Definition : Divides

We say that a divides b, denoted $a \mid b$, iff $\exists\, d : a \cdot d = b$. If a does not divide b, then we write $a \nmid b$.

Properties : Divides

- If $a \mid b$ and $b \mid c$, then $a \mid c$.
- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
- If $a \mid b$ and $a \mid c$, then $a \mid (m \cdot b + n \cdot c)$ for any integers m and n.
- If $d \mid a$, then $d \mid (c \cdot a)$ for any integer c.

Definition : Greatest Common Divisor

We say that d is the greatest common divisor of a and b, denoted $d = (a, b) = \gcd(a, b)$ iff $d \mid a$ and $d \mid b$, and if $c \mid a$ and $c \mid b$, then $c \leq d$.

Remark

If $(a, b) = 1$, then we will say that a and b are relatively prime.

Theorem : (1.1)

If $(a, b) = d$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Theorem : Division Algorithm (1.2)

Given positive integers a and b, $b \neq 0$, there exists unique integers q and r, with $0 \leq r < b$, such that:

$$a = b \cdot q + r$$

Lemma : (1.3)

If $a = bq + r$, then $(a, b) = (b, r)$.

Theorem : The Euclidean Algorithm

If a and b are positive integers, $b \neq 0$ and

$$\begin{aligned} a &= bq + r, & 0 &\leq r < b \\ b &= rq_1 + r_1, & 0 &\leq r_1 < r \\ r &= r_1 q_2 + r_2 & 0 &\leq r_2 < r_1 \\ &\vdots \end{aligned}$$

Then for k large enough, say $k = t$, we have that $r_{t-1} = r_t q_{t+1}$ and $(a, b) = r_t$.

Theorem : (1.4)

If $(a, b) = d$, then there are integers x and y such that

$$ax + by = d$$

Corollary : (1.1)

If $d \mid (ab)$ and $(d, a) = 1$, then $d \mid b$.

Corollary : (1.2)

Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$, then $c \mid d$.

Corollary : (1.3)

If $a \mid m$, $b \mid m$, and $(a, b) = 1$, then $(ab) \mid m$.

Definition : Prime Numbers

A prime number is an integer that is greater than 1 and has no positive divisors other than 1 and itself. An integer that is greater than 1 but is not prime is called composite. We call 1 neither a prime nor a composite number.

Lemma : (2.1)

Every integer $n > 1$ is divisible by a prime number.

Lemma : (2.2)

Every integer $n > 1$ can be written as a product of primes.

Theorem

There are infinitely many primes.

Lemma : (2.5)

If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.

Lemma : (2.6)

If $p \mid (a_1 a_2 \dots a_k)$, then $p \mid a_i$ for some i, $i = 1, 2, \dots, k$.

Lemma : (2.7)

If $q_1, q_2, \dots, q_n$ are primes, and $p \mid (q_1 q_2 \dots q_k)$, then $p = q_k$ for some k.

Theorem : Fundamental Theorem of Arithmetic

Any positive integer can be written as a product of primes in one and only one way.

Lemma : (3.1)

If x_0, y_0 is a solution of $ax + by = c$, then for any integer t,

$$x = x_0 + bt$$
$$y = y_0 - at$$

is also a solution.

Lemma : (3.2)

Consider the equation $ax + by = c$. If $(a, b) \mid c$, then $ax + by = c$ has a solution. If $(a, b) \nmid c$, then $ax + by = c$ has no solutions.

Lemma : (3.3)

Consider the equation:

$$ax + by = c$$

Suppose that $(a, b) = 1$ and (x_0, y_0) is a solution, then:

$$x = x_0 + bt, \quad y = y_0 - at$$

provides all of the solutions.

Theorem : (3.1)

Consider $ax + by = c$, if $(a, b) \mid c$, then there are infinitely many solutions of the form

$$x = x_0 + \frac{bt}{(a, b)}, \quad y = y_0 - \frac{at}{(a, b)}$$

Where x_0, y_0 is any solution, and $t \in \mathbb{Z}$.

Definition : Congruence

We say that a and b are congruent to each other modulo m,

$$a \equiv b \mod m$$

if $m \mid (a - b)$.

Theorem : (4.1)

If $a \equiv b \mod m$, then there exists k such that $a = b + km$.

Theorem : (4.2)

There is a unique r, call this the least residue modulo m.

$$a \equiv r \mod m$$

$$r \in \{0, 1, 2, \ldots, m-2, m-1\}$$

Theorem : (4.3)

$a \equiv b \mod m$ if and only if they have the same remainder when divided by m.

Lemma : (4.1)

For integers a, b, c, d, we have that:

- $a \equiv a \mod m$
- If $a \equiv b \mod m$, then $b \equiv a \mod m$
- If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$
- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$
- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$

Theorem : (4.4)

This is listed as a lemma in the in-person notes.

Suppose $ab \equiv ac \mod m$, then if $(a, m) = 1$, then $b \equiv c \mod m$.

Theorem : (4.5)

This is listed as a lemma in the in-person notes.

If $ac \equiv bc \mod m$ and $(c, m) = d$, then $a \equiv b \mod \frac{m}{d}$.

Definition : Linear Congruence

A linear congruence is of the form

$$ax \equiv b \mod m$$

This has a solution if and only if there are integers x and k such that

$$ax = b + km \Leftrightarrow ax - km = b$$

These can be viewed as Diophantine equations.

If one integer satisfies $ax \equiv b \mod m$, then there are infinitely many.

Lemma : (5.1)

If $(a, m) \nmid b$, then $ax \equiv b \mod m$ has no solutions.

Lemma : (5.2)

If $(a, m) = 1$, then $ax \equiv b \mod m$ has exactly one solution.

Lemma : (5.3)

Let $d = (a, m)$. If $d \mid b$, then $ax \equiv b \mod m$ has d solutions.

Theorem : The Chinese Remainder Theorem

The linear congruence system

$$x \equiv a_1 \mod m_1, \qquad x \equiv a_2 \mod m_2, \quad \ldots \quad , x = a_n \mod m_n$$

has a unique solution modulo $m_1 \times m_2 \times \cdots \times m_n$ if for each (m_i, m_j), where $i \neq j$, $(m_i, m_j) = 1$.

Lemma : (6.1)

If $(a, m) = 1$, then the least residues of

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (m-1)\,a \mod m$$

are given by

$$1, \quad 2, \quad 3, \quad \ldots, \quad m-1$$

in some order

Theorem : Fermat's Theorem (Little Theorem)

If p is a prime, and $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \mod p$$

Lemma : (6.2)

$$x^2 \equiv 1 \mod p$$

has exactly 2 solutions, 1 and $p - 1$.

Definition : Modular Multiplicative Inverse

The modular multiplicative inverse of an integer a is an integer a' such that

$$aa' \equiv 1 \mod m$$

If $(a, p) = 1$, we know that $ax \equiv 1 \mod p$ has exactly one solution. Thus, the inverses exist for each non-zero element.

Lemma : (6.3)

Let p be an odd prime, and let a' be the solution of $ax \equiv 1 \mod p$, for $a = 1, 2, \ldots, p-1$. Then, $a' \equiv b' \mod p$ if and only if $a \equiv b \mod p$. Furthermore, $a \equiv a' \mod p$ if and only if $a = 1$ or $a = p - 1$.

Theorem : Wilson's Theorem

p is a prime if and only if

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

Definition

Let n be a positive integer. Then, $d(n)$ is the number of positive divisors of n, including 1 and n. Also, $\sigma(n)$ is the sum of the positive divisors of n. That is,

$$d(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d$$

(Note $\sum_{d|n}$ means the sum over the positive divisors of n)

Theorem : (7.1)

If $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ is the prime-power decomposition of n, then we have that

$$d(n) = d\left(p_1^{e_1}\right) \times d\left(p_2^{e_2}\right) \times \cdots \times d\left(p_k^{e_k}\right)$$

Lemma : (7.1)

If p and q are different primes, then

$$\sigma\left(p^e q^f\right) = \sigma\left(p^e\right) \cdot \sigma\left(q^f\right)$$

Theorem : (7.2)

If $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ is a prime-power decomposition of n, then

$$\sigma(n) = \sigma\left(p_1^{e_1}\right) \sigma\left(p_2^{e_2}\right) \ldots \sigma\left(p_k^{e_k}\right)$$

Definition : Multiplicative Functions

A function f, defined for the positive integers, is said to be multiplicative if and only if

$$(m, n) = 1 \quad \text{implies} \quad f(mn) = f(m) f(n)$$

Theorem : (7.3)

The function d is multiplicative.

Theorem : (7.4)

The function σ is multiplicative.

Theorem : (7.5)

If f is a multiplicative function and the prime power decomposition of n is $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, then

$$f(n) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_k^{e_k}\right)$$

Definition : Perfect Numbers

A number is called perfect if and only if it is equal to the sum of its positive divisors, excluding itself. That is, a number is perfect if and only if

$$\sigma(n) = 2n$$

Theorem : (8.1) (Euclid)

If $2^k - 1$ is prime, then $2^{k-1}\left(2^k - 1\right)$ is perfect.

Lemma

If k is composite, then $2^k - 1$ is composite.

Theorem : (8.2) (Euler)

If n is an even perfect number, then

$$n = 2^{p-1}\left(2^p - 1\right)$$

for some prime p and $2^p - 1$ is also prime.

Definition : Euler's ϕ Function / Euler's Totient Function

If m is a positive integer, let $\phi(m)$ denote the number of positive integers less than or equal to m and relatively prime to m.

Lemma : (9.1)

If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\phi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues modulo m of

$$ar_1, \quad ar_2, \quad \ldots, \quad ar_{\phi(m)}$$

are a permutation of

$$r_1, \quad r_2, \ldots, \quad r_{\phi(m)}$$

Theorem : (9.1) / Euler's Theorem

If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \mod m$$

Lemma : (9.2)

For p prime, and all positive integers n,

$$\phi\left(p^n\right) = p^{n-1}\left(p-1\right)$$

Lemma : (9.3)

If $(a, m) = 1$ and $a \equiv b \mod m$, then $(b, m) = 1$.

Corollary : (9.1)

If the least residues modulo m of $r_1, r_2, \ldots, r_m$ are a permutation of $0, 1, \ldots, m-1$, then $r_1, r_2, \ldots r_m$ contains exactly $\phi\left(m\right)$ elements relatively prime to m.

Theorem : (9.2)

The function ϕ is multiplicative.

Theorem : (9.3)

If n has a prime power decomposition given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. then

$$\phi\left(n\right) = p_1^{e_1-1}\left(p_1-1\right) p_2^{e_2-1}\left(p_2-1\right) \cdots p_k^{e_k-1}\left(p_k-1\right)$$

Corollary : (9.2)

If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi\left(n\right) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

Definition : Arithmetic Functions

An arithmetic function is a function whose domain is the set of positive integers.

Theorem : (9.5)

Let f be an arithmetic function for $n \in \mathbb{Z}$ with $n > 0$. Then, consider the following arithmetic function.

$$F(n) = \sum_{d \mid n} f(d)$$

If f is multiplicative, then F is multiplicative.

Theorem : Gauss' Theorem

Let $n \in \mathbb{Z}$ with $n > 0$. Then

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

Definition : The Möbius μ Function

If $n \in \mathbb{Z}$ with $n > 0$, then the Möbius μ-function, denoted $\mu(n)$, is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ with } p \text{ prime} \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r \text{ with } p_1, \dots, p_r \text{ distinct primes} \end{cases}$$

Theorem : (9.6)

The Möbius μ-function is multiplicative.

Corollary : (9.7)

Let $n \in \mathbb{Z}$ with $n > 0$. Then

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Theorem : Möbius Inversion Formula

Let f and g be arithmetic functions. Then

$$f(n) = \sum_{d \mid n} g(d)$$

If and only if

$$g(n) = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) f(d)$$

Definition : Order

The order of a modulo m is the smallest positive integer t such that

$$a^t \equiv 1 \mod m$$

Theorem : (10.1)

Suppose that $(a, m) = 1$ and a has order t modulo m. Then, $a^n \equiv 1 \mod m$ if and only if n is a multiple of t.

Theorem : (10.2)

If $(a, m) = 1$ and a has order t modulo m, then $t \mid \phi(m)$.

Theorem : (10.3)

If p and q are odd primes and $q \mid a^p - 1$, then $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Corollary : (10.1)

Any divisor of $2^p - 1$ is of the form $2kp + 1$.

Theorem : (10.4)

If the order of a modulo m is t, then $a^r \equiv a^s \mod m$ if and only if $r \equiv s \mod t$.

Definition : Primitive Roots

If a is the least residue and the order of a modulo m is $\phi(m)$, we will say that a is a primitive root of m.

Theorem : (10.5)

If g is a primitive root of m, then the least residues of

$$g, \qquad g^2, \qquad \ldots, \qquad g^{\phi(m)}$$

are a permutation of the $\phi(m)$ positive integers less than m and relatively prime to m.

Lemma : (10.1)

Suppose that a has order t modulo m. Then a^k has order t modulo m if and only if $(k, t) = 1$.

Corollary : (10.2)

Suppose that g is a primitive root of p. Then the least residue of g^k is a primitive root of p if and only if $(k, p-1) = 1$.

Lemma : (10.2)

If f is a polynomial of degree n, then

$$f(x) \equiv 0 \mod p$$

has at most n solutions

Lemma : (10.3)

If $d \mid p-1$, then $x^d \equiv 1 \mod p$ has exactly d solutions.

Theorem : (10.6)

Every prime p has $\phi(p-1)$ primitive roots.

Theorem

The only positive integers with primitive roots are 1, 2, 4, p^e, and $2p^e$, where p is an odd prime.

Theorem : (11.1)

Suppose that p is an odd prime. If $p \nmid a$, then $x^2 \equiv a \mod p$ has exactly two solutions or has no solutions.

Definition : Quadratic Residues

If $x^2 \equiv a \mod m$ has a solution, then a is called a quadratic residue modulo m.

If $x^2 \equiv a \mod m$ has no solution, then a is called a quadratic non-residue modulo m.

Theorem : Euler's Criterion (11.2)

If p is an odd prime and $p \nmid a$, then $x^2 \equiv a \mod p$ has a solution or no respectively, if

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

or

$$a^{\frac{p-1}{2}} \equiv -1 \mod p$$

Theorem : (11.3)

The Legendre symbol has the properties:

1. If $a \equiv b \mod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$
3. If $p \nmid a$ and $p \nmid b$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Theorem : Quadratic Reciprocity Theorem (11.4)

If p and q are odd primes and $p \equiv q \equiv 3 \mod 4$, then

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

If p and q are odd primes and $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

Theorem : (11.5)

If p is an odd prime, then

$$\left(-\frac{1}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 4$$

$$\left(-\frac{1}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 4$$

Theorem : (11.6)

If p is an odd prime, then

$$\left(\frac{2}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 8 \quad \text{or} \quad p \equiv 7 \mod 8$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 8 \quad \text{or} \quad p \equiv 5 \mod 8$$

Theorem : Gauss's Lemma (12.1)

Suppose that p is an odd prime, $(a,p)=1$, and there are among the least residues modulo p of

$$a, \qquad 2a, \qquad 3a, \qquad \ldots, \qquad \frac{p-1}{2}\cdot a$$

Exactly g that are strictly greater than $\frac{p-1}{2}$. Then,

$$\left(\frac{a}{p}\right) = (-1)^g$$

Lemma : (12.1)

If p and q are different odd primes, then

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}$$

Theorem : (12.4)

If p and q are odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Theorem : (12.3)

If p and $4p+1$ are both primes, then 2 is a primitive root modulo $4p+1$.

Theorem

If $p \equiv 2 \mod 3$, then all $x^3 \equiv a \mod p$ have solutions.