Number Theory Math 5840 notes.

Section 1: Axioms.

In number theory we will generally be working with integers, though occasionally fractions and irrationals will come into play.

Notation: $\mathbf{Z}$ denotes the set of all integers $\mathbf{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\}$ and $\mathbf{Z}^+$ denotes the set of positive integers $\{1, 2, 3, ...\}$.

Axioms about addition and multiplication: There exists two operations on the integers: addition denoted by "+" and multiplication denoted by "$\cdot$". Strictly speaking + is a map from the cross product of the integers with itself into the integers with certain properties as defined by the axioms, and similarly for multiplication . Note that $a \cdot b$ is usually written as ab.

Axioms about addition.

A1. If $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ then $a + b \in \mathbf{Z}$. [Closure.]

A2. If $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ then $a + b = b + a$. [Commutativity.]

A3. If $a \in \mathbf{Z}$, $b \in \mathbf{Z}$ and $c \in \mathbf{Z}$ then $a + (b + c) = (a + b) + c$. [Associativity.]

A4. There exists an element $0 \in \mathbf{Z}$ so that if $a \in \mathbf{Z}$ then $a + 0 = a$. [Identity element.]

A5. If $a \in \mathbf{Z}$ then there exits an element in $\mathbf{Z}$ denoted by $-a$ so that $-a + a = 0$. [Additive inverse. Note that the negative numbers are, by definition, the additive inverses of the positive numbers.]

Definition: $a - b$ means $a + (-b)$.

Assuming Axioms A1-A5 is equivalent to saying that that $\mathbf{Z}$ is a commutative group under the operation of addition.

Axioms about multiplication.

B1. If $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ then $a \cdot b \in \mathbf{Z}$. [Closure.]

B2. If $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ then $a \cdot b = b \cdot a$. [Commutivity.]

B3. If $a \in \mathbf{Z}$, $b \in \mathbf{Z}$ and $c \in \mathbf{Z}$ then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. [Associativity.]

B4. There exists an element $1 \in \mathbf{Z}$ so that if $a \in \mathbf{Z}$ then $a \cdot 1 = a$. [Identity element.]

B5. If $a \in \mathbf{Z}$, $b \in \mathbf{Z}$, $c \in \mathbf{Z}$ and $ac = bc$ then $a = b$. [Cancellation rule.]

Axioms on the relationship between addition and multiplication.

C1. If $a \in \mathbf{Z}$, $b \in \mathbf{Z}$ and $c \in \mathbf{Z}$ then $a \cdot (b+c) = a \cdot b + a \cdot c$. [Distributive law.] Note the assumption that the order of operation is to perform $\cdot$ first then $+$.

C2. $0 \neq 1$. (Note that this axiom is really implicit in definition of $\mathbf{Z}$ and that axioms A4 and B4 selected different specific elements of $\mathbf{Z}$.)

Definition: If $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ then $a < b$ means that $b - a \in \mathbf{Z}^+$. [Definition of order.]

Axioms on order.

D1. If $a \in \mathbf{Z}^+$ and $b \in \mathbf{Z}^+$ then $a + b \in \mathbf{Z}^+$ and $a \cdot b \in \mathbf{Z}^+$. [Closure of addition and multiplication for positive integers.]

D2. If $a \in \mathbf{Z}$ then either $a < 0$, $a = 0$, or $0 < a$. [Trichotomy Law.]

Induction axiom.

E1. Every nonempty subset of $\mathbf{Z}^+$ has a least element. [Well ordered property.]

Axiom E1 is equivalent to the following:

If S is a subset of $\mathbf{Z}^+$ containing 1 such that if $n \in S$ then $n+1 \in S$; then $S = \mathbf{Z}^+$.

Definition: $a^0 = 1$, $a^1 = a$, $a^{n+1} = a^n \cdot a$.

Theorem 1.1. Suppose that each of a, b and c is an integer.

a. $(a + b) \cdot c = a \cdot c + b \cdot c$.

b. $a + (b + c) = (c + a) + b$.

c. $(a + b)^2 = a^2 + 2a \cdot b + b^2$.

d. $(-1) \cdot a = -a$.

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

f. $(-a) \cdot b = -(ab) = a \cdot (-b)$.

g. $(-a) \cdot (-b) = a \cdot b$.

h. $-0 = 0$.

i. The additive and multiplicative identities are both unique. (i.e. no number other than 0 is the additive identity and similarly for the multiplicative identity.)

j. $0 \cdot a = 0$.

Theorem 1.2. Suppose that each of a, b and c is an integer.

a. If $a < b$ then $a + c < b + c$.
b. If $a < b$ and $0 < c$ then $ac < bc$.
c. If $a < b$ and $0 > c$ then $ac > bc$.
d. If $a \neq 0$, then $a^2 > 0$.
e. If $ab = 0$ then either $a = 0$ or $b = 0$.
f. If $a, b, c \in \mathbf{Z}^+$ and $ac < bc$, then $a < b$.

Theorem 1.3. There is no integer between 0 and 1.

Section 2: Induction.

Definition. Suppose that a and r are real numbers. Then the sequence: $a, ar, ar^2, ar^3, ...$ is called a geometric sequence with common ratio r.

Theorem 2.1. If a and r are real numbers then.

$$\sum_{i=0}^{n} ar^i = \frac{ar^{n+1} - a}{r - 1}.$$

Definition. A sum in the form $\sum_{i=1}^{n} x_{i+1} - x_i$ is called a *telescoping series.*
Exercise 2.2. Verify that $\sum_{i=1}^{n} x_{i+1} - x_i = x_{n+1} - x_1$.

Exercise 2.3. Express $\frac{1}{i(i+1)}$ as a partial fraction (remember your integration techniques?), show that $\sum_{i=1}^{\infty} \frac{1}{i(i+1)}$ is a telescoping series and calculate its sum.

Exercise 2.4. What happens to the geometric series and the series of exercise 2.3 as $n \to \infty$?

Use mathematical induction to prove the next few theorems.

Theorem 2.5.

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

[The numbers $T_n = \sum_{i=1}^{n} i$ are called triangular numbers. (Why?)]

Theorem 2.6.

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Theorem 2.7.

$$\sum_{i=1}^{n} i^3 = [\frac{n(n+1)}{2}]^2.$$

Exercise 2.8.

Note that $\sum_{i=1}^{n}(i+1)^3 - i^3$ is a telescoping series and use exercise 2.2 to find the sum. Then expand each term of the sum by distributing the summation symbol to obtain an equation and solve for $\sum i^2$ in terms of $\sum i$. Then use theorem 2.5 to obtain the formula of theorem 2.6.

Exercise 2.9.

Repeat exercise 2.8 only replace 2 with 3, then with 4 and 5 and obtain the summation formulae for $\sum i^3$ and $\sum i^4$. Verify the second formula by induction if you are so inclined.

Definition: We define $1! = 1$; for $n > 1$, we define $(n+1)! = (n+1) \cdot n!$; and we define $0! = 1$.

Exercise 2.10. Verify for each positive integer n:

$$\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1.$$

Exercise 2.11.

a. Verify for each positive integer n:

$$1 + \frac{n}{2} \leq \sum_{i=1}^{2^n} \frac{1}{i} \leq 1 + n.$$

b. Verify for each positive integer n, $(2n)! < 2^{2n}(n!)^2$.

Theorem 2.12. If n is a positive integer and x and y are real numbers then $x - y$ is a factor of $x^n - y^n$.

Corollary:

$$\frac{x^n - y^n}{x - y} = \sum_{i=0}^{n} x^{n-i-1}y^i = x^{n-1} + x^{n-2}y + ... + y^{n-1}.$$

Definition. The Fibonacci numbers $\{F_n\}_{i=1}^{\infty}$ are defined as follows:

$F_1 = 1$.

$F_2 = 1$.

For $n \in \mathbf{Z}, n > 2$, $F_{n+1} = F_n + F_{n-1}$.

Exercise 2.13. Calculate:

a. $\sum_{i=1}^{n} F_i$, (answer: $F_{2n} - 1$;)

b. $\sum_{i=1}^{n} F_{2i-1}$. (answer: F_{2n}.)

Theorem 2.14. For each positive integer n:

a. $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$;

b. If $n > 1$, then $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$;

c. If $n > 2$, then $F_{n+1}F_n - F_{n-1}F_{n-2} = F_{2n-1}$;

d. $\sum_{i=1}^{2n-1} F_i F_{i+1} = [F_{2n}]^2$.

Exercise 2.15. Let n be a positive integer.

a. $F_n \leq 2^{n-1}$,

b. $F_n \leq \frac{7}{4}^{n-1}$,

c. If $\beta = \frac{1+\sqrt{5}}{2}$, then $F_n \leq \beta^{n-1}$. [Note: $\beta^2 = \beta + 1$.]

Theorem 2.16. Let α and β be the roots of $x^2 = x + 1$ with $\alpha < \beta$, then:

$$F_n = \frac{\beta^n - \alpha^n}{\sqrt{5}}.$$

Exercise 2.17. Let $M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then $M^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$.

Exercise 2.18. Verify:

$$\sum_{i=1}^{n} 2i - 1 = n^2.$$

Section 3: Binomial coefficients and combinations.

Definition. If n and r are nonnegative integer so that $r \leq n$, then

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} .$$

Theorem 3.1. Let n and r be positive integers so that $r \leq n$. Then:

a. $\binom{n}{0} = \binom{n}{n} = 1.$

b. $\binom{n}{r} = \binom{n}{n-r}$

c. $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}.$

Theorem 3.2. [The binomial theorem.] If n is a positive integer and x and y are numbers, then:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

Fact: [Which may be assumed.] The quantity $\binom{n}{i}$ is the number of different possible i-card hands that can be dealt from a deck of n cards.

Assume for the following theorems that the various quantities all take on the reasonably expected values. (E.g. if the symbol $\binom{n}{i}$ is used then assume i and n are non-negative integers with $i \leq n$.)

Theorem 3.3.

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

Theorem 3.4.

$$\sum_{i=0}^{n}(-1)^i \binom{n}{i} = 0.$$

Exercise 3.5. Show that:

$$\binom{n}{r}\binom{r}{i} = \binom{n}{i}\binom{n-i}{r-i}.$$

Exercise 3.6. Show that:

$$\sum_{i=0}^{n-r}\binom{r+i}{r} = \binom{n+1}{r+1}.$$

Exercise 3.7. Determine the value of k that makes the following equation true and prove the identity.

$$\sum_{i=0}^{k}\binom{n-i}{i} = F_{n+1}.$$

Section 4: Divisibility.

Definition. If a and b are integers then a is said to divide b if and only if there is an integer q so that $b{=}aq$. The standard notation is: $a|b$.

Theorem 4.1. If each of a, b, and c is an integer so that $a|b$ and $b|c$, then $a|c$.

Theorem 4.2. If each of a, b and c is an integer so that $a|b$ and $a|c$ then for arbitrary integers x and y, $a|(xb + yc)$.

Theorem 4.3. [The division algorithm.] If each of a and b is an integer with $0 < b$ then there exist unique integers q and r with $0 \leq r < b$ so that:

$$a = bq + r.$$

In the following exercises and theorems, as usual assume that the quantities are appropriately defined.

Exercise 4.4. Find integers a, b, and c so that $a|bc$ but $a \nmid b$ and $a \nmid c$.

Theorem 4.5. If $c \neq 0$ then $a|b$ iff $ac|bc$.

Theorem 4.6. If $a|b$ then $a \leq b$.

Exercise 4.7. If $a|b$ then $a^n|b^n$ for each positive integer n.

Theorem 4.8. If $a|b$ and $b|a$ then $a = b$.

Exercise 4.9. Show that if a is an integer then, $3|(a^3 - a)$.

Exercise 4.10. Show that $6|a(a+1)(a+2)$ for any integer a.

Exercise 4.11. Show that $5|(a^5 - a)$ for every positive integer a.

Exercise 4.12. The sum of the cubes of three successive integers is divisible by 9.

Exercise 4.13. Show that if $m > 1$ then $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$.

Exercise 4.14. Show that if $n|m$ then $F_n|F_m$. [Hint: use exercise 4.13.]

Section 5: Prime Numbers.

Definition. Suppose that n is a positive integer. If n is only divisible by one positive integer then n is called a *unit*; if there are only two positive integers that divide n then n is called a *prime* number; if n is divisible by *three* positive integers then n is called a *composite* number.

Observation. The positive integer p is a prime number iff it is not equal to 1 and it divisible only by itself and 1.

Theorem 5.1. If n is a positive integer then there exists a prime number p so that $p|n$.

Theorem 5.2. The set of prime numbers in infinite.

Theorem 5.3. If n is a composite number then there exists a prime number $p \leq \sqrt{n}$ so that $p|n$.

Definition. If x is a number then $\pi(x)$ denotes the number of primes less than or equal to x.

The proof of the following important theorem uses techniques that will not be covered in this course.

The Prime Number Theorem:

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{ln(n)}} = 1.$$

Exercise 5.4. Use the prime number theorem to estimate the number of primes less than $1,000,000$. How good an estimate is it for the number of primes less than 100?

Theorem 5.5. If n is a positive integer then at some point in the number system, there exists n consecutive composite integers.

Open problem: Goldbach's Conjecture: If $n > 2$ is an even positive integer then n is the sum of two primes.

Exercise 5.6. Determine the integers n for which the quantity $n^3 + 1$ is prime.

Exercise 5.7. Show that if $p > 3$ is prime, then one of $p + 2$ or $p + 4$ is not prime.

Exercise 5.8. Show that $x^2 - x + 41$ is prime for all positive integers $x < 41$. [Don't do this by hand, use a spreadsheet or something.] Show that for $x = 41$ this polynomial does not produce a prime.

Theorem 5.9. [Generalization of exercise 5.8.] Show that if $P(x)$ is a polynomial with integer coefficients then there is a positive integer n so that $P(n)$ is a composite number.

Exercise 5.10. Let $n > 1$; show that if $a^n - 1$ is prime then $a = 2$ and n is prime.

Exercise 5.11. Suppose that N is an integer and A is a set of primes less than N and B is the set of primes less than N that are not in A. Then $\prod_{a \in A} a + \prod_{b \in B} b$ is not divisible by a prime less than N.

Exercise 5.12. Suppose that p is the smallest prime factor of the integer n and that $\sqrt[3]{n} < p$ then either n or $\frac{n}{p}$ is prime.

Exercise 5.13. Show that every integer greater than 11 is the sum of two composite numbers.

Exercise 5.14. Suppose that n is a positive integer. Does it follow that $\binom{n}{r}$ is divisible by n? What if n is prime?

Theorem 5.15. The set $S = \{4k + 3 | k \in \mathbf{Z}^+\}$ contains infinitely many primes.

[Hint: note that is a and b are both in the form $4n + 1$ then so is ab.]

Section 6: Prime Factorization.

Definition. If each of a and b is an integer then the *greatest common divisor* of a and b is the largest positive integer that divides both a and b.

The common notation for the greatest common divisor d of a and b is: $d = (a, b)$ or $d = gcd(a, b)$. We will use the latter, though you should be aware that the former is more common.

Definition. If each of a and b is an integer then a and b are said to be *relatively prime* iff $gcd(a, b) = 1$.

Definition. The greatest common divisor for a set of numbers $\{a_i\}_{i=1}^n$ is similarly defined: $gcd(\{a_i\}_{i=1}^n)$ is the largest positive integer that divides all the elements of the set $\{a_i\}_{i=1}^n$.

Example: Find three integers so that $gcd(a, b, c) = 1$ but that are pairwise not relatively prime.

Theorem 6.1. Suppose that each of a, b and c is a positive integer and $d = gcd(a, b)$. Then:

a. $gcd(\frac{a}{d}, \frac{b}{d}) = 1$;
b. $gcd(a + cb, b) = gcd(a, b)$.

Theorem 6.2. Suppose that each of a and b is an integer and at least one of them is not 0. Let $S = \{na + mb | n \in \mathbf{Z}, m \in \mathbf{Z}, 0 < na + mb\}$. Then $gcd(a, b)$ is the least element of the set S.

Exercise 6.3. Find the gcd of the following pairs:

a. $gcd(a, a^2) =?$,
b. $gcd(a, a + 1) =?$,
c. $gcd(a, a + 2) =?$,
d. $gcd(ca, cb) =?$.

Exercise 6.4. Show that if $gcd(a, b) = 1$, then $gcd(a + b, a - b)$ is 1 or 2.

Exercise 6.5. If a and b are even then $gcd(a, b) = 2gcd(\frac{a}{2}, \frac{b}{2})$. If a is even and b is odd then $gcd(a, b) = gcd(\frac{a}{2}, b)$.

Theorem. 6.6. If $gcd(e, f) = 1$, $e|a$ and $f|a$, then $ef|a$.

Exercise 6.7.

a. If $gcd(a, b) = 1$ and $c|(a + b)$ then $gcd(a, c) = 1$.
b. If $a|bc$ then $a|gcd(a, c)gcd(a, b)$.
c. If $gcd(a, b) = 1$ then $gcd(a^n, b^n) = 1$.
d. If $gcd(a, b) = gcd(a, c) = 1$ then $gcd(a, bc) = 1$.
e. $gcd(3k + 2, 5k + 3) = 1$.

Theorem 6.8. [The Euclidean Algorithm to calculate the Greatest Common Divisor.] Suppose that a and b are two positive integers. Let $r_0 = a$ and $r_1 = b$, then recursively define r_{n+1} and q_n using the division algorithm by:

$$r_{n-1} = r_n q_n + r_{n+1}.$$

Then there exists an integer k so that $r_k = 0$ and if k is the first such integer then $gcd(a, b) = r_{k-1}$.

Definition Let a and b be two positive integers then the *least common multiple* of a and b is the smallest positive integer m so that $a|m$ and $b|m$.

The common notation for the least common multiple m of a and b is: $m = [a, b]$ or $d = lcm(a, b)$. We will use the latter, though you should be aware that the former is more common.

Theorem 6.9. Let a and b be two positive integers. Then:

$$lcm(a, b) = \frac{ab}{gcd(a, b)}.$$

Theorem 6.10. If $gcd(a, b) = 1$ and $a|bc$ then $a|c$.

Theorem 6.11. Suppose that p is a prime, that for each $i \leq n$, a_i is a positive number and

$$p| \prod_{i=1}^{n} a_i,$$

then there exists a k so that $p|a_k$.

Theorem 6.12. [The Fundamental Theorem of Arithmetic.] Every positive integer n greater that 1 has a unique representation as a product of primes:

$$n = p_1 p_2 p_3 ... p_k,$$

such that $p_i \leq p_{i+1}$.

Exercise 6.13. [Applications of the Fundamental Theorem of Arithmetic.] Assume as usual that each of r, s, are positive integer, a, b, ... etc take on reasonable values; assume that p denotes a prime.

a. If $a^3|b^2$ then $a|b$.
b. If $p^r|a$ and $p^s|b$ then $p^{r+s}|ab$.
c. If $p^r|a$ then $p^{nr}|a^n$.
d. If $a^2|b^2$ then $a|b$.

e. If m is a common multiple of a and b then $lcm(a,b)|m$.
f. If $a^r = b^r$ then $a = b$.

Exercise 6.14. [More applications.]
a. Show that $\log_2(3)$ is irrational.
b. Show that $\sqrt{2}$ is irrational.
c. Show that if p is a prime number then $\sqrt{p}$ is irrational.
d. Show that $\sqrt{6}$ is irrational.
e. Generalize b - d as much as you can.

Theorem 6.15. Suppose that each of a and b is a positive integer and that, by the fundamental theorem of arithmetic, $a = \prod_{i=1}^{n} p_i^{r_i}$ and $b = \prod_{i=1}^{n} p_i^{s_i}$; where each $p_i$is a prime and each of r_i and s_i is a positive integer or zero. Then:

$$gcd(a,b) = \prod_{i=1}^{n} p_i^{\min(r_i,s_i)},$$

$$lcm(a,b) = \prod_{i=1}^{n} p_i^{\max(r_i,s_i)}.$$

Exercise 6.16.

$$gcd(a,b)|lcm(a,b).$$

Exercise 6.17.
$lcm(a,b)|c$ if and only if $a|c$ and $b|c$.

Exercise 6.18. Let p be a prime,
a. If $p|a^2$ then $p|a$.
b. If $p|a^n$ then $p|a$.

Exercise 6.19.

$$gcd(a,b) = gcd(a+b, lcm(a,b)).$$

Exercise 6.20.

a. Show that there are infinitely many primes in the set

$$\{4k+3|k \in \mathbf{Z}^+\}.$$

[Hint: prove the following lemma first: the set $\{4k+1|k \in \mathbf{Z}^+\}$ is closed under multiplication.

b. Show that there are infinitely many primes in the set

$$\{6k+5|k \in \mathbf{Z}^+\}.$$

c. Generalize a and b as much as possible. [The generalization is called Dirichlet's Theorem on Primes.]

Exercise 6.21.
If $a^2|b^2$ then $a|b$.

Exercise 6.22.
If a, b, and c are positive integers so that $gcd(a,b) = 1$ and $ab|c^n$, then there exists integers u and v so that $a = u^n$ and $b = v^n$.

Exercise 6.23. Show that:

a. $\log_2(3)$ is irrational.
b. $\log_p(q)$ is irrational where p and q are primes.
c. Can b be generalized to the case where $gcd(p,q) = 1$?

Exercise 6.24. Show that:

a. $\sqrt{2}$ is irrational.
b. $\sqrt{p}$ is irrational, where p is a prime.
c. $\sqrt{6}$ is irrational.
d. Generalize b as much as possible.
e. $\sqrt[3]{5}$ is irrational.
f. Generalize as much as you can.

Definition. Suppose that each of a, b and c is an integer. Then the following equation in which integer solutions in x and y are sought is called a linear *Diophantine* equation in two variables:

$$ax + by = c.$$

Theorem 6.25. Suppose that each of a, b and c is an integer and $d = gcd(a, b)$ then the linear diophantine equation in two variables $ax + by = c$ has a solution (among the integers) if and only if $d|c$. Furthermore, if it has a solution $x = x_0$ and $y = y_0$ then it has infinitely many solutions and all of the solution are given by:

$$x = x_0 + \frac{b}{d}k, \quad y = y_0 - \frac{a}{d}k,$$

for $k \in \mathbf{Z}$.

Section 7: Congruence Relation.

Definition: Suppose that Z is a set and $\sim \subset Z \times Z$ is a relation. Then is called an *equivalence* relations provided it satisfies the following conditions:

Let $a \in Z$ then $a \sim a$; [Reflexive property.]

Let $a \in Z$ and $b \in Z$, if $a \sim b$ then $b \sim a$; [Symmetric property.]

Let $a \in Z$, $b \in Z$ and $c \in Z$, if $a \sim b$ and $b \sim c$ then $a \sim c$. [Transitive property.]

Definition: If $a \in \mathbf{Z}$, $b \in \mathbf{Z}$ and $m \in \mathbf{Z}^+$ then a is said to *equal* b *modulo* m means that:

$$m|b - a.$$

Notation: a equals b modulo m is denoted by:

$a \equiv_m b$ or

$a = b \bmod m$.

Theorem 7.1. The relation $a = b \bmod m$ is an equivalence relation on $\mathbf{Z}$.

Theorem 7.2. If $a \in \mathbf{Z}$, $b \in \mathbf{Z}$ and $m \in \mathbf{Z}^+$ then $a = b \bmod m$ if and only if there is an integer $k \in Z$ so that $a = b + km$.

Theorem 7.3. If each of a, b, r and $m > 0$ is an integer and $a = b \bmod m$, then:

a. $a + r = b + r \bmod m$;

b. $ar = br \bmod m$.

Theorem 7.4. If each of a, b, r and $m > 0$ is an integer, $1 = gcd(r, m)$ and $ar = br \bmod m$, then $a = b \bmod m$.

Theorem 7.5. If each of a, b, r, s and $m > 0$ is an integer, $a = b \bmod m$ and $r = s \bmod m$, then:

a. $a + r = b + s \bmod m$;

b. $ar = bs \bmod m$.

Definition. Suppose $m \in \mathbf{Z}_+$. Then set $S = \{r_i\}_{i=1}^n$ is called a *complete set of residues modulo* m provided that for any integer k there is exactly one element r_{i_k} so that,

$$k = r_{i_k} \bmod m.$$

Theorem 7.6. Suppose $m \in \mathbf{Z}_+$. Then set $S = \{i\}_{i=0}^{m-1} = \{0, 1, 2, ..., m-1\}$ is a complete set of residues modulo m.

Theorem 7.7. If $\{r_i\}_{i=1}^n$ is a complete set of residues modulo m then:

a. if a is an integer, then $\{r_i + a\}_{i=1}^n$ is a complete set of residues modulo m;

b. if k is an integer so that $gcd(k, m) = 1$,then $\{kr_i\}_{i=1}^n$ is a complete set of residues modulo m.

Exercise 7.8.

a. If a is even then $a^2 = 0 \bmod 4$;

b. If a is odd then $a^2 = 1 \bmod 4$.

c. If a is odd then $a^3 = 1 \bmod 8$.

Exercise 7.9. If $k|m$ and $a = b \bmod m$ then $a = b \bmod k$.

Exercise 7.10. If $a = b \bmod m$ then $ak = bk \bmod mk$.

Exercise 7.11. If $a = b \bmod m$, then $gcd(a, m) = gcd(b, m)$.

Exercise 7.12. If p is a prime and $a^2 = b^2 \bmod p$ then $a = b \bmod p$ or $a = -b \bmod p$. [Hint: use the least residues modulo p of a and b and prove the statement for the residues first.]

Exercise 7.13. [Hint: use induction.]

a. $n^3 + 5n = 0 \bmod 3$;

b. $4^n = 1 \bmod 3$;

c. $4^n = 1 + 3n \bmod 9$;

d. $5^n = 1 + 4n \bmod 16$.

Exercise 7.14.

a. Find a complete set of residues modulo 7 consisting of odd integers.

b. Find a complete set of residues modulo 7 consisting of even integers.

Exercise 7.15. If p is a prime and $x^2 = x \bmod p$, then $x = 0 \bmod p$ or $x = 1 \bmod p$.

Section 8: Congruence and the Chinese Remainder Theorem.

Theorem 8.1. If $a \in \mathbf{Z}$, $b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$ and $gcd(a, m) = d$, then the equation $ax = b \bmod m$ has a solution if and only if $d|b$. Furthermore, if $d|b$ then the equation has exactly d many pairwise non-congruent modulo m solutions.

Definition. If $a \in \mathbf{Z}$ and x is a number such that $ax = 1 \bmod m$ then x is called the *inverse of a modulo m*.

Notation. If $a \in \mathbf{Z}$ then a^{-1_m} denotes the inverse of a modulo m.

Theorem 8.2. The number a has an inverse modulo m if and only if $gcd(a, m) = 1$.

Theorem 8.3. The set $S = \{i\}_{i=1}^{n-1} = \{1, 2, ..., n-1\}$ is a abelian group under multiplication *mod* n if and only if n is prime.

Exercise 8.4. If $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ then $a^{-1_m} b^{-1_m} = (ab)^{-1_m}$.

Theorem 8.5. If p is prime, then $x^2 = 1 \bmod p$ if and only if either $x = 1 \bmod p$ or $x = -1 \bmod p$.

Theorem 8.6. If If $a, b \in \mathbf{Z}$, $m, n \in \mathbf{Z}^+$ and $gcd(m, n) = 1$, then the following system of equations:

$x = a \bmod m$,
$x = b \bmod n$,

has the solution $x = ann^{-1_m} + bmm^{-1_n}$. Furthermore the solution is unique modulo mn.

Exercise 8.7. Generalize Theorem 8.6 to solve the following system of equations.

$x = a \bmod m$,
$x = b \bmod n$,
$x = c \bmod k$.

Theorem 8.8 [Chinese Remainder Theorem]. Suppose that for each positive integer $i \leq N$, $a_i \in \mathbf{Z}$, $m_i \in \mathbf{Z}^+$ and $gcd(m_i, m_j) = 1$ for $i \neq j$. Then the system of equations:

$$x = a_i \bmod m_i,\ i \leq N,$$

has the unique solution $x = \_\_$ [Exercise 8.8: fill in the blank.] modulo $\prod_{i=1}^{N} m_i$.

Answer: Let $M = \prod_{i=1}^{N} m_i$, then:

$$x = \sum_{i=1}^{N} a_i \left(\frac{M}{m_i} \right) \left(\frac{M}{m_i} \right)^{-1_{\frac{M}{m_i}}} + kM.$$