MTH 310: HW 2

Instructor: Matthew Cha

Due: May 30, 2018

1. **(Hungerford 1.3.8)**
   (a) Verify that $x-1$ is a factor of $x^n - 1$.
   (b) If n is a positive integer, prove that the prime factorization of $2^{2n}3^n - 1$ includes 11 as one of the prime factors. [*Hint*: $(2^{2n}3^n = (2^2 3)^n)$.]

   Solution.

   (a) Consider the following product

   $$(x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1) = (x-1)\left(\sum_{i=0}^{n-1} x^i\right) = \sum_{i=0}^{n-1}(x^{i+1} - x^i)$$
   $$= x^n - 1,$$

   where the last equality follows since the sum is a telescoping sum. Thus, $x-1$ is a factor of $x^n - 1$.

   (b) Applying the law of exponents gives

   $$2^{2n}3^n - 1 = (2^2 3)^n - 1 = 12^n - 1.$$

   From part (a) 11 is a factor of $12^n - 1$.

2. **(Hungerford 1.3.21)** If $c^2 = ab$, the gcd of $(a, b) = 1$ and $0 \leq a, b$ prove that a and b are perfect squares.

   Solution. Note that we must have that $a, b \geq 0$ for them to be perfect squares, that is, $a = n^2$ and $b = m^2$ for some $m, n \in \mathbb{Z}$.

   First, we prove that a is a perfect square if and only if $a = p_1^2 p_2^2 \cdots p_k^2$ for some primes $p_1, \ldots p_k$. Suppose that $a = n^2$ is a perfect square. Then, by the FTA we can write a prime factorization for $n = p_1 p_2 \cdots p_k$ for some primes $p_1, \ldots p_k$. Thus, $a = p_1^2 p_2^2 \cdots p_k^2$.

   By the FTA, we can write $c = p_1 p_2 \cdots p_k$ for some primes $p_1, \ldots, p_k$ and WLOG assume the primes are positive. We have that

   $$c^2 = p_1^2 p_2^2 \cdots p_k^2 = ab.$$

   The FTA and the equation above imply that the prime decompositions for a and b must only consist of the prime $p_1, p_2, \ldots, p_k$. Thus, it follows that

   $$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \qquad \text{where} \quad n_j = 0, 1, \text{ or } 2 \quad \forall j$$
   $$b = p_1^{2-n_1} p_2^{2-n_2} \cdots p_k^{2-n_k}.$$

   Suppose $n_j = 1$. Then, $p_j | a$ and $p_j | b$ is a common divisor of a and b and $p_j > 1$ since p_j is a prime. This contradicts the assumption that gcd of $(a, b) = 1$. Thus, $n_j = 0$ or 2. Therefore, by applying the criteria for perfect square we proved earlier, a and b are perfect squares.

3. **(Hungerford 1.3.31)** If p is a positive prime, prove that $\sqrt{p}$ is irrational.

Solution. Let $p > 0$ be a prime and suppose that $\sqrt{p}$ is rational, that is,

$$p = \frac{a^2}{b^2} \qquad \text{for some} \quad a, b \in \mathbb{Z}.$$

By the FTA, we can write $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_l$ for some primes p_i and q_j. From $N = pb^2 = a^2$ it follows that

$$N = p(q_1^2 q_2^2 \cdots q_l^2) = p_1^2 p_2^2 \cdots p_k^2.$$

Thus, we have achieved two prime decompositions for the integer N. The first $N = p(q_1^2 q_2^2 \cdots q_l^2)$ has $2l+1$ an odd number of primes in the decomposition while the second $N = p_1^2 p_2^2 \cdots p_k^2$ has $2k$ an even number of primes in the decomposition. This contradicts the FTA. Therefore, $\sqrt{p}$ is not rational.

4. **(Hungerford 1.3.33)** Let $p > 1$. If $2^p - 1$ is prime, prove that p is prime. [*Hint*: Prove the contrapositive: If p is composite, so is $2^p - 1$.]

Solution. Suppose $p > 1$ is composite, that is, $p = ab$ for some $a, b \in \mathbb{Z}$ neither equal to 0 or ± 1.

WLOG we can assume that $a, b > 1$, since $p > 1$ it is true that $p = |a||b|$.

By the law of exponents we have that $2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1$. Applying Problem 1, we know that $2^a - 1$ divides $2^p - 1$. Since $a > 1$, we have that $2 < 2^a$ and $1 < 2^a - 1$. Since $b > 1$, we have that $2^a < 2^{ab}$ so that $2^a - 1 < 2^p - 1$. Therefore, there exists a divisor $2^a - 1 | 2^p - 1$ that is strictly between 1 and $2^p - 1$. We conclude that $2^p - 1$ is not prime.

5. **(Hungerford 2.1.3)** Every published book has a ten-digit ISBN-10 number that is usually of the form $x_1 - x_2 x_3 x_4 - x_5 x_6 x_7 x_8 x_9 - x_{10}$, where each $0 \le x_i \le 9$ is a single digit. Sometimes the last digit is the letter X, and should be treated as if it were the number 10. The first 9 digits identify the book. The last digit x_{10} is a *check digit*; it is chosen so that

$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + x_{10} \equiv 0 \mod 11.$$

If an error is made when scanning or keying the ISBN number into a computer the left side of the congruence will not be congruent to 0 modulo 11, and the number will be rejected as invalid. Which of the following are apparently valid ISBN numbers?

(a) 3–540–90518–9 $\qquad (b)$ 0–031–10559–5 $\qquad (c)$ 0–385–49596–X.

Solution.

(a) 3–540–90518–9 is a valid ISBN-10 since

$$10 \cdot 3 + 9 \cdot 5 + 8 \cdot 4 + 7 \cdot 0 + 6 \cdot 9 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 1 + 2 \cdot 8 + 9 = 19 \cdot 11 \equiv 0 \mod 11.$$

(b) 0–031–10559–5 is not a valid ISBN-10 since

$$10 \cdot 0 + 9 \cdot 0 + 8 \cdot 3 + 7 \cdot 1 + 6 \cdot 1 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 5 + 2 \cdot 9 + 5 = 95 \not\equiv 0 \mod 11.$$

(c) 0–385–49596–X is a valid ISBN-10 since

$$10 \cdot 0 + 9 \cdot 3 + 8 \cdot 8 + 7 \cdot 5 + 6 \cdot 4 + 5 \cdot 9 + 4 \cdot 5 + 3 \cdot 9 + 2 \cdot 6 + 10 = 24 \cdot 11 \equiv 0 \mod 11.$$

6. **(Hungerford 2.1.8)** Prove that every odd integer is congruent to 1 modulo 4 or 3 modulo 4.

Solution. Let $n = 2k + 1$ be odd. Then, by the division algorithm for k when divided by 2 there exist $q, r \in \mathbb{Z}$ such that $k = 2q + r$ for $0 \le r < 2$.

Case 1. $(r = 0)$ Then, $n = 2(2j) + 1 = 4j + 1$. Therefore, $n - 1 = 4j$ so that $n \equiv 1 \mod 4$.

Case 2. $(r = 1)$ Then, $n = 2(2j + 1) + 1 = 4j + 3$. Therefore, $n - 3 = 4j$ so that $n \equiv 3 \mod 4$.

In both cases, n is congruent to 1 or 2 modulo 4.

7. **(Hungerford 2.1.15)** If the greatest common divisor $(a, n) = 1$, prove that there is an integer $b \in \mathbb{Z}$ such that $ab \equiv 1 \mod n$.

   Solution. Suppose that the gcd $(a, n) = 1$. Then, Theorem 1.2 there are $u, v \in \mathbb{Z}$ such that $au+nv = 1$. Therefore, $au - 1 = nv$ so that $au \equiv 1 \mod n$.

8. **(Hungerford 2.1.22)**

   (a) Give an example to show that the following statement is false: If $ab \equiv ac \mod n$ and $a \not\equiv 0 \mod n$, then $b \equiv c \mod n$.

   (b) Prove that the statement in part (a) is true whenever the gcd $(a, n) = 1$.

   Solution.

   (a) Let $a = 2$ and $n = 6$. For $b = 3$ and $c = 6$, we have that $2 \cdot 3 = 6$ and $2 \cdot 6 = 12$. So that $2 \cdot 3 \equiv 0 \mod 6$ and $2 \cdot 6 \equiv 0 \mod 6$. By transitivity of congruence, $2 \cdot 3 \equiv 2 \cdot 6 \mod 6$.
   But, by Corollary 2.5 we know that $3 \not\equiv 6 \mod 6$.

   (b) Suppose that $(a, n) = 1$ and $ab \equiv ac \mod n$. Then, $ab-ac = nk$ for some $k \in \mathbb{Z}$. Thus, $n|a(b-c)$. By Theorem 1.4, $n|a(b - c)$ and $(a, n) = 1$ implies that $n|(b - c)$. Therefore, $b - c = nj$ for some j and thus, $b \equiv c \mod n$.

9. **(Hungerford 2.2.11 and 15)** Solve the equation $x + x + x = [0]$ in $\mathbb{Z}_3$. (State the properties of modular arithmetic you are using in each step of your solution, see Theorem 2.7)
   Then, simplify the expression $([a] + [b])^3$ in $\mathbb{Z}_3$.

   Solution. Let $[a] \in \mathbb{Z}_3$ where $a \in \mathbb{Z}$ is any representative in the class $[a]$. Then, by the definition of addition for congruence classes

$$[a] + [a] + [a] = [a + a] + [a] = [a + a + a] = [3a].$$

   We have that $3a \equiv 0 \mod 3$ for any $a \in \mathbb{Z}$ and thus, by Theorem 2.3, $[3a] = [0]$. Therefore, all elements of $\mathbb{Z}_3$ are solutions to $x + x + x = [0]$.
   Now, simplify $([a] + [b])^3$ in $\mathbb{Z}_3$:

$$\begin{aligned}
([a] + [b])^3 &= ([a] + [b])([a] + [b])([a] + [b])^3 \\
&= ([a] + [b])([a][a] + [a][b] + [b][a] + [b][b]) && \text{(by distribution)} \\
&= ([a] + [b])([a^2] + [2ab] + [b^2]) && \text{(by multiplication of classes)} \\
&= ([a][a^2] + [a][2ab] + [a][b^2] + [b][a^2] + [b][2ab] + [b][b^2] && \text{(by distribution)} \\
&= [a^3] + [2a^2b] + [ab^2] + [a^2b] + [2ab^2] + [b^3] && \text{(by multiplication of classes)} \\
&= [a^3] + [3a^2b] + [3ab^2] + [b^3] && \text{(by addition of classes)} \\
&= [a]^3 + [0] + [0] + [b]^3 && \text{(by previous part of problem)} \\
&= [a]^3 + [b]^3.
\end{aligned}$$

10. **(Hungerford 2.2.16)** Find all $[a] \in \mathbb{Z}_5$ for which the equation $[a] \cdot x = [1]$ has a solution.

    Solution. The multiplication table for $\mathbb{Z}_5$ is given by

$\cdot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

From the multiplication table, every row besides [0] contains [1]. It follows that $[1], [2], [3], [4]$ are have solutions to the equation $[a] \cdot x = [1]$.

11. **(Hungerford 2.3.2 and 6)** Find all zero divisors in (a) $\mathbb{Z}_7$ and (b) $\mathbb{Z}_9$.

    Next, prove that if n is composite then that there is at least one zero divisor in $\mathbb{Z}_n$.

    Solution. Recall, a is a zero divisor if $a \neq 0$ and $ab = 0$. Thus, to find all zero divisor we look at the multiplication tables.

    The multiplication table for $\mathbb{Z}_7$ is given by,

$\mathbb{Z}_7$:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

[0] does not appear in the table out side of the row and column of [0]. Thus, there are no zero-divisors.

$\mathbb{Z}_9$:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[2]	[0]	[2]	[4]	[6]	[8]	[1]	[3]	[5]	[7]
[3]	[0]	[3]	[6]	[0]	[3]	[6]	[0]	[3]	[6]
[4]	[0]	[4]	[8]	[3]	[7]	[2]	[6]	[1]	[5]
[5]	[0]	[5]	[1]	[6]	[2]	[7]	[3]	[8]	[4]
[6]	[0]	[6]	[3]	[0]	[6]	[3]	[0]	[6]	[3]
[7]	[0]	[7]	[5]	[3]	[1]	[8]	[6]	[4]	[2]
[8]	[0]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Thus, there are two zero divisors in $\mathbb{Z}_9$, [3] and [6].

Next, suppose n is composite. Thus, there is a divisor $a|n$ such that $1 < a < n$ and $ak = n$ for some $k \in \mathbb{Z}$ and $1 < k < n$ It follows that $[ak] = [0]$. By multiplication of congruence classes, $[ak] = [a][k]$. Therefore, $[a][k] = [0]$ and since $1 < k < n$ we have that $[k] \neq [0]$. We can conclude that $[a]$ is a zero divisor in $\mathbb{Z}_n$.

12. **(Hungerford 2.3.10)** Prove that every nonzero element of $\mathbb{Z}_n$ is either a unit or a zero divisor, but not both.

    Solution. Let $[a]$ be a unit in $\mathbb{Z}_n$ and suppose $[a]$ is a zero divisor. Then, there exists $[b], [c] \in \mathbb{Z}_n$ such that $[a][b] = [1] = [b][a]$ and $[a][c] = [0]$ where $[c] \neq [0]$. By substitution, it follows that

$$\begin{aligned} [0] &= [b \cdot 0] = [b][0] \\ &= [b]([a][c]) = ([b][a])[c] \\ &= [1][c] \\ &= [c]. \end{aligned}$$

We have reached a contradiction, thus a cannot be both a unit and a zero-divisor.

Now let $[a] \in \mathbb{Z}_n$ and $a > 0$ be a representative of the class $[a]$. Then, either $(a, n) = 1$ or $(a, n) = d > 1$.

If $(a, n) = 1$ then by Theorem 2.10 $[a]$ is unit.

If $(a, n) = d > 1$, we can write $a = dk$ and $n = dl$ for some $k, l \in \mathbb{Z}$. Moreover, since $n > 0$ we can choose $0 < l < |n|$ so that $[l] \neq [0]$. It follows that $al = dkl = kn$ so that $[a][l] = [0]$ in $\mathbb{Z}_n$ with $[l] \neq [0]$. We conclude that $[a]$ is a zero divisor.

13. **(Hungerford 2.3.17)** Prove that the product of two units in $\mathbb{Z}_n$ is also a unit.

    Solution. Let $[a], [b] \in \mathbb{Z}_n$ be units. Then, there are $[c], [d] \in \mathbb{Z}_n$ such that $[a][c] = [1] = [c][a]$ and $[b][d] = [1] = [d][b]$. We check that $[cd]$ is an inverse for $[ab]$

$$\begin{aligned} [ab][cd] &= [abcd] = [acbd] \\ &= [ac][bd] \\ &= ([a][c])([b][d]) \\ &= [1][1] = [1] \end{aligned}$$

    and

$$[cd][ab] = [cdab] = [abcd] = [ab][cd] = [1].$$

    Therefore, $[a][b] = [ab]$ is a unit in $\mathbb{Z}_n$.

14. **(EC–worth .5% of final grade)** Find all elements of the set $[2]_7 \cap [3]_5$.