbb{Z}$. We have

$$\begin{aligned} y \quad & x_0 + t\tfrac{n}{d} \equiv x_0 + t' \pmod n \\ \iff \quad & t\tfrac{n}{d} \equiv t'\tfrac{n}{d} \pmod n \\ \iff \quad & t \equiv t' \pmod d \qquad - \text{ divide by } \tfrac{n}{d}, (4.2.1) \end{aligned}$$

So the solutions of $ax \equiv b \pmod n$ from exactly d congruence classes modulo n, namely $[x_0 + t\frac{n}{d}]_n, 0 \leq t < d$. □

We will now introduce two methods to find the solution of a linear congruence $ax \equiv b \pmod n$.

Method 1:

Step 1: Compute $d = \gcd(a, b)$. Check whether d divides b. If d does not divide b, the linear congruence has no solution. If d divides b, continue with Step 2.

Step 2: So assume now that $d \mid b$. In view of 4.2.1 we can divide the linear congruence by d to obtain an equivalent congruence

$$\frac{a}{d}x = \frac{b}{d} \pmod{\frac{n}{d}}$$

Step 3: In view of Step 2 we now assume that $\gcd(a, n) = 1$. Compute $e = \gcd(a, b)$. Since $e \mid a$ and $\gcd(a, n) = 1$ we have $\gcd(e, n) = 1$. So in view of 4.2.2 we can divide by e and obtain an equivalent congruence

$$\frac{a}{e}x \equiv \frac{b}{e} \pmod{n}$$

Step 4: If $a = \pm 1$, then x is a solution of $ax \equiv b \pmod{n}$ if and only if $x \equiv \pm b \pmod{n}$ and we are done. Otherwise continue with Step 5.

Step 5a: Find an integer c such that $\gcd(c, n) = 1$ and the remainder (or least absolute remainder) r of ca when divided by n is smaller than $|a|$. Let s be the remainder of cb modulo n. Then by 4.2.2 we obtain equivalent congruence

$$cn \equiv cn \pmod{n}$$

and

$$r \equiv s \pmod{n}$$

To find c, one can either take some guesses or use the Euclidean algorithm to find a solution of $ax + ny = 1$ and then use $c = x$ (which gives a remainder of 1 then ca is divided by n)

Instead of Step 5a one can also use

Step 5b: Find an integer c such that $\gcd(a, b + cn) \neq 1$ and use the equivalent congruence

$$a \equiv b + cn \pmod{n}$$

Note that such a c always exists: Since $\gcd(a, n) = 1$, the equation $ny \equiv -b \pmod{a}$ has a solution. Choose c to be a solution of this equation, then a divides $b + cn$ and so $\gcd(a, b + cn) = |a|$. For calculations by hand, it is best to take some guesses for c rather than solving that equation.

After Step 5a or Step 5b go back to Step 3. Note that in both case (Step 5a and Step5b) the absolute value of a will have decreased and so this procedure will find the solution in finitely many steps.

Example 4.2.4. [**ex:method 1**] *Solving* $30x \equiv 18 \pmod{14}$ *using Method 1*

Step 1: $\gcd(30, 14) = 2$ and $2 \mid 18$. So there are solutions.

Step 2: Dividing by 2 we obtain

$$15x \equiv 9 \pmod{7}$$

Step 3 $\gcd(15, 9) = 3$. Dividing by 3 we obtain:

$$5x \equiv 3 \pmod{7}$$

Step 4 Since $5 \neq \pm 1$, we have to continue.

Step 5b We choose $c = 1$ and add $1 \cdot 7$ to 3 to obtain

$$5x \equiv 10 \pmod 7$$

Step 3 $\gcd(5, 10) = 5$. Divide by 5:

$$x \equiv 2 \pmod 7$$

Step 4 The solution is $x \equiv 2 \pmod 7$.

Method 2: Method 1 works well for small numbers, where one easily compute gcd's and take good guesses in Step 5. Method 2 is a deterministic algorithm similar to the Euclidean algorithm 2.1.12

Observe first that $nx \equiv 0 \pmod n$ for all x in $\mathbb{Z}$. So the linear congruence $ax \equiv b \pmod n$ is equivalent to the system of two linear congruences

$$\begin{aligned} C_{-1}: \quad nx &\equiv 0 \pmod n \\ C_0: \quad ax &\equiv b \pmod n \end{aligned}$$

Suppose inductively that we already defined linear congruences $C_k : r_k x \equiv b_k \pmod n$ for $-1 \leq k \leq i$. If $r_i \neq 0$, let C_{i+1} be the linear congruence obtain by subtracting q_{i+1} times congruence C_{i-1} from C_i, where q_{i+1} is the integer quotient of r_{i-1} then divided by r_i. So r_{i+1} is the remainder of r_{i-1} when divided by r_i.

Let m be minimal with $r_m = 0$. Comparing with the Euclidean algorithm we see that $r_{m-1} = d$, where $d_0 \gcd(a, n)$. Note that the system (C_{i-1}, C_i) is equivalent to (C_i, C_{i+1}). Since the linear congruence $ax \equiv b \pmod n$ is equivalent to the system (C_{-1}, C_0) its is also equivalent to the system (C_{m-1}, C_m):

$$\begin{aligned} C_{m-1}: \quad dx &\equiv b_{m-1} \pmod n \\ C_m: \quad 0x &\equiv b_m \pmod n \end{aligned}$$

By 4.2.3 the latter has a solution if and only if $d \mid b_{m-1}$ and $n \mod b_m$. In this case 4.2.1 shows that the solution is

$$x \equiv \frac{b_{m-1}}{d} \pmod{\frac{n}{d}}$$

Example 4.2.5. [**ex:method 2**] *Solving* $30x \equiv 18 \pmod{14}$ *using Method 2.*

$$\begin{aligned} 14x &\equiv 0 && \pmod{14} \\ 30x &\equiv 18 && \pmod{14} \\ (q_2 = 0) \quad 14x &\equiv 0 && \pmod{14} \\ (q_3 = 2) \quad 2x &\equiv 18 && \pmod{14} \\ (q_4 = 7) \quad 0x &\equiv -7 \cdot 18 && \pmod{14} \end{aligned}$$

The last congruence always holds. Dividing the second two last congruence by 2 we obtain the solution:

$$x \equiv 9 \pmod 7$$

which of course is the same as

$$x \equiv 2 \pmod 7$$

4.3 Solving Systems of Linear Congruences

Corollary 4.3.1. [**lcm and congruence**] *Let A be finite set of integers. and $x, y \in \mathbb{Z}$. then*

$$x \equiv y \pmod a \text{ for all } a \in A$$

if and only if

$$x \equiv y \pmod{\operatorname{lcm}(A)}$$

Proof. Note that the following are equivalent

$$\begin{aligned}
x \equiv y & \pmod a && \text{for all } a \in A \\
a|y - x & && \text{for all } a \in A \\
A|y - x & && \\
\operatorname{lcm}(A)|y - x & && && \text{by (2.1.17)} \\
x \equiv y & \pmod{\operatorname{lcm}(A)} &&
\end{aligned}$$

□

Corollary 4.3.2. [**unique congruence**] *Let $n_1, n_2, \ldots, n_k$ be non-zero integers and let $a_1, a_2, \ldots a_k$ be any integers. Suppose that the system of congruences*

$$x \equiv a_i \pmod{n_i} \text{ for } 1 \le i \le k$$

has a solution. Then the solutions form a single congruence class modulo $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$

Proof. Let x_0 is a solution of the system of congruences. $x \in \mathbb{Z}$ is a solution if and only if $x \equiv a_i \pmod{n_i}$ for all $1 \le i \le k$. Since $x_0 \equiv a_i \pmod{p_j}$, this is the case if and only if $x \equiv x_0 \pmod{)} n_i$ for all i. By 4.3.1 this holds if and only if $x \equiv x_0 \pmod{\operatorname{lcm}(n_1, n_2, \ldots, n_k)}$. □

Theorem 4.3.3 (Chinese Remainder Theorem)**.** [**chinese**] *Let $n_1, n_2, \ldots, n_k$ be pairwise coprime non-zero integers and let $a_1, a_2, \ldots a_k$ be any integers. Then the system of congruences*

$$x \equiv a_i \pmod{n_i} \text{ for } 1 \le i \le k$$

has a solution and the solutions form unique congruence modulo $n_1 n_2 \ldots n_k$.

Proof. We will first show that the system has a solution. For this put $n = n_1 \ldots n_k$ and $c_i = \frac{n}{n_i} = n_1 \ldots n_{i-1} n_{i+1} \ldots n_k$. Since n_i is coprime to each $n_j, j \neq i$, n_i is also coprime to c_j. Thus by 4.2.3 the equation $c_i x \equiv a_i \pmod{n_i}$ has a solution d_i. Put

$$x_0 := c_1 d_1 + c_2 d_2 + \ldots + c_k d_k$$

We claim that x_0 is a solution of the system of congruence. Let $1 \leq i, j \leq k$ with $i \neq j$. Since $n_i \mid c_j$ we have $c_j d_j \equiv o \pmod{n_i}$. Also by choice of d_i, $c_i d_i \equiv a_i \pmod{n_i}$. Thus

$$c_0 \equiv 0 + 0 + \ldots + 0 + a_i + 0 + \ldots 0 \equiv a_i \pmod{n_i}$$

and

x_0 is a solution.

Since the n_i are pairwise coprime, $\operatorname{lcm}(n_1, n_2, \ldots, n_k) = n_1 n_2 \ldots n_k$, Thus the second statement follows from 4.3.2 □

Example 4.3.4. [**ex:chinese**] *Find all solutions of*

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7$$

$$\begin{array}{c|c|c}
n_1 = 3 & n_2 = 5 & n_3 = 7 \\
a_1 = 2 & a_2 = 3 & a_3 = 2 \\
c_1 = 5 \cdot 7 = 35 & c_2 = 3 \cdot 7 = 21 & c_3 = 3 \cdot 5 = 15 \\
35 d_1 \equiv 2 \pmod 3 & 21 d_2 \equiv 3 \pmod 5 & 15 d_3 \equiv 2 \pmod 7 \\
-d_1 \equiv 2 \pmod 3 & d_2 \equiv 3 \pmod 5 & d_3 \equiv 2 \pmod 7 \\
d_1 = -2 & d_2 = 3 & d_3 = 2
\end{array}$$

So $x_0 = -2 \cdot 35 + 3 \cdot 21 + 2 \cdot 15 = -70 + 63 + 30 = 23$ is a solution. $3 \cdot 5 \cdot 7 = 5 \cdot 21 = 105$ and so x is a solution if and only if

$$x \equiv 23 \pmod{105}$$

Example 4.3.5. [**ex:linear chinese**] *Find all solutions of*

$$3x \equiv 4 \pmod 7, \quad 5x \equiv 13 \pmod{19}$$

We will first solve each of the congruence by themselves , using Method 2 from above.

$$\begin{array}{lcc|cc}
C_{-1} & & 7x \equiv 0 \pmod 7 & & 19x \equiv 0 \pmod{19} \\
\hline
C_0 & & 3x \equiv 4 \pmod 7 & & 5x \equiv 13 \pmod{19} \\
\hline
C_1 & q_2 = 2 & x \equiv -8 \pmod 7 & q_2 = 4 & -x \equiv -52 \pmod{19} \\
C_1 & & x \equiv -1 \pmod 7 & & x \equiv -5 \pmod{19} \\
\hline
C_2 & q_3 = 3 & 0x \equiv 7 \pmod 7 & q_3 = 5 & 0x \equiv 38 \pmod{19}
\end{array}$$

So we have to solve the system of congruences

$$x \equiv -1 \pmod 7, \quad x \equiv -5 \pmod{19}$$

We use the method from the Chinese remainder theorem

$n_1 = 7$	$n_2 = 19$
$a_1 = -1$	$a_2 = -5$
$c_1 = 19$	$c_2 = 7$
$19d_1 \equiv -1 \pmod 7$	$7d_2 \equiv -5 \pmod{19}$
$-2d_1 \equiv 6 \pmod 7$	$7d_2 \equiv 14 \pmod{19}$
$d_1 = -3$	$d_2 = 2$

Thus $x_0 = (-3) \cdot 19 + 2 \cdot 7 = -57 + 14 = -43$ is a particular solution. $7 \cdot 19 = 133$ and so x is a solution if and only if

$$x \equiv -43 \pmod{133}$$

Theorem 4.3.6 (General Chinese Remainder Theorem)**.** [**general chinese**] *Let $n_1, n_2, \ldots n_k$ be non-zero integers and $a_1, \ldots, a_k$ arbitray integers. Then the system of congruence*

$$x \equiv a_i \pmod{n_i}, 1 \leq k$$

has a solution if and only if

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)}, \text{ for all } 1 \leq i < j \leq k$$

In this case the set of solutions forms a single congruence class modulo $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$.

Proof. The second statement follows from 4.3.2. For the forward direction of the first stament let x_0 be a solution of the system of congruence. Then for each $1 \leq i < j \leq n$..

$$a_i \equiv x_0 \pmod{n_i} \text{ and } a_j \equiv x_0 \pmod{n_j}$$

Since $\gcd(n_i, n_j)$ divides n_i and n_j this gives

$$a_i \equiv x_0 \pmod{\gcd(n_i, n_j)} \text{ and } a_j \equiv x_0 \pmod{\gcd(n_i, n_j)}$$

Thus also

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$$

For the backward direction of the first statement let P the set of primes which devide at least one of the n_i's. Then there exist non-zero integers e_{ip}, $1 \leq i \leq k$, $p \in P$ such that

$$a_i = \prod_{p \in P} p^{e_{ip}}$$

For $p \in P$ define $e_p = \max(e_{ip} \mid 1 \leq i \leq k)$ and pick $1 \leq i_p \leq k$ with $e_p = e_{i_p p}$. Set $b_p = a_{i_p}$. By the Chinese Remainder Theorem the system of congruences

$$x \equiv b_p \pmod{p^{e_p}}, p \in P$$

has a solution, say x_0. We will show that x_0 is also a solution of the original system of congruences. For this let $1 \leq i \leq k$ and $p \in P$. Then

$$x_0 \equiv b_p \pmod{p^{e_p}}$$

and since $e_{ip} \leq e_p$ also

$$(*) \qquad x_0 \equiv a_{i_p} \pmod{p^{e_{ip}}}$$

By assumption

$$a_i \equiv a_{i_p} \pmod{\gcd\left(n_i, n_{i_p}\right)}$$

Note that $p^{e_{ip}}$ divides n_i and since $e_{ip} \leq e_p = e_{i_p p}$, $p^{e_{ip}}$ also devides n_{i_p}. Thus

$$a_i \equiv a_{i_p} \pmod{p^{e_{ip}}}$$

Together with (*) this gives

$$x_0 \equiv a_i \pmod{p^{e_{ip}}}$$

for all $p \in P$. Note that $\mathrm{lcm}(p^{e_{ip}}, p \in P)$ is $\prod_{p \in P} p^{e_{ip}} = n_i$. Thus 4.3.1 gives

$$x_0 \equiv a_i \pmod{n_i}$$

This holds for all $1 \leq i \leq k$ and so x_0 is indeed a solution of $x \equiv a_i \pmod{n_i}, 1 \leq i \leq k$. $\square$

Example 4.3.7. [ex:general chinese]

$$x \equiv 5 \pmod{12} \textit{ and } x \equiv 11 \pmod{18}$$

$$12 = 2^2 3, 18 = 2 \cdot 3^2, \gcd(12, 18) = 2 \cdot 3 = 6, \mathrm{lcm}(12, 18) = 2^2 3^2 = 36$$

Since $11 - 5 = 6$ is divisible 6, we see that the system of linear congruence has a solution. $2^2 | 12$ and $3^2 | 18$, so the system is equivalent to

$$x \equiv 5 \pmod 4 \text{ and } x \equiv 11 \pmod 9$$

and so to

$$x \equiv 1 \pmod 4 \text{ and } x \equiv 2 \pmod 9$$

We use the algorithm from the Chinese remainder theorem to solve the system

$$\begin{array}{c|c}
a_1 = 1 & a_2 = 2 \\
c_1 = 9 & c_2 = 4 \\
9d_1 \equiv 1 \pmod 4 & 4d_2 \equiv 2 \pmod 9 \\
d_1 \equiv 1 \pmod 4 & 8d_2 \equiv 4 \pmod 9 \\
 & -d_2 = 4 \pmod 9 \\
d_1 = 1 & d_2 = -4
\end{array}$$

So

$$c_1d_1 + c_2d_2 = 9 \cdot 1 + 4 \cdot -4 = 9 - 16 = -7$$

is a solution. This x is a solution if and only if

$$x \equiv -7 \pmod{36}$$

4.4 Polynomial congruences

Let $f \in \mathbb{Z}[x]$ and n a non-zero integer. In this section we provide an algorithm to solve the polynomial congruence

$$f(x) \equiv 0 \pmod{n}$$

It follows from 4.1.8, that if x_0 is a solution, then also any number congruent to x_0 modulo n is a solutions. So the set of solutions is a union of congruence classes modulo n.

We first consider the case $n = p^e$, where p is a prime and $e \in \mathbb{Z}^+$. Observe that if x_i is a solution of $f(x) \equiv 0 \pmod{p^i}$, then x_i is also a solution of $f(x) \equiv 0 \pmod{p^{i-1}}$. This allows an inductive approach:

Given a solution x_i of $f(x) \equiv 0 \pmod{p^i}$ we need to find all solutions $x_{i+1} \in \mathbb{Z}$ such that

$$(*) \qquad f(x_{i+1}) \equiv 0 \pmod{p^{i+1}} \text{ and } x_{i+1} \equiv x_i \pmod{p}^i.$$

Unfortunately our inductive approach does not work for $i = 0$ and we therefore assume that we are somehow able to solve the congruence $f(x) \equiv 0 \pmod{p}$. For small primes p, this can be done by computing $f(i)$ for all $0 \leq i < p$.

Suppose now that $i \geq 1$. Since $x_{i+1} \equiv x_i \pmod{p^i}$

$$x_{i+1} = x_i + k_i p^i$$

for some $k_i \in \mathbb{Z}$.

Let $f = \sum_{l=0}^{m} a_l x^l$ with $m \in \mathbb{N}$ and $a_l \in \mathbb{Z}$. Note that

$$x_{i+1}^l = (x_i + k_i p^i)^l = \sum_{t=0}^{l} \binom{l}{t} k_i^t p^{it} x_i^{l-t}$$

If $t \geq 2$, then $it \geq 2i \geq i+1$ and so $p^{it} \equiv 0 \pmod{p^{i+1}}$. Thus

$$x_{i+1}^l \equiv \sum_{t=0}^{1} \binom{l}{t} k_i^t p^{it} x_i^{l-t} \equiv x_i^l + k_i p^i l x_i^{l-1} \pmod{p^{i+1}}$$

and so

$$\begin{array}{rcrl} f(x_{i+1}) & \equiv & \sum_{l=0}^{m} a_l x_{i+1}^l & \pmod{p^{i+1}} \\ & \equiv & \sum_{l=0}^{m} a_l (x_i^l + k_i p^i x_i^{l-1}) & \pmod{p^{i+1}} \\ & \equiv & \left(\sum_{l=0} a_l x_i^l\right) + k_i p^i \left(\sum_{l=0}^{m} a_l l x_i^{l-1}\right) & \pmod{p^{i+1}} \\ & \equiv & f(x_i) + k_p^{i+1} f'(x_i) & \pmod{p^{i+1}} \end{array}$$

Since $f(x_i) \equiv 0 \pmod{p^i}$ we have $f(x_i) = q_i p^i$ for some $q_i \in \mathbb{Z}$. Thus

$$\begin{array}{cccc} f(x_{i+1}) & \equiv & 0 & \pmod{p^{i+1}} \\ q_i p^i + k_o p^i f'(x_i) & \equiv 0 & \pmod{p^{i+1}} & \\ q_i + k_i f'(x_i) & \equiv 0 & \pmod{p} & \\ k_i f'(x_i) & \equiv -q_i & \pmod{p} & \end{array}$$

So (*) holds if and only of

$$(**) \qquad k_i f'(x_i) \equiv -q_i \pmod{p}$$

So there are three cases to consider:

Case 1 $f'(x_i) \not\equiv 0 \mod p$

Then k_i is uniquely determined by (**) modulo p and so there x_{i+1} is uniquely determined by (*) modulo p^{i+1}.

Case 2 $f'(x_i) \equiv 0 \mod p$ and $q_i \not\equiv 0 \pmod{p}$.
Then (**) does not holds for ant k_i and so also (*) does not hold for any x_{i+1}.

Case 3 $f'(x_i) \equiv 0 \mod p$ and $q_i \equiv 0 \pmod{p}$.

Then (**) holds for all k_i and so there are (modulo p) p choices for k_i which fulfill (**). So any x_{i+1} with $x_{i+1} \equiv x_i \pmod{p^i}$ fulfills (**) and there are (modulo p^{i+1}) p choices for x_{i+1} which fulfill (*).

Note that $x_i \cong x_1 \pmod{p}$ and so by 4.1.8 $f'(x_1) \equiv f'(x_i)$. So (**) is equivalent to

$$(***) \qquad k_i f'(x_1) \equiv -q_i \pmod{p}$$

So it suffices it compute $f'(x_1)$

Example 4.4.1. [**ex:polynomial congruence**] *Find all solutions of* $x^3 - x^2 + 4x + 1 \equiv 0 \pmod{5^3}$

Put $f(x) = x^3 - x^2 + 4x + 1$. We start with the congruence

$$f(x) \equiv 0 \pmod{5}$$

We have

$$\begin{array}{ccccc} f(0) & \equiv & 0^3 - 0^2 + 4 \cdot 0 + 1 & \equiv 1 & \pmod{5} \\ f(1) & \equiv & 1^3 - 1^2 + 4 \cdot 1 + 1 & \equiv 5 & \pmod{5} \\ f(2) & \equiv & 2^3 - 2^2 + 4 \cdot 2 + 1 & \equiv 13 & \pmod{5} \\ f(-2) & \equiv & (-2)^3 - (-2)^2 + 4 \cdot (-2) + 1 & \equiv -19 & \pmod{5} \\ f(-1) & \equiv & (-1)^3 - (-1)^2 + 4 \cdot (-1) + 1 & \equiv -5 & \pmod{5} \end{array}$$

So the solutions of $f(x) \equiv 0 \pmod 5$ are

$$x_1 \equiv 1 \pmod 5 \text{ and } x_1 \equiv -1 \pmod 5$$

Before proceeding, let's compute:

$$f'(x) = 3x^2 - 2x + 4 \equiv 3x^2 - 2x - 1 \pmod 5$$

Thus $f'(1) \equiv 3 - 2 - 1 \equiv 0 \pmod 5$ and $f'(-1) = 3 + 2 - 1 = -1 \pmod 5$, We record:

$$f'(1) \equiv 0 \pmod 5 \text{ and } f'(-1) \equiv -1 \pmod 5$$

We now compute all solutions of

$$f(x) \equiv 0 \pmod{5^2}$$

Let $x_2 = x_1 + 5k_1$ and $f(x_1) = 5q_1$. We need to solve

$$k_1 f'(x_1) \equiv -q_1 \pmod 5$$

If $x_1 = 1$, then $f(x_1) = 5 = 1 \cdot 5$ and $f(x_1) \equiv 0 \pmod 5$. Thus $q_1 = 1$ and we get

$$k_1 \cdot 0 \equiv -1 \pmod 5$$

This has no solution.
If $x_1 - 1$, the $f(x_1) = -5 = -1 \cdot 5$ and $f(x_1) \equiv -1 \pmod 5$. Thus $q_1 = -1$ and we get

$$k_1 \cdot (-1) \equiv -(-1) \pmod 5$$

Thus $k_1 \equiv -1 \pmod 5$ and so $x_2 \equiv x_1 + 5k_1 \equiv = -1 + 5(-1) \equiv -6 \pmod{25}$. So $f(x) \equiv 0 \pmod{5^2}$ has a unique solution modulo 5^2 namely

$$x_2 \equiv -6 \pmod{5^2}$$

We are now able to compute all solutions of

$$f(x) \equiv 0 \pmod{5^3}$$

We have $x_2 = -6$, $x_3 = x_2 + 25k_2$, $f(x_2) = (-6)^3 - (-6)^2 + 4(-6) = 1 = -216 - 36 - 24 + 1 = -215 - 60 = -275 = (-11)\dot{2}5$. So $q_2 = -11$. Also $f'(-6) \equiv f'(-1) \equiv -1 \pmod 5$. So the congruence $k_2 f'(x_2)$
$equiv - q_2 \pmod 5$ is

$$-k_2 \equiv -(-11) \pmod 5$$

and so $k_2 \equiv -11 \equiv -1 \pmod 5$. So $x_3 \equiv x_2 + 25k_2 \equiv -6 - 25 \equiv -31 \pmod{5^3}$
So $f(x) \equiv 0 \pmod{5^3}$ has a unique solution modulo 5^3 namely

$$x_3 \equiv -31 \pmod{5^3}$$

Solving $f(x) \equiv 0 \pmod n$ for an arbitrary $n \in \mathbb{Z}^+$:

If n is not a prime power, write $n = p_1^{e_1} \dots p_k^{e_k}$. Then solve the equation $f(x) \equiv 0 \pmod{p_i^{e_i}}$. Say $x_{i1}, \dots x_{ir_i}$ are the solutions. Then for each $1 \leq j_i \leq r_i$, $1 \leq i \leq k$ use the Chinese Remainder Theorem to solve

$$x \equiv x_{ij_i} \pmod{p_i^{e_i}}, 1 \leq i \leq k$$

to obtain the $r_1 r_2 \dots r_k$ solutions of $f(x) \equiv 0 \pmod{n}$.

Chapter 5

Groups

5.1 Basic Properties of Groups

Definition 5.1.1. [**def:binary operation**]

(a) [**a**] *A binary operation on a set S is a function $* : S \times S \to T$. We denote the image of (a, b) under $*$ by $a * b$ or ab.*

(b) [**b**] *A binary operation $* : S \times S \to T$ is called*

   (a) [**a**] closed *if $a * b \in S$ for all $a, b \in S$.*

   (b) [**b**] associative *if its closed and $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.*

   (c) [**c**] commutative *if $a * b = b * a$ for all $a, b \in S$.*

(c) [**c**] *Let $*$ be a binary operation on the set S. An identity for $*$ is an element $e \in S$ with $a * e = a = e * a$ for all $a \in S$.*

(d) [**d**] *Let $*$ be a binary operation on S and e an identity for $*$. Let a and $b \in S$. Then b is called an inverse of a with respect to $*$ if $a * b = e = b * a$. If a has an inverse in S then a is called invertible with respect to $*$.*

(e) [**e**] *Let $*$ be a binary operation on the set G. Then $(G, *)$ is called a group if*

   (i) [**i**] *$*$ is closed;*

   (ii) [**ii**] *$*$ is associative;*

   (iii) [**iii**] *$*$ has an identity e in G; and*

   (iv) [**iv**] *each element $a \in G$ is invertible with respect to $*$.*

(f) [**f**] *A group $(G, *)$ is called abelian if $*$ is commutative.*

$(\mathbb{N}, +)$ is closed, associative, commutative and has an identity. But 0 is the only element with an inverse.

$(\mathbb{Z}, +)$ is a abelian group.

$(\mathbb{N}, -)$ is not closed, not associative, not commutative and has no identity. (so we can't even talk about inverses)

Let $\mathbb{R}^*$ be the set of non-zero real numbers. Then $(\mathbb{R}^*, \cdot)$ is a group.

Lemma 5.1.2. [**unique identity**] *Let $*$ be a binary operation on the set S with and identity e.*

(a) [**a**] *e is the only identity of $*$.*

(b) [**b**] *If $a \in S$ is invertible and $*$ is associative, then a has a unique inverse in S. We will denote the unique inverse by a^{-1}.*

Proof. (a) Let f be an identity in S. Then $ef = e$ since e is an identity and $ef = f$ since f is an identity. So $e = f$.

(b) Let b and c be inverse of a. Then

$$b = eb = (ca)b = c(ab) = ce = c$$

□

Lemma 5.1.3 (Cancellation Law)**.** [**cancellation**] *Let G be a group and $a, b, c \in G$. Then*

$$\begin{aligned} & ab = ac \\ \iff & \quad b = c \\ \iff & ba = ac \end{aligned}$$

Proof. Suppose $ab = ac$. Then $a^{-1}(ab) = a^{-1}(ac)$ and so $(a^{-1}a)b = (a^{-1}a)c$, $eb = ec$ and $b = c$.

If $b = c$, then clearly $ab = ac$. So the first two statements are equivalent. Similary, the last two statement are equivalent. □

Corollary 5.1.4. [**eq in group**] *Let G be a groups and $a, b \in G$. Then*

(a) [**a**] *The equation $ax = b$ has a unique solution in G, namely $x = a^{-1}b$.*

(b) [**b**] *$(a^{-1})^{-1} = a$.*

(c) [**c**] *$(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. (a): By the Cancellation Law, $ax = b$ if and only if $a^{-1}(ax) = a^{-1}b$ and so if and only if $x = a^{-1}b$.

(b) By definition of a^{-1},

$$aa^{-1} = e = a^{-1}a$$

and so

$$a^{-1}a = e = aa^{-1}$$

Hence $a = (a^{-1})^{-1}$.

(c) $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = a^{-1} = e = (ab)(ab)^{-1}$ and so by (a) $b^{-1}a^{-1} = (ab)^{-1}$. □

Definition 5.1.5. [**def:subgroup**] *Let G be a group and H a subset of G. Then H is called an* subgroup *of G and we write $H \leq G$ provided that*

(i) [**a**] *$e \in H$;*

(ii) [**b**] *$ab \in H$ for all $a, b \in H$; and*

(iii) [**c**] *$a^{-1} \in H$ for all $a \in H$*

Note that if H is a subgroup of G, then H together with $* |_{H\times H}$ is a group.

For $n \in \mathbb{Z}$ let $n\mathbb{Z} = \{nm \mid n \in \mathbb{Z}\}$. Then $n\mathbb{Z}$ is subgroup of $\mathbb{Z}$ with respect to addition. Also $a \in n\mathbb{Z}$ if and only if $n|a$.

Definition 5.1.6. [**def:cosets**] *Let G be a group and $H \leq G$*

(a) [**a**] *The relation $\equiv_H$ on G is defined by $a \equiv_H b$ if $ab^{-1} \in H$.*

(b) [**b**] *For $a \in H$, $Ha = \{ha \mid h \in H\}$. Ha is called the* right coset *of H in G containing a.*

(c) [**c**] *$G/H = \{Ha \mid a \in G\}$.*

Consider for example the subgroup $n\mathbb{Z}$ of $(\mathbb{Z}, +)$. Let $a, b \in \mathbb{Z}$. Then the inverse of b with respect of " + " is $-b$. So

$$\begin{array}{rc} & a \equiv_{n\mathbb{Z}} b \\ \Longleftrightarrow & a + (-b) \in n\mathbb{Z} \\ \Longleftrightarrow & a - b \in n\mathbb{Z} \\ \Longleftrightarrow & n|a - b \\ \Longleftrightarrow & a \equiv_n b \end{array}$$

Lemma 5.1.7. [**equiv h**] *Let G be a groups and H a subgroup of G. Then $\equiv_H$ is an equivalence relation of G.*

Proof. Let $a, b, c \in G$. Then $aa^{-1} = e \in H$ and so $a \equiv_H a$. So $\equiv_H$ is reflexive.

If $a \equiv_H b$, then $ab^{-1} \in H$ and so also $(ab^{-1})^{-1} \in H$. Now $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$ and so $ba^{-1} \in H$ and $b \equiv_H a$. Thus $\equiv_H$ is symmetric.

Suppose that $a \equiv_H b$ and $b \equiv_H c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus $(ab^{-1})(bc^{-1} \in H$. Since

$$(ab^{-1})(bc^{-1}) = ((ab^{-1})b)c^{-1} = (a(b^{-1}b))c^{-1} = (ae)c^{-1} = ac^{-1}$$

we have $ac^{-1} \in H$ and so $a \equiv_H c$. Thus $\equiv_H$ is transitive and hence an equivalence relation. □

Theorem 5.1.8 (Lagrange's Theorem)**.** [**lagrange**] *Let G be a groups and H a subgroup of G. Then*

$$|G| = |G/H| \cdot |H|$$

So if G is finite, then $|H|$ divides $|G|$.

Proof. Since each element of G lies in exactly one equivalence class of $\equiv_H$ and G/H is the set of equivalence classes of $\equiv_H$ we have

$$|G| = \sum_{T \in G/H} |T|$$

We will show that $|T| = |H|$ for all $T \in G/H$. Indeed, let $g \in G$ with $T = Hh$ and define

$$\alpha : H \to Hg, h \to hg$$

If $t \in T$, then by definition Hg, $t = hg$ for some $h \in H$ and so $t = \alpha(h)$. Thus $\alpha(h) = t$ and α is onto. let $h, k \in H$ with $\alpha(h) = \alpha(k)$. Then $hg = kg$ and so by the Cancellation Law, $h = k$. Thus α is 1-1.

Since α is 1-1 and onto, $|H| = |T|$. Thus

$$|G| = \sum_{T \in G/H} |T| \sum_{T \in G/H} |H| = |G/H| \cdot |H|$$

□

Definition 5.1.9. [**def:order**] *Let G be a group and $g \in G$.*

(a) [**z**] *For $n \in \mathbb{Z}^+$ define g^n inductively by $g^0 = e$ and $g^{n+1} = g^b g$. Also define $g^{-n} = (g^{-1})^n$.*

(b) [**a**] *$\langle g \rangle := \{g^n | n \in \mathbb{Z}\}$. $\langle g \rangle$ is called the subgroup of G* generated *by G.*

(c) [**b**] *G is called* cyclic *if $G = \langle h \rangle$ for some $h \in G$. Such an h is called a generator for G.*

(d) [**c**] *We say that g has* finite order *if there exists $n \in \mathbb{Z}^+$ with $g^n = e$. In this case the smallest such n is called the* order *of g and is denoted by $|g|$. If no such n exists we say that g has* infinite order *and write $|g| = \infty$.*

(e) [**d**] *C_n= $(\mathbb{Z}_n, +)$.*

By Homework 2, C_n is a group and $[1]_n$ has order n. Thus $C_n = \langle [1]_n \rangle$ and so C_n is a cyclic group.

Lemma 5.1.10. [**order n**] *Let G be a group, $g \in G$ and $k, l \in \mathbb{Z}$. Then*

(a) [**a**] *$g^{k+l} = g^k g^l$.*

(b) [**b**] *$(g^k)^{-1} = g^{-k}$.*

(c) [**c**] *$g^{kl} = (g^k)^l$.*

(d) [**d**] *$\langle g \rangle$ is a subgroup of G.*

Proof. (a) and (b) If $l = 0$, then $g^{k+l} = g^k = g^k e = g^k g^0 = g^k g^l$.

Suppose $l = 1$ and $k \geq 0$. The by definition $g^{k+l} = g^{k+1} = g^k g = g^k g^l$. Suppose $l = 1$ and $k = -1$. The $g^{k+l} = g^{1-1} = g^0 = g^{-1} g = g^k g^l$. Suppose $l = 1$ and $k < -1$. Then

$$g^k g^l = g^k g = (g^{-1})^{-k}) g = (g^{-1})^{-k-1} g^{-1} g = (g^{-1})^{-(k+1)} = g^{k+1} = g^{k+l}.$$

Suppose (a) holds for some $l \geq 0$. Then using the "l=1" case twice:

$$g^{k+(l+1)} = g^{(k+l)+1} = g^{k+l} g = (g^k g^l) g = g^k (g^l g) = g^k g^{l+1}$$

So (a) holds for $l + 1$ and so by the principal of induction, for all $l \in \mathbb{N}$ and all $k \in \mathbb{Z}$.

We conclude that for all $l \in \mathbb{N}$, $g^{-l} g^l = g^{-l+l} = g^0 = e$ and so $(g^l)^{-1} = g^{-l}$ and $(g^{-l})^{-1} = g^l = g^{-(-l)}$. Thus (b) holds.

Suppose that $l < 0$. Then

$$g^{k+l} (g^l)^{-1} = g^{k+l} g^{-l} = g^{(k+l)+(-l)} = g^k$$

and multiplying with g^l from the right give $g^{k+l} = g^k g^l$. Thus (a)lso holds for negative l.

(c) If $l = 0$, both sides are equal to e. Suppose (c) holds for some positive $l \in \mathbb{N}$. Then

$$g^{k(l+1)} = g^{kl+k} = g^{kl} + g^k = (g^k)^l * (g^k)^1 = (g^k)^{l+1}$$

and so (c) holds for all $l \in \mathbb{N}$. If $l < 0$, then

$$g^{kl} = (g^{-1})^{k(-l)} = (g^{-1})^k)^{-l} = (g^{-k})^{-l} = ((g^{-k})^{-1})^l = (g^k)^l$$

(d) Let $a, b \in \langle g \rangle$. Then $a = g^k$ and $b = a^l$ for some $k, l \in \mathbb{Z}$. Since $e = g^0$, $e \in \langle g \rangle$. $ab = g^k g^l = g^{k+l} \in \langle g \rangle$ and $a^{-1} = (g^k)^{-1} = g^{-k} \in \langle g \rangle$. Thus $\langle g \rangle$ is indeed a subgroup of G. □

Lemma 5.1.11. [**order n ii**] *Let G be a group and $g \in G$ an element of finite order n. Let $k, l \in \mathbb{Z}$.*

(a) [**a**] $g^k = g^l \iff k \equiv l \pmod{n}$.

(b) [**b**] $g^k = e \iff n|k$.

(c) [**f**] $|g^k| = \frac{n}{\gcd(k,n)}$.

Proof. (a) Suppose first that $k \equiv l \pmod{n}$. Then $k = l + mn$ for some $m \in \mathbb{Z}$ and so

$$g^k = g^{l+mn} = g^l (g^n)^m = g^l e^m = g^l.$$

Suppose next that $g^k \equiv g^l \pmod{n}$. Then $e = g^{-k} g^l = g^{l-k}$. let r be the remainder of $l - k$ when divided by n. Then $l - k \equiv r \pmod{n}$ and $0 \leq r < n$. By the first paragraph

$$g^r = g^{l-k} = e.$$

Since n is the smallest positive integer with $g^n = e$ and since $g^r = e$ and $r < n$, r cannot be a positive integer. Thus $r = 0$. Hence $k - l \equiv 0 \pmod{n}$ and so $k \equiv n \pmod{n}$.

(b) $g^k = e$ iff $g^k = g^0$ iff $k \equiv 0 \pmod{n}$ iff $n|k$.

(c) Put $d = \gcd(k, n)$.

$$\begin{aligned} & (g^k)^l = e & \\ \iff \quad & g^{kl} = e & \\ \iff \quad & n|kl & \text{by (b)} \\ \iff \quad & \tfrac{n}{d}\,|\,\tfrac{k}{d} l & \\ \iff \quad & \tfrac{n}{d}\,|\,l & \text{since } \gcd\left(\tfrac{n}{d}, \tfrac{n}{d}\right) = 1 \end{aligned}$$

and so $|g^k| = \frac{n}{d}$. □

Definition 5.1.12. [**def:hom**] *Let G and H groups and $f : G \to H$ a function.*

(a) [**a**] *f is called a homomorphism (of groups) if $f(ab) = f(a)f(b)$ for all $a, b \in G$.*

(b) [**b**] *f is called an isomorphism if f is a 1-1 and onto homomorphism.*

(c) [**c**] *We say that G is isomorphic to H and write $G \cong H$ if there exists an isomorphism from G to H.*

Lemma 5.1.13. [**order n iii**] *Let G be a group and $g \in G$ an element of finite order n. Then* *(a)* [**a**] $\langle g\rangle \cong C_n$.

(b) [**b**] $|g| = |\langle g\rangle|$.

(c) [**c**] $\langle g\rangle = \{e, g, g^2, \dots, g^{n-1}\}$.

Proof. (a) Define

$$\alpha : C_n \to \langle g\rangle, [k]_n \to g^k$$

We will show that α is well-defined isomorphism of groups.
Let $k, l \in \mathbb{Z}$. Then

$$\begin{aligned} & [k]_n = [l]_n \\ \iff\ & k \equiv l \pmod n \\ \iff\ & g^k = g^l \qquad \text{by (a)} \end{aligned}$$

The forward direction shows that α is well-defined; and the backward direction that α is 1-1. By definition of $\langle g\rangle$ each element of $\langle g\rangle$ is of the form g^k and so α is onto. We have

$$\alpha([k]_n + [l]_n) = \alpha([k+l]_n) = g^{k+l} = g^k g^l = \alpha([k]_n)\alpha([l]_n)$$

and so α is an homorphism. This shows that α is an isomorphism and so $\langle C_n\rangle \cong \langle g\rangle$.

(b) We have $|g| = n = |C_n| \overset{\text{(a)}}{=} |\langle g\rangle$.

(c) By (a) $e, g, g^2, \dots g^{n-1}$ are n pairwise distinct elements. By (b), $\langle g\rangle$ has exactly n elements and so (c) holds. $\square$

Corollary 5.1.14. [**lagrange for elements**] *Let G be a finite abelian group and $g \in G$. Then g has finite order, $|g|\,\big|\,|G|$. and $g^{|G|} = e$ for all $g \in G$.*

Proof. By Lagrange's Theorem $\langle g\rangle$ divides $|G|$ and by 5.1.10 $|g| = |\langle g\rangle|$. $\square$

Chapter 6

The group U_n of units in $\mathbb{Z}_n$

6.1 Fermat's Little Theorem

Definition 6.1.1. [**un**] *Let $n \in \mathbb{Z}^+$.*

(a) [**a**] *Then $U_n = \{[a]_n \mid a \in \mathbb{Z}, \gcd(a,n) = 1\}$.*

(b) [**b**] $\phi(n) = |U_n|$.

For example $U_6 = \{[1]_6, [5]_6\}$ and $\phi(6) = 2$.
$U_8 = \{[1], [3], [5], [7]\}$ and $\phi(8) = 4$

Lemma 6.1.2. [**zn***] *Let $n \in \mathbb{Z}^+$.*

(a) [**a**] *$(U_n, \cdot)$ is an abelian group.*

(b) [**b**] *$a^k \equiv b^l$ for all $a \in \mathbb{Z}$ and $k, l \in \mathbb{N}$ with $k \equiv l \pmod{\phi(n)}$.*

(c) [**c**] **(Euler's Theorem)** *$a^{\phi(n)} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$.*

Proof. (a) Let $a, b \in n$ with $\gcd(a,n) = 1 = \gcd(b,n)$. Then also $\gcd(ab,n) = 1$ and so $[a] \cdot [b] \in U_n$ for all $[a], [b] \in U_n$. Thus U_n is closed with respect to $\cdot$.

Since multiplication in $\mathbb{Z}$ is commutative and associative, multiplication in U_n is also commutative and associative.

[1] is an identity element,

Since $\gcd(a,n) = 1$, the equation

$$ax \equiv 1 \pmod{n}$$

has a solution c. Then $[a][c] = 1 = [c][a]$ and so $[a]$ is invertible. U_n is a group. (b) By 5.1.14, $|[a]|$ divides $|U_n| = \phi(n)$. So $k \equiv l \pmod{\phi(n)}$ implies $k \equiv l \pmod{|[a]|}$ Hence (a) follows from 5.1.11(a).

(c) follows from (a) □

Since $\phi(8) = 4$ and $102 \equiv 2 \pmod 4$, $5^{102} \equiv 5^2 \equiv 25 \equiv 1 \pmod 8$.

Lemma 6.1.3. [**little fermat**] *Let p be a prime.*

(a) [**a**] $U_p = \{[n]_p \mid p \nmid n\} = \{[1], [2], \ldots, [p-1]\}$

(b) [**b**] $\phi(p) = p - 1$

(c) [**c**] $n^k \equiv n^l \pmod p$ *for all* $n \in \mathbb{Z}$ *and* $k, l \in \mathbb{N}$ *with* $k \equiv l \pmod{p-1}$ *and* $p \nmid n$*,*

(d) [**d**] **(Fermat's Little Theorem)** $n^{p-1} \equiv 1 \pmod p$ *for all* $n \in \mathbb{Z}$ *with* $p \nmid n$*.*

(e) [**e**] $n^p \equiv n \pmod p$ *for all* $n \in \mathbb{Z}$*.*

Proof. Let $n \in \mathbb{Z}$. Since p is a prime $\gcd(n,p) = 1$ iff $p \nmid n$. So (a) holds.

By (a) $\phi(p) = |U_p| = p - 1$. (c) and (d) follows from 6.1.2(b), (c) and (b).

To proof (e), let $n \in \mathbb{Z}$. if $p \not| n$, then by (c), $n^{p-1} \equiv 1 \pmod p$ and multiplying with n gives $n^p \equiv n \pmod p$. If $p \mid n$. The $n \equiv 0 \pmod p$ and so also $n^p \equiv 0 \pmod p$. So again (e). holds. □

Example 6.1.4. [**ex:fermat 1**] *Compute* 11^{12} *modulo* 13 *and* 5^{67} *modul0* 17

By Fermat's Little Theorem $11^{12} \equiv 1 \pmod{13}$.
Since $67 \equiv 3 \pmod{16}$ we have modulo 17:

$$5^{67} \equiv 5^3 \equiv 25 \cdot 5 \equiv 8 \cdot 5 \equiv 40 \equiv 6 \pmod{17}$$

Example 6.1.5. [**ex:fermat 2**] *Find all solutions of* $x^{13} + x^7 + x^3 + x + 1 = 0 \pmod 5$*:*

We compute in $\mathbb{Z}_5$:

$$\begin{array}{rcl}
 & x^{14} + x^7 + 2x + 2 & = 0 \\
\iff & x^2 + x^3 + 2x + 2 & = 0 \\
\iff & x^3 + x^2 + 2x + 2 & = 0 \\
0: & 0 + 0 + 0 + 3 & \neq 0 \\
1: & 1 + 1 + 2 + 2 = 6 & \neq 0 \\
2: & 8 + 4 + 4 + 2 = 18 & \neq 0 \\
-2: & -8 + 4 - 4 + 2 = -6 & \neq 0 \\
-1: & -1 + 1 - 2 + 2 & = 0
\end{array}$$

Thus $x^{13} + x^7 + x^3 + x + 1 = 0 \pmod 5$ if and only if $x \equiv -1 \pmod 5$.

Lemma 6.1.6. [**2l-1**] *Let* l *and* m *be coprime positive integers. Then* $2^l - 1$ *and* $2^m - 1$ *are coprime.*

Proof. Let $d = \gcd\left(2^l - 1, 2^m - 1\right)$. Then

$$(*) \qquad 2^l \equiv 1 \pmod d \text{ and } 2^m \equiv 1 \pmod d$$

Since d is odd, $[2]_d \in U_d$. Let e be the order of $[2]_d \in U_d$. From 5.1.11(b) and (*) we conclude that $e \mid l$ and $e \mid m$. Since $\gcd(l, m) = 1$ this gives $e = 1$. Thus $2^1 \equiv 1 \pmod d$ and $d|1$. Thus $d = 1$. □

Lemma 6.1.7. [**unique order 2**] *Let* A *be a finite Abelian group with a unique element* t *of order* 2*. Then*

$$\prod_{a \in A} A = t$$

Proof. Let $a \in A$. Then $a = a^{-1}$ iff $a^2 = e$ iff a has order 1 or 2 and so iff $a = e$ or $a = t$. So we can find elements $a_1, a_2, \dots, a_k$ such that

$$A = \{e, t, a_1, a_1^{-1}, a_2, a_2^{-1}, \dots a_k, a_k^{-1}\}$$

and each element of A is listed excatly once. Thus

$$\prod_{a \in A} a = e \cdot t \cdot a_1 \cdot a_1^{-1} \cdot \dots \cdot a_k \cdot a_k^{-1}$$

and so

$$\prod_{a \in A} = t$$

$\square$

Lemma 6.1.8. [**order 2**] *Let p be an odd prime. U_p has exactly one element of order 2, namely $[-1]_p$.*

Proof. Let $a \in \mathbb{Z}$. Then

$$\begin{aligned} a^2 \equiv 1 \pmod p \\ p \mid a^2 - 1 \\ p \mid= (a+1)(a-1) \\ p \mid a+1 \text{ or } p \mid a-1 \\ a \equiv -1 \pmod p \text{ or } a \equiv 1 \pmod p \end{aligned}$$

Since $[1]_p$ has order 1, $[-1]_p$ is the unique element of order 2. $\square$

Lemma 6.1.9. [**wilson**] *Let $n \in \mathbb{Z}$ with $n > 1$. Then n is a prime if and only if $(n-1)! \equiv -1 \pmod n$.*

Proof. Suppose first $n = p$ for a prime p. If $p = 2$. Then $(p-1)! = 1 \equiv -1 \pmod n$. Suppose that p is an odd prime. Then by 6.1.8, $[-1]_p$ is the unique element of order 2 in U_p and so by 6.1.7

$$\prod_{a \in U_p} a = [-1]_p$$

Since $U_p = \{[1]_p, [2]_p, \dots [p-1]_p\}$ this says

$$[1]_p[2]_p \dots [p-1]_p = [-1]_p$$

and so

$$(p-1)! \equiv -1 \pmod p$$

Suppose next that $(n-1)! \equiv -1 \pmod n$ and let $m \mid n$ with $1 \leq m < n$. Then $(n-1)! \equiv -1 \pmod m$ and m is one of the factor of $(n-1)!$. hence $(n-1)! \equiv 0 \pmod m$. Thus $-1 \equiv 0 \pmod m$, $m \mid 1$ and $m = 1$. So n is a prime $\square$

Lemma 6.1.10. [**sqrt -1**] *Let p be an odd prime. Then*

$$x^2 + 1 \equiv 0 \pmod p$$

has a solution in $\mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$.

Proof. Let $k = \frac{p-1}{2}$. Then $p = 2k + 1$ and since p is odd, k is a positive integer.

Suppose first that $x^2 + 1 \equiv 0 \pmod p$ for some $x \in \mathbb{Z}$. Then $x^2 \equiv -1 \pmod p$ and $p \nmid x$. Thus by Fermat's Little Theorem 6.1.3, $x^{p-1} \equiv 1 \pmod p$. Since $x^{p-1} = x^{2k} = (x^2)^k \equiv (-1)^k \pmod p$ we conclude that $(-1)^k \equiv 1 \pmod p$. Since p is odd, this implies that k is even. So $k = 2l$ for some $l \in \mathbb{Z}$ and $p = 2k + 1 = 4l + 1$. Thus $p \equiv 1 \pmod 4$.

Suppose next that $p \equiv 1 pmod 4$. By Wilson's Theorem

$$\begin{aligned}
(p-1)! &\equiv -1 \pmod p \\
1 \cdot 2 \cdot \ldots \cdot k \cdot k+1 \cdot \ldots \cdot p-2 \cdot p-1 &\equiv -1 \pmod p \\
1 \cdot 2 \cdot \ldots \cdot k \cdot p-k \cdot \ldots \cdot p-2 \cdot p-1 &\equiv -1 \pmod p \\
1 \cdot 2 \cdot \ldots \cdot k \cdot -k \cdot \ldots \cdot -2 \cdot -1 &\equiv -1 \pmod p \\
(-1)^k 1 \cdot 2 \cdot \ldots \cdot k \cdot k \cdot \ldots \cdot 2 \cdot 1 &\equiv -1 \pmod p \\
(-1)^k (k!)^2 &\equiv -1 \pmod p
\end{aligned}$$

Since $p \equiv 1 \pmod 4$, k is even. Then $(-1)^k = 1$ and so $(k!)^2 \equiv -1 \pmod p$. Hence $x = k!$ is an solutions of $x^2 + 1 \pmod p$. □

Consider $p = 13$. Then $k = 6$ and

$$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = (2 \cdot 6) \cdot (3 \cdot 4) \cdot 5 \equiv -1 \cdot -1 \cdot 5 = 5 \pmod{13}$$

So $x = 5$ is a solution of $x^2 + 1 = 0 \pmod{13}$. Indeed $5^2 = 25 \equiv -1 \pmod{13}$

6.2 Pseudo Primes and Carmichael Numbers

Definition 6.2.1. [**def:pseudo prime**] *Let $n \in \mathbb{Z}$ such that $n > 1$ and n is not a prime. Then*

(a) [**a**] *n is called a Carmichael number if*

$$a^n \equiv a \pmod n$$

for all integers a.

(b) [**b**] *n is called a pseudo prime if*

$$2^n \equiv 2 \pmod n$$

We claim that 341 is a pseudo prime. Indeed $341 = 11 \cdot 31$ and so 341 is not a prime. Also $2^{341} \equiv 2 \pmod 2$ if and only if $2^{341} \equiv 2 \pmod{11}$ and $2^{341} \equiv 2 \pmod{31}$. Since $341 \equiv 1 \pmod{10}$ we have $2^{341} \equiv 2^2 = 1 \pmod{11}$. Since $341 = 330 + 11$, $341 \equiv 11 \pmod 3)0$ and so $2^{341} \equiv 2^{11} = 2^5 \cdot 2^5 \cdot 2 \equiv 1 \cdot 1 \cdot 2 = 2 \pmod{31}$. So indeed 341 is a pseudo-prime. The next lemma now shows that there are infinite many pseudo primes:

Lemma 6.2.2. [**pseudo primes**] *Let n be a pseudo prime. Then $2^n - 1$ is a pseudo prime. In particular, there are infinitely many pseudo primes*

Proof. By 3.3.5 since n is not a prime, also $2^n - 1$ is not prime. Since n is a pseudo prime, $2^n \equiv 2 \pmod{n}$ and so $2^n = nk + 2$ for some $k \in \mathbb{Z}$. By 3.3.2, $2^n - 1$ divide $2^{nk} - 1$. Hence $2^{nk} \equiv 1 \pmod{2^n - 1}$. Thus modulo $2^n - 1$

$$2^{2^n - 1} = 2^{nk+1} = 2^{nk}2 \equiv 2 \pmod{2^n - 1}$$

So $2^n - 1$ is indeed a pseudo prime. ☐

Definition 6.2.3. [**def:squarefree**] *$n \in \mathbb{Z}$ is called a square free if 1 is the only positive integers m with $m^2 \mid n$.*

Observe that an integer large than 1 is square free if and only if its a product of distinct primes.

Lemma 6.2.4. [**carmichael**] *Suppose n is a square free integer, $n > 1$ and $p - 1 \mid n - 1$ for all prime divisors p of n. Then n is a prime or a Carmichael number.*

Proof. Let $n = p_1 p_2 \dots p_k$, where each p_i is a prime. Since n is square free, $p_i \neq p_j$ for all $1 \leq i < j \leq k$. Thus $\mathrm{lcm}(p_1, p - 2, \dots \phi_k) = n$ and

$$a^n \equiv a \pmod{n}$$

for all $a \in \mathbb{Z}$ if and only if

$$a^n \equiv a \pmod{p_i}$$

for all $a \in \mathbb{Z}$ and all $1 \leq i \leq k$.

By assumption $p_i - 1 \mid n - 1$ and so $n \equiv 1 \pmod{p_i}$. Thus by 6.1.3(c) $a^n \equiv a^1$ for all $a \in \mathbb{Z}$ and all $1 \leq i \leq k$. If n is not a prime, we conclude that n is a Carmichael number. ☐

Chapter 7

Units in Rings

7.1 Basic Properties of the Group of Units

Definition 7.1.1. [**def:unit**] *Let $(R, +, \cdot)$ be a ring identity 1. Then $a \in R$ is called a* unit *if there exists $b \in R$ with $ab = 1 = ba$. $\mathrm{U}(R)$ denotes the set consisting of all the units in R.*

Lemma 7.1.2. [**unit**] *Let R be a ring with identity. Then for each unit a in R there exists a unique element $b \in R$ with $ab = 1$ and a unique element $c \in R$ with $ca = 1$. Moreover $b = c$. This unique elements of R is called the* inverse *of R and is denoted by a^{-1}.*

Proof. By definition of a unit there exists an element with d in R with $ad = da = 1$. Now let b and c be any elements in R with $ab = 1 = ca$. Then

$$b = 1b = (ca)b = c(ab) = c1 = c$$

With d in place of c we see that $b = d$ and with d in place of b we also get $a = d$. □

Lemma 7.1.3. [**u(r)**] *Let $(R, +, \cdot)$ be a ring with identity. Then $(\mathrm{U}(R), \cdot)$ is a group.*

Proof. Let $a, b \in \mathrm{U}(R)$. Then $(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (a1)a^{-1} = aa^{-1} = 1$ and similarly $(b^{-1}a^{-1})(ab) = 1$. Thus $ab \in \mathrm{U}(R)$ and so $\mathrm{U}(R)$ is closed under multiplication.

Since R is a ring, multiplication is associative.

Since $1 \cdot 1 = 1$, 1 is a unit. So $1 \in \mathrm{U}(R)$ and so $\mathrm{U}(R)$ has an identity with respect to multiplication.

Let $a \in U(R)$. Then $aa^{-1} = 1 = a^{-1}a$. So a is an inverse of a^{-1} and $a^{-1} \in \mathrm{U}(R)$. Thus a has a multiplicative inverse in $\mathrm{U}(R)$.

We verified the four axioms of a group and so $(\mathrm{U}(R), \cdot)$ is a group. □

Lemma 7.1.4. [**znm**] *Let n and m be positive integers with $\gcd(n, m) = 1$. Then*

$$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m \qquad \textit{as rings}$$

Proof. Define

$$\alpha : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m, a \to ([a]_n, [a]_m).$$

We have

$$\alpha(a+b) = ([a+b]_n, [a+b]_m) = ([a]_n + [b]_n, [a]_m + [b]_m) = ([a]_n, [a]_m) + ([b]_n, [b]_m) = \alpha(a) + \alpha(b)$$

and

$$\alpha(a \cdot b) = ([a \cdot b]_n, [a \cdot b]_m) = ([a]_n \cdot [b]_n, [a]_m \cdot [b]_m) = ([a]_n, [a]_m) \cdot ([b]_n, [b]_m) = \alpha(a) \cdot \alpha(b)$$

Thus α is a ring homomorphism
Let $a \in \mathbb{Z}$. Then

$$\begin{array}{rcl}
 & a \in \ker \alpha & \\
\iff & \alpha(a) = 0 & \\
\iff & ([a]_n, [a]_m) = ([0]_n, [0]_m) & \\
\iff & [a]_n = [0]_n \text{ and } [a]_m = ([0]_m) & \\
\iff & n|a \text{ and } m|a & \\
\iff & nm|a & \text{since } \gcd(n,m) = 1 \\
\iff & a = knm \text{ for some } k \in \mathbb{Z} & \\
\iff & a \in nm\mathbb{Z}. &
\end{array}$$

Thus $\ker \alpha = nm\mathbb{Z}$. Hence by the First Isomorphism Theorem for Rings:

$$\mathbb{Z}_{nm} = \mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/\ker \alpha \cong \operatorname{Im} \alpha$$

In particular, $|\operatorname{Im} \alpha| = |\mathbb{Z}_{nm}| = nm$.
Since $\operatorname{Im} \alpha \leq \mathbb{Z}_n \times \mathbb{Z}_m$ and $|\mathbb{Z}_n \times \mathbb{Z}_m| = nm$ we conclude that $\operatorname{Im} \alpha = \mathbb{Z}_n \times \mathbb{Z}_m$. Thus

$$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m.$$

□

We remark that we just obtained a new proof for the Chinese Remainder Theorem. Since α is onto for any $b, c \in \mathbb{Z}$ there exists $x \in \mathbb{Z}$ with $([x]_n, [x]_m) = ([b]_n, [c]_m)$, that is with $x \equiv b \pmod{n}$ and $x \equiv c \pmod{m}$. Also since $\ker \alpha = nm\mathbb{Z}$, this x is unique modulo nm.

Lemma 7.1.5. [**iso and units**] *Let R and S be rings with identity.*

(a) [**a**] *Let $\alpha : R \to S$ be an isomorphism of rings. Then*

$$\beta : \mathrm{U}(R) \to \mathrm{U}(S), r \to \alpha(r)$$

is a well defined isomorphism of multiplicative groups.

(b) [**b**] $\mathrm{U}(R \times S) = \mathrm{U}(R) \times \mathrm{U}(S)$.

Proof. (a): Let $r \in R$.

We claim that r is a unit in R if and only if $\alpha(r)$ is a unit in S. So suppose that r is a unit. Then $rt = 1 = tr$ for some $t \in R$. Thus

$$\alpha(r)\alpha(t) = \alpha(rt) = \alpha(1) = 1$$

and similarly $\alpha(t)\alpha(r) = 1$. Thus $\alpha(t)$ is a unit with inverse $\alpha(r)$.

Since α^{-1} is an isomorphism from S to R, a similar argument shows that if $\alpha(r)$ is unit in S with inverse say u, then r is unit in R with inverse $\alpha^{-1}(u)$.

This completes the proof of the claim. In particular, $\alpha(r) \in U(S)$ for all $r \in \mathrm{U}(R)$ and so β is well-defined. Since α is a ring homomorphism, β is a group homomorphism. The map $\mathrm{U}(S) \to \mathrm{U}(R), s \to \alpha^{-1}(s)$ is the inverse of β and so β is a bijection. Thus β is an group isomorphism and (a) holds.

(b): Let $r \in R$ and $s \in S$. Then

$$\begin{array}{cc} & (r,s) \in \mathrm{U}(R \times S) \\ \iff & \text{there exists } (u,v) \in R \times S \text{ with } (r,s)\cdot(u,v) = (1,1) = (u,v)\cdot(r,s) \\ \iff & \text{there exist } u \in R, v \in S \text{ with } ru = 1 = ur \text{ and } sv = 1 = vs \\ \iff & r \in \mathrm{U}(R), s \in \mathrm{U}(S) \\ \iff & (r,s) \in \mathrm{U}(R) \times \mathrm{U}(S) \end{array}$$

□

Lemma 7.1.6. [**unm**] *Let n and m be positive integers with $\gcd(n,m) = 1$. Then*

(a) [**a**] $U_{nm} \cong U_n \times U_m$ *as abelian groups.*

(b) [**b**] $\phi(nm) = \phi(n)\phi(m)$.

Proof. (a) By 7.1.4 we have $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ as rings. Thus by 7.1.5

$$U_{nm} = \mathrm{U}(\mathbb{Z}_{nm}) \cong \mathrm{U}(\mathbb{Z}_n \times \mathbb{Z}_m) = \mathrm{U}(\mathbb{Z}_n) \times \mathrm{U}(\mathbb{Z}_m) = U_n \times U_m$$

(b) $\phi(nm) = |U_{nm}| \overset{(a)}{=} |U_n \times U_m| = |U_n| \cdot |U_m| = \phi(n)\phi(m)$. □

Lemma 7.1.7. [**phin**]

(a) [**a**] *Let p be a prime and e a positive integer. Then* $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

(b) [**b**] *Let $n > 1$ be a integer and suppose $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where $p_1, \dots, p_k$ are pairwise distinct primes and $e_1, e_2, \dots e_k$ are positive integers. Then*

$$\phi(n) = p_1^{e-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1)\dots p_k^{e_k-1}(p_k - 1)$$

Proof. (a) Note first that $\phi(p^e) = |U_{p^e}| = \{[a]_{p^e} \mid 0 \le a < p^e, \gcd(a, p^e) = 1\}$. Let $0 \le a < p^e$. Then $\gcd(a, p^e) \neq 1$ iff $p|a$ iff $a = pb$ for some $0 \le b < p^{e-1}$. So among the p^e integers a with $0 \le a < p^e$, there are p^{e-1} integers with $\gcd(a, p^e) \neq 1$. Thus $\phi(p^e) = p^e - p^{e-1}$

(b) From 7.1.6(b) and induction we have

$$\phi(n) = \phi(p_1^{e_1})\phi(p_e^{e_2})\dots\phi(p_k^{e_k})$$

and so (b) follows from (a). □

7.2 Public key cryptography

We define a code to be bijection f from a set W to a set V. Given a code f, then a decoding of f is the inverse function f^{-1} of f..

Examples:

$W = V = \{A, B, C, \cdot, Z\}$,
$f : A \to B, B \to C, \ldots, Z \to A$
$f^{-1} : A \to Z, B \to A, C \to B, \ldots Z \to Y$.

W set of sequence of 5 symbols found on a regular keyboard,
$f(s_1s_2s_3s_4s_5) = s_3s_5s_2s_1s_4$
$f^{-1}(t_1t_2t_3t_4t_5) = t_4t_3t_1t_5t_2$

$W = V = \mathbb{Z}_{26}$
$f(x) = x + 1$.
$f^{-1} = x - 1$

$W = V = \mathbb{Z}_{26}$
$f(x) = 5x + 3$
$f^{-1}(x) = -5(x - 3)$

p a prime, $1 \leq e < p - 1$, $V = \mathbb{Z}_p = W$,
$f(x) = x^e$
$f^{-1}(x) = x^g$,
what is g? We need $x = f^{-1}(f(x)) = x^{eg}$. Since $x^1 \equiv x^{eg} \pmod p$. if $eg \equiv 1 \pmod{p-1}$, we can choose g to be a solution of $ex \equiv 1 \pmod{p-1}$.

In a secret code f is only known to the sender and receiver. But this requires secretly sharing information between the sender and receiver.

In a public code $f(x)$ is know to the public, but $f^{-1}(x)$ is only know to the receiver. For this to work in must be impossible to computer the inverse of $f(x)$. (At least computing the inverse must take to long to be useful.)

Let n, k be positive integers with $\gcd(k, \phi n) = 1$ and consider the function $f : U_n \to U_n, x \to x^k$. To decode f we need to find an integer l such $(x^k)^l = x$ for all $x \in U_n$. By Euler's Theorem 6.1.2(c) we just need $kl \equiv 1 \pmod{\phi(n)}$. Computing the inverse of k modulo $\phi(n)$ is easy. But computing $\phi(n)$ is not easy. Indeed to find $\phi(n)$ we has to compute the prime factorization of n which does take a very long times to do. So f is a good candidate for a public code. One chooses a few big prime $p_1, p_2, \ldots p_k$, Computes the $n = p_1, p_2 \ldots p_k$, chooses a number k coprime to $\phi(n)$ and then publicizes n and k. Essentially this works, since multiplying numbers is very fast, but factorizing numbers is very slow.

7.3 The structure of the groups U_n

In this section we investigate the structure of the groups U_n. In particular, we will determine for which n, U_n is cyclic.

Definition 7.3.1. [**def:primitive**] *An element $a \in U_n$ is called primitive if $U_n = \langle a \rangle$*

Observe that U_n has primitive element if and inly of U_n is cyclic. Also $a \in U_n$ is primitive if and only if $|a| = \phi(n)$.

Notation 7.3.2. [**sum dn**] *Let $f : \mathbb{Z}+ \to \mathbb{R}$ be a function. Then*

$$\sum_{d|n} f(d) = \sum_{d \in \mathbb{Z}^+ | d|n} f(n)$$

Lemma 7.3.3. [**sum phi n**] *Let $n \in \mathbb{Z}^+$. Then*

$$\sum_{d|n} \phi(d) = n$$

Proof. Let $D = \{d \in \mathbb{Z}^+ \mid d \mid n\}$, $S = \{1, 2, 3, \ldots, n\}$ and $d \in D$ put $S_d = \{s \in S \mid \gcd(s, n) = \frac{n}{d}\}$. Let s in S. The s lies in a unique S_d namely

$$s \in S_d \iff d = \frac{n}{\gcd(s, n)}$$

So it suffices to prove that $|S_d| = \phi(d)$.

$$\begin{array}{rcl} & a \in S_d & \\ \iff & 1 \leq a \leq n, \gcd(a, n) = \frac{n}{d} & \\ \iff & a = b\frac{n}{d}, 1 \leq b \leq d, \gcd\left(b\frac{n}{d}, n\right) = \frac{n}{d} & \\ \iff & a = b\frac{n}{d} 1 \leq b \leq d, \gcd(b, d) = 1 & \text{divide by } \dfrac{n}{d} \text{ Homework 1 \#5} \end{array}$$

Hence $|S_d| = \phi(n)$. □

Lemma 7.3.4. [**order in up**] *Let p be a prime and d a positive divisor of $p - 1$. Then U_p has exactly $\phi(d)$ elements of order d. In particular U_p has $\phi(p - 1)$ primitive elements and U_p is cyclic.*

Proof. Let $\Omega_d = \{a \in U_p \mid |a| = d\}$ and put $\psi(d) = |\Omega_d|$. We will first show that

1°. [**1**] $\psi(d) = 0$ *or* $\psi(d) = \phi(d)$.

We may assume that $\psi(d) \neq 0$ and so there exists $a \in \Omega(d)$. Then $(a^i)^d = (a^d)^i = 1$ for all $0 \leq i < d$ and so each a^i is a root of the polynomial $x^d - 1$ in $\mathbb{Z}_p[x]$. By 5.1.11(a), $a^i \neq a^j$ for $0 \leq i < j < p$ and since $x^d - 1$ has at most d roots in $\mathbb{Z}_p$, So $\{a^i \mid 0 \leq i < p\}$ is a complete set of roots of $x^d - 1$. Since every element of Ω_d is a root of $x^d - 1$ we conclude that

$$\Omega_d = \{a^i \mid 0 \leq i < p, |a^i| = d\}$$

From 5.1.11(c) we have $|a^i| = \frac{d}{\gcd(i,d)}$ and so $|a^i| = 1$ if and only if $\gcd(i, d) = 1$. Hence

$$\Omega_d = \{a^i \mid 0 \leq i < p, \gcd(i, d) = 1\}$$

and so $\psi(d) = |\Omega_d| = \phi(d)$. Thus (1°) holds.

2°. [2] $\sum_{d|p-1} \psi(d) = p-1$

Let $a \in U_p$ and $d = |a|$. Since $a^{p-1} = 1$, $d \mid p-1$. Hence each of the $p-1$ elements of U_p lies in exactly one of the sets Ω_d, $d \mid p-1$. Thus (2°) holds.

From (2°) and 7.3.3 we have

$$\sum_{d|p-1} \psi(d) = p-1 = \sum_{d|p-1} \phi(d)$$

By (1°) $\psi(d) \leq \phi(d)$ for all $d \mid p-1$ and it follows that $\psi(d) = \phi(d)$ for all $d \mid p-1$. □

Lemma 7.3.5. [**order mod pn**] *Let a, n and p be integers with n positive and p a prime. Suppose* $\gcd(a,n) = 1$ *and* $p \big| n$. *Then*

(a) [**a**] *Let $d = |[a]_n|$, the order of $[a]_n$ in U_n. Then $|[a]_{pn}|$ is either d or dp.*

(b) [**b**] *Let $m \in \mathbb{Z}^+$ with $a^m \equiv 1 \pmod{n}$. Then $a^{pm} \equiv 1 \pmod{pn}$.*

Proof. (a) Let $f = |[a]_{pn}|$. Then $a^f \equiv 1 \pmod{pn}$ and so also $a^f \equiv 1 \pmod{n}$. Thus $d \mid f$.

Since $a^d \equiv 1 \pmod{n}$, $a^d = 1 + kn$ for some $k \in \mathbb{Z}$. Thus by the binomial theorem

$$a^{dp} = (a^d)^p = (1+kn)^p = \sum_{i=0} \binom{p}{i} (kn)^i = 1 + pkn + \sum_{i=1}^{p} \binom{p}{i} k^i n^i$$

Observe that pn divides pkn and since $p|n$, it also divides $n^i = n^{i-1}n$ for all $i \geq 2$. Thus $a^{dp} \equiv 1 \pmod{pn}$ and so $f \mid dp$. Since $d \mid f$, this implies $\frac{f}{d} \mid p$. Since p is a prime we conclude that $\frac{f}{d} = 1$ or p and so $f = d$ or $d = dp$.

(b) Since $a^m \equiv 1 \pmod{n}$, $d \mid m$. Thus $dp \mid pm$ and so by (a) $|a|_{pn} \mid pm$ and so $a^{pm} \equiv 1 \pmod{pn}$. □

Lemma 7.3.6. [**primitive elements**] *Let p be an odd prime and $a \in \mathbb{Z}$.*

(a) [**a**] *If $[a]_p$ is a primitive element in U_p, then $[a]_{p^2}$ or $[a+p]_{p^2}$ is a primitive element of U_{p^2}.*

(b) [**b**] *If $[a]_{p^2}$ is a primitive element in U_{p^2}, then $[a]_{p^e}$ is a primitive element of U_{p^e} for all $e \in Z$ with $e \geq 2$.*

Proof. (a) Since $[a]_p$ is a primitive element, $[a]_p$ has order $p-1$. Thus by 7.3.5, $[a]_{p^2}$ has order $p-1$ or $(p-1)p$. In the latter case we are done. So suppose $[a]_{p^2}$ has order $p-1$. Thus

$$(*) \qquad a^{p-1} \equiv 1 \pmod{p^2}$$

Note that

$$(a+p)^{p-1} = a^{p-1} + (p-1)a^{p-2}p + + \sum_{i=2}^{p-1} \binom{p-1}{i} a^{p-1-i}p^i a^{p-1} \equiv 1 + (p-1)a^{p-2} \pmod{p}^2$$

Since $p \neq 2$, $p \nmid p-1$. Also $p \nmid a$ and so $p \nmid a^{p-2}$. Thus $(a+p)^{p-1} \neq 1 \pmod{p}^2$ and so $[a+p]_{p^2}$ does not have order $p-1$. Since $[a+p]_p = [a]_p$ has order $p-1$, 7.3.5, implies that $[a+p]_p$ has order $(p-1)p$. Hence $[a+p]_{p^2}$ is primitive and (a) is proved.

(b) Thus clearly holds for $e = 2$. Suppose inductively that it holds for e. Then $[a]_{p^e}$ has order $(p-1)p^{e-1}$ and thus

$$a^{(p-1)p^{e-2}} \neq 1 \pmod{p^e}$$

On the other hand 4.1.5(c) applied to $n = p^{e-1}$,

$$a^{(p-1)p^{e-2}} = 1 \pmod{p^{e-1}}$$

Thus

$$a^{(p-1)p^{e-2}} = 1 + kp^{e-1}$$

with $k \in \mathbb{Z}$ and $p \nmid k$. Thus

$$\begin{aligned} a^{(p-1)p^{e-1}} &= (1+kp^{e-1})^p &= 1 + pkp^{e-1} + \binom{p}{2}k^2p^{2(e-1)} + \textstyle\sum_{i=3}^{p}\binom{p}{3}k^ip^{i(e-1)} \\ & &= 1 + kp^e + \frac{p-1}{2}k^2p^{2e-1} + \textstyle\sum_{i=3}^{p}\binom{p}{3}k^ip^{i(e-1)} \end{aligned}$$

Since $e \geq 2$, $2e-1 = (e+1)+(e-2) \leq e+1$ and for $i \geq 3$, $i(e-1) \geq 3(e-1) = e + 2e - 3 \geq e + 4 - 3 \geq e+1$. Thus

$$a^{(p-1)p^{e-1}} \equiv 1 + kp^e \pmod{p^{e+1}}$$

Since $p \nmid k$ this implies $a^{(p-1)p^{e-1}} \neq 1 \pmod{p}^{e+1}$ and $|[a]_{p^{e+1}}| \neq (p-1)p^{e-1}$. Since $|[a]_{p^e}| = (p-1)p^{e-1}$ we conclude from 7.3.5 that

$$|[a]_{p^{e+1}}| = (p-1)p^{e-1}p = (p-1)p^{(e+1)-1}$$

Hence (b) holds for $e+1$ and so for all $e \geq 2$. □

Corollary 7.3.7. [**upe cyclic**] *Let p be an odd prime and e a positive integer. Then U_{p^e} is cyclic.*

Proof. We just need to show that U_{p^e} has a primitive element. By 7.3.4, U_p has a primitive element. Thus by 7.3.6(a), U_{p^2} has a primitive element and so by 7.3.6(a), U_{p^e} has a primitive element for all $e \geq 2$. □

Example 7.3.8. [**ex:primitive**] *Find a primitive element in U_{7^e}*

Consider $U_7 = \{1,2,3,4,5,6\}$. $2^3 = 8 = 1$ in U_7 and so 2 is not a primitive element. Let d be the order of 3 in U_7. Then d divides $\phi(7) = 6$ and so $d = 2, 3$ or 6. $3^2 = 9 = 2 \neq 1$ and $3^3 = 2 \cdot 3 = 6 \neq 1$. So d is neither 2 nor 3. Hence 3 is a primitive element in U_7.

In U_{49} we have $3^4 = 81 = -17$ and so $3^5 = -51 = -2$ and $3^6 = -6$. Hence 3 does not have order 6 in U_{49} and so by 7.3.5 3 has order 42. Thus 3 is a primitive element of U_{49} and so also in U_{3^e} for all $e \in \mathbb{Z}^+$.

Lemma 7.3.9. [**exp u2e**] *Let e be an integer with $e \geq 3$. Then $a^{2^{e-2}} = 1$ for all $a \in U_{2^e}$.*

Proof. $U_8 = \{\pm 1, \pm 3\}$, $(\pm 1)^1 = 1$, $(\pm 3)^2 = 9 = 1$ and $a^2 = a^{2^{3-2}} = 1$ for all $a \in U_{2^3}$. Thus the statement holds for $e = 3$.

Suppose inductively that $a^{2^{e-2}} \equiv 1 \pmod{2^e}$ for all $a \in \mathbb{Z}$ with $\gcd(a,2) = 1$. Then by 7.3.5(b), $a^{2^{e-1}} \equiv 1 \pmod{2^{e+1}}$ and so the statement also holds for $e+1$. □

Notation 7.3.10. [**not:exactly divide**] *Let p, e, a be integers with p a prime and $e \geq 0$. We write $p^e || a$ if $p^e | p$ but $p^{e+1} \not| a$.*

Lemma 7.3.11. [**order 5 u2e**] *Let $e \in \mathbb{Z}$ with $e \geq 2$.*

(a) [**a**] $2^e || 5^{2^{e-2}} - 1$.

(b) [**b**] $|[5]_{2^e}| = 2^{e-2}$.

Proof. (a) $4||5-1$ and so (a) holds for $e = 2$. Suppose inductively that $2^e||5^{2^{e-2}} - 1$. We

$$5^{2^{e-1}} - 1 = (5^{2^{e-2}})^2 - 1 = (5^{2^{e-2}} - 1)(5^{2^{e-2}} + 1)$$

Since $5^{2^{e-2}} + 1 \equiv 1^{2^{e-2}} + 1 \equiv 2 \pmod 4$, $2||5^{2^{e-2}} + 1$. Hence $2^{e+1}||5^{2^{e-1}} - 1$ and (a) also hold for $e + 1$.

(b) By $5^{2^{e-2}} \equiv 1 \pmod 2)^e$ and so $|[5]_{2^e}|$ divides 2^{e-2}. For $e = 2$ this gives $|[5]_4 = 1$. If $e > 2$, then by (a) applies to $e - 1$, $2^{e-1}||5^{2^{e-3}} - 1$, so $2^e \not| 5^{2^{e-3}} - 1$ and $5^{2^{e-3}} \not\equiv 1 \pmod{2^e}$. Thus (b) holds. □

Definition 7.3.12. [**def:exponent**] *Let G be a group. We say that G has finite* exponent *if the exists $n \in \mathbb{Z}^+$ with $g^n = e$. In this case the smallest such n is denotes is called the* exponent *of G and is denoted by* $\exp(G)$.

If no such n exists we say that G has infinite exponent and write $\exp(G) = \infty$.

Note that C_n has exponent n and $(\mathbb{Z}, +)$ has infinite exponent.

Corollary 7.3.13. [**exp u2e ii**] *Let $e \in \mathbb{Z}^+$.*

(a) [**a**] *If $e \leq 2$, then* $\exp(U_{2^e}) = 2^{e-1}$ *and U_{2^e} is cyclic.*

(b) [**b**] *If $e \geq 3$, then* $\exp(U_{2^e}) = 2^{e-2}$ *and U_{2^e} is not cyclic.*

Proof. $U_2 = \{1\}$ has exponent $1 = 2^{1-1}$ and is cyclic. $U_4 = \{\pm 1\}$ has exponent $2 = 2^{2-1}$ and is cyclic.

Suppose $e \geq 3$, then by 7.3.9, $\exp(U_{2^e}) \leq 2^{e-2}$ and by 7.3.11 $\exp(U_{2^e}) \geq 2^{e-2}$. Thus $\exp(U_{2^e}) = 2^{e-2}$. In particular U_{2^e} has no element of order 2^{e-1} and so is not cyclic. □

Proposition 7.3.14. [**ab**] *Let G be a finite abelian group and A and B subgroups of G. Suppose that*

(i) [**i**] $A \cap B = \{e\}$.

(ii) [**ii**] $|A| \cdot |B| = |G|$.

Then $G \cong A \times B$.

Proof. Define $\alpha : A \times B \to G, (a, b) \to ab$. Then for $a, c \in A$, $b, d \in B$:

$$\alpha((a, b)(c, d)) = \alpha((ac, bd)) = (ac)(bd) = (ab)(cd) = \alpha((a, b))\alpha((c, d))$$

and so α is a homomorphism.

Suppose $\alpha((a, b)) = \alpha((c, d))$. Then $ab = cd$ and so also $c^{-1}a = db^{-1}$. Since A is a subgroup of G, $c^{-1}a \in A$ and since B is a subgroup of G, $db^{-1} \in B$. So $c^{-1}a = db^{-1} \in A \times B = \{e\}$ and thus $c^{-1}a = e = db^{-1}$. It follows that $a = c$, $b = d$ and α is 1-1.

In particular

$$|\alpha(A \times B)| = |A \times B| = |A| \times |B| = |G|$$

Since G is finite this implies $\alpha(A \times B) = G$ and so α is onto.

We proved that α is a 1-1 and onto homomorphism and so an isomorphism. Thus $A \times B \cong G$. $\square$

Lemma 7.3.15. [**u2e**] *Let $e \in \mathbb{Z}^+$.*

(a) [**a**] *If $e \leq 2$, then $U_e \cong C_e$.*

(b) [**b**] *If $e \geq 3$, then $U_e \cong C_2 \times C_2^{e-2}$.*

Proof. (a) $U_2 = \{[1]_2\} \cong C_1$ and $U_4 = \{] \pm 1]_4\} = \langle [-1]_4 \rangle \cong C_2$.

(b) Suppose $e \geq 3$. Let $A = \langle [-1]_{2^e} \} = \{[\pm 1]_{2^e}\} \cong C_2$ and $B = \langle [5]_{2^e} \rangle$. By 7.3.11 $[5]_{2^e}$ has order 2^{e-2} and so $|B| = 2^{e-2}$ and $B \cong C_{2^{e-2}}$. Also $|A| = 2$ and so $|A||B| = 2^{e-1} = \phi(2^e) = |U_{2^e}|$. Let $[d]_{2^e} \in A \cap B$ the $d \equiv 5^m \pmod{2^e}$ for some $m \in \mathbb{N}$ and so $d \equiv 1 \pmod 4$. Since $-1 \not\equiv 1 \pmod 4$, we conclude $d \neq -1 \pmod{2^e}$. Since $[d]_{2^e} \in A$ this gives $[d] = [1]_{2^e}$. Hence $A \cap B = \{[1]\}_{2^e}$. Thus 7.3.14 gives $U_{2^e} \cong A \times B \cong C_2 \times C_{2^{e-2}}$. $\square$

Lemma 7.3.16. [**exp**] *Let G be a finite group.*

(a) [**a**] $\exp(G) = \operatorname{lcm}(\{|g| \big| g \in G\})$.

(b) [**b**] *Let $n \in \mathbb{Z}$. Then $g^n = e$ for all $g \in G$ if and only if* $\exp(G)|n$.

(c) [**c**] $\exp(G) \big| |G|$.

Proof. (a) and (b): Let $n \in \mathbb{Z}$. Then

$$\begin{array}{rcll} & g^n = e & \text{for all } g \in G & \\ \iff & |g| \big| n & \text{for all } g \in G & \text{by 5.1.10(b)} \\ \iff & \operatorname{lcm}(\{|g| \big| g \in G\}) \big| n & & \end{array}$$

The smallest positive integer fulfilling the last equation is $\operatorname{lcm}(\{|g| \big| g \in G\})$ and so (a) holds. Since $|g| \big| |G|$ for all $g \in G$, (b) follows from (a) and 2.1.17(b)

(c): By 5.1.14 $g^{|G|} = e$ for all $g \in G$ and so (c) follows from (b). $\square$

Lemma 7.3.17. [**order coprime**] *Let G an abelian group and $g_1, \dots g_n \in G$ be elements of finite order. Let $d = \operatorname{lcm}(|g_1|, |g_2|, \dots, |g_n|)$ and $g = g_1 g_2 \dots g_n$. Then*

(a) [**a**] $g^d = 1$.

(b) [**b**] *If $\gcd(|g_i|, |g_j|) = 1$ for all $\leq i < j \leq n$, then $|g| = d$.*

Proof. (a) Let $1 \leq i \leq n$. Then $|g_i| \big| d$ and so $g_i^d = e$. Since G is Abelian we conclude that

$$g^d = g_1^d g_2^d \dots g_n^d = e$$

(b) Put $f = \operatorname{lcm}(|g_2|, \dots, |g_n|)$, $h = g_2 \dots g_n$ and $c = |g|$. Then $(g_1 h)^c = 1$ and $h^f = 1$. Thus $g_1^c = (h^c)^{-1}$. Put $k = g_1^c$. Then $k^{|g_1|} = (g_1^{|g_1|})^c = e$ and $k^f = ((h^f)^c))^{-1} = e$. So $|k|$ divides $|g_1|$ and f. But $|g_1|$ and f are coprime. Hence $|k| = 1$ and so $g_1^c = e$. Hence $|g_1| \big| c$ and so also $d = \operatorname{lcm}(|g_1|, |g_2|, \dots, |g_n|) \big| c$. Since $g^d = e$, we also have $c \big| d$. and thus $c = d$. $\square$

Corollary 7.3.18. [**char cyclic**] *Let G be a finite abelian group, then G is cyclic if and only* $\exp G = |G|$.

Proof. If G is cyclic, then G has an element of order $|G|$ and so $\exp G = |G|$.

Suppose next that $\exp G = |G|$. Let $|G| = p_1^{e_1} \dots p_k^{e_k}$, where $p_1, \dots p_k$ are distinct primes and $e_i \in \mathbb{Z}^+$. Since $\exp G = \operatorname{lcm}(\{|g| \big| g \in G\},)$, there exists element $h_i \in G$ with $p_i^{e_i} \big| |h_i|$. Put $g_i = h^{\frac{|h_i|}{p_i^{e_i}}}$. Then $|g_i| = p_i^{e_i}$. Put $g = g_1 g_2 \dots g_k$. Then by 7.3.17 g has order $p_1^{e_1} \dots p_k^{e_k} = |G|$ and so G is cyclic. □

Lemma 7.3.19. [**order direct product**] *Suppose $G = G_1 \times G_2 \times \dots G_k$ for some $k \in \mathbb{Z}^+$ and some groups G_i.*

(a) [**a**] *Let $g_i \in G_i$ for $1 \leq i \leq k$. Then*

$$|(g_1, g_1, \dots . g_k)| = \operatorname{lcm}(|g_1|, |g_2|, \dots, |g_k|)$$

(b) [**b**]

$$\exp(G) = \operatorname{lcm}(\exp(G_1), \exp(G_2), \dots, \exp(G_k))$$

Proof. (a)

$$\begin{aligned} & g^n = e \\ \iff & (g_1, g_2, \dots, g_k)^n = (e, e, \dots, e) \\ \iff & g_1^n = e, g_2^n = 2 \dots, g_k^n = e \iff \quad |g_1| \big| n, |g_2| \big| n, \dots |g_k| \big| n \\ \iff & \quad \operatorname{lcm}(|g_1|, |g_2|, \dots, |g_k|) \big| n \end{aligned}$$

Thus (a) holds.

(b) $\exp G = \operatorname{lcm}(\{|g| \big| g \in G\}) = \operatorname{lcm}(\{\operatorname{lcm}(|g_1|, |g_2|, \dots, |g_k|) \mid g_1 \in g_1 \in G_1, \dots g_k \in G_k\}) = \operatorname{lcm}(\operatorname{lcm}(\{|g_1| \big| g_1 \in G_1\}), \dots, \operatorname{lcm}(\{|g_1| \big| g_1 \in G_1, \dots, \})) = \operatorname{lcm}(\exp(G_1), \exp(G_2), \dots, \exp(G_k))$ □

Lemma 7.3.20. [**cyclic**] *Let A and B be finite groups. Then $A \times B$ is cyclic if and only if $|A|$ is cyclic, $|B|$ is cyclic and* $\gcd(|A|, |B|) = 1$.

Proof. By 7.3.18 G if cyclic if and only of $\exp(G) = |G|$. Also

$$\exp(A \times B) = \operatorname{lcm}(\exp A, \exp B) = \frac{\exp A \exp B}{\gcd(\exp A, \exp B)} \leq \frac{|A||B|}{1}$$

and

$$|A \times B| = |A||B|$$

Thus
$|A \times B| = \exp(A \times B)$ if and only if $|\exp A| = |A|$, $\exp B = |B|$ and $\gcd(|A|, |B|) = 1$. □

Theorem 7.3.21. [**structure of un**] *Let $n \in \mathbb{Z}^+$ and let $n = 2^{e_0} p_1^{e_1} \dots p_k^{e_k}$ where $p_1, \dots p_k$ are pairwise distinct odd primes, $e_0 \in \mathbb{N}$ and $p_1, \dots p_k \in \mathbb{Z}^+$. Then*

(a) [**a**] *If $e_0 \leq 1$, then $U_n \cong C_{p_1^{e_1}(p_1 - 1)} \times \dots \times C_{p_k^{e_k - 1}(p_k - 1)}$.*

(b) [**b**] *If* $e_0 = 2$ *then* $U_n \cong C_2 \times C_{p_1^{e_1}(p_1-1)} \times \ldots \times C_{p_k^{e_k-1}(p_k-1)}$.

(c) [**c**] *If* $e_0 \geq 3$, *then* $U_n \cong C_2 \times C_{2^{e_0-2}} \times C_{p_1^{e_1}(p_1-1)} \times \ldots \times C_{p_k^{e_k-1}(p_k-1)}$.

(d) [**d**] U_n *is cyclic if and only if* $n = 1, 2, 4, p^e$ *or* $2p^e$, *where* p *is an odd prime and* $e \in Z^+$.

Proof. By 7.1.6 and induction

$$U_n \cong U_{2^{e_0}} \times U_{p_1^{e_1}} \times \ldots U_{p_k}^{e_k}$$

By 7.3.7 $U_{p_i^{e_i}}$ is cyclic for all $1 \leq i \leq k$. Since $|U_{p_i^{e_i}}| = \phi\,(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$ we conclude and so $U_{p_i^{e_i}} \cong C_{p_i^{e_i-1}(p_i-1)}$.

Also by 7.3.15, $|U_1| = |U_2| = 1$, $U_4 \cong C_2$ and $U_{2^{e_0}} \cong C_2 \times C_{2^{e_0-2}}$ for $e_0 \geq 3$. Thus (a), (b) and (c) holds.

By 7.3.20 (and induction) U_n is cyclic if and only the factors listed in (a), (b), (c) have coprime orders. But each of the factors has even order. So U_n is cyclic if and only if U_n has at most one factor. In case (a), we conclude that U_n is cyclic if and only if $k \leq 1$ and so $n = 1$, $n = 2$, $p_1^{e_1}$ or $2p_1^{e_1}$. In case (b) U_n is cyclic if and only if $k = 0$, that is $n = 4$ and in case (c) U_n is never cyclic. $\square$

Chapter 8

Quadratic Residue

8.1 Square in Abelian Groups

Lemma 8.1.1. [**basic hom**] *Let $\alpha : G \to H$ be a homomorphism of groups and a. Then*

(a) [**a**] $\alpha(e) = e$.

(b) [**b**] $\alpha(a^{-1}) = \alpha(a)^{-1}$

Proof. (a) $\alpha(e) = \alpha(ee) = \alpha(e)\alpha(e)$ and multiplying with $\alpha(e)^{-1}$ gives $\alpha(e) = e$. (b) $\alpha(a)\alpha(a^{-1}) = \alpha(aa^{-1}) = \alpha(e) = e$ and so $\alpha(a^{-1}) = \alpha(a)^{-1}$. b □

Lemma 8.1.2. [**ker and img**] *Let $\alpha : G \to H$ be a homomorphism. Put* $\ker\alpha = \{g \in G \mid \alpha(g) = e\}$ *and* $\operatorname{Im}\alpha = \{\alpha(g) \mid g \in G\}$. *Then* $\ker\alpha$ *is a subgroup of G and* $\operatorname{Im}\alpha$ *is a subgroups of H.*

Proof. Since $\alpha(e) = e$, $e \in \ker\alpha$. Let $a, b \in \ker\alpha$. Then $\alpha(ab) = \alpha(a)\alpha(b) = ee = e$ and $\alpha(a^{-1}) = \alpha(a)^{-1} = e^{-1} = e$. Hence $ab \in \ker\alpha$ and $a^{-1} \in \ker\alpha$. So $\ker\alpha$ is a subgroup of G.

Since $\alpha(e) = e$, $e \in \operatorname{Im}\alpha$. Let $s, t \in \operatorname{Im}\alpha$. Then $s = \alpha(a)$ and $t = \alpha(b)$ for some $a, b \in G$. Thus $st = \alpha(a)\alpha(b) = \alpha(ab)$ and $s^{-1} = \alpha(a)^{-1} = \alpha(a)^{-1}$. Hence st and s^{-1} are in $\operatorname{Im}\alpha$ and so $\operatorname{Im}\alpha$ is a subgroup of G. □

Lemma 8.1.3. [**coset and hom**] *Let $\alpha : G \to H$ be a homomorphism of groups and $h \in H$.*

(a) [**a**] *If $\alpha(x) = h$ has a solution in G, then the solutions form a coset of* $\ker\alpha$ *in G.*

(b) [**b**] *If $h \in \operatorname{Im}\alpha$, then $\alpha(x) = h$ has $|\ker\alpha|$ solutions. If $h \notin \operatorname{Im}\alpha$, then $\alpha(x) = h$ has no solutions.*

(c) [**c**] $|H| = |\ker\alpha||\operatorname{Im}\alpha|$.

Proof. (a) Let a be a fixed solution of $\alpha(x) = h$ and let $b \in G$. Then

$$\begin{aligned} & \alpha(b) = h \\ \iff & \alpha(b) = \alpha(a) \\ \iff & \alpha(b)\alpha(a)^{-1} = e \\ \iff & \alpha(ba^{-1}) = e \\ \iff & ba^{-1} = \ker\alpha \\ \iff & b \in (\ker\alpha)\, a \end{aligned}$$

So the set of solutions of $\alpha(x) = h$ is the coset $(\ker \alpha)\, a$.

(b) Since $|\,(\ker \alpha)\, a| = |\ker \alpha|$, (b) follows from (a).

(c) Each $a \in G$ is the solution of exactly one of the equations $\alpha(x) = h$, $h \in \operatorname{Im} \alpha$. (namely the equation $\alpha(x) = \alpha(a)$). By (b) each of whose equations has exactly $|\ker \alpha|$ solutions. Hence $|G| = |\ker \alpha| \cdot |\operatorname{Im} \alpha|$. $\square$

Definition 8.1.4. [**def:i and q**] *Let A be an abelian group. Then $Q(A) := \{a^2 \mid a \in A\}$ and $T(A) := \{a \in A \mid a^2 = e\}$.*

Lemma 8.1.5. [**qi=g**] *Let A be a finite abelian group and $b \in A$. Define $\alpha : A \to A, a \to a^2$. Then*

(a) [**z**] *α is a homomorphism.*

(b) [**a**] *$Q(A) = \ker \alpha$ and $T(A) = \operatorname{Im} \alpha$. In particular, $Q(A)$ and $T(A)$ are subgroups of G.*

(c) [**b**] *$x^2 = b$ has a solution in A if and only if $b \in Q(A)$.*

(d) [**c**] *If $b \in Q(A)$, then the solutions of $x^2 = b$ in A form a coset of $T(A)$ in A.*

(e) [**d**] *The numbers of solutions of $x^2 = b$ is either 0 or $|T(A)|$.*

(f) [**e**] *$|A| = |Q(A)| \cdot |T(A)|$.*

Proof. (a) $\alpha(ab) = (ab)^2 = a^2 b^2 = \alpha(a)\alpha(b)$. (b) $a \in \ker \alpha$ iff $\alpha(a) = e$ iff $a^2 = e$ iff $a \in T(A)$.

$a \in \operatorname{Im} \alpha$ iff $a = \alpha(b)$ for some $b \in A$, iff $a = b^2$ for some $b \in A$ iff $a \in Q(A)$.

(c) Follows from the definition of $Q(A)$.

(d),(e) and (f) now follow from 8.1.3 applied to the homomorphism $\alpha : a \to a^2$. $\square$

Lemma 8.1.6. [**q of cyclic**] *Let A be a cyclic group of finite order n generated g.*

(a) [**a**] *Suppose that n is even. Let $a \in A$ and $i \in Z$ with $a = g^i$. Then following are equivalent*

1. [**a**] *i is even.*
2. [**b**] *$a \in \langle g^2 \rangle$.*
3. [**c**] *$a \in Q(A)$.*
4. [**d**] *$a^{\frac{n}{2}} = 1$*

(b) [**b**] *$Q(A) = \langle g^2 \rangle = \{a \in A \mid a^{\frac{n}{2}} = e\}$ is cyclic of order $\frac{n}{2}$ and $T(A) = \langle g^{\frac{n}{2}} \rangle$ is cyclic of order 2.*

(c) [**c**] *Suppose n is odd. Then $Q(A) = A$ and $T(A) = \{e\}$.*

Proof. (a) Suppose i is even. Then $a = g^i = (g^2)^{\frac{i}{2}} \in \langle g^2 \rangle$.

Suppose $a \in \langle g^2 \rangle$. Then $a = (g^2)^j$ for some $j \in \mathbb{Z}$ and so $a = (g^j)^2 \in Q(A)$.

Suppose $a \in Q(A))$. Then $a = b^2$ for some $b \in A$ and so $a^{\frac{n}{2}} = b^{2\frac{n}{2}} = b^n \in e$ Since $|b|\big||A| = n$.

Suppose $a^{\frac{n}{2}} = e$. Then $g^{i\frac{n}{2}} = (g^i)^{\frac{n}{2}} = a^{\frac{n}{2}} = e$ and so $n \mid i\frac{n}{2}$. Thus $2 \mid i$ and i is even.

(b) By (a) $Q(A) = \langle g^2 \rangle = \{a \in A \mid a^{\frac{n}{2}} = e\}$. Since g^2 has order $\frac{n}{\gcd(2,n)} = \frac{n}{2}$, $Q(A)$ is cyclic of order $\frac{n}{2}$. Thus $T(A)$ has order $\frac{|A|}{Q(A)} = \frac{n}{\frac{n}{2}} = 2$. Also $g^{\frac{n}{2}}$ has order $\frac{n}{\frac{n}{2}} = 2$ and so $T(A) = \langle g^{\frac{n}{2}} \rangle$.

(c) Let $a \in T(A)$. Then $a^2 = e$ and so $|a|\big|2$. Also $|a| \mid n$ and so $|a|$ is odd. Thus $|a| = 1$ and $a = e$. So $T(A) = \{e\}$, $|Q(A)| = \frac{|A|}{T(A)} = |A|$ and $Q(A) = A$. $\square$

Lemma 8.1.7. [**q and t for direct products**] *Let $A_1, A_2, \ldots A_k$ be abelian groups and $A = A_1 \times A_2 \times \ldots A_k$. Then* *(a)* [**a**] $Q(A) = Q(A_1) \times Q(A_2) \times \ldots Q(A_k)$

(b) [**b**] $T(A) = T(A_1) \times T(A_2) \times \ldots T(A_k)$

Proof. (a)

$$\begin{aligned} Q(A) &= \{(a_1, a_2, \ldots, a_k)^2 \mid (a_1, a_2, \ldots a_k) \in A_1 \times \ldots A_l\} \\ &= \{a_1^2, a_2^2, , \ldots a_k^2) \mid a_1 \in A_1, \ldots a_k \in A_k\} \\ &= \{b_1, b_2, \ldots, b_k) \mid b_1 \in Q(A_1), b_2 \in Q(A_2), \ldots b_k \in Q(A_k)\} \\ &= Q(A_1) \times Q(A_2) \times \ldots \times Q(A_k) \end{aligned}$$

(b)

$$\begin{aligned} T(A) &= \{(a_1, a_2, \ldots, a_l) \in A_1 \times \ldots \times A_k \mid (a_1, a_2, \ldots a_k)^2 = (e, e, \ldots, e)\} \\ &= \{a_1, a_2, \ldots, a_l) \in A_1 \times \ldots \times A_k \mid a_1^2 = e, a_2^2 = e, \ldots, a_k^2 = e\} \\ &= \{(a_1, a_2, \ldots, a_k) \mid a_1 \in T(A_1), \alpha_2 \in T(A_2), \ldots, a_k \in T(A_k)\} \\ &= T(A_1) \times T(A_2) \times \ldots \times T(A_k) \end{aligned}$$

□

Definition 8.1.8. [**def:gn**] *If G is a group and $n \in \mathbb{Z}^+$, then* $G^n = \underbrace{G \times G \times \ldots G}_{n-times}$

Lemma 8.1.9. [**tun**] *Let n be a positive integer and write $n = 2^{e_0} p_1^{e_1} \ldots p_k^{e_k}$ where $2, p_1, \ldots, p_k$ are positive integers and $e_0 \in \mathbb{N}$ and $e_1, \ldots e_k \in \mathbb{Z}^+$. Put*

$$m = \begin{cases} k & \text{if } e_0 \leq 1 \\ k+1 & \text{if } e_0 = 2 \\ k+2 & \text{if } e_0 \geq 3 \end{cases}$$

Then $T(U_n) \cong C_2^m$

Proof. By 7.3.21 $U_n \cong A_1 \times \ldots A_m$, where each A_i is a cyclic group of even order. Thus $T(A_i) \cong C_2$ by 8.1.6 and hence

$$T(U_n) \cong T(A_1) \times \ldots T(A_m) \cong C_2^m$$

□

So $x^2 \equiv 1 \pmod n$ has 2^m solutions. How to find these solutions:

Case 1: $n = p^e$, p an odd prime, $e \in \mathbb{Z}^+$. Then $|T(U_n)| = 2$ and there are two solutions. Namely $x \equiv \pm 1 \pmod{p^e}$

Case 2: $n = 2^e, e \in \mathbb{Z}^+$.

If $e = 1$, one solution: $x \equiv 1 \pmod 2$
If $e = 2$, two solutions: $x \equiv \pm 1 \pmod 4$.
If $e \geq 3$, four solutions: $x \equiv \pm 1, \pm(1 + 2^{e-1}) \pmod{2^e}$

Case 3 The general case, $n = 2^{e_0} p_1^{e_1} \dots p_k^{e_k}$

For each $0 \leq i \leq k$, use the previous two cases to compute find all the solutions of $x^2 \equiv 1 \pmod{p_i^{e_i}}$ Lets say $x_{i1}, \dots x_{ir_i}$ are the solutions. Then for each tuple $(s_0, \dots s_k)$ with $1 \leq s_i \leq r_i$ use the Chinese Remainder Theorem to find a solution of

$$x \equiv x_{is_i} \pmod{p_i^{e_i}}, \quad 0 \leq i \leq k$$

Example 8.1.10. [**ex:x2=1**] *Find all solutions of $x^2 \equiv 1 \pmod{20}$.*

We have $20 = 4 \cdot 5$. The solutions of $x^2 \equiv 1 \pmod 4$ or $x \equiv \pm 1 \pmod 4$ and the solutions of $x^2 \equiv 1 \pmod 5$ are $x \equiv \pm 1 \pmod 2$0. Now

$$\begin{array}{rclllrcllrcll}
x & \equiv & 1 & \pmod 4 & \text{and} & x & \equiv & 1 & \pmod 5 & \iff & x & \equiv & 1 & \pmod{20} \\
x & \equiv & 1 & \pmod 4 & \text{and} & x & \equiv & -1 & \pmod 5 & \iff & x & \equiv & 9 & \pmod{20} \\
x & \equiv & -1 & \pmod 4 & \text{and} & x & \equiv & 1 & \pmod 5 & \iff & x & \equiv & -9 & \pmod{20} \\
x & \equiv & -1 & \pmod 4 & \text{and} & x & \equiv & -1 & \pmod 5 & \iff & x & \equiv & -1 & \pmod{20}
\end{array}$$

So the solutions of $x^2 \equiv 1 \pmod{20}$ are $x \equiv \pm 1, \pm 9 \pmod{20}$.

Definition 8.1.11. [**def:lsym**] *Let a and n be integers and p a prime. Then*

(a) [**a**] $Q_n = Q(U_n) = \{[b^2]_n \mid b \in \mathbb{Z}, \gcd(b, n) = 1\}$.

(b) [**b**] $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } [a]_p = [0]_p \\ 1 & \text{if } [a]_p \in Q_p \\ -1 & \text{if } [a]_p \notin Q_p \end{cases}$

In U_{11} we have $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^3 = 9$, $(\pm 4)^2 = 16 = 5$ and $(\pm 5)^2 = 25 = 3$. So $Q_{11} = \{1, 3, 4, 5, 9\}$ and

$$\left(\frac{a}{11}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{11} \\ 1 & \text{if } a \equiv 1, 3, 4, 5, 9 \pmod{11} \\ -1 & \text{if } a \equiv 2, 6, 7, 8, 10 \pmod{11} \end{cases}$$

Lemma 8.1.12. [**lsym and primitive**] *Let g be an odd prime, g a primitive element modulo p and $i \in \mathbb{N}$. Then*

$$\left(\frac{g^i}{p}\right) = (-1)^i$$

Proof. By 8.1.6 $[g^i]_p \in Q_p$ if and only if i is even and so if and only of $(-1)^i = 1$. $\square$

Lemma 8.1.13. [**lsym mult**] *Let p be an odd prime and $a, b \in \mathbb{Z}$. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. Suppose that $p \mid a$ or $p \mid b$. Then also $p \mid ab$ and both sides of equation in question are equal to 0.

Suppose $p \nmid a$ and $p \nmid b$ and let g be a primitive element modulo p. The there exists $i, j \in \mathbb{Z}$ with $a \equiv g^i$ and $b \equiv g^j$ modulo p. Hence $ab \equiv g^i g^j \equiv g^{i+j}$ and so by 8.1.12

$$\left(\frac{ab}{p}\right) = \left(\frac{g^{i+j}}{p}\right) = (-1)^{i+j} = (-1)^i(-1)^j = \left(\frac{g^i}{p}\right)\left(\frac{g^j}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Theorem 8.1.14. [**ap**] *Let p be an odd prime p and a an integer. Then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Proof. If $p \mid a$, then both side of the equation are equal to 0. So suppose $p \nmid a$. Then $[a]_p \in U_p$, $[a]_p = g^i$ for some primitive element $g \in U_p$ and some $i \in \mathbb{Z}$ and $\left(\frac{a}{p}\right) = (-1)^i$. Put $h = g^{\frac{p-1}{2}}$. Then h has order 2 and so $h = [-1]_p$. Thus

$$[a^{\frac{p-1}{2}}]_p = (g^i)^{\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^i = h^i = [(-1)^i]_p = [\left(\frac{a}{p}\right)]_p$$

□

Corollary 8.1.15. [**-1 in qp**] *Let p be an odd prime, Then $[-1]_p \in Q_p$ if and only if $p \equiv 1 \pmod{4}$.*

Proof. We have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

So $[-1] \in Q_p$ if and only if $\frac{p-1}{2}$ is even and if and only if $p \equiv 1 \pmod{4}$. □

Corollary 8.1.16. [**1 mod 4**] *There are infinitely many primes p with $p \equiv 1 \pmod{4}$.*

Proof. Let $p_1, \dots p_n$ be a primes with $p_i \equiv 1 \pmod{4}$. Define $m = (2p_1p_2 \dots p_k)^2 + 1$. Since m is odd, m is divisible by an odd prime p. Since $m \equiv 0 \pmod{p}$ and $m \equiv 1 \pmod{p}_i$, $p \neq P - i$ for all $1 \leq i \leq n$. Also $m \equiv 0 \pmod{p}$ implies

$$2(p_1 \dots p_k)^2 \equiv -1 \pmod{p}$$

and so $[-1]_p \in Q_p$. Thus 8.1.15 gives $p \equiv 1 \pmod{4}$ and so we found another prime congruent to 1 module 4. □

Definition 8.1.17. [**def:ah**] *Let G be a group, $a \in G$ and $H \subseteq G$. Then $aH = \{ah \mid h \in H\}$.*

Lemma 8.1.18 (Gauss)**.** [**ap via p**] *Let p be an odd prime and $P = \{1, 2, \dots, \frac{p-1}{2}\}$. For $x \in \mathbb{Z}$ and $X \subseteq \mathbb{Z}$ put $\overline{x} = [x]_p$ and $\overline{X} = \{[x]_p \mid x \in X\}$. Let $a \in \mathbb{Z}$ with $p \nmid p$ and put $\mu = |\overline{a}\overline{P} \cap \overline{-P}|$. Then*

$$\left(\frac{a}{p}\right) = (-1)^\mu$$

Proof. In this proof, we will just write m for $[m]_p$. Note that $-P = \{-1, -2, \ldots, -\frac{p-1}{2}\} = \{p-1, p-2, \ldots \frac{p-1}{2}\}$ and so $P \cap -P = \emptyset$ and $U_p = P \cup -P$. Put $H = \langle \pm 1 \rangle = \langle -1 \rangle \leq H$. Let $u, v \in aP$ with $uH = vH$. The $u = \pm v$ and $u = ax$ and $v = ay$ for some $x, y \in P$. Thus $ax = \pm ay$ and so $x = \pm y$. Since $P \cap -P = \emptyset$ this gives $x = y$ and so also $ax = ay$. Thus is $u = v$ and so the map $\phi_a : aP \to U_p/H, u \to uH$ is 1-1. Since $|aP| = |P| = \frac{p-1}{2} = \frac{|U_p|}{2} = |U_p/H|$. ϕ_a is a bijection. Hence also ϕ_1 is a bijection and for each $u \in aP$ there exist a unique $i \in P$ with $uH = iH$. Thus $u = \epsilon_i i$ for a unique $i \in P$ and $\epsilon_i \in H = \{\pm i\}$. Thus $aP = \{\epsilon_i i \mid\in P\}$.

We now compute $\prod_{u \in aP} u$ in two different ways:

$$\prod_{u \in aP} u = \prod_{i \in P} ai = a^{\frac{p-1}{2}} \prod_{i \in P} i$$

and

$$\prod_{u \in aP} u = \prod_{i \in P} \epsilon_i i = \prod_{i \in P} \epsilon_i \prod_{i \in P} i$$

Thus

$$a^{\frac{p-1}{2}} = \prod_{i \in P} \epsilon_i = (-1)^{|\{i \in P | \epsilon_i = -1\}|}$$

Observe that $\epsilon_i = -1$ if and only if $\epsilon_i i \in -P$ and so

$$|\{i \in P \mid \epsilon_i = -1\}| = |\{i \in P \mid \epsilon_i i \in -P\}| = |\{u \in aP \mid u \in -P\}| = |aP \cap -P| = \mu$$

So

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^\mu$$

$\square$

Corollary 8.1.19. [**2p**] *Let p be an odd prime. Then $[2]_p \in Q_p$ if and only if $p \equiv \pm 1 \pmod 8$.*

Proof. We apply Gauss' Lemma with $a = 2$. Note that $[2]_p \in Q_p$ if and only if μ is even.

Let $1 \leq i \leq \frac{p-1}{2}$., then $2 \leq 2i \leq p - 1$ and so

$$\begin{array}{cc} & [2i]_p \in P \\ \iff & 2i \leq \frac{p-1}{2} \\ \iff & i \leq \frac{p-1}{4} \\ \iff & i \leq \left\lfloor \frac{p-1}{4} \right\rfloor \end{array}$$

hence

$$\mu | [2P \cap -P| = |2P \setminus (2P \cap P)| = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$$

If $p \equiv 1 \pmod 4$, then $\frac{p-1}{4}$ is an integer and so $\mu = \frac{p-1}{4}$. Then μ is even if and only if $2 \mid \frac{p-1}{4}$ and so iff $8 \mid p - 1$ and iff $p \equiv 1 \pmod 8$.

If $p \equiv 3 \pmod 4$, then $\left\lfloor \frac{p-1}{4} \right\rfloor = \frac{p-3}{4}$ and $\mu = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$. So μ is even if and only if $8 | p+1$ and iff $p \equiv -1 \pmod 8$. $\square$

Theorem 8.1.20. [**quad rep**] *Let p and q be odd primes. Then*

(a) [**a**]

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

(b) [**b**] *If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.*

(c) [**c**] *If $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.*

Proof. Put $P = \{1, 2 \ldots, \frac{p-1}{2}\}$ and $Q = \{1, 2 \ldots \frac{q-1}{2}\}$. By Gauss' Lemma

$$\left(\frac{q}{p}\right) = (-1)^{\mu}, \text{ where } \mu = |\overline{q}\overline{P} \cap \overline{-P}|$$

For $x \in P$,

$$\begin{array}{lcl}
 & [qx]_p \in \overline{-P} & \\
\iff & [qx]_p = [z]_p & \text{for some } z \in -P \\
\iff & qx = z + py & \text{for some } z \in -P \text{ and } y \in \mathbb{Z} \\
\iff & qx - py \in -P & \text{for some } y \in \mathbb{Z} \\
\iff & -\frac{p-1}{2} \leq qx - py < 0 & \text{for some } y \in \mathbb{Z}
\end{array}$$

Observe that y is uniquely determined by x. We will show that any such y is in Q. Indeed

$$\frac{p-1}{2} \leq qx - py < 0$$

implies

$$\frac{p-1}{2} \geq py - qx > 0$$

and

$$qx + \frac{p-1}{2} > py > 0$$

Since $x \leq \frac{p-1}{2}$,

$$0 < y < \frac{qx + \frac{p-1}{2}}{p} \leq \frac{q\frac{p-1}{2} + \frac{p-1}{2}}{p} = \frac{q+1}{2}\frac{p-1}{p} < \frac{q+1}{2}$$

Since y is an integer and q is odd, this gives $1 \leq y \leq \frac{q-1}{2}$ and so $y \in Q$. Also since $qx - py$ is an integer, $-\frac{p-1}{2} \leq qx - py$ if and only if $-\frac{p}{2} \leq qx - py$. So

$$\mu = |\{(x, y) \in P \times Q \mid -\frac{p}{2} < qx - py < 0\}|$$

Similarly

$$\left(\frac{p}{q}\right) = (-1)^\nu \text{ where } \nu = |\{(y,x) \in Q \times P \mid -\frac{q}{2} < py - qx < 0\}|$$

Note that

$$\nu = |\{(x,y) \in P \times Q \mid 0 < qx - py < \frac{q}{2}\}|$$

Hence

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^\mu(-1)^\nu = (-1)^{\mu+\nu} = (-1)^t$$

where

$$t = \mu + \nu = |\{(x,y) \in P \times Q \mid -\frac{p}{2} < qx - py < 0 \text{ or } 0 < qx - py < \frac{q}{2}\}|$$

Since q and p are coprime, $qx = py$ implies $q \mid y$ and so $qx - py \neq 0$ for all $(x,y) \in P \times Q$. Thus

$$t = |\{(x,y) \in P \times Q \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}|$$

Define

$$I = \{(x,y) \in P \times Q \mid -\frac{p}{2} \geq qx - py\}$$

and

$$J = \{(x,y) \in P \times Q \mid qx - py \geq \frac{q}{2}\}$$

Then

$$t = |P \times Q| - |I| - |J|$$

We will show that $|I| = |J|$. Define

$$\rho : \mathbb{R} \times \mathbb{R} : (x,y) \to (x', y')$$

where

$$(x', y') = (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$$

Note that x and y are integers if and only of x' and y' are integers.
Also

$$\begin{aligned} & 1 \leq x' \leq \tfrac{p-1}{2} \\ \iff \quad & 1 \leq \tfrac{p+1}{2} - x \leq \tfrac{p-1}{2} \\ \iff \quad & -\tfrac{p-1}{2} \leq -x \leq -1 \\ \iff \quad & 1 \leq x \leq \tfrac{p-1}{2} \end{aligned}$$

and

$$\begin{array}{rc} & 1 \leq y' \leq \frac{q-1}{2} \\ \iff & 1 \leq \frac{q+1}{2} - y \leq \frac{q-1}{2} \\ \iff & -\frac{q-1}{2} \leq -y \leq -1 \\ \iff & 1 \leq y \leq \frac{q-1}{2} \end{array}$$

Thus $\rho(P \times Q) = P \times Q$

$$\begin{array}{rc} & qx' - py' \geq \frac{q}{2} \\ \iff & q(\frac{p+1}{2} - x) - p(\frac{q+1}{2} - y) \geq \frac{q}{2} \\ \iff & \frac{qp}{2} + \frac{q}{2} - qx - \frac{pq}{2} - \frac{p}{2} - py \geq \frac{q}{2} \\ \iff & -\frac{p}{q} \geq qx + py \end{array}$$

Hence $(x, y) \in I$ if and only if $(x', y') \in J$. So $\rho(I) = J$ and $|I| = |J|$.
Thus

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t = (-1)^{|P \times Q| - |I| - |J|} = (-1)^{\frac{(p-1)(q-1)}{4} - 2|I|} = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Hence (a) holds. Note that $\frac{(p-1)(q-1)}{4} = \frac{p-1}{2}\frac{q-1}{2}$ and both $\frac{p-1}{2}\frac{q-1}{2}$. So $\frac{(p-1)(q-1)}{4}$ is odd, if and only if both $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd and so if and only if both p and q are congruent to $3 \pmod 4$. Thus (b) and (c) hold. □

Lemma 8.1.21. [**qpe**] *Let p be an odd prime, $e \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Then $[a]_{p^e} \in Q_{p^e}$ if and if $[a]_p \in Q_p$ and if and only of $\left(\frac{a}{p}\right) = 1$.*

Proof. We may assume that $p \nmid a$, since otherwise none of the three statement holds. Let g be a primitive root modulo p^e. Then there exists $i \in \mathbb{Z}^+$ with $a \equiv g^i \pmod{p^e}$. Then also $a \equiv g^i \pmod p$. In particular, g is a primitive root modulo p. Hence applying 8.1.6(a) twice, we see that $[a]_{p^e} \in Q_{p^e}$ if and only if i is even and if and only if $[a]_p \in Q_p$. By definition, the latter is equivalent to $\left(\frac{a}{p}\right) = 1$. □

Lemma 8.1.22. [**q2e**] *Let $e \in \mathbb{N}$ and $a \in \mathbb{Z}$.*

(a) [**a**] $Q_{2^e} = \langle [25]_{p^e} \rangle$

(b) [**b**] $[a]_2 \in Q_2$ *if and only of* $a \equiv 1 \pmod 2$

(c) [**c**] $[a]_4 \in Q_4$ *if and only of* $a \equiv 1 \pmod 4$.

(d) [**d**] *If $e \geq 3$, then* $[a]_{2^e} \in Q_{2^e} \equiv a \equiv 1 \pmod 8$

(e) [**e**] *Put $f = \min\{e, 3\}$. Then* $[a]_{2^e} \in Q_{2^e} \equiv a \equiv 1 \pmod 2)^f$

Proof. By the proof of 7.3.15, $U_{2^e} = \{[\pm 5^i]_{2^e} \mid i \in \mathbb{N}\}$ and so $Q_{2_e} = \{[\pm 5^i]^2 \mid i \in \mathbb{N}\} = \langle [25]_{2^e} \rangle$.
Hence (a) holds. (b) and (c) are obvious.

Suppose $[a]_{2^e} \in Q_{2^e}$. Then by (a) $a \equiv 1 \pmod 8$. So suppose that $a \equiv 1 \pmod 8$, then $a \equiv \epsilon 5^i \pmod{2^e}$ for some $i \in \mathbb{N}$ and $\epsilon \in \{1, -1\}$. Since $e \geq 3$, $1 \equiv a \equiv \epsilon 5^i \pmod 8$. Note that this implies $\epsilon = 1$ and i is even. So $a \equiv (5^{\frac{i}{2}})^2 \pmod{2^e}$ and $[a]_{2^e} \in Q_{2^e}$. Thus (d) holds.

(e) follows from (b)-(d). □

Lemma 8.1.23. [**qn**] *Let $n_1, \dots, n_k$ be pairwise coprime positive integers, $n = n_1 n_2 \dots n_k$ and $a \in \mathbb{Z}$. Then*

$$[a]_n \in Q_n \text{ if and only if } [a]_{n_i} \in Q_{n_i} \text{ for all } 1 \le i \le k$$

Proof. This follows from the isomorphism

$$U_n \to U_{n_1} \times U_{n_2} \times \dots \times U_{n_k}$$
$$[a]_n \to ([a]_{n_1}, \dots, [a]_{n_k})$$

and from

$$Q(U_{n_1} \times U_{n_2} \times \dots \times U_{n_k}) = Q_{n_1} \times Q_{n_2} \times \dots \times Q_{n_k}$$

□

Lemma 8.1.24. [**char a in qp**] *Let $a \in \mathbb{Z}$, $n = 2^{e_0} p_1^{e_1} \dots p_k^{e_k}$ where $2, p_1, \dots p_k$ are pairwise distinct primes, $e_0 \in \mathbb{N}$, and $e_i \in \mathbb{Z}^+$ for $1 \le i \le k$. Put $e = \min(e_0, 3)$. Then $[a]_n \in Q_n$, if and only if $a \equiv 1 \mod 2^e$ and $\left(\frac{a}{p_i}\right) = 1$ for all $1 \le i \le k$.*

Proof. By 8.1.23, $[a]_n \in Q_n$ iff $[a]_{p_i^{e_i}} \in Q_{p_i^{e_i}}$ for all $0 \le i \le k$. By 8.1.22, $[a]_{2^{e_0}} \in Q_{2^{e_0}}$ if and only if $a \equiv 1 \pmod{2^e}$ and by 8.1.21, $[a]_{p_e^{e_i}} \in Q_{p_i^{e_i}}$ if and only if $\left(\frac{a}{p_i}\right) = 1$. □

Example 8.1.25. [**ex: a in qp**] *Is $[73]_{180} \in Q_{180}$?*

$180 = 2^2 \cdot 3^2 \cdot 5$. $73 \equiv 1 \pmod 4$, $\left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = -1$ and $\left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$. So 73 is not a square modulo 180.

Chapter 9

Arithmetic Functions

9.1 Dirichlet Products

Definition 9.1.1. [**def:arith**] *An arithmetic function is a function $f : \mathbb{Z}^+ \to \mathbb{C}$.*

Example 9.1.2. [**ex:arith**]

1. [**1**] $\phi : \mathbb{Z}^+ \to \mathbb{C}, n \to |U_n|$, *the Euler function.*
2. [**2**] $\tau : \mathbb{Z}^+ \to \mathbb{C}, n \to \sum_{d|n} 1$, *the number divisors of* n.
3. [**3**] $\sigma : \mathbb{Z}^+ \to \mathbb{C}, n \to \sum_{d|n} d$, *the sum of the divisors of* n.
4. [**4**] $u : \mathbb{Z}^+ \to \mathbb{C}, n \to 1$, *the unit function.*
5. [**5**] $N : \mathbb{Z}^+ \to \mathbb{C}, n \to n$, *the identity function.*
6. [**6**] $I : \mathbb{Z}^+ \to \mathbb{C}$, $I(1) = 1$ *and* $I(n) = 0$ *if* $n \geq 1$.

Definition 9.1.3. [**def:mult**] *An function f is called multiplicative if its is arithmetic and $f(nm) = f(n)f(m)$ for all $n, m \in \mathbb{Z}^+$ with* $\gcd(n, m) = 1$.

Lemma 9.1.4. [**mult**]

(a) [**a**] *u, N, ϕ and I are multiplicative.*

(b) [**b**] *If f and g are multiplicative functions, then fg is a multiplicative function.*

(c) [**c**] *If f is multiplicative function and $n \in \mathbb{N}$, then f^n is multiplicative function.*

Proof. let $n, m \in \mathbb{Z}^+$ with $\gcd(n, m) = 1$. (a): $u(nm) = 1 = 1 \cdot 1 = u(n)u(m)$
$N(nm) = nm = N(n)N(M)$
By 7.1.6 $\phi(nm) = \phi(n)\phi(m)$.
If $n = 1$ and $m = 1$, then $nm =$ and $I(nm) = 1 = I(n)I(m)$. If $n > 1$ or $m > 1$, then $nm > 1$ and one of $I(n)$ or $I(m)$ is equal to 0. So $I(nm) = 0 = I(n)I(m)$. and so (a) holds.
(b) $(fg)(nm) = f(nm)g(nm) = f(n)f(m)g(n)g(m) = f(n)g(n)f(m)g(m) = (fg)(n)(fg)(m)$
(c) If $n = 0$, then $f^0 = u$ and so f^0 is multiplicative. Suppose that f^n is multiplicative, Then $f^{n+1} = f^n f$. By the induction assumption, f^n is multiplicative and by assumption f is multiplicative. So by (b), f^{n+1} is multiplicative. □

Definition 9.1.5. [**def:dirichlet**] *Let f and g be arithmetic function. Then $f * g$ is the arithmetic function defined by*

$$(f*g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{de=n} f(d)g(e)$$

$f * g$ is call the Dirichlet product of f and g. It is also called the convolution of f and g.

Lemma 9.1.6. [**basic:dirichlet**] *Let f, g, h be arithmetic functions.*

(a) [**a**] $f * g = g * f$.

(b) [**b**] $(f * g) * h = f * (g * h)$.

(c) [**c**] $I * f = f = f * I$.

Proof. (a)

$$(f*g)(n) = \sum_{de=n} f(d)g(e) = \sum_{ed=n} g(e)f(d) = \sum_{de=n} g(d)f(e)) = (g*f)(n)$$

(b)

$$\begin{array}{rcllcl}
((f*g)*h)(n) & = & \sum_{de=n}(f*g)(d)h(e) & & = & \sum_{de=n}\left(\sum_{bc=d}(f(b)g(c))h(d)\right) \\
& = & \sum_{de=n}\sum_{bc=d}(f(b)g(c))h(e) & & = & \sum_{bce=n}(f(b)g(c))h(e) \\
& = & \sum_{bce=n} f(b)(g(c)h(e)) & & = & \sum_{ba=n}\sum_{ce=a} f(b)(g(c)h(e)) \\
& = & \sum_{ba=n} f(b)\left(\sum_{ce=a} g(c)h(e)\right) & & = & \sum_{ba=n} f(b)(g*h)(a) \\
& = & (f*(g*h))(n) & & &
\end{array}$$

(c) $(I * f)(n) = \sum_{d|n} I(d)f\left(\frac{n}{d}\right) = I(1)f(\frac{n}{1}) = f(n)$. So $I * f = f$. By (a) $f * I = I * f$ and so also $f * I = f$. ☐

Lemma 9.1.7. [**identities**] *Let f be an arithmetic function.*

(a) [**d**] $(f * u)(n) = \sum_d f(d)$.

(b) [**e**] $u * u = \tau$.

(c) [**f**] $N * u = \sigma$.

(d) [**g**] $\phi * u = N$.

Proof. (a) $(f * u)(n) = \sum_{d|n} f(d)u(\frac{n}{d}) = \sum_d f(d)$.
(b): $u * u(n) = \sum_{d|n} u(n) = \sum_{d|n} 1 = \tau(n)$
(c): $(N * u)(n) \sum_{d|n} N(d) = \sum_{d|n} d = \sigma(n)$.
(d) By 7.3.3, $\sum_{d|n} \phi(d) = n$ and so by (a), $\phi * u = N$. ☐

Lemma 9.1.8. [**easy mult**] *Suppose that f is a multplicative function. Then either $f = 0$ or $f(1) = 1$.*

Proof. Suppose $f \neq 0$. Then $f(n) \neq 0$ for some $n \in \mathbb{Z}^+$. Thus $f(n) = f(n1) = f(n)f(1)$ and so $f(1) = 1$. ☐

Lemma 9.1.9. [**dirichlet and mult**] *Let f and g be arithmetic function. Suppose f is non-zero and multiplictaive. Then g is multiplicative if and only if $f * g$ is multiplicative.*

Proof. We will prove the following:

1°. [**1**] *Let $n, m \in \mathbb{Z}^+$ with $\gcd(n, m) = 1$. Suppose that for all divisors a of n and b of m with $(a, b) \neq (n, m)$ we have $g(ab) = g(a)g(b)$. Then $(f * g)(nm) = (f * g)(n)(f * g)(m)$ if and only if $g(nm) = g(n)g(m)$.*

Note that any divisor x of nm can be unique written as $x = ab$ where a is a divisor of n and b is a divisor of m. So if $nm = xy$ with $x, y \in \mathbb{Z}^+$, then there exist unique $a, b, c, d \in \mathbb{Z}^+$ with $x = ab, y = cd$, $n = ac$ and $m = bd$. Moreover, $\gcd(a, b) = 1 = \gcd(c, d)$

Thus

$$\begin{aligned}
(f * g)(nm) &= \sum_{xy=nm} f(x)g(y) \\
&= \sum_{ab=x,cd=y,ac=n,bd=m} f(x)g(y) \\
&= \sum_{ac=n,bd=m} f(ab)g(cd) \\
&= f(1)g(nm) + \sum_{ac=n,bd=m,(c,d)\neq(n,m)} f(a)f(b)g(c)g(d)
\end{aligned}$$

and

$$\begin{aligned}
(f * g)(n)(f * g)(m) &= \left(\sum_{ac=n} f(a)g(c)\right)\left(\sum_{bd=m} f(b)g(d)\right) \\
&= f(1)f(1)g(n)g(m) + \sum_{ac=n,bd=m,(c,d)\neq(n,m)} f(a)g(c)f(b)g(d)
\end{aligned}$$

Since $f(1) = 1 = f(1)f(1)$ we conclude that (1°) holds.

If g is multiplicative, (1°) shows that $f * g$ is multiplicative. Suppose now that $f * g$ is multiplicative, and inductively that $g(ab) = g(a)g(b)$ for all a, b with $ab < nm$ and $\gcd(a, b) = 1$. Then (1°) shows that $g(nm) = g(n)g(m)$ and so g is multiplicative. □

Corollary 9.1.10. [**tau and sigma**] *Let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where $p_1, \dots, p_k$ are pairwise distinct primes and $e_1, \dots e_k \in \mathbb{Z}^+$.*

(a) [**a**] *τ and σ are multiplicative.*

(b) [**b**] $\tau(n) = \prod_{i=1}^k (e_i + 1)$

(c) [**c**] $\sigma(n) = \prod_{i=1}^k \left(\sum_{j=0}^{e_i} p_i^j\right) = \prod_{i=1}^k \frac{p_i^{e_i+1}-1}{p_i-1}$.

Proof. (a) Since u and N are multiplicative, so are $\tau = u * u$ and $\sigma = N * u$.

(b) and (c): In view of (a) we only need to consider the case $n = p^e$, p a prime, $e \in \mathbb{N}$. Then the divisors of p^e or $p^i, 0 \leq i \leq e$. Thus p^e has $e + 1$ divisors and $\sigma(p^e) = \sum_{i=0}^e p^i = \frac{p^{i+1}-1}{p-1}$. □

9.2 Perfect Numbers

Definition 9.2.1. [**def:perfect**] *A positive integer n is called* perfect *if $n = \sum_{d|n, d\neq n} d$.*

Observe that $n \in \mathbb{Z}^+$ is perfect if and only of $n = \sigma(n) - n$, that is $\sigma(n) = 2n$.

Example 9.2.2. [**small perfect**] *The first three perfect numbers*

$\sigma(6) = \sigma(2 \cdot 3) = \frac{2^2-1}{2-1}\frac{3^2-1}{3-1} = 3 \cdot 4 = 12 = 2 \cdot 6.$
$\sigma(28) = \sigma(2^2 \cdot 7) = \frac{2^3-1}{2-1}\frac{7^2-1}{7-1} = 7 \cdot 8 = 56 = 2 \cdot 28.$
$\sigma(496) = \sigma(16 \cdot 31) = \frac{2^5-1}{2-1}\frac{31^2-1}{31-1} = \frac{3}{1} \cdot 32 = 2 \cdot 496.$

Lemma 9.2.3. [**mersenne and perfect**] *Let n be a positive even integer. Then n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ where p is a prime such that $2^p - 1$ is a prime.*

Proof. Suppose first that $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are primes. Then

$$\sigma(n) = \frac{2^p - 1}{2 - 1}\frac{(2^p - 1)^2 - 1}{(2^p - 1) + 1} = (2^p - 1)((2^p - 1) + 1) = (2^p - 1)2^p = 2n$$

and so n is perfect.

Suppose next that n is perfect.Since n is even, $n = 2^{p-1}q$ where $p, q \in \mathbb{Z}^+$ with q is odd and $p \geq 2$. Hence

$$(*) \qquad 2^p q = 2n = \sigma(2^{p-1}q) = \sigma(2^{p-1})\sigma(q) = \frac{2^p - 1}{2 - 1}\sigma(q) = (2^p - 1)\sigma(q)$$

Thus $2^{p-1} \mid q$ and so $q = 2^{p-1}r$ for some $r \in \mathbb{Z}^+$. Substitution in (*) gives

$$2^p(2^p - 1)r = (2^p - 1)\sigma(m)$$

and so

$$\sigma((2^p - 1)r) = \sigma(q) = 2^p r$$

Since $(2^p - 1)r$ and r are distinct divisors of $(2^p - 1)r$ we get that $2^p r = (2^p - 1)r + r \leq \sigma((2^p - 1)r)) = 2^p r$. Hence $(2^p - 1)r$ and r are the only divisors of $q = (2^p - 1)r$. It follows that $r = 1$ and $2^p - 1$ is a prime. By 3.3.5 also p is a prime. □

9.3 The group of non-zero multiplicative functions

Definition 9.3.1. [**def:inverse**] *Let f be an arithmetic function. We say f is Dirichlet-invertible if there exists an arithmetic function g with $f * g = I$. Such a g is called an Dirchlet-inverse of f.*

Lemma 9.3.2. [**inverses**] *Let f be an arithmetic function. Then*

(a) [**a**] *The set of Dirichlet-invertible arithmetic function together with the Dirichlet product form an abelian group.*

(b) [**b**] *If f is Dirichlet-invertible, it has a unique Dirchlet-inverse, (which we will denote by f^{-*}). f^{-*} can be computed inductively by*

$$f^{-*}(1) = \frac{1}{f(1)}$$

$$f^{-*}(n) = -\frac{1}{f(1)} \sum_{de=n, e\neq n} f(d) f^{-*}(e)$$

(c) [**c**] *f is Dirichlet-invertible if and only $f(1) \neq 0$.*

(d) [**d**] *Suppose f is multiplicative and non-zero. Then f is Dirchlet-invertible and f^{*-1} is multiplicative. In particular, the set of non-zero multiplicative functions is a subgroup of the group Dirchlet-invertible functions.*

Proof. (a) If f and g are Dirchlet invertible with inverse f' and g'. Then f is the inverse of f' and $g' * f'$ is the inverse of $f * g$. Since I is an idendity with respect to $*$, and $*$ is associative and commuative, (a) hold.

(b) This holds in any group.

(c) Suppose f is Dirchlet invertible with inverse g. Then $1 = I(1) = (f * g)(1) = f(1)g(1)$ and so $f(1) \neq 0$.

Suppose now that $f(1) \neq 0$. Define the aritmetic function g by $g(1) = \frac{1}{f(1)}$ and inductively for $n > 1$ by

$$g(n) = -\frac{1}{f(1)} \sum_{de=n, e\neq n} f(d) g(e)$$

Then $(f * g)(1) = f(1)g(1) = 1$ and for $n > 1$,

$$(f * g)(n) = \sum_{de=n} f(d)g(e) = \sum_{de=n, e\neq 1} f(d)g(e) + f(1)\left(-\frac{1}{f(1)} \sum_{de=n, e\neq n} f(d)g(e)\right) = 0$$

and so $f * g = I$.

(d) By 9.1.8, $f(1) = 1$ and so by (c), f is Dirichlet invertible. Since $f * f^{-*} = I$ and f and I are multiplicative, we conclude from 9.1.9 then f^{-*} is multiplcative. Also by 9.1.9, the set of non-zero multiplicative function is closed under '$*$' and so (d) is proved. □

Definition 9.3.3. [**def: fp**]

(a) [**a**] *Let p be a prime. Then the arithmetic function ϵ_p is define by $\epsilon_p(n) = e$, where $e \in \mathbb{N}$ with $p^e || n$.*

(b) [**b**] *Let f be a non-zero multiplicative function and p a prime. Define function $f_p : \mathbb{N} \to \mathbb{C}$ is defined by $f_p(e) = f(p^e)$.*

Note here that $f_p(0) = 1$ for all primes p.

Lemma 9.3.4. [**fp**]

(a) [**a**] *Let f be a non-zero multiplicative function. Then $f(n) = \prod_p f_p(\epsilon_p(n))$. (Note here that infinite product is defined, since $\epsilon_p(n) = 0$ for almost all primes p and so $f_p(\epsilon_p(n)) = 1$ for all all primes p.*

(b) [**b**] *Two non-zero multiplicative functions f and h are equal, if and only $f_p = h_p$ for all primes p.*

(c) [**c**] *Let $g_p : \mathbb{N} \to \mathbb{C}$, p a prime, be functions with $g_p(0) = 1$. Define the arithmetic functions f be $f(n) = \prod_p g_p(\epsilon_p(n))$. Then f is multiplicative and $g_p = f_p$.*

(d) [**d**] *Let f and h be non-zero multiplicative functions. Then $h * f = I$ if and only if*

$$(*) \qquad h_p(e) = -\sum_{k=0}^{e-1} h_p(k)f_p(e-k) = -\left(f_p(e) + h_p(1)f_p(e-1) + \ldots + h_p(e-1)f_p(1)\right)$$

for all primes p and all $e \in \mathbb{Z}^+$.

Proof. (a) -(c) are obvious.

For (d), note that $h * f = I$ if and only if $h = f^{-*}$. Since f^{-*} is multiplicative this holds if and only if $h_p(e) = (f^{-*})_p(e)$ for all primes p and all $e \in \mathbb{Z}^+$. We have

$$(f^{-*})_p(e) = f^{-*}(p^e) = -\frac{1}{f(1)} \sum_{d|p^e, d \neq p^e} f^{-*}(d) f(\frac{p^e}{p^k}) = -\sum_{k=0} f_p^{-*}(k) f_p(e-k)$$

Note that $h_p(0) = 1 = f_p^{-*}(0)$ and inductively we see that $h_p(e) = (f^{-*})_p(e)$ for all primes p and all $e \in \mathbb{Z}^+$ if and only if (*) holds. □

Example 9.3.5. [**ex:fp**] *Let $\alpha \in \mathbb{R}$. Compute $(N^\alpha)^{-*}$.*

Put $f = N^\alpha$, so $f(n) = n^\alpha$. Then $f_p(k) = p^{k\alpha}$. Let $h = (N^\alpha)^{-*}$. Then $h_p(0) = 1$.

$$h_p(1) = -\sum_{k=0}^{0} h_p(k) f_p(1-k) = -h_p(0) f_p(1) = -p^\alpha$$

$$h_p(2) = -\sum_{k=0}^{1} -h_p(k) f_p(2-k) = -(h_p(0) f_p(2) + h_p(1) f_p(1) = -(p^{2\alpha} + (-p^\alpha p^\alpha)) = 0$$

We claim that $h_p(e) = 0$ for all $e \geq 2$. For $e = 2$ we already proved this, so suppose $h_p(k) = 0$ for all $2 \leq k \leq e-1$. Then

$$h_p(e) = -\sum_{k=0}^{e-1} h_p(k) f_p(e-k) = -(h_p(0) f_p(e) + h_p(1) f_p(e-1)) = -(p^{e\alpha} + (-p^\alpha) p^{(e-1)\alpha}) = 0$$

So

$$h_p(e) = \begin{cases} 1 & \text{if } e = 0 \\ -p^\alpha & \text{if } e = 1 \\ 0 & \text{if } e \geq 2 \end{cases}$$

Let $n = p_1^{e_1} \ldots p_k^{e_k}$ where $p_1, \ldots, p_k$ are pairwise distinct primes. If $e_i \geq 2$ for some $1 \leq i \leq k$, then $h_{p_i}(e_i) = 0$ and so also $h(n) = 0$. So suppose that $e_i = 1$ for all $1 \leq i \leq k$. Then

$$h(n) = \prod_{i=1}^{k} -p_i\alpha = (-1)^k (\prod_{i=1}^{l} p_i)^\alpha = (-1)^k n^\alpha$$

Thus

$$(N^\alpha)^{-*}(n) = \begin{cases} (-1)^k n^\alpha & \text{if } n \text{ is square free and } k \text{ is the number of primes dividing } n \\ 0 & \text{if } n \text{ is not square free} \end{cases}$$

Definition 9.3.6. [**def:moebius**] $\mu := u^{-*}$. *μ is called the Möbius function.*

Lemma 9.3.7. [**moebuis**] *Let p be a prime and $n, e \in \mathbb{Z}^+$ with $n, e \geq 2$. Then*

(a) [**z**] $u * \mu = I$.

(b) [**a**] $\mu(1) = 1$.

(c) [**b**] $\sum_{d|n} \mu d = 0$ *and* $\mu(n) = -\sum_{d|n, d\neq n} \mu(d)$.

(d) [**c**] *μ is multiplicative.*

(e) [**d**] $\mu(p) = -1$ *and* $\mu(p^e) = 0$.

(f) [**e**] *If n is square free, $\mu(n) = (-1)^k$, where k is the number of prime divisors of n.*

(g) [**f**] *If n is not square free, then $\mu(n) = 0$.*

(h) [**g**] *Let $\alpha \in \mathbb{R}$. Then $(N^\alpha)^{-*} = \mu N^\alpha$.*

Proof. (a): This is just the defintion of μ.
(b) Follows from (h) and $u(1) = I(1) = 1$.
(c) Follows from (h).
(d) Since u is multiplicative, this follows from 9.3.2(d).
(e)-(g) This is the special case $\alpha = 0$ in Example 9.3.5
(h) Follows from 9.3.5, (f) and (g). □

Lemma 9.3.8. [**moebius identities**] *Let f and g be arithmetic function.*

(a) [**a**] $f * u = g$ *if and only if* $f = g * \mu$.

(b) [**b**] $u = \tau * \mu$.

(c) [**c**] $N = \sigma * \mu$.

(d) [**d**] $\phi = N * \mu$.

(e) [**e**] *If p is a prime and $e \in \mathbb{Z}^+$, then $(f * \mu)(p^e) = f(p^e) - f(p^{e-1})$.*

Proof. (a) If $f * u = g$, then $g * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f$. Similarly, if $f = g * \mu$, then $f * u = g$. By 9.1.7, $u * u = \tau$, $N * u = \sigma$ and $\phi * u = N$. Thus by (a), $u = \tau * \mu$, $N = \sigma * \mu$ and $\phi = N * u$. So (a)-(d) hold

$$(f * \mu)(p^e) = (\mu * f)(p^e) = \sum_{d|p^e} \mu(d) f(\frac{p^e}{d}) = \mu(1) f(p^e) + \mu(p) f(p^{e-1}) = f(p^e) - f(p^{e-1})$$

□

From (d) and (e) can be used to compute ϕ: $\phi(p^e) = N(p^e) - N(p^{e-1}) = p^e - p^{e-1} = p^{e-1}(p-1)$. Of course we already know this.

Chapter 10

The Riemann Zeta function and Dirichlet Series

10.1 The Riemann Zeta function

Definition 10.1.1. [**def:zeta**] $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. *$\zeta$ is called the Riemann Zeta function.*

Lemma 10.1.2. [**zeta converges**] *$\zeta(s)$ converges for all real numbers s with $s > 1$ and diverges for all real numbers s with $s \leq 1$. Moreover,* $\lim_{s\to\infty} \zeta(s) = 1$.

Proof. Suppose first that $s > 1$. We partition $\mathbb{Z}^+$ into subintervals $I_k = \{n \in \mathbb{Z} \mid 2^k \leq n < 2^{k+1}\}$. Note that $|I_k| = 2^k$

$$\zeta(s) = \sum_{n\in I_k} \frac{1}{n^s} \leq \sum_{n\in I_k} \frac{1}{(2^k)s} = \frac{2^k}{2^{ks}} = \left(\frac{1}{2^{s-1}}\right)^k$$

Since $0 < \frac{1}{2^{s-1}} < 1$, we get $\zeta(s) = \sum_{k=0}^{\infty} \sum_{n\in I_k} \frac{1}{n^s} \leq \sum_{k=0}^{\infty} \left(\frac{1}{2^{s-1}}\right)^k = \frac{1}{1-\frac{1}{2^{s-1}}}$ and so $\zeta(s)$ converges by the comparison test.

Note that $1 \leq \lim_{s\to\infty} \zeta(s) \leq \lim_{s\to\infty} \frac{1}{1-\frac{1}{2^{s-1}}} = 1$ and so $\lim_{s\to\infty} \zeta(s) = 1$.

Suppose next that $s \leq 1$. If $s \leq 0$, then $\frac{1}{n^s} = n^{-s} \geq 1$ and $\zeta(s)$ diverges. So suppose $0 < s \leq 1$. We partition $\mathbb{Z}^+$ into the subintervals, $J_k = \{n \in \mathbb{Z} \mid 2^{k-1} < n \leq 2^k\}$ and note that for $k \geq 1$, $|J_k| = 2^{k-1}$.

We have

$$\sum_{n\in J_k} \frac{1}{n^s} \geq \sum_{n\in J_k} \frac{1}{(2^k)^s} = \frac{2^{k-1}}{(2^k)^s} \geq \frac{2^{k-1}}{2^k} = \frac{1}{2}$$

Since the constant series $\frac{1}{2}$ diverges, also $\zeta(s)$ diverges. $\square$

10.2 Evaluating $\zeta(2k)$

To compute $\zeta(2k)$, where k is an integer, we will take to following formula from Analysis for granted:

$$\sin z = z\prod_{n\neq 0}\left(1-\frac{z}{n\pi}\right) = z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right)$$

Taking the natural logarithm on both sides we obtain

$$\ln\sin z = \ln z + \sum_{n=1}^{\infty}\ln\left(1-\frac{z^2}{n^2\pi^2}\right)$$

Differentiating both sides with respect to gives

$$\frac{1}{\sin z}\cos z = \frac{1}{z} + \sum_{n=1}^{\infty}\frac{1}{1-\frac{z^2}{n^2\pi^2}}\frac{-2z}{n^2\pi} = \frac{1}{z} - 2\sum_{n=1}^{\infty}\frac{z}{n^2\pi^2}\frac{1}{1-\frac{z^2}{n^2\pi^2}}$$

Use the geometric series:

$$\frac{z}{n^2\pi}\frac{1}{1-\frac{z^2}{n^2\pi^2}} = \frac{z}{n^2\pi^2}\sum_{k=0}^{\infty}\left(\frac{2^2}{n^2\pi^2}\right)^k = \sum_{k=0}^{\infty}\frac{z^{2k+1}}{n^{2k+2}\pi^{2k+2}} = \sum_{k=1}^{\infty}\frac{z^{2k-1}}{n^{2k}\pi^{2k}}$$

and so

$$(*)\qquad \cot z = \frac{1}{z} - 2\sum_{k=1}^{\infty}\frac{z^{2k-1}}{n^{2k}\pi^{2k}} = \frac{1}{z} - 2\sum_{k=1}^{\infty}\frac{\zeta(2k)}{\pi^{2k}}z^{2k-1}$$

We will now compute a second expression for $\cot z$. We start with proving that

$$(**)\qquad \cot z = -i + \frac{1}{z}\frac{-2iz}{e^{-2iz}-1}$$

where $i=\sqrt{-1}$. Canceling the z and adding i we have

$$cot z + i = \frac{-2i}{e^{-2iz}-1}$$

Multiplying with $i(e^{-2iz}-1)$

$$(i\cot z - 1)(e^{-2iz}-1) = 2$$

by Euler's Formula, $e^{ix} = \cos x + i\sin x$ and so $e^{-ix} = \cos x - i\sin x$. Thus

$$(i\cot z - 1)(\cos 2z - i\sin 2z - 1) = 2$$

and

$$i\cot z\cos 2z + \cot z\sin 2z - i\cot z - \cos 2z + i\sin 2z + 1 = 2$$

So it suffices to prove:

$$\cot z\sin 2z - \cos 2z = 1 \text{ and } (cot z\cos 2z - \cot z + \sin 2z)i = 0$$

Using that $\cot z = \frac{\cos z}{\sin z}$, $\sin 2z = 2\sin z\cos z$ and $\cos 2z = \cos^z - \sin^2 z$ these two equations transform to

$$2\frac{\cos z}{\sin z}\sin z\cos z-\cos^2 z+\sin^2 z=1 \text{ and } \frac{\cos z}{\sin z}(\cos^2 z-\sin^2 z)-\frac{\cos z}{\sin z}+2\sin z\cos z=0$$

Simplifying and multiplying the second equation with $\sin z$ gives

$$2\cos^2 z-\cos^2 z+\sin^2 z=1 \text{ and } \cos^2 z\cos z-\cos z\sin^2 z-\cos z+2\sin^2\cos z=0$$

and

$$\cos^2 z+\sin^2=1 \text{ and } (\cos^2 z+\sin^2 z)\cos z-\cos z=0$$

Since $\cos^2 z+\sin^2 z=1$, these last two equations are true and so (**) is proved.

Put $t=-2iz$. Then (**) reads

$$\cot z=-i+\frac{1}{z}\frac{t}{e^t-1}$$

Let

$$(***)\qquad \frac{t}{e^t-1}=\sum_{m=0}^{\infty}\frac{B_m}{m!}t^m$$

be the Taylor series for $\frac{t}{e^t-1}$. B_m is called the m'th Bernoulli number.

Then

$$(****)\qquad \cot z=-i+\frac{1}{z}\sum_{m=0}^{\infty}\frac{B_m}{m!}(-2iz)^m=-i+\sum_{m=0}^{\infty}\frac{(-2i)^m B_m}{m!}z^{m-1}$$

We now compare the coefficient of z^{m-1} in (*) and (****)

For $m=0$ we get $B_0=1$. For $m=1$, $-i-2B_1 i=0$ and so $B_1=-\frac{1}{2}$. For $m=2k+1>1$ we get $B_{2k+1}=0$ and for $m=2k\geq 2$,

$$-2\frac{\zeta(2k)}{\pi^{2k}}=\frac{(-2i)^{2k}B_{2k}}{2k!}$$

and so

$$\zeta(2k)=\frac{(-1)^{k-1}2^{2k-1}\pi^{2k}}{2k!}B_{2k}$$

For example,

$$\zeta(2)=\pi^2 B_2,\quad \zeta(4)=-\frac{\pi}{3}B_4, \text{ and } \zeta(6)=\frac{2\pi^6}{45}B_6.$$

It remains to obtain a formula for the B_m's. From (***) $t=(e^t-1)\sum_{m=0}^{\infty}\frac{B_m}{m!}t^m$. We have $e^t=\sum_{n=0}^{\infty}\frac{t^n}{n!}$ and so $e^t-1=\sum_{n=1}\frac{t^n}{n!}$. Thus

$$t=\left(\sum_{n=1}^{\infty}\frac{t^n}{n!}\right)\left(\sum_{m=0}^{\infty}\frac{B_m}{m!}\right)$$

The coefficient of t^r in the right hand side is

$$\sum_{m=0}^{r-1} \frac{1}{(r-m)!} \frac{1}{m!} B_m = \frac{1}{r!} \sum_{m=0}^{r-1} \binom{r}{m} B_m$$

We now compare that coefficient with the coefficient of t^r in t. For $r = 1$ we obtain $B_0 = 1$ and for $r > 1$,

$$\sum_{m=0}^{r-1} \binom{r}{m} B_m = 0$$

and so

$$B_{r-1} = -\frac{1}{r} \sum_{m=0}^{r-2} \binom{r}{m} B_m$$

For example $B_1 = -\frac{1}{2}\binom{2}{0}B_1 = -\frac{1}{2}$
$B_2 = -\frac{1}{3}\left(\binom{3}{0}B_0 + \binom{3}{1}B_1\right) = -\frac{1}{3}\left(1 - \frac{3}{2}\right) = -\frac{3}{2} \cdot -\frac{1}{2} = \frac{1}{6}$.
$B_3 = 0$,
$B_4 = -\frac{1}{5}\left(\binom{5}{0}B_0 + \binom{5}{1}B_1 + \binom{5}{2}B_2 + \binom{5}{3}B_3\right) = -\frac{1}{5}\left(1 - 5\frac{1}{2} + 10\frac{1}{6}\right) = -\frac{1}{5}\frac{6-15+10}{6} = -\frac{1}{30}$.
Thus

$$\zeta(2) = \pi^2 B_2 = \frac{\pi^2}{6} \text{and } \zeta(4) = -\frac{\pi^4}{3} \cdot -\frac{1}{30} = \frac{\pi^4}{90}$$

10.3 Probability of being Co-Prime

In this subsection we compute the probability that two randomly chosen positive integers are co-prime. More generally let p_n be the probability that $\gcd(x, y) = n$, where x and y are two random integers. Then

$$(*) \qquad \sum_{n=1}^{\infty} p_n = 1$$

Now

$$\gcd(x, y) = n \Longleftrightarrow n \mid x, n \mid y \text{ and } \gcd\left(\frac{x}{n}, \frac{y}{n}\right) = 1$$

The probability that $n \mid x$ is $\frac{1}{n}$, the probability that $n \mid y$ is $\frac{1}{n}$ and the probability that $\gcd\left(\frac{x}{n}, \frac{y}{n}\right) = 1$ is p_1. Thus

$$p_n = \frac{1}{n} \cdot \frac{1}{n} \cdot p_1 = p_1 \frac{1}{n^2}$$

Substitution into (*) gives

$$1 = \sum_{n=1}^{\infty} p_1 \frac{1}{n^2} = p_1 \sum_{n=1}^{\infty} \frac{1}{n^2} = p_1 \zeta(2)$$

and so

$$p_1 = \frac{1}{\zeta(2)} \text{ and } p_n = \frac{1}{n^2\zeta(2)}$$

Since

$$\zeta(2) = \frac{\pi^2}{6}$$

we get

$$p_1 = \frac{6}{\pi^2} \approx 0.608$$

So the probability that two randomly chosen positive integers are coprime is roughly 60%.

10.4 Dirichlet Series

Definition 10.4.1. [**def:dirchlet series**] *Let f be a arithmetic function. Then*

$$\hat{f}(s) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

is called the Dirichlet series of f.

Example 10.4.2. [**ex:dirichlet series**] *Dirichlet series for u, N and I.*

$\hat{u}(s) == \sum_{n=1}^{\infty} \frac{u(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$.
$\hat{N}(s) = \sum_{n=1}^{\infty} \frac{N(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^{s-1}} = \zeta(s-1)$.
$\hat{I}(s) = \sum_{n=1}^{\infty} \frac{I(n)}{n^s} = \frac{1}{1^1} = 1$.

Lemma 10.4.3. [**series and convolution**] *Let f and g be the arithmetic function f, g and h. If $h = f * g$, then*

$$\widehat{f * g}(s) = \hat{f}(s)\hat{g}(s)$$

for all s such that both $\hat{f}(s)$ and $\hat{g}(s)$ converge absolutely.

Proof.

$$\begin{aligned}
\hat{f}(s)\hat{g}(s) &= \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \sum_{m=1}^{\infty} \frac{g(m)}{m^s} \\
&= \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(n)g(m)}{(nm)^s} \\
&= \sum_{k=1}^{\infty} \frac{\sum_{nm=k} f(n)g(m)}{k^s} \\
&= \sum_{k=1}^{\infty} \frac{(f * g)(k)}{k^s} \\
&= \widehat{f * g}(s)
\end{aligned}$$

□

Corollary 10.4.4. [**series and inverse**] *If f is Dirichlet invertible, then $\widehat{f^{-*}} = \hat{f}^{-1} = \frac{1}{\hat{f}}$.*

Proof. From $f * f^{-*} = I$ we get $\hat{f}\widehat{f^{-*}} = \hat{I} = 1$. $\square$

Example 10.4.5. [**series for mu and phi**] *Dirichlet series for μ and ϕ:*

$\hat{\mu} = \widehat{u^{-*}} = \frac{1}{\hat{u}} = \frac{1}{\zeta}$.
$\phi * u = N$ and so $\hat{\phi}\hat{u} = \hat{N}$ and $\hat{\phi}(s)\zeta(s) = \zeta(s-1)$. Thus $\hat{\phi}(s) = \frac{\zeta(s)}{\zeta(s-1)}$.

10.5 Euler products

Definition 10.5.1. [**def:completely mult**] *An arithmetic function f is called completely multiplicative, if $f(nm) = f(n)f(m)$ for all $n, m \in \mathbb{Z}^+$.*

Theorem 10.5.2. [**euler products**] *Let f be an arithmetic function such that $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent.*

(a) [**a**] *If f is multiplicative, then*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(\sum_{i=0}^{\infty} f(p^i) \right)$$

(b) [**b**] *If f is completely multiplicative, then*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(\frac{1}{1 - f(p)} \right)$$

Proof. (a) Let $p_1 = 2$ and inductively let p_{k+1} be the smallest prime larger than p_k. Put $A_k = \{p_1^{e_1} \dots p_k^{e_k} \mid e_1, e_2, \dots, e_k \in \mathbb{N}\}$ and

$$P_k = \prod_{i=1}^{k} \left(\sum_{e_i=0}^{\infty} f(p_i^{e_i}) \right)$$

We need to show that $\lim_{k\to\infty} P_k = \sum_{n=1}^{\infty} f(n)$.
Since $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent we have

$$\begin{aligned} P(k) &= \sum_{e_1=0}^{\infty} \sum_{e_2=0}^{\infty} \dots \sum_{e_k=0}^{\infty} f(p_1^{e_1}) f((p_2^{e_2}) \dots f(p_k^{e_k}) \\ &= \sum_{e_1=0}^{\infty} \sum_{e_2=0}^{\infty} \dots \sum_{e_k=0}^{\infty} f(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) \\ &= \sum_{n \in A_k} f(n) \end{aligned}$$

Note that $n > p_k$ for all $n \in \mathbb{N} \setminus A_k$ and so

$$\left|P_k - \sum_{n=1}^{\infty} f(n)\right| = \left|\sum_{n\notin A_k} f(n)\right| \leq \sum_{n\notin A_k} |f(n)| \leq \sum_{n=p_k+1}^{\infty} |f(n)$$

Since $\sum_{n=1} f(n)$ is absolutely convergent, $\lim_{m\to\infty} \sum_{n=m}^{\infty} |f(n)| = 0$. Since $\lim_{k\to\infty} p_k = \infty$ this implies $\lim_{k\to\infty} |P_k - \sum_{n=1}^{\infty} f(n)| = 0$ and so $\lim_{k\to\infty} P_k = \sum_{n=1}^{\infty} = f(n)$.

(b) Suppose that f is completely multiplicative, then $f(p^i) = f(p)^i$ and so

$$\sum_{i=0}^{\infty} f(p^i) = \sum_{i=0}^{\infty} f(p)^i = \frac{1}{1 - f(p)}$$

Thus (b) follows from (a). $\square$

Corollary 10.5.3. [**hat and multiplicative**] *Let f be an arithmetic function and $s \in \mathbb{R}$ such that $\hat{f}(s)$ converges absolutely.*

(a) [**a**] *If f is multiplicative, then $\hat{f}(s) = \prod_p \left(\sum_{i=0}^{\infty} \frac{f(p^i)}{p^{is}}\right)$.*

(b) [**b**] *If f is absolutely multiplicative, then $\hat{f}(s) = \prod_p \frac{1}{1-\frac{f(p)}{p^s}}$.*

Proof. If f is (completely) multiplicative, then also $\frac{f(n)}{n^s}$ is (completely) multiplicative. So 10.5.3 follows from 10.5.2 applied to the arithmetic function $\frac{f(n)}{n^s}$ in place of f. $\square$

Example 10.5.4. [**euler for u and mu**] *Since u is completely multiplicative and $\hat{u} = \zeta$, we have*

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

Since μ is multiplicative and $\sum_{i=0}^{\infty} \frac{\mu(p^i)}{p^{is}} = 1 - \frac{1}{p^s}$ we have

$$\hat{\mu}(s) = \prod_p \left(1 - \frac{1}{p^s}\right)$$

Observe that these two results match, since $\zeta(s) = \frac{1}{\hat{\mu}(s)}$.

10.6 Complex Dirichlet Series

In this section we consider the Dirichlet series $\hat{f}(s)$ of an arithmetic function, where we allow s to be any complex numbers. Recall that n^s for $s \in \mathbb{C}$ and $n \in \mathbb{Z}^+$ is defined as $e^{s\ln n}$. If $s = a + ib$ with $a, b \in \mathbb{R}$, then $\operatorname{Re} s := a$.

Lemma 10.6.1. [**abscissa**] *Let f be a arithmetic function. Then there exist $\sigma_a(f) \in \mathbb{R} \cup \{-\infty, \infty\}$ such that $\hat{f}(s)$ is absolutely convergent for all $s \in \mathbb{C}$ with $\operatorname{Re} s > \sigma_a(f)$ and is absolutely divergent for all $s \in \mathbb{C}$ with $\operatorname{Re} s < \sigma_a(f)$.*

Proof. We will first show:

1°. [**1**] *Let $s, \tilde{s} \in \mathbb{C}$ with $\operatorname{Re} \tilde{s} \geq \operatorname{Re} s$. If $\hat{f}(s)$ is absolutely convergent, then also $\hat{f}(\tilde{s})$ is absolutely convergent,* For this let $s = a + ib$ and $\tilde{s} = \tilde{a} + i\tilde{b}$ with $a.b, \tilde{a}, \tilde{b} \in \mathbb{R}$. Then $\tilde{a} \geq a$. Also $|n^s| = |n^{a+ib}| = |n^a n^{ib}| = |n^a e^{ib \ln n}| = n^a$ and so

$$\left|\frac{f(n)}{n^{\tilde{s}}}\right| = \frac{|f(n)|}{|n^{\tilde{s}}|} = \frac{|f(n)|}{n^{\tilde{a}}} \leq \frac{|f(n)|}{n^a} = \left|\frac{f(n)}{n^s}\right|$$

Hence since $\sum_{n=1}^{\infty} |\frac{f(n)}{n^s}|$ is convergent also $\sum_{n=1}^{\infty} |\frac{f(n)}{n^{\tilde{s}}}|$ is convergent. Thus (1°) holds.

Let $R = \{\operatorname{Re} s \mid s \in \mathbb{C}, \hat{f}(s) \text{ is absolutely divergent }\}$.

2°. [**2**] *Let $s \in \mathbb{C}$ such that $\operatorname{Re} s$ is not an upper bound for R. Then $\hat{f}(s)$ is absolutely divergent,*

Since $\operatorname{Re} s$ is not an upper bound of R, there exists $\tilde{s} \in \mathbb{C}$ with $\operatorname{Re} s < \operatorname{Re} \tilde{s}$ and $\tilde{s}$ is absolutely divergent, If $\hat{f}(s)$ would be absolutely convergent, then (1°) would imply that also $\hat{f}(\tilde{s})$ is absolutely convergent. So (2°) holds.

If $R = \emptyset$, (that is $\hat{f}(s)$ is absolutely convergent for all $s \in \mathbb{R}$), put $\sigma_a(f) = -\infty$. Then lemma holds.

So suppose $R \neq \emptyset$. If R has no upper bound, put $\sigma_a(f) = \infty$. (2°) shows that $\hat{f}(s)$ is absolutely divergent for all $s \in \mathbb{C}$ and so the lemma hold in this case.

Suppose finally that $R \neq \emptyset$ and R has an upper bound. Then R has a least upper bound $\sigma_a(f)$. Let $s \in \mathbb{C}$ with $\operatorname{Re} s < \sigma_a(f)$. Then $\operatorname{Re} s$ is not an upper bound for R and so by (2°) $\hat{f}(s)$ is absolutely divergent. Now let $s \in \mathbb{C}$ with $\operatorname{Re} s > \sigma_a(f)$. Since $\sigma_a(f)$ is an upper bound for R, $\operatorname{Re} s \notin R$ and so $\hat{f}(s)$ is absolutely convergent. So again the Lemma holds. □

10.7 The Riemann Hypothesis

$s \in \mathbb{C}$ is called a root of ζ if $\zeta(s) = 0$. Some known facts (which we will not prove)

- All negative even integers are roots of ζ, (these roots's are called the trivial roots's of ζ.)
- If s is a non-trivial root of ζ, then $0 \leq \operatorname{Re} s \leq 1$.
- There are infinitely many roots s of ζ with $\operatorname{Re} s = \frac{1}{2}$.

Conjecture 10.7.1 (Riemann Hypothesis)**.** [**riemann hypothesis**] *If s is a non-trivial root of ζ, then $\operatorname{Re} s = \frac{1}{2}$.*

Chapter 11

Sums of square

For $k \in \mathbb{Z}^+$ define $S_k := \{x_1^2 + x_2^2 + \ldots + x_k^2 \mid x_1, x_2, \ldots x_k \in \mathbb{Z}\}$. In this chapter we determine S_2, figure out all possible ways to write an elements of S_2 as the sum of two integral square and show that $S_4 = \mathbb{N}$. So every non-negative integer can be written as the sum of squares of four integers.

11.1 Gaussian Integers and Sums of Two Squares

Definition 11.1.1. [**def:gauss**]

(a) [**a**] $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. *$\mathbb{Z}[i]$ is called the ring of Gaussian intgers.*

(b) [**c**] *For $x = a+bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$ let $\overline{x} = a-bi$ and $\delta(x) = a^2+b^2$. The map $\mathrm{cc} : \mathbb{C} \to \mathbb{C}, x \to \overline{x}$ is is called complex conjugation.*

Lemma 11.1.2. [**the elements in Z[i]**] *$\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ containing 1.*

Proof. Clearly 0 and 1 are in $\mathbb{Z}[i]$. Since $(a+bi)+(c+di) = (a+c)+(b+d)i$ and $(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i$, $\mathbb{Z}[i]$ is closed under addition and multiplication. Also $-(a+bi) = (-a)+(-b)i \in \mathbb{Z}[i]$ and so $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. □

Lemma 11.1.3. [**Properties of complex conjugation**]

(a) [**a**] *Complex conjugation is ring automorphism of $\mathbb{C}$.*

(b) [**b**] *Restricted to $\mathbb{Z}[i]$, complex conjugation is a ring automorphism of $\mathbb{Z}[i]$*

(c) [**c**] *$\delta(x) = x\overline{x}$ and $\delta(xy) = \delta(x)\delta(y)$ for all $x, y \in \mathbb{C}$.*

(d) [**d**] *Let $x \in \mathbb{C}$. Then $\delta(x) \geq 0$ with equality if and only if $x = 0$.*

(e) [**e**] *$\delta(x) \in \mathbb{N}$ for all $x \in \mathbb{Z}[i]$*

Proof. (a) Since $\overline{\overline{a+bi}} = \overline{a-bi} = a+bi$, cc is an inverse of cc and so complex conjugation is a bijection. Let $a, b, c, d \in \mathbb{R}$. Then

$$\overline{a+bi} + \overline{c+di} = (a-bi) + (c-di) = (a+c) - (b+d)i = \overline{(a+c) + (b+d)i} = \overline{(a+bi) + (c+di)}$$

and

$$\overline{a+bi}\cdot\overline{c+di} = (a-bi)\cdot(c-di) = (ac+bd)-(ac+bc)i = \overline{(ac+bd)-(ac+bc)i} = \overline{(a+bi)\cdot(c+di)}$$

So cc is a ring homomorphism. Thus (a) holds.

(b) Observe that $\overline{x} \in \mathbb{Z}[i]$ for all $x \in \mathbb{Z}[i]$. Thus the restriction of cc to $\mathbb{Z}[i]$ is its own inverse and is ring homomorphism.

(c) Let $x = a+bi$ with $a, b \in \mathbb{R}$. Then $\delta(x) = a^2+b^2 = (a+bi)(a-bi) = x\overline{x}$. Also

$$\delta(xy) = (xy)\overline{xy} = xy\overline{x}\overline{y} = (x\overline{x})(y\overline{y}) = \delta(x)\delta(y).$$

(d) Clearly $\delta(x) = a^2+b^2 \geq 0$ and $\delta(x) = 0$ if and only if $a = b = 0$ and so if and only if $x = 0$.

(e) Obvious. □

Lemma 11.1.4. [**char s2**] *$S_2 = \{\delta(z) \mid z \in \mathbb{Z}[i]\}$ and S_2 is closed under multiplication.*

Proof. $S_2 = \{a^2+b^2 \mid a, b \in \mathbb{Z}\} = \{\delta(a+bi) \mid a, b \in \mathbb{Z}\} = \{\delta(z) \mid z \in \mathbb{Z}[i]\}$. Let $n, m \in S_2$. Then $n = \delta(x)$ and $m = \delta(y)$ for some $x, y \in \mathbb{Z}[i]$. Hence $nm = \delta(x)\delta(y) = \delta(xy) \in S_2$. □

Lemma 11.1.5. [**prime in s2**] *Let p be a prime with $p \not\equiv 3 \pmod 4$. Then $p \in S_2$.*

Proof. If p is even, then $p = 2 = 1^2+1^2 \in S_2$. So suppose p is odd.

1°. [**0**] *There exists $m \in \mathbb{Z}^+$ with $1 \leq m < p$ and $mp \in S_2$.*

Since $p \not\equiv 3 \pmod 4$ an dp is odd, we have $p \equiv 1 \pmod 4$. b8.1.15 $[-1]_p \in Q_p$ and so $-1 = u^2 + mp$ for some $u, m \in \mathbb{Z}$ with $1 \leq u < p$. Hence $mp = u^2 + 1^1 \in S_2$. Since $|u| \leq (p-1)^2$ we have $u^2 + 1 < p^2$ and so $m < p$.

2°. [**1**] *Let $m \in \mathbb{Z}^+$ with $mp \in S_2$ and $m < p$. Then either $m = 1$ or there exists $s \in \mathbb{Z}$ with $1 \leq s \leq \frac{m}{2}$ and $sp \in S_2$.*

Let $mp = a_1^2 + a_2^2$ and choose $b_i \in \mathbb{Z}$ with $a_i \equiv b_i \pmod m$ and $|a_i| \leq \frac{m}{2}$. Then $b_1^2 + b_2^2 \equiv a_1^2 + a_2^2 \equiv pm \equiv 0 \pmod m$ and so $b_1^2 + b_2^2 = sm$ for some $s \in \mathbb{N}$. Note that

$$b_1^2 + b_2^2 \leq \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = \frac{m^2}{2}$$

and so $0 \leq s \leq \frac{m}{2} < m$.

Suppose first that $s = 0$, then $b_1 = b_2 = 0$ and so $a_i \equiv 0 \pmod m$. Thus m divides a_1 and a_2 and so m^2 divides $mp = a_1^2 + a_2^2$. Hence $m \mid p$. Since p is a prime and $0 < m < p$ we get $m = 1$. So (2°) holds in this case.

Suppose next that $s > 0$. Put $x = a_1 - ia_2$ and $y = b_1 + ib_2$. Then have

$$spm^2 = (mp)(sm) = ((-a_1)^2 + a_2^2)(b_1^2 + b_2^2) = \delta(x)\delta(y) = \delta(xy)$$

Since $xy = (a_1b_1 + a_2b_2) + i(a_1b_2 - a_2b_1)$, this gives

$$(*) \qquad (a_1b_1 + a_2b_2)^2 + (a_1b_2 - a_2b_1)^2 = spm^2$$

Observe that modulo m:

$$a_1b_1 + a_2b_2 \equiv a_1a_1 + a_2a_2 \equiv sm \equiv 0 \pmod m \text{ and } a_1b_2 - a_2b_1 \equiv a_1a_2 - a_2a_1 \equiv 0 \pmod m$$

So dividing (*) by m^2 we obtain

$$\left(\frac{a_1b_1 + a_2b_2}{m}\right)^2 + \left(\frac{a_1b_2 - a_2b_1}{m}\right)^2 = sp.$$

Hence $sp \in S_2$ and so again (2°) holds.

Now let $m \in \mathbb{Z}^+$ be minimal with $mp \in S_2$. Then $m \leq r < p$ and so (2°) shows that $m = 1$. Thus $p \in S_2$. □

Corollary 11.1.6. [**primes in s2**] *Let p be prime. Then $p \in S_2$ if and only of $p = 2$ or $p \equiv 1 \pmod 4$.*

Proof. If $p = 2$ or $p \equiv 1 \pmod 4$, then $p \in S_2$ by 11.1.5. So suppose $p \in S_2$. Then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Then $a^2 \equiv 0, 1 \pmod 4$ and $b^2 \equiv 0, 1 \pmod 4$. Thus $p \equiv 0, 1, 2 \pmod 4$. If $p \equiv 0, 2 \pmod 4$, p is even and so $p = 2$. □

Lemma 11.1.7. [**approximation by gaussian integers**] *Let $x \in \mathbb{C}$ then there exist $y \in \mathbb{Z}[i]$ with $\delta(x - y) \leq \frac{1}{2}$.*

Proof. Let $x = x_1 + x_2 i$ with $x_i \in \mathbb{R}$. Then there exists $y_i \in \mathbb{Z}$ with $|x_i - y_i| \leq \frac{1}{2}$ (Just round x_i to the nearest integer). Let $y = y_1 + y_2 i$. Then

$$\delta(x - y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

□

Lemma 11.1.8. [**division alg for gauss**] *Let $a, b \in \mathbb{Z}[i]$ with $b \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ with*

$$a = qb + r \text{ and } \delta(r) < \delta(b).$$

Proof. By 11.1.7 there exists $q \in \mathbb{Z}[i]$ with $\delta(\frac{a}{b} - q) \leq \frac{1}{2} < 1$. Put $r = a - qb$. Then

$$\delta(r) = \delta(a - qb) = \delta\left(b\frac{a - qb}{b}\right) = \delta(b)\delta\left(\frac{a}{b} - q\right) < \delta(b)$$

and

$$a = sb + r.$$

□

Lemma 11.1.9. [**gauss euclid**] *$\mathbb{Z}[i]$ is a Euclidean domain.*

Proof. It is readily verified that $\mathbb{Z}[i]$ is an integral domain. By 11.1.3(d), $\delta(a) = 0$ if and only if $a = 0$. Let $a, b \in R$ with $ab \neq 0$, then $a \neq 0$. Thus $\delta(a) \geq 1$ and so $\delta(ab) = \delta(a)\delta(b) \geq \delta(b)$.

By 11.1.8 also the last property of an Euclidean domain holds. □

Lemma 11.1.10. [**units in gaussian integers**] *Let a be a Gaussian integer. Then the following are equivalent:*

(a) [**a**] *a is a unit in $\mathbb{Z}[i]$.*

(b) [**b**] $\delta(a) = 1$

(c) [**c**] *a is one of $1, -1, i$ and $-i$.*

Proof. (a) $\Longrightarrow$ (b): Suppose that $ab = 1$ for some $b \in \mathbb{Z}[i]$. Then $\delta(a)\delta(b) = \delta(ab) = \delta(1) = 1$. Since $\delta(a)$ and $\delta(b)$ are non-negative integers we conclude that $\delta(a) = 1$.

(b) $\Longrightarrow$ (c): Let $a = x + iy$ with $x, y \in \mathbb{Z}$. Then $x^2 + y^2 = \delta(a) = 1$ and so $\{|x|, |y|\} = \{0, 1\}$. Hence either $x = 0$ and $y = \pm 1$ or $y = 0$ and $x = \pm 1$. Thus $a = \pm 1, \pm i$.

(c) $\Longrightarrow$ (b): In each case $\delta(a) = (\pm 1)^2 + 0^2 = 1$.

(b) $\Longrightarrow$ (a): $a\overline{\delta}a = 1$ and a is a unit. □ □

Lemma 11.1.11. [**associates of gaussian integers**] *Let $x, y \in \mathbb{Z}$ and put $a = x + yi$.*

(a) [**a**] *The associates of a in $\mathbb{Z}[i]$ are $a = x + yi, -a = -x - yi, ia = -y + xi$ and $-ia = y - xi$.*

(b) [**d**] *The elements in $\mathbb{Z}[i]$ associate to a or $\overline{a}$ are $\pm x \pm yi$ and $\pm y \pm xi$.*

(c) [**b**] *Define $Q_0 := \{x + yi \mid x, y \in \mathbb{R}, x \geq 0, y > 0\}$ and for $0 \leq r \leq 3$ define $Q_r = i^{r-1}Q_0$. If $0 \neq z \in \mathbb{C}$, then z lies in exactly one of Q_r's. If $a \neq 0$, then each Q_r contains exactly one associate of a.*

(d) [**c**] *$a \sim \overline{a}$ if and only if one of the following holds*

1. [**a**] *$\overline{a} = a$ and $a = r$ for some $r \in \mathbb{R}$.*
2. [**b**] *$\overline{a} = -a$ and $a = ri$ for some $r \in \mathbb{R}$.*
3. [**c**] *$\overline{a} = ia$ and $a = r(1 - i)$ for some $r \in \mathbb{R}$.*
4. [**d**] *$\overline{a} = -ia$ and $a = r(1 + i)$ for some $r \in \mathbb{R}$.*

Proof. (a): Let $b \in \mathbb{Z}[i]$. By A.0.6(b) $b \sim a$ if and only if $b = ua$ for some unit u in $\mathbb{Z}[i]$ and so by 11.1.10 if and only if b is one of $a, -a, ia, -ia$. So (a) holds.

(b) The associates of a are listed in (a) . The associates of $\overline{a}$ are

$$\overline{a} = x - iy, -\overline{a} = \overline{-a} = -x + iy, i\overline{a} = \overline{-ia} = y + ix, \text{ and } -i\overline{a} = \overline{ia} = -y - ix$$

and so (c) holds. (c) Note the

$$Q_1 = iQ_0 = \{-y + xi \mid x, y \in \mathbb{R}, x \geq 0, y > 0\} = \{x + yi \mid x, y \in \mathbb{R}, x < 0, y \geq 0\},$$

$$Q_2 = iQ_1 = \{-y + xi \mid x, y \in \mathbb{R}, x < 0, y \geq 0\} = \{x + yi \mid x, y \in \mathbb{R}, x \leq 0, y < 0\},$$

and

$$Q_3 = iQ_2 = \{-y + xi \mid x, y \in \mathbb{R}, x \leq 0, y < 0\} = \{x + yi \mid x, y \in \mathbb{R}, x > 0, y \leq 0\},$$

Let $0 \neq z \in \mathbb{C}$. Clearly there exists a unique r with $z \in Q_r$. If $0 \leq s \leq 3$ then $i^{s-r}a$ is the unique associate of a contained in Q_s.

(d) We have $\overline{a} \sim a$ if and only if $\overline{a} \in \{\pm a, \pm ia\}$. $a = \overline{a}$ if and only if (d:1) holds. If $a = -\overline{a}$ if and only if (d:2) holds. $\overline{a} = ia$ if and only if $x - iy = -y + ix$ and so if and only if $x = -y$ and if and only if $a = r(1 - i)$ for some $r \in \mathbb{R}$, and so if and only if (d:3) holds. Applying complex conjugation, we conclude tat $\overline{a} = -ia$ if and only if (d:4) holds □

Lemma 11.1.12. [**gaussian primes**] *Let a be a Gaussian prime. Then there exists a unique prime p with $a \mid p$. Moreover, one of the follwing holds:*

1. [**a**] $p \equiv 3 \pmod 4$, $d(a) = p^2$, $\overline{a} \sim a \sim p$, *and p is a Gaussian prime.*

2. [**b**] $p \equiv 1 \pmod 4$, $\delta(a) = p$, $\overline{a} \nsim a \nsim p$, *and p is not a Gaussian prime.*

3. [**c**] $p = 2$, $\delta(a) = p$, $\overline{a} \sim a \nsim p$ *and p is not a Gaussian prime.*

Proof. Since $\delta(a)$ is a positive integer, $\delta(a) = p_1 p_2 \ldots p_n$ where each p_i is a prime. Since $\delta(a) = a\overline{a}$, a divides $\delta(a)$. Since a is a Gaussian prime we conclude from A.0.9(b) that $a \mid p_i$ (in $\mathbb{Z}[i]$) for some $1 \leq i \leq n$. So there exists a prime p with $a \mid p$.

Since $a \mid p$ we have $p = ab$ for some $b \in \mathbb{Z}[i]$ and so

$$(*) \qquad p^2 = \delta(p) = \delta(ab) \overset{11.1.3(c)}{=} \delta(a)\delta(b)$$

Thus $\delta(a)$ divides $\delta(p) = p^2$ in $\mathbb{Z}$. Since a is not a unit, 11.1.10 implies that $\delta(a) > 1$ and so $\delta(a) \in \{p, p^2\}$.

In particular, p is the only prime with $a|p$ in $\mathbb{Z}[i]$.

If $\delta(a) = p^2$ we get $\delta(b) = 1$. So by 11.1.10 b is a unit and $a \sim p$. Since a is a Gaussian prime, A.0.7(h) implies that p is a Gaussian prime. Suppose that $p \not\equiv 3 \pmod 4$. Then by 11.1.6 $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Hence $p = (x + iy)(x - iy)$. Since p is a Gaussian prime, p is irreducible and so $x + iy$ or $x - iy$ is a unit. But then by 11.1.10, $1 = x^2 + y^2 = p$, a contradiction. Thus $p \equiv 3 \pmod 4$. Since $a \sim p$, 11.1.11(d) shows that $\overline{a} \sim a$ and so (1) holds in this case.

If $\delta(a) = p$ then also $\delta(b) = p$. So by 11.1.10 b is not a unit. It follows that p is not irreducible and so by A.0.8 p also not a Gaussian prime. Let $a = x + iy$ with $x, y \in \mathbb{Z}$. Then $p = \delta(a) = x^2 + y^2$ and so by 11.1.6 $p \not\equiv 3 \pmod 4$.

If $p = 2$, then $a = \pm 1 \pm i$ and so by 11.1.11(d) $\overline{a} \sim a$ and (3) holds. Suppose $\overline{a} \sim a$. Since $\delta(a) = p$, $\delta(a)$ is not square and so $a \notin \mathbb{Z}$ and $a \notin \mathbb{Z}i$. Thus 11.1.11(d) shows that $a = r(1 \pm i)$ for some $r \in \mathbb{R}$. Since $a \in \mathbb{Z}[i]$, $r \in \mathbb{Z}$. Also $p = \delta(a) = 2r^2$ and since p is a prime we get $r = \pm 1$ and $p = 2$. So if $p \equiv 1 \pmod 4$, then $\overline{a} \nsim a$ and (2) holds. □

Corollary 11.1.13. [**primes and gaussian primes**] *Let p be a prime. The one of the following holds.*

1. [**a**] $p = 2$, 2 *is not a Gaussian prime,* $1+i$ *is a Gaussian prime with* $1+i \sim 1+i$ *and* $2 \sim (1+i)^2$.

2. [**b**] $p \equiv 1 \pmod 4$ *and there exists a Gaussian prime σ with* $p = \delta(\sigma) = \sigma\overline{\sigma}$ *and* $\sigma \nsim \overline{\sigma}$.

3. [**c**] $p \equiv 3 \pmod 4$ *and p is a Gaussian prime.*

Proof. Since every non zero, non unit in $\mathbb{Z}[i]$ is a product of Gaussian primes, there exists a Gaussian prime σ with $\sigma|p$. Now apply 11.1.12. □

Theorem 11.1.14. [**s2**] *Let $n \in \mathbb{Z}^+$ and write*

$$n = 2^e \prod_{s=1}^{k} p_s^{e_s} \prod_{t=1}^{l} q_t^{f_t}$$

where $2, p_1, p_2, \ldots, p_k, q_1, q_2, \ldots q_l$ *are pairwise distinct primes,* $e \in \mathbb{N}$, $p_s \equiv 1 \pmod 4$, $e_s \in \mathbb{Z}^+$, $q_t \equiv 3 \pmod 4$ *and* $f_t \in \mathbb{Z}^+$. *For* $1 \leq s \leq k$ *let* σ_s *be Gaussian prime dividing* p_s.

(a) [**a**] $n \sim (1+i)^{2e} \prod_{s=1}^{k} \sigma_s^{e_s} \overline{\sigma_s}^{e_s} \prod_{t=1}^{l} q_t^{f_t}$

(b) [**b**] *$n \in S_2$ if and only if f_t is even for all $1 \leq t \leq l$.*

(c) [**c**] *Let $a, b \in \mathbb{Z}$ and suppose $n \in S_2$. Then $a^2 + b^2 = n$ if and only if*

$$a + ib = i^g (1+i)^e \prod_{s=1}^{k} \sigma_s^{b_s} \overline{\sigma_s}^{e_s - b_s} \prod_{t=1}^{l} q_t^{\frac{f_t}{2}}$$

for some $g \in \mathbb{Z}$ with $0 \leq g \leq 3$ and $b_s \in \mathbb{Z}$ with $0 \leq b_s \leq e_s$.

(d) [**d**] *Let $m = \prod_{s=1}^{k} p_s^{e_s}$ and suppose $n \in S_2$. Then the number of pairs $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $a^2 + b^2 = n$ is $4\tau(m)$.*

Proof. Observe that $2 \sim (1+i)^2$ and $p_s = \delta(\sigma_s) = \sigma_s \overline{\sigma_s}$.

$$n \sim (1+i)^{2e} \prod_{s=1}^{k} \sigma_s^{e_s} \overline{\sigma_s}^{e_s} \prod_{t=1}^{l} q_t^{f_t} \text{ is the Gaussian prime factorization of } n$$

and so (a) holds.

Let $y \in \mathbb{Z}[i]$ such that y divides n in $\mathbb{Z}[i]$. Then any Gaussian prime dividing y also divides n and so is associate to one of $1+i$, σ_s, $\overline{\sigma_s}$ and q_t. Thus y is associate to

$$z := (1+i)^{a_0} \prod_{s=1}^{k} \sigma_s^{b_s} \overline{\sigma_s}^{c_s} \prod_{t=1}^{l} q_t^{d_t}$$

where a_0, b_t, c_t, d_t are in $\mathbb{N}$ with $a_0 \leq e$, $b_t \leq e_t, c_t \leq e_t$ and $d_t \leq f_t$.

We compute $\delta(y)$:

$$\begin{aligned}
\delta(y) = \delta(z) = z\overline{z} &= \left((1+i)^{a_0} \prod_{s=1}^{k} \sigma_s^{b_s} \overline{\sigma_s}^{c_s} \prod_{t=1}^{l} q_t^{d_t} \right) \cdot \left((1-i)^{a} \prod_{s=1}^{k} \overline{\sigma_s}^{b_s} \sigma_s^{c_s} \prod_{t=1}^{l} q_t^{d_t} \right) \\
&= (1+i)(1-i))^{a_0} \prod_{s=1}^{k} (\sigma_s \overline{\sigma_s})^{b_s} (\overline{\sigma_s} \sigma_s)^{c_s} \prod_{t=1}^{l} (q_t q_t)^{d_t} = 2^a \prod_{s=1}^{k} p_k^{b_s + c_s} \prod_{t=1}^{k} q_t^{2d_t}
\end{aligned}$$

The uniquess of prime factorization in $\mathbb{Z}$ now show that $\delta(y) = n$ if and only if

$$(*) \qquad a = e; \quad b_s + c_s = e_s, 1 \leq s \leq k; \quad \text{and } f_t = 2d_t, 1 \leq t \leq l$$

In partiuclar, there exists $y \in \mathbb{Z}[i]$ with $\delta(y) = n$ if and only of f_t is even for all $1 \leq t \leq l$. Thus (b) is proved.

Note that a and d_t are uniquely determined by (*); there are $e_s + 1$ choices for b_s (namely b_s is an arbitray integer with $0 \leq b_s \leq e_s$) and c_s is uniquely determined once b_s is choosen (namely $c_s = e_s - b_s$). So there are

$$\prod_{s=1}^{k} (e_s + 1)$$

choices for z. Note that this number is equal to $\tau(m)$.

Since $y \sim z$, $y = i^g z$ for some $0 \le g \le 3$. So we found all $y \in \mathbb{Z}[i]$ with $\delta(y) = n$:

$$y = i^g (1+i)^e \prod_{s=1}^{k} \sigma_s^{b_s} \overline{\sigma_s}^{e_s - b_s} \prod_{t=1}^{l} q_t^{\frac{f_t}{2}}$$

Thus (c) holds. In particular, there are $4\tau(m)$ such y's and so (d) is proved. □

Lemma 11.1.15. [**compare z and zi**]

(a) [**a**] *Let $a, b, c \in \mathbb{Z}$. Then $a \mid b + ci$ in $\mathbb{Z}[i]$ if and only if $a \mid b$ and $a \mid c$ in $\mathbb{Z}$.*

(b) [**b**] *Let $a, b \in \mathbb{Z}$. Then $a \mid b$ in $\mathbb{Z}$ if and only if $a \mid b$ in $\mathbb{Z}[i]$*

Proof. (a) $a \mid b + ci$ in $\mathbb{Z}[i]$ iff there exist $d, e \in \mathbb{Z}$ with $b + ci = a(d + ei)$, iff there exists $d, e \in \mathbb{Z}$ with $b = ad$ and $c = ae$ iff $a \mid b$ and $a \mid c$ in $\mathbb{Z}$.

(b) This follows from (a) applied with $c = 0$. □

Definition 11.1.16. [**def:s*2**] $S_2^* = \{a^2 + b^2 \mid a, b \in \mathbb{Z} \mid \gcd(a, b) = 1\}$.

Before determining the elements of S_2, we will describe $\gcd(a, b)$ in terms of $a + ib$.

Lemma 11.1.17. [**gcd gauss**] *Let $a_1, a_2 \in \mathbb{Z}$ and put $z = a_1 + ia_2$. Let 2^{e_i} be the largest power of 2 dividing a_i.*

(a) [**a**] *If $e_1 \neq e_2$, then $\gcd(z, \overline{z}) = \gcd(a_1, a_2)$.*

(b) [**b**] *If $e_1 = e_2$, then $\gcd(z, \overline{z}) = \gcd(a_1, a_2)(1 + i)$.*

(c) [**c**] $\gcd(a, b) = 1$ *if and only if* $\gcd(z, \overline{z}) \in \{1, 1 + i\}$.

Proof. Put $d = \gcd(a_1, a_2)$ and $c = \gcd(z, \overline{z})$. Since d divides a_1 and a_2, 11.1.15(a) shows that d divides z and $\overline{z}$ in $\mathbb{Z}[i]$. Thus $d \mid c$ in $\mathbb{Z}[i]$ and so $c = fd$ for some $f \in \mathbb{Z}[i]$. Since $c \mid z$ and $c \mid \overline{z}$ we have $c \mid z + \overline{z}$ and $c \mid i(z - \overline{z})$. Therefore $e \mid 2a_1$ and $e \mid 2a_2$. It follows that $fd = e \mid \gcd(2a_1, 2a_2) = 2d$ and so $f|2$. Since $2 \sim (1 + i)^2$ and $1 + i$ is a Gaussian prime, f is associate to $1, 1 + i$ or 2. If $f \sim 2$, then $2d \sim fd$ divides z and so by 11.1.15(a), $2d \mid a_1$ and $2d \mid a_2$. But this contradicts $\gcd(a_1, a_2) = d$. Thus $f \sim 1$ or $1 + i$. Hence $\gcd(z, \overline{z}) = d(1 + i)$ if $d(1 + i)$ divides z and $\overline{z}$, and $\gcd(z, \overline{z}) = d$ otherwise. Note that $d(1 + i)$ divides z if and only if $\overline{d(1 + i)} = d(1 - i)$ divides $\overline{z}$. Since $d(1 + i)$ and $d(1 - i)$ are associate, we conclude that $d(1 + i)$ divides z if and only if $d(1 + i)$ divides z and $\overline{z}$. Since $(1 + i)(1 - i) = 2$ we have $\frac{1}{1+i} = \frac{1-i}{2}$ and

$$\frac{z}{d(1+i)} = \frac{(a_1 + ia_2)(1 - i)}{2d} = \frac{a_1 + a_2}{2d} + i\frac{a_1 - a_2}{2d} = \frac{1}{2}\left(\frac{a_1}{d} + \frac{a_2}{d}\right) + i\frac{1}{2}\left(\frac{a_1}{d} - \frac{a_2}{d}\right)$$

Since d divides a_1 and a_2, we conclude that $\frac{z}{d(1+i)} \in \mathbb{Z}[i]$ if and only if $\frac{a_1}{d} \equiv \frac{a_2}{d} \pmod 2$. Note that $\min(e_1, e_2)$ is the largest power of 2 dividing d. If $e_1 = e_2$, then both $\frac{a_1}{d}$ and $\frac{a_2}{d}$ are odd and (a) holds. If $e_1 \neq e_2$, the one of $\frac{a_1}{d}$ and $\frac{a_2}{d}$ is even and the other is odd, so (b) holds.

(c) follows immediately from (a) and (b) □

Corollary 11.1.18. [**primitive sum of squares**]

(a) [**a**] *Let $n \in \mathbb{Z}^+$. Then $n \in S_2^*$ if and only if n is neither divisible by four nor by a prime congruent to 3 modulo 4.*

(b) [**b**] *Let $n \in S_2^*$ and let $a, b \in \mathbb{Z}$ with $n = a^2 + b^2$ and $\gcd(a, b) = 1$. Write*

$$n = 2^e \prod_{s=1}^{k} p_s^{e_s} \prod_{t=1}^{l} q_t^{f_t}$$

where $2, p_1, p_2, \dots, p_k, q_1, q_2, \dots q_l$ are pairwise distinct primes, $e \in \mathbb{N}$, $p_t \equiv 1 \pmod 4$, $e_t \in \mathbb{Z}^t$, $q_t \equiv 3 \pmod 4$ and $f_t \in \mathbb{Z}^+$. For $1 \leq s \leq k$ let σ_s be Gaussian prime dividing p_s. Then $a + bi$ is associated to

$$(1+i)^e \prod_{s=1}^{k} \mu_s^{e_s}$$

where for $1 \leq s \leq k$, $\mu_s \in \{\sigma_s, \overline{\sigma_s}\}$.

Proof. We may assume that $n \in S_2$ and let $a, b \in \mathbb{Z}$ with $a^2 + b^2 = n$. Put $z = a + bi$. By 11.1.17 $\gcd(a, b) = 1$ if and only if $\gcd(z, \overline{z}) \in \{1, 1+i\}$. Choose notation as in 11.1.14. So

$$z = a + ib \sim (1+i)^e \prod_{s=1}^{k} \sigma_s^{b_s} \overline{\sigma_s}^{e_s - b_s} \prod_{t=1}^{l} q_t^{\frac{f_t}{2}}$$

Thus

$$\overline{z} \sim (1+i)^e \prod_{s=1}^{k} \sigma_s^{e_s - b_s} \overline{\sigma_s}^{b_s} \prod_{t=1}^{l} q_t^{\frac{f_t}{2}}$$

and

$$\gcd(z, \overline{z}) \sim (1+i)^e \prod_{s+1}^{k} \sigma_s^{\min(b_s, e_s - b_s)} \overline{\sigma_s}^{\min(b_s, e_s - b_s)} \prod_{t=1}^{l} q_t^{\frac{f_t}{2}}$$

Hence $\gcd(a, b) = 1$ iff $\gcd(z, \overline{z}) \in \{1, 1+i\}$ iff $e \leq 1$, $\min(b_s, e_s - b_s) = 0$ and $l = 0$ iff $e \leq 1$, $b_s \in \{0, e_s\}$ and $l = 0$.

Thus there exist $a, b \in \mathbb{Z}$ with $n = a^2 + b^2$ and $\gcd(a, b) = 1$ if and only if $e \leq 1$ and $l = 0$. That is iff $4 \nmid n$ and there does not exists a prime q with $q \equiv 3 \pmod 4$ and $q \mid n$.

Suppose now $\gcd(a, b) = 1$. Then $b_s \in \{0, e_s\}$. Put $\mu_s = \sigma_s$ if $b_s = e_s$ and $\mu_s = \overline{\sigma_s}$ if $e_s = 0$. In either case $\sigma_s^{b_s} \overline{\sigma_s}^{e_s - b_s} = \mu_s^{e_s}$ and since $l = 0$

$$a + ib \sim (1+i)^e \prod_{s=1}^{k} \mu_s^{e_s}$$

So (b) is proved. □

Observe that if $n = a^2 + b^2$ and $d = \gcd(a, b)$, then $\frac{n}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2$ and $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. So we can compute all pairs (a, b) with $n = a^2 + b^2$ as follows: For each $d \in \mathbb{Z}^+$ such that $d^2 \mid n$ and d is divisible by $2^{\lfloor \frac{e}{2} \rfloor} \prod_{t=1}^{l} q_t^{\frac{f_t}{2}}$, use 11.1.18 to write $m = \frac{n}{d^2}$ as the sum of the squares of two coprime integers and then multiply each of the two integers with d.

Example 11.1.19. [ex:s2] *Let $n = 2^5 5^5 11^2$. Find all $a, b \in \mathbb{N}$ with $a^2 + b^2 = n$ and $a \leq b$.*

Let $d \in \mathbb{Z}^+$ such that $d^2 \mid n$ and $m := \frac{n}{d^2} \in S_2^*$. Then $d \mid 2^2 5^2 11$, $4 \nmid \frac{n}{d^2}$ and $11 \mid \frac{n}{d^2}$. Thus $4 \mid d$, $11 \mid d$ and so $d = 44 \cdot 5^x$ with $0 \leq x \leq 2$. Hence $m = 2 \cdot 5^y$, where $y = 5 - 2x \in \{5, 3, 1\}$.

Observe $5 = 1^2 + 2^2$ and so $\sigma = 1 + 2i$ is a Gaussian prime dividing 5. Let $a, b \in \mathbb{Z}$ with $n = a^2 + b^2$ and $\gcd(a, b) = 1$. Then $n = d^2 m = (da)^2 + (db)^2$. Put $z = a + ib$. Then by 11.1.18, z or $\overline{z}$ is associate to $(1+i)\sigma^y$. Note that $\sigma^2 = (1+2i)(1+2i) = (1-4) + (2+2)i = -3 + 4i$.

For $x = 2$ we have $d = 5^2 \cdot 44 = 1100$, $m = 2 \cdot 5 = 10$, $(1+i)\sigma = (1+i)(1+2i) = (1-2) + (2+1)i = -1 + 3i$. $10 = 1^2 + 3^2$ and

$$n = 1100^2 + 3300^2.$$

For $x = 1$ we have $d = 5 \cdot 44 = 220$, $m = 2 \cdot 5^3 = 250$, $(1+i)\sigma^3 = (1+i)\sigma\sigma^2 = (-1+3i)(-3+4i) = (3-12) + (-4-9) = -9 - 13i \sim 9 + 13i$, $250 = 9^2 + 13^2$ and

$$n = 1980^2 + 2860^2.$$

For $x = 0$ we have $d = 44$, $m = 2 \cdot 5^5 = 10 \cdot 5^4 = 6250$. $(1+i)\sigma^5 = (1+i)\sigma^3\sigma^2 \sim (9+13i)(-3+4i) = -27 - 52 + (36 - 39) = -79 - 3i \sim 79 + 3i$. $6250 = 3^2 + 79^2$ and

$$n = 132^2 + 3476^2.$$

11.2 Sum of Four Squares

Lemma 11.2.1. [**s4 s4**] *For $i = 1$ and 2 let $a_i, b_i, c_i, d_i \in \mathbb{R}$. Then*

$$\begin{aligned}(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) \quad = \quad & (a_1 a_2 + b_1 b_2 + c_1 c_2 + d_1 d_2)^2 \\ + \quad & (a_1 b_2 - b_1 a_2 - c_1 d_2 + d_1 c_2)^2 \\ + \quad & (a_1 c_2 + b_1 d_2 - c_1 a_2 - d_1 b_2)^2 \\ + \quad & (a_1 d_2 - b_1 c_2 + c_1 b_2 - d_1 a_2)^2\end{aligned}$$

Proof. The product on the left hand side is equal to

$$\begin{aligned}& a_1^2 a_2^2 + a_1^2 b_2^2 + a_1^2 c_2^2 + a_1^2 b_2^2 + b_1^2 a_2^2 + b_1^2 b_2^2 + b_1^2 c_2^2 + b_1^2 d_2^2 \\ + & c_1^2 a_2^2 + c_1^2 b_2^2 + c_1^2 c_2^2 + c_1^2 d_2^2 + d_1^2 a_2^2 + d_1^2 b_2^2 + d_1^2 c_2^2 + d_1^2 d_2^2\end{aligned}$$

The right hand side is equal two

$$\begin{aligned}& a_1^2 a_2^2 + b_1^2 b_2^2 + c_1^2 c_2^2 + d_1^2 d_2^2 + 2a_1 b_1 a_2 b_2 + 2a_1 c_1 a_2 c_2 + 2a_1 d_1 a_2 d_2 + 2b_1 c_1 b_2 c_2 + 2b_1 d_1 b_2 d_2 + 2c_1 d_1 c_2 d_2 \\ + & a_1^2 b_2^2 + b_1^2 a_2^2 + c_1^2 d_2^2 + d_1^2 c_2^2 - 2a_1 b_1 a_2 b_2 - 2a_1 c_1 b_2 d_2 + 2a_1 d_1 b_2 c_2 + 2b_1 c_1 a_2 d_2 - 2b_1 d_1 a_2 c_2 - 2c_1 d_1 c_2 d_2 \\ + & a_1^2 c_2^2 + b_1^2 d_2^2 + c_1^2 a_2^2 + d_1^2 b_2^2 + 2a_1 b_1 c_2 d_2 - 2a_1 c_1 a_2 c_2 - 2a_1 d_1 b_2 c_2 - 2b_1 c_1 a_2 d_2 - 2b_1 d_1 b_2 d_2 + 2c_1 d_1 a_2 b_2 \\ + & a_1^2 d_2^2 + b_1^2 c_2^2 + c_1^2 b_2^2 + d_1^2 a_2^2 - 2a_1 b_1 c_2 d_2 + 2a_1 c_1 b_2 d_2 - 2a_1 d_1 a_2 d_2 - 2b_1 c_1 b_2 c_2 + 2b_1 d_1 a_2 c_2 - 2c_1 d_1 a_2 b_2\end{aligned}$$

and so the lemma holds. ∎

Corollary 11.2.2. [**s4 closed**] *S_4 is closed under multiplication.*

Proof. This follows immediately from 11.2.1. ∎

Theorem 11.2.3. [**s4=n**] $S_4 = \mathbb{N}$, *that is is every non-negative integer is the sum of the squares of four integers.*

Proof. We have $0 = 0^2 + 0^2 + 0^2 + 0^2 \in S_4$ and $1 = 1^2 + 0^2 + 0^2 + 0^2 \in S_4$. Any integer larger than 1 is a product of primes, so in view of and in view of 11.2.2 it suffices to show that every prime p is contained in S_4. $2 = 1^2 + 1^2 + 0^2 + 0^2 \in S_4$. So we may assume that p is odd.

1°. [**1**] *There exists $m \in \mathbb{Z}$ with $1 \leq m < p$ and $mp \in S_4$.*

Let $K := \{a^2 \mid a \in \mathbb{Z}_p\} = Q_p \cup \{[0]_p\}$. Then $|K| = |Q_p| + 1 = \frac{p-1}{2} + 1 = \frac{p+1}{2} > \frac{p}{2}$. Put $L = [-1]_p - K = \{[-1-n^2]_p \mid n \in \mathbb{Z}\}$. Then $|L| = |K| > \frac{p}{2}$. Thus $|K| + |L| > p = |\mathbb{Z}_p|$ and so $K \cap L \neq \emptyset$. It follows that there exist $u, v \in \mathbb{Z}$ with $u^2 \equiv -1 - v^2 \pmod{p}$ and so $u^2 + v^2 + 1 = mp$ for some $m \in \mathbb{Z}$. Without loss $|u| \leq \frac{p}{2}$ and $|v| \leq \frac{p}{2}$. Thus

$$mp = u^2 + v^2 + 1 \leq \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2$$

and so $1 \leq m < p$. Since $mp = u^2 + v^2 + 1^1 + 0^2$, $mp \in S_4$ and (1°) holds.

2°. [**2**] *Let $m \in \mathbb{Z}$ with $1 \leq m < p$ with $pm \in S_4$. Then either $m = 1$ or there exists $s \in \mathbb{Z}$ with $1 \leq s < m$ and $sp \in S_4$.*

Pick $a_1, b_1, c_1, d_1 \in \mathbb{Z}$ with

$$mp = a_1^2 + b_1^2 + c_1^2 + d_1^2 \tag{$*$}$$

For $x \in \{a, b, c, d\}$ pick $x_2 \in \mathbb{Z}$ with $|x_2| \leq \frac{m}{2}$ and $x_2 \equiv x_1 \pmod{m}$. Then

$$a_2^2 + b_2^2 + c_2^2 + d_2^2 \equiv a_1^2 + b_2^2 + c_1^2 + d_1^2 \equiv pm \equiv 0 \pmod{m}$$

and so

$$sm = a_2^2 + b_2^2 + c_2^2 + d_2^2 \tag{$**$}$$

for some $s \in \mathbb{Z}$.

Case 1. [**s=0**] *Suppose that $s = 0$.*

Then $x_2 = 0$ for all $x \in \{a, b, c, d\}$. Hence $x_1 \equiv 0 \pmod{m}$ and so $m^2 \mid x_1^2$. Therefore m^2 divides $a_1^2 + b_1^2 + c_1^2 + d_1^2 = mp$. It follows that $m \mid p$. Since $1 \leq m < p$ and p is a prime, this gives $m = 1$ and so (2°) holds in this case.

Case 2. [**s odd**] *$s \geq 1$ and m is even*

Since $|\mathbb{Z}_2| = 2 < 4$, at least two of a_1, b_1, c_1 and d_1 are congruent modulo 2. So we may assume that $a_1 \equiv b_1 \pmod{2}$. Thus $a_1 + b_1 \equiv 0 \pmod{2}$. Also $k^2 \equiv k \pmod{2}$ for all $k \in \mathbb{Z}$. Since m is even, (*) gives

$$0 \equiv mp \equiv a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a_1 + b_1 + c_1 + d_1 \equiv c_1 + d_1$$

Hence also $c_2 \equiv d_2 \pmod{2}$.

We compute

$$\left(\frac{a_1+b_1}{2}\right)^2+\left(\frac{a_1-b_1}{2}\right)^2+\left(\frac{c_1+d_1}{2}\right)^2+\left(\frac{c_1-d_1}{2}\right)^2=\frac{2a_1^2+2b_1^2+2c_1^2+2d_1^2}{4}=\frac{mp}{2}$$

Thus $\frac{m}{2}p \in S_4$ and (2°) holds with '$s=\frac{m}{2}$'.

Case 3. [**s odd**] $s \geq 1$ *and* m *is odd.*

Since m is odd, $\frac{m}{2}$ is not an integer and so $|x_2| < \frac{m}{2}$ for all $x=a,b,c,d$. Thus (**) gives

$$sm < 4\left(\frac{m}{2}\right)^2 = m^2$$

and so $s<m$.

Observe that

$$\begin{array}{rclcll}
a_1a_2+b_1b_2+c_1c_2+d_1d_2 & \equiv & a_1^2+b_1^2+c_1^2+d_1^2 & \equiv & mp \equiv 0 & \pmod m \\
a_1b_2-b_1a_2-c_1d_2+d_1c_2 & \equiv & a_1b_1-b_1a_1-c_1d_1+d_1c_2 & \equiv & 0 & \pmod m \\
a_1c_2+b_1d_2-c_1a_2-d_1b_2 & \equiv & a_1c_1+b_1d_1-c_1a_1-d_1b_1 & \equiv & 0 & \pmod m \\
a_1d_2-b_1c_2+c_1b_2-d_1a_2 & \equiv & a_1d_1-b_1c_1+c_1b_1-d_1a_1 & \equiv & 0 & \pmod m
\end{array}$$

Using 11.2.1 we have

$$\begin{array}{rclcl}
spm^2=(sm)(pm) & = & (a_1^2+b_1^2+c_1^2+d_1^2) & \cdot & (a_2^2+b_2^2+c_2^2+d_2^2) \\
& = & (a_1a_2+b_1b_2+c_1c_2+d_1d_2)^2 & + & (a_1b_2-b_1a_2-c_1d_2+d_1c_2)^2 \\
& + & (a_1c_2+b_1d_2-c_1a_2-d_1b_2)^2 & + & (a_1d_2-b_1c_2+c_1b_2-d_1a_2)^2
\end{array}$$

Dividing by m^2 we obtain

$$\begin{array}{rlcl}
sp= & \left(\frac{a_1a_2+b_1b_2+c_1c_2+d_1d_2}{m}\right)^2 & + & \left(\frac{a_1b_2-b_1a_2-c_1d_2+d_1c_2}{m}\right)^2 \\
+ & \left(\frac{a_1c_2+b_1d_2-c_1a_2-d_1b_2}{m}\right)^2 & + & \left(\frac{a_1d_2-b_1c_2+c_1b_2-d_1a_2}{m}\right)^2
\end{array}$$

Thus $sp \in S_4$ and since $1 \leq s < m$, (2°) also holds in this case.

By (1°) we can choose $m \in \mathbb{Z}$ mininimal with $1 \leq m < p$ and $mp \in S_4$. (2°) now shows that $m=1$ and $p \in S_4$. □

Example 11.2.4. [**ex:s4**] *Use the proof of 11.2.3 to write* 11 *as the sum of squares of four integers.*

We have in $\mathbb{Z}_{11}$,

$$K=\{0^2,(\pm1)^2,(\pm2)^2,(\pm3)^2,(\pm4)^2,(\pm5)^2\}=\{0,1,4,9,16=5,25=3\}$$

and

$$L=-(1+K)=\{-1,-2,-5,-10,-6,-4\}=\{10,9,6,1,5,7\}$$

So $K\cap L=\{1,5,9\}$. Let's choose $5\in K\cap L$. Then

$$4^2 \equiv 5 \equiv -1 - 4^2 \pmod{11}$$

and

$$4^2 + 4^2 + 1^2 + 0^2 = 33 = 3 \cdot 11$$

So $m = 3$ and $m \geq 1$ and m is odd. So we are in Case 3 of 11.2.3. We have

$$a_1 \equiv 4 \equiv 1 \pmod{3} \text{ and so } a_2 = 1$$
$$b_1 \equiv 4 \equiv 1 \pmod{3}\text{and so } b_2 = 1$$
$$c_1 \equiv 1 \pmod{3}\text{and so } c_2 = 1$$
$$d_1 \equiv 0 \pmod{3}\text{and so } b_2 = 0$$

Thus

$$a_2^2 + b_2^2 + c_2^2 + d_2^2 = 1 + 1 + 1 + 0 = 3 = 1 \cdot 3 = 1 \cdot m$$

So $s = 1$.

$$\begin{aligned}
11 = sp = & \quad \left(\tfrac{a_1a_2+b_1b_2+c_1c_2+d_1d_2}{m}\right)^2 + \left(\tfrac{a_1b_2-b_1a_2-c_1d_2+d_1c_2}{m}\right)^2 \\
& + \left(\tfrac{a_1c_2+b_1d_2-c_1a_2-d_1b_2}{m}\right)^2 + \left(\tfrac{a_1d_2-b_1c_2+c_1b_2-d_1a_2}{m}\right)^2 \\
= & \quad \left(\tfrac{4\cdot1+4\cdot1+1\cdot1+0\cdot0}{3}\right)^2 + \left(\tfrac{4\cdot1-4\cdot1-1\cdot0+0\cdot1}{3}\right)^2 \\
& + \left(\tfrac{4\cdot1+4\cdot0-1\cdot1-0\cdot1}{3}\right)^2 + \left(\tfrac{4\cdot0-4\cdot1+1\cdot1-0\cdot1}{3}\right)^2 \\
= & \quad 3^2 + 0^2 + 1^2 + (-1)^2
\end{aligned}$$

So

$$11 = 3^2 + 1^2 + 1^2 + 0^2$$

Chapter 12

Fermat's Last Theorem

Fermat's Last Theorem: *Let a, b, c and n be positive integers with $n \geq 3$, then*

$$a^n + b^c \neq c^n$$

Fermat wrote this theorem on the margin of his copy of Diophantos' Arithmetica around 1637, Fermat did not give a proof, but just stated that the margin was too small to fit the proof. It took 320 years until Andrew Wiles finally gave a proof in 1993. In this chapter we will prove a couple of special cases of Fermat's last theorem.

Let m be a divisor of n with $m \geq 3$. Then $n = ml$ for some $l \in \mathbb{Z}^+$ and $a^n + b^n \neq c^n$ becomes $(a^l)^m + (b^l)^m \neq (c^l)^m$. So if the Fermat's Theorem holds for m in place of n it also holds for n. Observe that every integer large than 3 is divisible by 4 or by odd prime. So it suffices to prove Fermat's last theorem for $n = 4$ and for n an odd prime.

If $a^n + b^n = c^n$ and p is a prime dividing two of numbers a, b and c, then p also divides the third and $\left(\frac{a}{p}\right)^n + \left(\frac{b}{p}\right)^n = \left(\frac{c}{p}\right)^n$. So it suffices to prove Fermat's last theorem for a, b and c being pairwise coprime.

12.1 $a^2 + b^2 = c^2$

Definition 12.1.1. [**def:pythagorean triple**] *A triple (a, b, c) is called a* primitive Pythagorean triple *if*

(i) [**i**] *a, b and c are pairwise coprime integers.*

(ii) [**ii**] *$a^2 + b^2 = c^2$.*

(iii) [**iii**] *a is odd.*

Note here that if a and b are coprime integers, then a or b is odd. So condition (iii) can always be achieved by interchanging a and b if necessary.

Theorem 12.1.2. [**pythagorean triples**] *Let a, b and c be integers. Then the following are equivalent:*

(a) [**a**] *(a,b,c) is a primitive Pythagorean triple.*

(b) [**b**] *There exist coprime positive integers u and v with $u>v$, $u \not\equiv v \pmod 2$ and*

$$a=u^2-v^2, \quad b=2uv \text{ and } c=u^2+v^2$$

Proof. (a) $\Longrightarrow$ (b): Suppose (a) holds. By 11.1.18 c^2 is neither divisible by 4 nor by a prime congruent to 3 modulo 4. Thus c is odd and $c=\prod_{s=1}^k p_s^{e_s}$, where the p_s's are primes congruent to 1 (mod 4) and $e_s \in \mathbb{Z}^+$. For $1 \leq s \leq k$ let σ_s be a Gaussian prime with $\sigma_s \mid p_s$. Then $c^2=\prod_{s=1}^k \sigma^{2e_s}\overline{\sigma_s}^{2e_s}$ and so by 11.1.18 $a+ib$ is associate to $\prod_{s=1}^k \mu^{2e_s}$, where $\mu_s \in \{\sigma_s, \overline{\sigma_s}\}$. Put $\mu=\prod_{s=1}^k \mu_s^{e_s}$ and let $\mu=x+yi$ with $x,y\in\mathbb{Z}$. Then $a+ib$ is associated to $\mu^2=x^2-y^2+2xyi$ and so $\{a,b\}=\{|x^2-y^2|,|2xy|\}$. Since a is odd, $b=2|x||y|$ and $a=|x^2-y^2|$. Let $u=\max(|x|,|y|)$ and $v=\min(|x|,|y|$. Then $a=u^2-v^2$ and $b=2uv$. Hence $\gcd(u,v)$ divides a and b. Since $\gcd(a,b)=1$, this gives $\gcd(u,v)=1$. Since $p_s=\mu_s\overline{\mu_s}$ we have $c=\prod_{s=1}^k(\mu_s\overline{\mu_s})^{e_s}$ and so $c=\mu\overline{\mu}=x^2+y^2=u^2+v^2$. Since c is odd, $u \not\equiv v \pmod 2$ and so (b) holds.

(b) $\Longrightarrow$ (a): Suppose (b) holds. We compute

$$a^2+b^2=(u^2-v^2)^2+(2uv)^2=u^4-2u^2v^2+v^4+4u^2v^2=u^4+2u^2v^2+v^4=(u^2+v^2)^2=c^2$$

Since $u \not\equiv v \pmod 2$, a is odd, b is even and c is odd. Suppose p is a prime dividing two of a,b and c. Then it divides all three and hence p is odd and p divides $\frac{a+c}{2}=u^2$ and $\frac{c-a}{2}=v^2$. So p divides u and v, a contradiction to $\gcd(u,v)=1$. Thus a,b and c are pairwise coprime and (a,b,c) is a primitive Pythagorean triple and (a) holds. $\square$

Example 12.1.3. [**ex:pythagorean triples**] *Compute the Pythagorean triple associated to $u=6$ and $v=5$.*

$a=u^2-v^2=36-25$, $b=2uv=2\cdot 6\cdot 5=60$ and $c=u^2+v^2=36+25=61$.

12.2 $a^4+b^4=c^2$

Theorem 12.2.1. [**n=4**] *If a,b,c are positive integer, then $a^4+b^4\neq c^2$. In particular, Fermat's Last Theorem holds for $n=4$.*

Proof. Let a,b,c be a counter example with c minimal. If p is prime dividing, two of a, b and c, then p divides all three and p^2 divides c, thus

$$\left(\frac{a}{p}\right)^4+\left(\frac{b}{p}\right)^4=\left(\frac{c}{p^2}\right)^2$$

contradiction the minimality of c. Thus a,b,c are pairwise coprime and we may assume that a is odd. Thus by 12.1.2 there exist coprime positive integers u and v with $u>v$, $u\not\equiv v \pmod 2$ and

$$a^2=u^2-v^2, b^2=2uv, \text{ and } c=u^2+v^2 \tag{1}$$

Thus $a^2+v^2=u^2$. Since u and v are coprime and a is odd, we conclude from 12.1.2 that there exists coprime positive integers $\tilde{u},\tilde{v}$ with $\tilde{u}>\tilde{v}$, $\tilde{u}\not\equiv\tilde{v} \pmod 2$ and

(2) $$a = \tilde{u}^2 - \tilde{v}^2, v = 2\tilde{u}\tilde{v}, \text{ and } u = \tilde{u}^2 + \tilde{v}^2$$

Thus

(3) $$b^2 = 2uv = 4\tilde{u}\tilde{v}(\tilde{u}^2 + \tilde{v}^2)$$

Since u and v are coprime, $2\tilde{u}\tilde{v}$ and $\tilde{u}^2 + \tilde{v}^2$ are coprime. Since also $\tilde{u}$ and $\tilde{v}$ are coprime we conclude that $\tilde{u}, \tilde{v}$ and $\tilde{u}^2 + \tilde{v}^2$ are pairwise coprime. By (3) $\left(\frac{b}{2}\right)^2 = \tilde{u}\tilde{v}(\tilde{u}^2 + \tilde{v}^2)$. Hence 3.1.7(b) shows that each if the three coprime factors have to be square. So there exist $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ in in $\mathbb{Z}$ with

$$\tilde{u} = \tilde{a}^2, \tilde{v} = \tilde{b}^2, \text{ and } \tilde{u}^2 + \tilde{v}^2 = \tilde{c}^2$$

Thus

$$\tilde{a}^4 + \tilde{b}^4 = (\tilde{a}^2) + (\tilde{b}^2)^2 = \tilde{u}^2 + \tilde{v}^2 = \tilde{c}^2$$

Note that

$$\tilde{c} \leq (\tilde{c}^2)^2 = (\tilde{u}^2 + \tilde{v}^2)^2 = u^2 < u^2 + v^2 = c$$

and we obtained a contradiction of the minimal choice of c. □

12.3 $a^p + b^p = c^p$

Suppose $a^p + b^p = c^p$ where p is an odd prime and a, b, c are positive integers. Since p is odd, $(-c)^p = -c^p$ and $a^p + b^p + (-p)^n = 0$.

Thus Fermat's Last Theorem for an odd prime p is equivalent to

$$a^p + b^p + c^p \neq 0.$$

for all non-zero integers a, b and c. This formulation has the advantage that it is symmetric in a, b and c.

The proof of Fermat's Last Theorem for odd primes splits into two cases.

Case I of Fermat's Last Theorem *p divides none of a, b and c.*

Case II of Fermat's Last Theorem *p divides exactly one of a, b and c.*

In this section we will rule out Case II of Fermat's Last Theorem for certain primes p. The next Lemma makes sure that the conditions we will make on the primes is fulfilled for many primes.

Lemma 12.3.1. [**q=2p+1**] *Let q and p be odd primes with $q = 2p + 1$. Then*

(a) [**a**] *If $a \in \mathbb{Z}$ then $a^p \equiv 0, 1, -1 \pmod{q}$.*

(b) [**b**] *If $a^p + b^p + c^p \equiv 0 \pmod{q}$ for some $a, b, c \in \mathbb{Z}$ then q divides one of a, b, c.*

(c) [**c**] *If $a \in \mathbb{Z}$, then $p \not\equiv a^p \pmod{q}$.*

Proof. (a) If $q \mid a$, the $a \equiv 0 \pmod q$. So suppose $q \nmid a$. Then Fermat's Little Theorem implies $a^{q-1} \equiv 1 \pmod q$ and so

$$(a^p)^2 \equiv a^{2p} \equiv a^{q-1} \equiv 1 \pmod q$$

Thus $a^p \equiv \pm 1 \pmod q$ and (a) holds.

(b) Suppose that q divides none of a, b and c. Then $a^p \not\equiv 0 \pmod q$. and so by (a), a^p, b^p and c^p all are congruent to ± 1 modulo q. Thus $a^p + b^p + c^p$ is congruent to ± 1 or ± 3 modulo q. Since $q = 2p + 1 \geq 2 \cdot 3 + 1 > 3$, we conclude that $a^p + b^p + c^p \not\equiv 0 \pmod q$.

(c) Note that $0 < p - 1 < p < p + 1 < q$ and so q divides none of $p - 1, p$ and $p + 1$. Thus $p \not\equiv 1, 0, -1 \pmod q$. Hence (c) follows from (a). □

A prime p such that also $2p + 1$ is a prime, is called a *Sophie Germain prime*. The first seven Sophie Germain primes are 2, 3, 5, 11, 23, 29, and 41. Among the first 100,000 primes there are 9,667 Sophie Germain primes. It is conjectured that there are infinite many Sophie Germain primes.

Lemma 12.3.2. [**an+bn**] *Let a, b and n be integers with n odd. Define*

$$f_n : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto \sum_{i=0}^{n-1} (-1)^i a^i b^{n-1-i} = a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ldots + a^2 b^{n-3} - ab^{n-2} + b^{n-1}$$

Then

(a) [**d**] $f_n(a, b) = f_n(b, a)$.

(b) [**a**] $a^n + b^n = (a + b) f_n(a, b)$.

(c) [**b**] *If t is an integer with $a + b \equiv 0 \pmod t$, then $f_n(a, b) \equiv nb^{n-1} \pmod t$.*

(d) [**e**] *If t is an integer with $b \equiv 0 \pmod t$, then $f_n(a, b) \equiv a^{n-1} \pmod t$.*

(e) [**c**] *If a and b are coprime, then $\gcd(a + b, f_n(a, b))$ divides n.*

Proof. (a)

$$f_n(a, b) = \sum_{i=0}^{n-1} (-1)^i a^i b^{n-1-i} \overset{\text{j=n-1-i}}{=} \sum_{j=0}^{n-1} (-1)^{n-1-j} a^{n-1-j} b^j \overset{n-1 \text{ even}}{=} \sum_{j=0}^{n-1} (-1)^j b^j a^{n-1-j} = f_n(b, a).$$

(b) Just apply the formula $b^n - a^n = (b - a) \sum_{i=0}^{n-1} b^i a^{n-1-i}$ to $-a$ and b in place of a and b:

$$a^n + b^n = b^n - (-a)^n = (b - (-a)) \sum_{i=0}^{n-1} b^{n-1-i} (-a)^i = (b + a) f_n(a, b)$$

(c) Since $a + b \equiv 0 \pmod t$, $-a \equiv b \pmod t$ and so

$$f_n(a, b) \equiv \sum_{i=0}^{n-1} (-a)^i b^{n-1-i} \equiv \sum_{i=0}^{n-1} b^i b^{n-1-i} \equiv \sum_{i=0}^{n-1} b^{n-1} \equiv nb^{n-1} \pmod t$$

(d) Since $b \equiv 0 \pmod t$, $b^{n-1-i} \equiv 0 \pmod t$ for all $0 \leq i < n-1$ and so $f(a, b) \equiv (-1)^{n-1} a^{n-1} b^0 \equiv a^{n-1} \pmod t$.

(e) Put $t = \gcd(a+b, f_n(a,b))$. Then $f_n(a,b) \equiv 0 \pmod t$ and $a+b \equiv 0 \pmod t$. Hence (c) gives

$$(*) \qquad 0 \equiv f_n(a,b) \equiv nb^{n-1} \pmod t$$

Suppose p is a prime dividing t and b. Since $t \mid f_n(a,b)$, (b) implies $p \mid a^n + b^n$. So p divides $(a^n + b^n) - b^n = a^n$ and p divides a and b, a contradiction. Hence t and b are coprime. By (*) $t \mid nb^{n-1}$ and so $t \mid n$. □

Theorem 12.3.3 (Sophie Germain)**.** [**fermat for prime**] *Let p be an odd prime and suppose there exists an odd prime q such that the following two statements hold:*

(i) [**i**] *If $a^p + b^p + c^p \equiv 0 \pmod q$ for some $a, b, c \in \mathbb{Z}$, then q divides one of a, b, c.*

(ii) [**ii**] *If $a \in \mathbb{Z}$, then $p \neq a^p \pmod q$.*

If a, b and c are integers coprime to p, then

$$a^p + b^p + c^p \neq 0$$

Proof. Suppose for a contradiction that a, b and c are integers coprime to p with

$$(1) \qquad a^p + b^p + c^p = 0.$$

As usual we may assume that a, b and c are pairwise coprime.
Define f_p as in 12.3.2. Then by 12.3.2(b)

$$(2) \qquad (-a)^p = -a^p = b^p + c^p = (b+c)f_p(b,c)$$

Put $t = \gcd(b+c, f_p(b,c))$. Since b and c are coprime, 12.3.2(e) implies $t \mid p$. By (2) $t \mid b^p + c^p = -a^p$. Since $\gcd(a,p) = 1$ we conclude that $t = 1$. Thus

$$(3) \qquad b + c \text{ is coprime to } f_p(b,c).$$

From (2), (3) and 3.1.7 we conclude that there exist integers r and u with

$$(4) \qquad b + c = r^p, \quad f_p(b,c) = u^p, \text{ and } -a = ru.$$

By symmetry in a, b and c, there also exist integers s, t, v and w with

$$(5) \qquad a + c = s^p, \quad f_p(a,c) = v^p, \text{ and } -b = sv,$$

and

$$(6) \qquad a + b = t^p, \quad f_p(a,b) = w^p, \text{ and } -c = tw.$$

We now consider the above equations modulo q. From (1) modulo q and the assumption (i) we conclude that q divides one of a,b and c. Without loss q divides c. Observe that

$$r^p + s^p + (-t)^p \equiv r^p + s^p - t^p \equiv (b+c) + (a+c) - (a+b) \equiv 2c \equiv 0 \pmod q$$

and so by (i), q must divide one of r, s and t. If q divides r, then q also divides $b = r^p - c$, a contradiction since b and c are coprime. By symmetry, q does not divide s and so q divides t. Hence q divides $a + b = t^p$ and so $a + b \equiv 0 \pmod q$. Thus by (6) and 12.3.2(c),

$$w^p \equiv f_p(a,b) \equiv pb^{p-1} \pmod q \tag{7}$$

and since $c \equiv 0 \pmod q$, (4) and 12.3.2(d) give

$$u^p \equiv f_p(b,c) \equiv b^{p-1} \pmod q \tag{8}$$

If q divides u, it also divides $a = -ru$. But this is a contradiction, since q divides c and a and c are coprime. Thus there exist an integer $\tilde{u}$ with $u\tilde{u} \equiv 1 \pmod q$ and so by (8) $b^{p-1}\tilde{u}^p \equiv (u\tilde{u})^p \equiv 1 \pmod q$. Hence

$$(w\tilde{u})^p \equiv w^p\tilde{u}^p \overset{(7)}{\equiv} pb^{p-1}\tilde{u}^p \equiv p \pmod q$$

But this contradicts (ii). $\square$

Chapter 13

Continued Fractions

13.1 The Continued Fraction of a Real Number

Definition 13.1.1. [**def:simple sequence of real**] *Let α be a real number. We will inductively define $k \in \mathbb{Z}^+ \cup \{\infty\}$ and the (finite or infinite) sequences of real numbers*

$$(\alpha_n)_{n=0}^{k-1}, \quad (\beta_n)_{n=0}^{k-1} \quad \textit{and} \quad (q_n)_{n=0}^{k-1}$$

as follows:

$$\alpha_0 = \alpha$$

and if α_n has already been defined put

$$q_n = \lfloor \alpha_n \rfloor \qquad \textit{and } \beta_n = \alpha_n - q_n.$$

If $\beta_n = 0$, put $k = n+1$ and so all terms of the three sequences have been defined.
If $\beta_n \neq 0$, put $\alpha_{n+1} = \frac{1}{\beta_n}$ and proceed inductively.
If the inductive definition does not terminate in finitely many steps put $k = \infty$

The sequence $(q_n)_{n=0}^{k-1}$ is called the simple sequence associated to α.

Lemma 13.1.2. [**simple sequence of real**] *Let $\alpha \in \mathbb{R}$ and use the notation from 13.1.1 Let $0 \leq n < k$. Then*

(a) [**a**] *$q_n \in \mathbb{Z}$, $0 \leq \beta_n < 1$ and $\alpha_n = q_n + \beta_n \approx q_n$*

(b) [**b**] *If $n+1 < k$, then $\alpha_n = q_n + \frac{1}{\alpha_{n+1}} \approx q_n + \frac{1}{q_{n+1}}$*

(c) [**c**] *If $n \geq 1$, then $\beta_{n-1} > 0$, $\alpha_n > 1$ and $q_n \geq 1$.*

(d) [**d**] *If $1 < k < \infty$, then $q_{k-1} > 1$.*

Proof. (a) We have $q_n = \lfloor \alpha_n \rfloor$ and so $q_n \in \mathbb{Z}$ and $q_n \leq \alpha_n < q_n + 1$. Since $\beta_n = \alpha_n - q_n$ we get $0 \leq \beta_n < 1$ and $\alpha_n = q_n + \beta_n$.

(b) Since $n+1 < k$, α_{n+1} is defined and $\alpha_{n+1} = \frac{1}{\beta_n}$. So (b) follows from (a).

(c) Since $1 \leq n < k$, $\beta_{n-1} \neq 0$ and so by (a) $0 < \beta_{n-1} < 1$. Thus $\alpha_n = \frac{1}{\beta_{n-1}} > 1$ and $q_n = \lfloor \alpha_n \rfloor \geq 1$. (d) Since $k < \infty$, $\beta_{k-1} = 0$ and so $q_{k-1} = \alpha_{k-1}$. Since $k-1 > 0$, (c) gives $\alpha_{k-1} > 1$ and so (d) is proved. □

In view of the preceeding lemma we have

$$\alpha = \alpha_0 = q_0 + \frac{1}{\alpha_1} \approx q_0 + \frac{1}{q_1}$$

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\alpha_2}} \approx q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}$$

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\alpha_3}}} \approx q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}}$$

Example 13.1.3. [**ex:continued fraction of sqrt 2**] *Compute the simple sequence associated to* $\sqrt{2}$.

Let $\alpha = \sqrt{2}$. Then $q_0 = \lfloor \sqrt{2} \rfloor = 1$ and so $\beta_0 = \sqrt{2} - 1$. Thus

$$\alpha_1 = \frac{1}{\beta_0} = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} = \frac{\sqrt{2}+1}{2-1} = \sqrt{2}+1$$

Hence $q_1 = \lfloor \alpha_1 \rfloor = \lfloor \sqrt{2}+1 \rfloor = 2$ and $\beta_1 = \alpha_1 - q_1 = (\sqrt{2}+1) - 2 = \sqrt{2} - 1 = \beta_0$
It follows that $\alpha_i = \alpha_1 = \sqrt{2} - 1$, $\beta_i = \beta_0 = \sqrt{2} - 1$ and $q_i = q_1 = 2$ for all $i \geq 1$. Thus

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \dots}}}}$$

The first few approximations for $\sqrt{2}$ are
1, $1 + \frac{1}{2} = \frac{3}{2}$, $1 + \cfrac{1}{2 + \cfrac{1}{2}} = 1 + \frac{1}{\frac{5}{2}} = 1 + \frac{2}{5} = \frac{7}{5}$ and $1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}} = 1 + \cfrac{1}{2 + \cfrac{2}{5}} = 1 + \frac{5}{12} = \frac{17}{12}$.

13.2 Simple Sequences

Definition 13.2.1. [**def:continued**] *Let* $k \in \mathbb{N} \cup \{\infty\}$ *and* $(q_0)_{n=0}^{k-1} = q_0, q_1, \dots q_n, \dots$ *be sequence of* k *real numbers such that* $q_i \geq 1$ *for all* $1 \leq i < k$. *For* $0 \leq n < k$ *define* $[q_0, q_1, \dots, q_n]$ *inductively by*

$$[q_0] = q_0$$

and if $n > 0$

$$[q_0, q_1, \dots, q_n] = q_0 + \frac{1}{[q_1, q_2, \dots, q_n]}$$

The sequence

$$[q_0], [q_0, q_1], [q_0, q_1, q_2], \ldots, [q_0, q_1, \ldots, q_n], \ldots$$

is called the continued fraction *associated to* $q_0, q_1, q_2 \ldots, q_n$.

If this sequence converges we denote its limit by

$$[q_n]_{n=0}^{k-1} \text{ or } [q_0, q_1, q_2, \ldots, q_n, \ldots]$$

Suppose in addition that $q_n \in \mathbb{Z}$ *for all* $0 \leq n < k$ *and that if* k *is finite and* $k > 1$, *then* $q_{k-1} > 1$. *Then* $(q_n)_{n=0}^{k-1}$ *is called a* simple sequence *and its continued fraction is called a* simple continued fraction.

Note that

$$[q_0, q_1, \ldots, q_n] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cfrac{\ddots \ddots \ddots}{q_{n-2} + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}}$$

Lemma 13.2.2. [**alphai for alpha**] *Let* $\alpha \in \mathbb{R}$ *and let* $(q_n)_{n=0}^{k-1}$,$(\beta_n)_{n=0}^{k-1}$ *and* $(\alpha_n)_{n=0}^{k-1}$ *be as in 13.1.2. Then*

(a) [**a**] $(q_n)_{n=0}^{k-1}$ *is a simple sequence.*

(b) [**b**] *For all* $0 \leq i \leq j < k$, $\alpha_i = [q_i, q_{i+1}, \ldots, q_{j-1}, \alpha_j]$.

(c) [**c**] *For all* $0 \leq j < k$, $\alpha = [q_0, q_1, \ldots, q_{j-1}, \alpha_j]$.

Proof. (a) By 13.1.2(a), $q_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$. By 13.1.2(c), $q_n \geq 1$ for all $n \in \mathbb{Z}^+$, and by 13.1.2(d), $q_{k-1} > 1$ if $1 \leq l < \infty$, so $(q_n)_{n=0}^{\infty}$ is indeed a simple sequence.

(b) The proof is by induction on $j - i$. If $j - i = 0$, then $i = j$ and $\alpha_i = [\alpha_i]$ and so (b) holds in this case. So suppose that $j - i > 0$ and so $i < i + 1 \leq j < k$. By 13.1.2(b) and induction

$$\alpha_i = q_i + \frac{1}{\alpha_{i+1}} = q_i + \frac{1}{[q_{i+1}, \ldots, q_{j-1}, \alpha_j]} = [q_i, q_{i+1}, \ldots . q_{j-1}, \alpha_j]$$

(c) Since $\alpha = \alpha_0$, this is the special case $i = 0$ of (a). □

Lemma 13.2.3. [**alt def continued**] *Let* $(q_n)_{n=0}^{k-1}$ *be a simple sequence and let* $0 \leq l \leq n < k$. *Then*

$$[q_0, q_1, \ldots, q_{l-1}, [q_l, q_{l+1}, \ldots q_n]] = [q_0, q_1, \ldots, q_n]$$

Proof. If $l = 0$ there is nothing to prove.

So suppose $l > 0$ and assume inductively that $[q_1, \ldots q_{l-1}, [q_l, q_{l+1}, \ldots q_n]] = [q_1, q_2, \ldots, q_n]$. Then

$$\begin{aligned}
[q_0, q_1, \ldots, q_n] &= q_0 + \tfrac{1}{[q_1, q_2, \ldots, q_n]} \\
&= q_0 + \tfrac{1}{[q_1, q_2, \ldots, q_{l-1}, [q_l \ldots, q_n]]} \\
&= [q_0, q_1, \ldots, q_{l-1}, [q_l, q_{l+1}, \ldots q_n]]
\end{aligned}$$

□

Lemma 13.2.4. [**basic continued**] *Let $(q_n)_{n=0}^{k-1}$ be a simple sequence. Inductively define*

$$a_{-2} = 0, a_{-1} = 1, a_{n+1} = q_{n+1}a_n + a_{n-1}, -1 \leq n < k-1$$

and

$$b_{-2} = 1, b_{-1} = 0, b_{n+1} = q_{n+1}b_n + b_{n-1}, -1 \leq n < k-1$$

Let α be a real number with $\alpha \geq 1$.

(a) [**c**] *$a_n \in \mathbb{Z}$ and $b_n \in \mathbb{Z}$ for all $-2 \leq n < k$.*

(b) [**d**] *The first few terms of $(a_n)_{n=-2}^{k-1}$ and $(b_n)_{n=-2}^{k-1}$ are*

$$\begin{array}{lccccccc}
a_n: & 0 & 1 & q_0 & q_1q_0+1 & q_2q_1q_0+q_2+q_0 & \ldots \\
b_n: & 1 & 0 & 1 & q_1 & q_2q_1+1 & \ldots
\end{array}$$

(c) [**a**] *$[q_0, q_1, \ldots, q_n, \alpha] = \frac{\alpha a_n + a_{n-1}}{\alpha b_n + b_{n-1}}$ for all $n \geq -1$.*

(d) [**b**] *$[q_0, q_1, \ldots q_n] = \frac{a_n}{b_n}$ for all $n \geq 0$.*

Proof. (a) Observe that $a_{-2}, a_{-1}, b_{-2}, b_{-1} \in \mathbb{Z}$. Since $q_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$, (a) follows by induction on n.

(b) Readily verified.

(c) For $n = -1$ the left hand side is $[\alpha] = \alpha$. The right hand side is $\frac{\alpha \cdot 1 + 0}{\alpha \cdot 0 + 1} = \alpha$. Hence (c) holds for $n = -1$. Suppose (c) holds for n, then

$$\begin{aligned}
[q_0, \ldots, q_n, q_{n+1}, \alpha] &\overset{13.2.3}{=} [q_0, \ldots q_n, [q_{n+1}, \alpha]] = [q_0, \ldots q_n, q_{n+1} + \tfrac{1}{\alpha}] \\
&= \frac{(q_{n+1} + \frac{1}{\alpha})a_n + a_{n-1}}{(q_{n+1} + \frac{1}{\alpha})b_n + b_{n-1}} = \frac{\alpha q_{n+1}a_n + a_n + \alpha a_{n-1}}{\alpha q_{n+1}b_n + b_n + \alpha b_{n-1}} \\
&= \frac{\alpha(q_{n+1}a_n + a_{n-1}) + a_n}{\alpha(q_{n+1}b_n + b_{n-1}) + b_n} = \frac{\alpha a_{n+1} + a_n}{\alpha b_{n+1} + b_n}
\end{aligned}$$

So (c) also hold for $n + 1$.

(d) Let $n \geq -1$. Applying (c) with $\alpha = q_{n+1}$ in (c) gives

$$[q_0, q_1, \ldots, q_n, q_{n+1}] = \frac{q_{n+1}a_n + a_{n-1}}{q_{n+1}b_n + b_{n-1}} = \frac{a_{n+1}}{b_{n+1}}$$

So (d) holds for all $n \geq 0$. □

Lemma 13.2.5. [**between**]

(a) [**a**] *Let x, y, s, t be real number with $s + t = 1$, $0 < s, t < 1$ and $x \neq y$. Then $tx + sy$ lies strictly between x and y, that is either $x < sx + ty < y$ or $y < sx + ty < x$.*

(b) [**b**] *Let a, b, c, d be real numbers with b and d positive and $\frac{a}{b} \neq \frac{c}{d}$ Then $\frac{a+c}{b+d}$ lies strictly between $\frac{a}{b}$ and $\frac{c}{d}$.*

Proof. (a) We may assume that $x < y$. Then

$$x = (s + t)x = sx + tx < sx + ty < sy + ty = (s + t)y = y.$$

(b) Note that $\frac{a+b}{c+d} = \frac{b}{b+d}\frac{a}{b} + \frac{d}{b+d}\frac{c}{d}$. Also $\frac{b}{b+d} + \frac{d}{b+d} = 1$ and so (b) follows from (a).

□

Lemma 13.2.6. [**converge**] *Let $(q_n)_{n=0}^{k-1}$ be a simple sequence.*

(a) [**a**] *For all $-2 \leq n < k - 1$, $a_n b_{n+1} - a_{n+1} b_n = (-1)^{n+1}$*

(b) [**b**] *For all $-2 \leq n < k$, $\gcd(a_n, b_n) = 1$.*

(c) [**c**] *$-1 < b_{-1} = 0 < b_0 = 1 \leq b_1$ and for all $1 \leq n < k$, $n \leq b_n < b_{n+1}$.*

(d) [**f**] *For all $0 \leq n < k$, $\frac{a_n}{b_n} - \frac{a_{n+1}}{b_{n+1}} = \frac{(-1)^{n+1}}{b_n b_{n+1}}$.*

(e) [**d**] $\frac{a_0}{b_0} < \frac{a_2}{b_2} < \frac{a_4}{b_4} < \ldots < \frac{a_{2n}}{b_{2n}} < \ldots < \ldots < \frac{a_{2n+1}}{b_{2n+1}} < \ldots \frac{a_5}{b_5} < \frac{a_3}{b_3} < \frac{a_1}{b_1}$.

(f) [**e**] *All infinite simple continued fractions converge.*

Proof. (a) $a_{-2}b_{-1} - a_{-1}b_{-2} = 0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{-1}$. Also

$$a_n b_{n+1} - a_{n+1} b_n = a_n(q_{n+1} b_n + b_{n-1}) - (q_{n+1} a_n + a_{n-1}) b_n = -(a_{n-1} b_n - a_n b_{n-1})$$

So (a) is true by induction.

(b) Follows from (a).

(c) By 13.2.4(b), $-1 < 0 = b_{-1} < 1 = b_0 \leq q_1 = b_1$. Suppose $n \geq 1$, $b_n \geq n$ and $b_{n-1} > 0$ (and observe that this is true for $n = 1$) then

$$b_{n+1} = q_{n+1} b_n + b_{n-1} > q_{n+1} b_n \geq b_n \geq n$$

Thus (c) holds by induction on n.

(d) By (c), $b_n \neq 0 \neq b_{n+1}$. So (c) follows from (a) by dividing by $b_n b_{n+1}$.

(e) By (d) $\frac{a_0}{b_0} - \frac{a_1}{b_1} = -1$ and so $\frac{a_0}{b_0} < \frac{a_1}{b_1}$. Let $n \geq 1$. By (e) $\frac{a_n}{b_n} \neq \frac{a_{n-1}}{b_{n-1}}$. Also

$$\frac{a_{n+1}}{b_{n+1}} = \frac{q_{n+1} a_n + a_{n-1}}{q_{n+1} b_n + b_{n-1}}$$

and so by 13.2.5(b), $\frac{a_{n+1}}{b_{n+1}}$ lies strictly between $\frac{q_{n+1} a_n}{q_{n+1} b_n} = \frac{a_n}{b_n}$ and $\frac{a_{n-1}}{b_{n-1}}$. (e) now follows by induction.

(f) By (d) and (c) $|\frac{a_n}{b_n} - \frac{a_{n+1}}{b_{n+1}}| = \frac{1}{b_n b_{n+1}} \leq \frac{1}{n(n+1)}$. Let $n < m < k$. By (e) $\frac{a_m}{b_m}$ is between $\frac{a_n}{b_n}$ and $\frac{a_{n+1}}{b_{n+1}}$. Thus

$$\left|\frac{a_n}{b_n} - \frac{a_m}{b_m}\right| \leq \left|\frac{a_n}{b_n} - \frac{a_{n+1}}{b_{n+1}}\right| \leq \frac{1}{n(n+1)}$$

Hence $(\frac{a_n}{b_n})_{n=0}^{\infty}$ is a Cauchy sequence and so converges. □

Lemma 13.2.7. [**alpha i**] *Let $(q_n)_{n=0}^{k-1}$ be a simple sequence. Put $\alpha_i = [q_n]_{n=i}^{k-1}$. Then*

(a) [**a**] $\alpha_i = [q_i, \ldots, q_{j-1}, \alpha_j]$ *for all* $0 \le i \le j < k$.

(b) [**c**] $[q_i, \ldots, q_j] \ge 1$ *for all* $1 \le i \le j < k$.

(c) [**b**] $\alpha_i > 1$ *for all* $1 \le i < k$.

Proof. (a) If k is finite, this follows from 13.2.3. So we may suppose $k = \infty$. Since $\alpha_i = [\alpha_i]$, (c) holds for $i = j$. By induction on $j - i$ assume that $\alpha_{i+1} = [q_{i+1}, \ldots, q_{j-1}, \alpha_j]$. Then

$$\begin{array}{rcccc}
\alpha_i & = & \lim\limits_{l\to\infty}[q_i, q_{i+1}, \ldots, q_l] & = & \lim\limits_{l\to\infty}\left(q_i + \dfrac{1}{[q_{i+1}, \ldots, q_l]}\right) \\
 & = & q_i + \dfrac{1}{\lim\limits_{l\to\infty}[q_{i+1}, \ldots, q_l]} & = & q_i + \frac{1}{\alpha_{i+1}} \\
 & = & q_i + \frac{1}{[q_{i+1}, \ldots, q_{j-1}, \alpha_j]} & = & [q_i, \ldots, q_{j-1}, \alpha_j]
\end{array}$$

(b) Since $[q_i] = q_i \ge 1$, (b) holds for $i = j$. So suppose $i < j$ and by induction on $j - i$ that $[q_{i+1}, \ldots . q_j] \le 1$. Then $\frac{1}{[q_{i+1}, \ldots, q_j]} > 0$. Thus

$$[q_i, \ldots, q_j] = q_i + \frac{1}{[q_{i+1}, \ldots, q_j} > q_i \ge 1$$

(c) Let $1 \le i < k$. By (c), $[q_i, \ldots, q_j] \ge 1$ and so also $\alpha_i = \lim_{j\to\infty}[q_i, \ldots, q_j] \ge 1$. If $i < k-1$, then by (a) $\alpha_i = [q_i, \alpha_{i+1}] = q_i + \frac{1}{\alpha_{i+1}} > q_i \ge 1$. If $i = k-1$, then $\alpha_{k-1} = q_{k-1} > 1$ by definition of a simple sequence. □

Lemma 13.2.8. [**simple of limit**] *Let $(q_n)_{n=0}^{k-1}$ be a simple sequence and put $\alpha = [q_n]_{n=0}^{k-1}$. Then $(q_n)_{n=0}^{k-1}$ is the simple sequence associated to α.*

Proof. Define $\alpha_i = [q_n]_{n=i}^{k-1}$ and let $(\tilde{q}_i)_{i=0}^{\tilde{k}-1}$ be the simple sequence associated to α. So there exist $\tilde{\alpha}_i, \tilde{\beta}_{i-1} \in \mathbb{R}$ with $\tilde{\alpha}_0 = \alpha$, $\tilde{\alpha}_i = \tilde{q}_i + \tilde{\beta}_i$ and $\tilde{\beta}_i \in [0, 1)$ for all $0 \le i < \tilde{k}$. Moreover, if $0 < i < \tilde{k} - 1$, then $\tilde{\beta}_i \ne 0$ and $\tilde{\alpha}_{i+1} = \frac{1}{\tilde{\beta}_i}$ and if $\tilde{k}$ is finite, then $\tilde{\beta}_{\tilde{k}-1} = 0$.

Let $0 \le i < k$. We will first show

1°. [**1**] *Suppose $i < \tilde{k}$ and $\alpha_i = \tilde{\alpha}_i$. Then*

(a) [**a**] $q_i = \tilde{q}_i$.

(b) [**b**] *If $i < k-1$, then $i + 1 < \tilde{k}$ and $\alpha_{i+1} = \tilde{\alpha}_{i+1}$.*

(c) [**c**] *If $i = k-1$, then $k = \tilde{k}$.*

Suppose $i < k-1$. Then by 13.2.7(b), $\tilde{\alpha}_i = \alpha_i = [q_i, \alpha_{i+1}] = q_i + \frac{1}{\alpha_{i+1}}$. By 13.2.7(b), $\alpha_{i+1} > 1$ and so $\frac{1}{\alpha_{i+1}} < 1$. It follows that $\tilde{q}_i = q_i$ and $\tilde{\beta}_i = \frac{1}{\alpha_{i+1}} \ne 0$. Thus $\tilde{k} \ne i+1$, $\tilde{k} > i+1$ and $\tilde{\alpha}_{i+1} = \frac{1}{\tilde{\beta}_i} = \alpha_{i+1}$.

Suppose that $i = k-1$. Then $\tilde{\alpha}_{k-1} = \alpha_{k-1} = [q_n]_{n=k-1}^{k-1} = q_{k-1}$. Thus $\tilde{q}_{k-1} = q_i$, $\beta_{k-1} = 0$ and $\tilde{k} = k$. so (1°) is proved.

2°. [**2**] *Let $0 \le i < k$. then $i < \tilde{k}$ and $\alpha_i = \tilde{\alpha}_i$.*

Note that (2°) holds for $i = 0$. So (2°) follows from (1°) and induction on i.

If k is finite, then by (2°) we can apply (1°) to $i = k - 1$ and so $\tilde{k} = k$. If k is infinite, (2°) shows that $\tilde{k} > i$ for all $i \in \mathbb{N}$ and so $\tilde{k} = \infty$. In either case (1°) and (2°) now show $q_n = \tilde{q}_n$ for all $0 \leq i < k$ and so that $(q_n)_{n=0}^{k-1} = (\tilde{q}_n)_{n=0}^{\tilde{k}-1}$. □

Lemma 13.2.9. [**rational-finite**] *Let $\alpha \in \mathbb{R}$ and $(q_n)_{n=0}^{k-1}$ the associate simple sequence.*

(a) [**a**] *If k is finite, then α is rational and $\alpha = [q_n]_{n=0}^{k-1}$.*

(b) [**b**] *α is rational if and only if k is finite.*

Proof. Let $(\alpha_n)_{n=0}^{k-1}$ be as in 13.1.1.

(a) Suppose k is finite. Then $\beta_{k-1} = 0$ and so $\alpha_{k-1} = q_{k-1} + \beta_{k-1} = q_{k-1} \in \mathbb{Z}$. For $0 < i < k-1$, $\alpha_i = q_i + \frac{1}{\alpha_i}$ and downwards induction on i shows that $\alpha_i \in \mathbb{Q}$ for all $0 \leq i < k$. Thus $\alpha = \alpha_0 \in \mathbb{Q}$. By 13.2.2, $\alpha = [q_0, \ldots, q_{k-2}, \alpha_{k-1}] = [q_0, \ldots, q_{k-1}]$ and so (a) holds.

(b) If k is finite, α is rational by (a). Suppose next that α is rational and say $\alpha = \frac{x}{y}$ with $x \in \mathbb{Z}, y \in \mathbb{Z}^+$.

By the division algorithm, $x = qy + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < y$. Then

$$q_0 = \lfloor \alpha \rfloor = \left\lfloor \frac{qy + r}{y} \right\rfloor = \left\lfloor q + \frac{r}{y} \right\rfloor = q.$$

If $r = 0$, then the continued fraction of α is (q_0) and so is finite. Also $\alpha = q_0 = [q_0]$.

So suppose $r \neq 0$. Then

$$\alpha_1 = \frac{1}{\beta_1} = \frac{1}{\alpha - q_0} = \frac{1}{\frac{r}{y}} = \frac{y}{r}.$$

Since $0 < r < y$ we conclude by induction on y that the simple sequence of α_1 is finite. Observe that the simple sequence associated to α_1 is $(q_n)_{n=1}^{k-1}$ and so k is finite. □

Lemma 13.2.10. [**irrational**] *Let $\alpha \in \mathbb{R} \backslash \mathbb{Q}$. Then the continued fraction associated to α converges to α.*

Proof. Let $(q_n)_{n=0}^{k-1}$ and $(\alpha_n)_{n=0}^{k-1}$ be as in 13.1.1 By 13.2.9, $k = \infty$. Let $0 \leq n < \infty$ By 13.2.2(c), $\alpha = [q_0, \ldots, q_n, \alpha_{n+1}]$ and so by 13.2.4(a),

$$\alpha = [q_0, \ldots, q_n, \alpha_{n+1}] = \frac{\alpha_{n+1} a_n + a_{n-1}}{\alpha_{n+1} b_n + b_{n-1}}.$$

So by 13.2.5, α lies between $\frac{a_n}{b_n}$ and $\frac{a_{n-1}}{b_{n-1}}$. By 13.2.4(d), the sequence $(\frac{a_n}{b_n})_{n=0}^{\infty}$ is the continued fraction associated to α and so by 13.2.6(f) converges to some $\tilde{\alpha} \in \mathbb{R}$. Then $\tilde{\alpha} = \lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{a_{n-1}}{b_{n-1}}$ Since α lies between $\frac{a_n}{b_n}$ and $\frac{a_{n-1}}{b_{n-1}}$. this gives $\alpha = \tilde{\alpha}$ and the lemma is proved. □

13.3 Periodic Simple Sequences

Notation 13.3.1. [**not:periodic**] *In this section, $(q_n)_{n=0}^{k-1}$ is simple sequence, $\alpha_i := [q_n]_{n=i}^{k-1}$ and $\alpha = \alpha_0$. Note that by 13.2.8 $(q_n)_{n=0}^{k-1}$ is the simple sequence associated to α.*

Definition 13.3.2. [**def:periodic**] *A simple sequence $(q_n)_{n=0}^{k-1}$ is called* periodic *if $k = \infty$ and there exist $l \in \mathbb{N}$ and $m \in \mathbb{Z}^+$ with $q_i = q_{i+m}$ for all $l \leq i < \infty$.*

Lemma 13.3.3. [**easy periodic**] *The simple sequence $(q_n)_{n=0}^{k-1}$ is periodic if and only if $\alpha_l = \alpha_j$ for some $0 \le l < j < k$.*

Proof. Suppose first that $(q_n)_{n=0}^{k-1}$ is periodic. Then $k = \infty$ and there exists $l \in \mathbb{N}$ and $m \in \mathbb{Z}^+$ with $q_i = q_{i+m}$ for all $l \le i < k$. The $(q_n)_{n=l}^{\infty} = (q_n)_{n=l+m}^{\infty}$ and so $\alpha_l = \alpha_{l+m}$.

Suppose next that $\alpha_l = \alpha_j$ for some $0 \le l < j < k$. Then

$$[q_n]_{n=l}^{k-1} = \alpha_l = \alpha_j = [q_n]_{n=j}^{k-1}$$

Hence by 13.2.8 $[q_n]_{n=l}^{k-1}$ and $[q_n]_{n=j}^{k-1}$ both are equal to the simple sequence associated to $\alpha_l = \alpha_j$. Thus $(q_n)_{n=l}^{k-1} = (q_n)_{n=j}^{k-1}$. In particular, those two sequences have length and so $k - l = k - j$. Since $l \neq j$ we conclude that $k = \infty$. Moreover, $q_n = q_{n+(j-i)}$ for all $l \le n < k$ and thus $(q_n)_{n=0}^{k-1}$ is periodic. □

Lemma 13.3.4. [**qd**] *Let $z \in \mathbb{Q}$ with $z > 0$ and $\sqrt{z} \notin \mathbb{Q}$. Define define*

$$\mathbb{Q}[\sqrt{z}] := \{x + y\sqrt{z} \mid x, y \in \mathbb{Q}\}/$$

(a) [**a**] *$\mathbb{Q}[\sqrt{z}]$ is a subfield of $\mathbb{R}$.*

(b) [**b**] *Let $x, y, \tilde{x}, \tilde{y} \in \mathbb{Q}$ with $x + y\sqrt{z} = \tilde{x} + \tilde{y}\sqrt{z}$. Then $x = \tilde{x}$ and $y = \tilde{y}$.*

(c) [**c**] *The map $\sigma : \mathbb{Q}[\sqrt{z}] \to \mathbb{Q}[\sqrt{z}], x + y\sqrt{z} \mapsto x - y\sqrt{z}$ is a field automorphism.*

Proof. Readily verified. □

Lemma 13.3.5. [**periodic**] *$(q_n)_{n=0}^{k-1}$ is periodic if and only if $\alpha = x + y\sqrt{z}$ for some $x, y, z \in \mathbb{Q}$ with $y \neq 0$, $z \ge 0$ and $\sqrt{z} \notin \mathbb{Q}$.*

Proof. Let $0 \le l < k$. Then by 13.2.7(a) and 13.2.4(c)

$$\alpha = [q_0, q_1, \ldots, q_{l-1}, \alpha_l] = \frac{\alpha_l a_{l-2} + a_{l-1}}{\alpha_l b_{l-1} + b_{l-2}}. \tag{1}$$

$\Longrightarrow$: Suppose first that $(q_n)_{n=0}^{\infty}$ is periodic. Then by definition of periodic, $k = \infty$ and so by 13.2.9, $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. By 13.3.3 $\alpha_l = \alpha_j$ for some $0 \le l < j < \infty$. Thus by 13.2.7(a),

$$\alpha_l = [q_l, \ldots, q_{j-1}, \alpha_j] = [q_l, \ldots, q_{j-1}, \alpha_l]$$

and so by 13.2.4(c) applied to the simple sequence $(q_{n+l})_{n=0}^{\infty}$

$$\alpha_l = \frac{r\alpha_l + s}{t\alpha_l + u}$$

for some $r, s, t, u \in \mathbb{Z}$. Multiplying with $t\alpha_l + u$ we get $t\alpha_l^2 + (u - r)\alpha_l - s = 0$. So α_l is the root of quadratic polynomial with coefficients in $\mathbb{Z}$. The quadratic formula now shows that $\alpha_l \in \mathbb{Q}[\sqrt{z}]$ for some $z \in \mathbb{Q}$.

Since $\mathbb{Q}[\sqrt{z}]$ is a subfield of $\mathbb{R}$ and since the a_i's and b_i's are integers we conclude from (1) also $\alpha \in \mathbb{Q}[\sqrt{z}]$. Thus $\alpha = x + y\sqrt{z}$ for some $x, y \in \mathbb{Q}$. Since $\alpha \notin \mathbb{Q}$, $y \neq 0$ and $\sqrt{z} \notin \mathbb{Q}$. Since $\alpha \in \mathbb{R}$, $z \ge 0$.

$\Longleftarrow$: Suppose next that $\alpha = x + y\sqrt{z}$ for some $x, y, z \in \mathbb{Q}$ with $y \neq 0$, $z \geq 0$ and $\sqrt{z} \notin \mathbb{Q}$. Then $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and so by 13.2.9, $k = \infty$. For $u = x, y, z$ let $u = \frac{u_1}{u_2}$ with $u_i \in \mathbb{Z}$ and $u_2 \neq 0$. Since $y \neq 0$, $y_1 \neq 0$. Replacing x_1 by $-x_1$ and x_2 be $-x_2$, if necessary, we may assume that $x_2 y_2 z_2$ is positive and so $x_2 y_1^2 y_2 z_2 = \sqrt{x_2^2 y_1^4 y_2^2 z_2^2}$. Then

$$\begin{aligned}\alpha = \frac{x_1}{y_1} + \frac{x_2}{y_2}\sqrt{\frac{z_1}{z_2}} = \frac{x_1 y_1 y_2^2 z_2 + (x_2 y_1^2 y_2 z_2)\sqrt{\frac{z_1}{z_2}}}{y_1^2 y_2^2 z_2} &= \frac{x_1 y_1 y_2^2 z_2 + \sqrt{\frac{z_1 x_2^2 y_1^4 y_2^2 z_2^2}{z_2}}}{y_1^2 y_2^2 z_2} \\ &= \frac{x_1 y_1 y_2^2 z_2 + \sqrt{x_2^2 y_1^4 y_2^2 z_1 z_2}}{y_1^2 y_2^2 z_2}\end{aligned}$$

Put $c_0 = x_1 y_1 y_2^2 z_2$, $d = x_2^2 y_1^4 y_2^2 z_1 z_2$ and $e_0 = y_1^2 y_2^2 z_2$. Then $c_0, d_0, e_0 \in \mathbb{Z}$, $e_0 \neq 0$ and

$$\alpha_0 = \alpha = \frac{c_0 + \sqrt{d}}{e_0}.$$

Since $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ we get $d > 0$ and $\sqrt{d} \notin \mathbb{Q}$. Note that e_0 divides c_0^2 and d_0. So $e_0 \mid d - c_0^2$. Inductively, define

$$c_{i+1} = q_i e_i - c_i \text{ and } e_{i+1} = \frac{c_{i+1} + \sqrt{d}}{\alpha_{i+1}}.$$

Then

$$\alpha_i = \frac{c_i + \sqrt{d}}{e_i} \quad \text{for all } i \in \mathbb{N}. \tag{2}$$

We will now show that

$$c_i \in \mathbb{Z}, e_i \in \mathbb{Z} \quad \text{and} \quad e_i \mid d - c_i^2 \quad \text{for all } i \in \mathbb{N} \tag{3}$$

This is true for $i = 0$ and suppose inductively it is true for i. Then q_i, e_i and c_i are integers and so also c_{i+1} is an integer. Note that $\alpha_i = [q_i, \alpha_{i+1}] = q_i + \frac{1}{\alpha_{i+1}}$ and so

$$\begin{aligned} e_{i+1} &= (c_{i+1} + \sqrt{d})\tfrac{1}{\alpha_{i+1}} &&= (c_{i+1} + \sqrt{d})(\alpha_i - q_i) \\ &= (c_{i+1} + \sqrt{d})(\tfrac{c_i + \sqrt{d}}{e_i} - q_i) &&= (c_{i+1} + \sqrt{d})\tfrac{c_i - e_i q_i + \sqrt{d}}{e_i} \\ &= (\sqrt{d} + c_{i+1})\tfrac{\sqrt{d} - c_{i+1}}{e_i} &&= \tfrac{d - c_{i+1}^2}{e_i}. \end{aligned}$$

Since $c_{i+1} = q_i e_i - c_i$, we have $c_{i+1} \equiv -c_i \pmod{e_i}$. Since e_i divides $d - c_i^2$ we get $d - c_{i+1}^2 \equiv d - c_i^2 \equiv 0 \pmod{e_i}$. Thus e_i divides $d - c_{i+1}^2$. We conclude that e_{i+1} is an integer and since $e_{i+1} e_i = d - c_{i+1}^2$, e_{i+1} divides $d - c_{i+1}^2$. Thus (3) is proved.

Next we will show that almost all e_i are positive. From (1) we get

$$\begin{aligned}
\alpha(\alpha_i b_{i-1} + b_{i-2}) &= \alpha_i a_{i-1} + a_{i-2}.\\
(\alpha b_{i-1} - a_{i-1})\alpha_i &= -(\alpha b_{i-2} - a_{i-2}).\\
\alpha_i &= -\tfrac{\alpha b_{i-2} - a_{i-2}}{\alpha b_{i-1} - a_{i-1}}.\\
\alpha_i &= -\tfrac{b_{i-2}}{b_{i-1}} \tfrac{\alpha - \frac{a_{i-2}}{b_{i-2}}}{\alpha - \frac{a_{i-1}}{b_{i-1}}}.
\end{aligned}$$

Let σ be the automorphism of $\mathbb{Q}[\sqrt{d}]$ with $\sigma(x + y\sqrt{d}) = x - y\sqrt{d})$ for all $x, y \in \mathbb{Q}$ (see 13.3.4). Applying σ to the last equation we obtain:

$$(*) \qquad \sigma(\alpha_i) = -\frac{b_{i-2}}{b_{i-1}} \frac{\sigma(\alpha) - \frac{a_{i-2}}{b_{i-2}}}{\sigma(\alpha) - \frac{a_{i-1}}{b_{i-1}}}.$$

Observe that

$$\lim_{i\to\infty} \frac{\sigma(\alpha) - \frac{a_{i-2}}{b_{i-2}}}{\sigma(\alpha) - \frac{a_{i-1}}{b_{i-1}}} = \frac{\sigma(\alpha) - \alpha}{\sigma(\alpha) - \alpha} = 1.$$

Thus there exists $N \in \mathbb{Z}^+$ with

$$(**) \qquad \frac{\sigma(\alpha) - \frac{a_{i-2}}{b_{i-2}}}{\sigma(\alpha) - \frac{a_{i-1}}{b_{i-1}}} > 0 \quad \text{for all } i \geq N.$$

Since b_i is positive for all $i > 0$, we conclude from (*) and (**) that $\sigma(\alpha_i) < 0$ for all $i \geq N$. As $\alpha_i \geq 1$ for all $i > 0$, this gives

$$0 < \alpha_i - \sigma(\alpha_i) = \frac{c_i + \sqrt{d}}{e_i} - \frac{c_i - \sqrt{d}}{e_i} = 2\frac{\sqrt{d}}{e_i} \quad \text{for all } i \geq N.$$

Thus $e_i > 0$ for all $i \geq N$.

Hence $0 < e_i e_{i+1} = d - c_{i+1}^2$ and so

$$(4) \qquad 0 < e_i \leq d \text{ and } c_{i+1}^2 \leq d \quad \text{for all } i \geq N.$$

Thus for $i > N$ there are only finitely many choices for the pair (e_i, c_i) and so also only finitely many choices for α_i. Since there are infinitely many $i \geq N$ this means that $\alpha_i = \alpha_j$ for some $N \leq i < j$. Thus by 13.3.3 the simple sequence $(q_n)_{n=0}^{\infty}$ is periodic. □

13.4 Pell's Equation

Theorem 13.4.1 (Pell's Equation)**.** [**pell**] *Let $d \in \mathbb{Z}^+$ and suppose d is not a square in $\mathbb{Z}^+$. Then there exist positive integers x and y with*

$$x^2 - dy^2 = 1.$$

Proof. We use the notations introduced in the proof of 13.3.5 for $\alpha = \sqrt{d}$. By (1) and (2) in that proof:

$$\sqrt{d} = \frac{\alpha_i a_{i-1} + a_{i-2}}{\alpha_i b_{i-1} + b_{i-2}} = \frac{\frac{c_i + \sqrt{d}}{e_i} a_{i-1} + a_{i-2}}{\frac{c_i + \sqrt{d}}{e_i} b_{i-1} + b_{i-2}} = \frac{(c_i + \sqrt{d})a_{i-1} + e_i a_{i-2}}{(c_i + \sqrt{d})b_{i-1} + e_i b_{i-2}}.$$

Multiplying with $(c_i + \sqrt{d})b_{i-1} + e_i b_{i-2}$ gives

$$\sqrt{d}\left((c_i + \sqrt{d})b_{i-1} + e_i b_{i-2}\right) = (c_i + \sqrt{d})a_{i-1} + e_i a_{i-2}$$

and so

$$db_{i-1} + (c_i b_{i-1} + e_i b_{i-2})\sqrt{d} = (c_i a_{i-1} + e_i a_{i-2}) + a_{i-1}\sqrt{d}.$$

Since $\sqrt{d} \notin \mathbb{Q}$, we conclude from 13.3.4(b) that

$$db_{i-1} = c_i a_{i-1} + e_i a_{i-2} \text{ and } a_{i-1} = c_i b_{i-1} + e_i b_{i-2}.$$

Subtracting b_{i-1}-times the first equation from a_{i-1}-times the second equation and using 13.2.6(a) yields:

$$\begin{aligned} a_{i-1}^2 - b_{i-1}^2 d &= a_{i-1} c_i b_{i-1} + a_{i-1} e_i b_{i-2} - b_{i-1} c_i a_{i-1} - b_{i-1} e_i a_{i-2} \\ &= -e_i(a_{i-2} b_{i-1} - a_{i-1} b_{i-2}) = -(-1)^{i-1} e_i = (-1)^i e_i. \end{aligned}$$

By (4) in 13.3.5 $0 < e_i \leq d$ for all $i \geq N$. Hence $\{(-1)^i e_i \mid i \in \mathbb{N}\}$ is a finite set. So there exists $e \in \mathbb{Z}$ with $e \neq 0$ such that

$$a_i^2 - b_i^2 d = e$$

for infinitely many $i \in \mathbb{N}$. By 13.2.6(b), $\gcd(a_i, b_i) = 1$. Since $(a_i, b_i) \neq (a_j, b_j)$ for $i \neq j$ and we conclude that the set

$$S := \{(u, v) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid u^2 - v^2 d = e, \gcd(u, v) = 1\}$$

is infinite. Define the relation $\approx$ on S by $(u_1, v_1) \approx (u_2, v_2)$ if $u_1 \equiv u_2 \pmod{e}$ and $v_1 \equiv v_2 \pmod{e}$. This is an equivalence relation with at most e^2 equivalence classes. Since S is infinite, one of the equivalence classes must by infinite. In particular, there exist distinct but equivalent (u_1, v_1) and (u_2, v_2) in S.

Put

$$x = \frac{u_1 u_2 - d v_1 v_2}{e} \text{ and } y = \frac{u_1 v_2 - v_1 u_2}{e}.$$

We have

$$u_1 u_2 - d v_1 v_2 \equiv u_1^2 - d v_1^2 \equiv e \equiv 0 \pmod{e}$$

and

$$u_1 v_2 - v_1 u_2 \equiv u_1 v_1 - v_1 u_1 \equiv 0 \pmod{e}.$$

So x and y are integers.

Also

$$x + y\sqrt{d} = \frac{(u_1u_2 - dv_1v_2) + (u_1v_2 - v_1u_2)\sqrt{d}}{e} = \frac{(u_1 - v_1\sqrt{d})(u_2 + v_2\sqrt{d})}{e}$$

and so

$$\begin{array}{rcccl} x^2 - y^2d & = & (x + y\sqrt{d})(x - y\sqrt{d}) & = & (x + y\sqrt{d})\sigma(x + y\sqrt{d}) \\ & = & \frac{(u_1 - v_1\sqrt{d})(u_2 + v_2\sqrt{d})}{e}\sigma\left(\frac{(u_1 - v_1\sqrt{d})(u_2 + v_2\sqrt{d})}{e}\right) & = & \frac{(u_1 - v_1\sqrt{d})(u_1 + v_1\sqrt{d})(u_2 + v_2\sqrt{d})(u_2 - v_2\sqrt{d})}{ee} \\ & = & \frac{(u_1^2 - v_1^2d)(u_2^2 - v_2^2d)}{e^2} & = & \frac{e \cdot e}{e^2} = 1. \end{array}$$

It remains to show that $x \neq 0$ and $y \neq 0$. If $x = 0$ we get $1 = x^2 - y^2d = -y^2d \leq 0$, a contradiction. Suppose $y = 0$, then $u_1v_2 = v_1u_2$. Since $\gcd(u_1, v_1) = 1$ this gives $u_1 \mid u_2$ and $v_1 \mid v_2$. As $\gcd(u_2, v_2) = 1$ we also have $u_2 \mid u_1$ and $v_2 \mid v_1$. The u_i and v_i are positive and so $u_1 = v_1$ and $u_2 = v_2$, a contradiction to $(u_1, v_1) \neq (u_2, v_2)$. Thus x and y are non-zero and the theorem is proved. $\square$

Appendix A

Euclidean Domains

Definition A.0.2. [**def:euclidean**]

(a) [**a**] *An integral domain is a commutative ring R with identity $1 \neq 0$ such that for all $a, b \in R$ with $ab = 0$ we have $a = 0$ or $b = 0$.*

(b) [**b**] *An Euclidean domain is an integral domain R together with a function $\delta : R \to \mathbb{N}$ such that for all $a, b \in R$:*

  (i) [**c**] *$\delta(a) = 0$ if and only if $a = 0_R$;*

  (ii) [**a**] *if $ab \neq 0$ then $\delta(ab) \geq \delta(b)$; and*

  (iii) [**b**] *if $b \neq 0$, then there exist q, r in R with*

$$a = qb + r \text{ and } \delta(r) < \delta(b).$$

  Such a δ is called an Euclidean function.

Definition A.0.3. [**def:divide int**] *Let R be an integral domain and $a, b \in R$.*

(a) [**a**] *We say that a* divides *b and write $a \mid b$ if $b = ra$ for some $r \in R$.*

(b) [**b**] *We say that a and b are* associate *and write $a \sim b$ if $a \mid b$ and $b \mid a$.*

(c) [**e**] *We say that a is* irreducible *if $a \neq 0$, a is not a unit and $a = bc$ with $b, c \in R$ implies that b or c is a unit.*

(d) [**f**] *We say that a is a* prime *if $a \neq 0$, a is not a unit and $a \mid bc$ with $b, c \in R$ implies $a \mid b$ or $a \mid c$.*

Proposition A.0.4 (Cancellation Law)**.** [**int and cancel**] *Let R be an integral domain and $a, b, c \in R$ with $a \neq 0$. Then*

$$\begin{array}{rrcl} & ab & = & ac \\ \iff & b & = & c \\ \iff & ba & = & ca \end{array}$$

Proof. Suppose $ab = ac$. Then $ab - ac = 0$ and so $a(b - c) = 0$. Since $a \neq 0$ and R is an integral domain, $b - c = 0$. Thus $b = c$.

If $b = c$ then clearly $ab = ac$.

Finally since R is commutative, $ba = ca$ implies $ab = ac$. □

Lemma A.0.5. [**easy unit**] *Let R be an integral domain and $a \in R$. The the following are equivalent*

(a) [**a**] *a is a unit.*

(b) [**b**] *$a \mid 1$.*

(c) [**c**] *$a \sim 1$.*

Proof. Suppose a is a unit. Then $ba = 1$ for some $r \in R$ and so $a \mid 1$.

Suppose $a \mid 1$. Since $a = 1a$, $1 \mid a$ and so $a \sim 1$.

Suppose $a \sim 1$. Then $a \mid 1$ and so $ab = 1$ for some $b \in R$. Thus a is a unit. □

Lemma A.0.6. [**unit and sim**] *Let R be an integral domain and $a, b \in R$.*

(a) [**a**] *If $b \neq 0$, then $b \sim ab$ if and only if a is a unit.*

(b) [**b**] *$a \sim b$ if and only if $a = ub$ for some unit u in R.*

Proof. (a) Suppose that a is a unit. Then $ca = 1$ for some $c \in R$. Thus $b = 1b = (ca)b = c(ab)$ and so $ab \mid b$. Clearly $b \mid ab$ and so $b \sim ab$.

Suppose that $b \sim ab$. Then $b = c(ab)$ for some $c \in R$ and so $1b = b = c(ab) = (ca)b$. By the Cancellation Law A.0.4, $ca = 1$. So a is a unit.

(b) Suppose first that $a \sim b$. Then $b \mid a$ and so $a = ub$ for some $u \in R$. If $b \neq 0$, then by (a) u is a unit. If $b = 0$, then also $a = 0$ and $a = 1b$. So in both cases $a = ub$ for a unit b in R.

Suppose next that $a = ub$ for a unit $u \in R$. Then $b = u^{-1}a$. Hence $a \mid b$ and $b \mid a$ and so $a \sim b$. □

Lemma A.0.7. [**easy divide**] *Let R be an integral domain and $a, b, c \in R$*

(a) [**a**] *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

(b) [**b**] *If $a \mid b$ and $a \mid c$, then for all $s, t \in R$, $a \mid sa + tb$.*

(c) [**c**] *$\sim$ is an equivalence relation.*

(d) [**d**] *If $a \sim b$, then $a \mid c$ if and only if $a \mid c$.*

(e) [**e**] *If $a \sim b$, then $c \mid a$ if and only if $c \mid b$.*

(f) [**r**] *If $a \sim b$, then $a = 0$ if and only if $b = 0$.*

(g) [**s**] *If $a \sim b$, then a is a unit if and only if b is a unit.*

(h) [**f**] *If $a \sim b$ then a is a prime if and only if b is prime.*

(i) [**g**] *If $a \sim b$ then a is a irreducible if and only if b is irreducible.*

Proof. (a) We have $b = da$ and $c = eb$ for some $d, e \in R$. Thus $c = eb = e(da) = (ed)a$ and so $a \mid c$.

(b) We have have $b = da$ and $c = ea$ for some $d, e \in R$. Thus $sa + tb = s(da) + t(ea) = (sd + te)a$ and $a \mid sa + tb$.

(c) Clearly $\sim$ is reflexive and symmetric. Suppose $a \sim b$ and $b \sim c$. Then $a \mid b$ and $b \mid c$. So by (a), $a \mid c$. Similarly $c \mid a$ and so $a \sim c$. Hence $\sim$ is transitive.

(d) Suppose $a \mid c$. Since $a \sim b$, we have $b \mid a$ and so by (a), $b \mid c$. Similarly $b \mid c$ implies $a \mid c$.

(e) Suppose $c \mid a$. Since $a \sim b$, we have $a \mid b$ and so by (a), $c \mid b$. Similarly $c \mid c$ implies $c \sim a$.

[**r**] Obvious.

[**s**] a is a unit if and only if $a \sim 1$ and so if and only if $b \sim 1$ and if and only if b is a unit.

(h) Suppose a is a prime and $d, e \in R$ with $b \mid de$. Then by (d), $a \mid de$. Since a is a prime, $a \mid d$ or $a \mid e$. Thus by (d), $b \mid d$ or $b \mid e$. Also since a is neither 0 nor a unit, b is neither 0 nor a unit and so b is a prime.

(i) Suppose a is a irreducible and $d, e \in R$ with $b = de$. Let u be unit in R with $a = ub$. The $a = (ud)e$ and since a is a irreducible, ud or e is a unit. Hence d or e is a unit. or $a \mid e$. Also since a is neither 0 nor a unit, b is neither 0 nor a unit and so b is a irreducible. □

Lemma A.0.8. [**primes are irreducible**] *Let R be an integral domain and $a \in R$ a prime. Then a is irreducible.*

Proof. By definition of a prime, $a \neq 0$ and a is not a unit. Suppose $a = bc$ for some $b, c \in R$. Since $a \mid a$ we get $a \mid bc$ and so by the definition of a prime, $a \mid b$ or $a \mid c$. Without loss $a \mid b$. Since $a = bc$ we have $b \mid a$ and so $a \sim b$ and $bc \sim b$. Since $a \neq 0$ we have $b \neq 0$. A.0.6(a) implies that c is a unit. So a is irreducible. □

Lemma A.0.9. [**divide and irreducible**] *Let R be an integral domain and let p be a prime in R.*

(a) [**a**] *Suppose q in R is irreducible and $p \mid q$, then $q \sim p$.*

(b) [**b**] *Suppose $b_1, b_2, \ldots b_n \in R$ with $p \mid b_1 b_2 \ldots b_n$ then $p \mid b_i$ for some $1 \leq i \leq n$.*

(c) [**c**] *Suppose $b_1, b_2, \ldots b_n \in R$ are irreducible and $p \mid b_1 b_2 \ldots b_n$ then $p \sim p_i$ for some $1 \leq i \leq n$.*

Proof. (a) Since $p \mid q$ we have $q = pa$ for some $a \in R$. Since q is irreducible either p or a is a unit. p is not a unit and so a is a unit. Thus A.0.6(b) implies that $q \sim p$.

(b) If $n = 1$, then $p = b_1$. So suppose $n > 1$ and put $a = b_1 \ldots b_{n-1}$. Then $b = ab_n$ and since $p \mid b$ and p is a prime, $p \mid a$ or $p \mid b_n$. In the first case we conclude by induction on n, that $p \mid b_i$ for some $1 \leq i \leq n - 1$. So (b) holds.

(c) By (b), $p \mid b_i$ for some $1 \leq i \leq n$ and so by (a), $p \sim b_i$. □

Proposition A.0.10. [**Uniqueness of prime factorizations**] *Let R be an integral domain and $a \in R$. Suppose that $a = p_1 p_2 \ldots p_n$ and $a = q_1 q_2 \ldots q_m$ where $n, m \in \mathbb{Z}^+$, p_i is a prime for $1 \leq i \leq n$ and q_j is a irreducible for $1 \leq i \leq m$. Then $n = m$ and after reordering the q_i's*

$$p_1 \sim q_1, p_2 \sim q_2, \ldots, p_n \sim q_n$$

Proof. Note that $p_n \mid a$. Hence by A.0.9(c), $p_n \sim q_i$ for some $1 \leq i \leq m$. Without loss, $i = m$. Then $p_n \sim q_m$ and so $up_n = q_m$ for some unit $u \in R$.

Suppose $m = 1$. If $n = 1$ we are done. So suppose for a contradiction that $n > 1$. Then $(p_1 \ldots p_{n-1})p_n = a = q_1 = q_m$ and so $((p_1 \ldots p_{n-1})p_n \sim p_n$. Thus by A.0.6, $p_1 \ldots p_{n-1}$ is a unit and so divides 1. Hence also p_1 divides 1 and so p_1 is a unit. A contradiction, since p_1 is a prime and so not a unit.

Suppose $m > 1$. Then $q_{m-1}q_m = q_{m-1}(up_n) = (uq_{m-1})p_n$. By A.0.6 $uq_{m-1} \sim q_{m-1}$. So uq_{m-1} and p_n are both irreducible. Replacing q_m by p_n and q_{m-1} by uq_{m-1} we may assume that $p_n = q_m$. Put $b = p_1 \dots p_{n-1}$ if $n > 1$ and $b = 1$ if $n = 1$. Then

$$(q_1 \dots q_{m-1})q_m = a = (p_1 \dots p_{n-1})p_n = bp_n = bq_m.$$

The Cancellation Law A.0.4 implies

$$q_1 \dots q_{m-1} = b.$$

Suppose that $n = 1$. Then $b = 1$ and so q_1 is a unit, a contradiction as q_1 is irreducible. Thus $n > 1$ and

$$p_1p_2 \dots p_{n-1} = q_1 \dots q_{m-1}.$$

So by induction on n, $n - 1 = m - 1$ and after reordering

$$p_1 \sim q_1, p_2 \sim q_2, \dots, p_{n-1} \sim q_{n-1}.$$

Hence also $n = m$ and since $p_n = q_m$, the proposition is proved. □

Lemma A.0.11. [**divisor in Euclidean domains**] *Let R be an Euclidean domain. Let $a, b \in R$ with $a \neq 0 \neq b$ and $a \mid b$.*

(a) [**a**] $\delta(a) \leq \delta(b)$.

(b) [**b**] *$a \sim b$ if and only $\delta(a) = \delta(b)$.*

Proof. (a) Note that $b = ra$ for some $r \in R$. Since $b \neq 0$ the definition of an Euclidean domain implies $\delta(b) \geq \delta(a)$.

(b) Suppose $a \sim b$. Then $a \mid b$ and $b \mid a$. By (a), $\delta(a) \leq \delta(b)$ and $\delta(b) \leq \delta(a)$. Thus $\delta(a) = \delta(b)$.

So suppose that $\delta(a) = \delta(b)$. Let $q, r \in R$ with $a = qb + r$ and $\delta(r) < \delta(b)$. Then $r = a - qb$ and since $a \mid b$ we conclude that $a \mid r$. If $r \neq 0$, then (a) implies that $\delta(a) \leq \delta(r) < \delta(b) = \delta(a)$, a contradiction. Thus $r = 0$ and $b \mid a$. So $a \sim b$. □

Proposition A.0.12. [**Euclidean domains are UFD**] *Let R be a Euclidean domain. Then every non-zero, non-unit in R is a finite product of irreducible elements.*

Proof. Let $a \in R$ be a non-zero and a non-unit. If a is irreducible we are done. So suppose $a = bc$ with neither b nor c units. Then by A.0.6(a) $a \nsim b$ and $a \nsim c$. Hence by A.0.11(b), $\delta(a) \neq \delta(b)$ and $\delta(a) \neq \delta(c)$. So by A.0.11(a), $\delta(b) < \delta(a)$ and $\delta(c) < \delta(a)$. Thus by induction on $\delta(a)$, b and c are products of irreducible elements. Thus also a is. □

Definition A.0.13. [**def:gcd int**] *Let R be an integral domain and a, b, d in R. Then we say that d is a greatest common divisor of a and b and write $d \sim \gcd(a, b)$ if*

(a) [**a**] *$d \mid a$ and $d \mid b$; and*

(b) [**b**] *if $c \in R$ with $c \mid a$ and $c \mid b$, then $c \mid d$.*

Lemma A.0.14. [**gcd is unique up to associates**] *Let R be an integral domain, $a, b \in R$ and d any greatest common divisor for a and b. Let $e \in R$. Then e is a greatest common divisor of a and b if and only if $d \sim e$.*

Proof. Suppose first that e is a greatest common divisor of a and b. Since d is a common divisor for a and b and since e is a greatest common divisor $d \mid e$. By symmetry $e \mid d$ and so $d \sim e$.

Suppose next that $d \sim e$. Then $e \mid d$. Since $d \mid a$ and $d \mid b$ we conclude that $e \mid a$ and $e \mid b$. Let $c \in R$ with $c \mid a$ and $c \mid b$. Since $d \sim \gcd(a, b)$, $c \mid d$. Since $d \sim e$ we have $d \mid e$ and so $c \mid e$. Thus e is a greatest common divisor of a and b. $\square$

Proposition A.0.15. [**gcd in euclid**] *Let R be a Euclidean domain and $a, b \in R$ not both zero. Let $\Delta = \{sa + tb \mid s, t \in R, sa + tb \neq 0\}$. Then $\Delta \neq \emptyset$. Moreover if $d \in R$, then $d \sim \gcd(a, b)$ if and only if $d \in \Delta$ and $\delta(d) \leq \delta(e)$ for all $e \in \Delta$. In particular, there exists greatest common divisor of a and b.*

Proof. Note that $a = 1a + 0b$ and $b = 0a + 1b$. Since $a \neq 0$ or $b \neq 0$ we conclude that $\Delta \neq \emptyset$. In particular, there exists $d \in \Delta$ with $\delta(d)$-minimal. Let $s, t \in R$ with $d = sa + tb$.

Let $c \in R$ with $c \mid a$ and $c \mid b$. By A.0.7(b), $c \mid d$.

Set $q, r \in R$ with $a = qd + r$ and $\delta(r) < \delta(d)$. Then

$$r = a - qd = a - q(ta + sb) = (1 - qt)a + (-qs)b.$$

If $r \neq 0$, then $r \in \Delta$ and $\delta(r) < \delta(d)$, a contradiction to the minimal choice of $\delta(d)$. Thus $r = 0$ and so $d \mid a$. Similarly $d \mid b$ and so $d \sim \gcd(a, b)$.

Noe let e by any greatest common divisor of a and b. Then $e \sim d$ and so $e = ud$ for some unit u in R. Hence $e = (us)a + (ut)b$ and so $e \in \Delta$. Moreover, by A.0.11(b), $\delta(d) = \delta(e)$. $\square$

Lemma A.0.16. [**prime and divide int**] *Let R be an Euclidean domain and $a, b, c \in R$ with $\gcd(a, b) \sim 1$ and $a \mid bc$. Then $a \mid c$.*

Proof. By A.0.15 there exist $s, t \in R$ with $1 = ra + sb$. Thus

$$c = c1 = c(ra + sb) = (cr)a + s(bc)$$

Since $a \mid a$ and $a \mid bc$ we conclude that $a \mid c$. $\square$

Lemma A.0.17. [**prime=irr**] *Let R be a Euclidean domain and $a \in R$. Then a is a prime if and only if a is irreducible.*

Proof. Suppose first that a is a prime. Then by A.0.8, a is irreducible.

Suppose next that a is irreducible. Then $a \neq 0$ and a is not a unit. Suppose $b, c \in R$ with $a \mid bc$. Let $d \sim \gcd(a, b)$. Then $d \mid a$ and so $a = de$ for some $e \in R$. Since a is irreducible, d is a unit or e is a unit.

Assume that d is a unit. Then $\gcd(a, b) \sim 1$ and so by 3.1.6 $a \mid c$.

Assume that e is a unit. Then $d \sim a$. Since $d \mid b$ we get $a \mid b$.

We proved that $a \mid b$ or $a \mid c$ and so a is a prime. $\square$

Proposition A.0.18. [**prime factors**] *Let R be a Euclidean domain and $a \in R$. If $a \neq 0$ and a is not a unit, then there exist primes $p_1, p_2 \ldots p_k$ in R with $a = p_1 p_2 \ldots p_k$. Moreover, this prime factorization is unique up to reordering and associates.*

Proof. By A.0.12 a is a product of irreducible elements. By A.0.17 all irreducible elements are primes and so a is a product of primes. By A.0.10 prime factorizations are unique. $\square$

Index

Bibliography

[Hu] T.W. Hungerford *Abstract Algebra, An Introduction,* 2nd edition, Brooks/Cole **1997**.

[Text Book] G.A. Jones and J. M. Jones *Elementary Number Theory,* Springer UMS **1998**

[Ro] H.E. Rose *A Course in Number Theory,* 2nd edition, Oxford Science Publications **1999**

Index