Math 310-001 **Review for Exam 1** **Fall, 2014**

Theorem. (The Division Algorithm) Let a, b be integers with $b \neq 0$. Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.

Theorem. Let a and b b integers, not both 0, and let d be their greatest common divisor. Then there exist, not necessarily unique, integers a and v such that $d = au + bv$. Furthermore, d is the smallest positive integer that can be written in the form $au + bv$.

Theorem. Let p be an integer such that $p \neq 0, \pm 1$. Then p is prime if and only if p has the following property: If $p \mid bc$, then $p \mid b$ or $p \mid c$.

Theorem. (The Fundamental Theorem of Arithmetic) Every integer, except 0, ± 1 is a product of primes. This prime factorization is unique in the following sense: If $n = p_1 \ldots p_k$ and $n = q_1 \ldots q_s$ with each p_i, q_j prime and $p_i \leq p_{i+1}$, $q_j \leq q_{j+1}$, for $i = 1, \ldots k-1$, $j = 1, \ldots s-1$, then $k = s$ and $p_i = \pm q_i$ for all $i = 1, \ldots k$.

Theorem. Let a, b, n be integers with $n > 0$. Then the following statements are equivalent

(a) $b = a + kn$ for some integer k.

(b) $n \mid b - a$.

(c) $a \equiv b \pmod{n}$.

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

(e) a and b have the same remainder when divided by n.

Definition A ring is a triple $(R, +, \cdot)$ such that

(i) R is a set;

(ii) $+$ is a function (called ring addition), $R \times R$ is a subset of the domain of $+$ and for $(a, b) \in R \times R$, $a + b$ denotes the image of (a, b) under $+$;

(iii) $\cdot$ is a function (called ring multiplication), $R \times R$ is a subset of the domain of $\cdot$ and for $(a, b) \in R \times R$, $a \cdot b$ (and also ab) denotes the image of (a, b) under $\cdot$; and such that the following eight axioms hold:

(A1) $a + b \in R$ for all $a, b \in R$; [closure for addition]

(A2) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$; [associative addition]

(A3) $a + b = b + a$ for all $a, b \in R$. [commutative addition]

(A4) there exists an element in R, denoted by 0_R and called 'zero R', such that $a + 0_R = a = 0_R + a$ for all $a \in R$; [additive identity]

(A5) for each $a \in R$ there exists an element $x \in R$, such that $a + x = 0_R$; [additive inverses]

(A6) $ab \in R$ for all $a, b \in R$; [closure for multiplication]

(A7) $a(bc) = (ab)c$ for all $a, b, c \in R$; [associative multiplication]

(A8) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$. [distributive laws]

Theorem. Let S be a nonempty subset of a ring R such that

(1) S is closed under subtraction;

(1) S is closed under multiplication.

Then S is a subring of R.

I. Review homework problems.

II. Review quizzes.

III. Be able to prove short and straightforward theorems (e.g. see Problem 11 below).

Some practice problems for review

1. Let a, b be integers and let $k = ab + 1$. Prove that $\gcd(k, a) = \gcd(k, b) = 1$.

2. Let a, b be integers. Prove that $\gcd(a, b) = \gcd(a, b + at)$ for every $t \in \mathbb{Z}$,

3. Prove that $\sqrt{77}$ is irrational.

4. If $a \equiv 2 \pmod{4}$, prove that there are no integers c and d such that $a = c^2 - d^2$.

5. Prove or disprove: If a and b are integers with $[a] = [b + 2]$ in $\mathbb{Z}_6$, then $a - b$ is not a prime.

6. Solve the equation $x^2 + 3x + 2 = 0$ in Z_p, where $p \geq 3$ is a prime.

7. Solve the equations in $\mathbb{Z}_{12}$:
   (a) $3x = 9$ (b) $5x = 7$ (c) $4x = 6$.

8. Let d be an integer that is not a perfect square. Show that $\mathbb{Q}(\sqrt{d}) = a + b\sqrt{d} \mid a, b \in \mathbb{Q}$ is a subfield of $\mathbb{C}$.

9. Define new addition and new multiplication on $\mathbb{Z}$ by $a \oplus b = a + b - 1$ and $a \odot b = ab - (a + b) + 2$. Prove that with these new operations $\mathbb{Z}$ is an integral domain.

10. The addition and multiplication table for a three element commutative ring with an identity are given below. Use the ring laws to complete the tables.

+	a	b	c
a	c		b
b	a	b	c
c			a

·	a	b	c
a		b	
b		b	
c	a	b	c

Solve the given equation $c + x = a^2$ for x in the given ring.

11. Be able to prove any of the statements in the following

Theorem. For any elements a and b of a ring R,

(a) $a \cdot 0_R = 0_r = 0_R \cdot a$.

(b) $a(-b) = -(ab) = (-a)b$.

(c) $-(-a) = a$.

(d) $-(a + b) = (-a) + (-b)$.

(e) $(-a)(-b) = ab$.

12. Can a ring have more than one zero element? How about more than one identity element?