Definition

If a and b are integers with $a \neq 0$, we say that a *divides* b if there exists an integer c such that $b = ac$. When a divides b we say that a is a *factor* of b and that b is a *multiple* of a.
The notation $a \mid b$ denotes a divides b and $a \not\mid b$ denotes a does not divide b.

Theorem (1)

Let a, b, and c be integers. Then,

1. *if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$;*
2. *if $a \mid b$ then $a \mid bc$ for all integers c;*
3. *if $a \mid b$ and $b \mid c$ then $a \mid c$;*

Corollary (1)

If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Theorem (2, The division algorithm)

Let a be an integer and d a positive integer. Then, there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Division Algorithm: *If a is any integer and d is any positive integer, then there exist unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.*

Well-Ordering Principle: *Every nonempty set of nonnegative integers has a least element.*

Proof of the Division Algorithm:

Existence:

Let $S = \{a - dn : n \in \mathbb{Z} \text{ and } a - dn \geq 0\}$.

To see that S is nonempty:

If $a \geq 0$, then $a - d \cdot 0 = a \in S$.

If $a < 0$, then $a - d \cdot (2a) = a(1 - 2d) \in S$.

Thus, $S \neq \emptyset$.

Therefore, by well-ordering principle, S has a least element; call it r.

This means that $r = a - dq$ for some integer q.

Since $r \in S$, we have $r \geq 0$.

We must show that $r < d$.

Suppose $r \geq d$.

Then, $r - d \geq 0$.

But, $r = a - dq$. So, we have $r - d = a - dq - d = a - (q + 1)d \geq 0$.

So, $a - (q + 1)d \in S$.

But, $a - (q + 1)d < r$.

This is a contradiction since r was specified to be the least element of S.

Thus, $r < d$.

We have found a pair of integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Uniqueness:

Suppose there exists another pair of integers q' and r', such that $0 \leq r' < d$ and $a = dq' + r'$.

Suppose $r \geq r'$ (a similar proof follows for $r < r'$).

Then $r - r' \geq 0$.

Since $a = dq + r = dq' + r'$, we know that $dq' - dq = r - r'$.

But, $0 \leq r - r'$, so $0 \leq d(q' - q) < d$.

This means that $0 \leq q' - q < 1$.

But $q' - q$ is an integer, so $q' - q = 0$ and hence $q' = q$.

Then $r = a - dq = a - dq' = r'$.

Thus, we have proved that there exist a unique pair of integers q and r, such that $0 \leq r < d$ and $a = dq + r$.

Definition

If a and b are integers and m is a positive integer, then a is *congruent to* b *modulo* m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ if this is the case, and $a \not\equiv b \pmod{m}$, otherwise.

Theorem (3)

Let a and b be integers and let m be a positive integer. Then, $a \equiv b \pmod{m}$ if and only if $a \textbf{ mod } m = b \textbf{ mod } m$.

Theorem (4)

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$

Theorem (5)

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Corollary (2)

Let m be a positive integer and let a and b be integers. Then,

$$(a+b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m$$

Definition

A positive integer $p > 1$ is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than one and is not prime is called *composite*.

Theorem (The Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Theorem

There are infinitely many primes.

Definition

Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b, and is denoted by $\gcd(a, b)$.

Definition

The integers a and b are *relatively prime* if $\gcd(a, b) = 1$.

Proposition

Let a and b be positive integers and let $p_1, p_2, \ldots, p_n$ be all the primes that appear in the prime factorization of a or b, so that

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each $a_i, b_i \geq 0$ for $1 \leq i \leq n$. Then,

$$\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

Definition

The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b, denoted by lcm(a, b).

Proposition

Let a and b be positive integers and let $p_1, p_2, \ldots, p_n$ be all the primes that appear in the prime factorization of a or b, so that

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each $a_i, b_i \geq 0$ for $1 \leq i \leq n$. Then,

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

Theorem

Let a and b be positive integers. Then,

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

Lemma

Let $a = bq + r$ where a, b, q and r are integers. Then gcd$(a, b) =$gcd(b, r).

Theorem (A)

If a and b are positive integers, then there exist integers s and t such that gcd$(a, b) = sa + tb$.

Lemma (A)

If a, b, and c are positive integers such that gcd$(a, b) = 1$ and $a|bc$, then $a|c$.

Lemma (B)

If p is a prime and $p|a_1a_2\cdots a_n$, where each a_i is an integer, then $p|a_i$ for some i.

Theorem (B)

Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and gcd$(c, m) = 1$, then $a \equiv b \pmod{m}$.

Theorem

If a and m are relatively prime integers with $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

Computing the inverse of 24 modulo 7

Applying the extended Euclidean Algorithm:

$$\begin{aligned} 24 &= 3 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

Using backward substitution:

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (24 - 3 \cdot 7) = -2 \cdot 24 + 7 \cdot 7.$$

So $s = -2$ and $t = 7$.

$$-2 \cdot 24 \equiv 1 \pmod{7}$$

You can use as an inverse of 24 modulo 7, any integer equivalent to -2 modulo 7, such as: $\ldots, -9, -2, 5, 12, 19, \ldots$

Example:
5 is an inverse of $3 \pmod 7$, since $5 \cdot 3 \equiv 15 \equiv 1 \pmod 7$.
Using this we can solve:

$$\begin{aligned} 3x &\equiv 4 \pmod 7 \\ 5 \cdot 3x &\equiv 5 \cdot 4 \pmod 7 \\ 1 \cdot x &\equiv 20 \pmod 7 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Substitute back into the original linear congruence to check that 6 is a solution:

$$3 \cdot 6 \equiv 18 \equiv 4 \pmod 7.$$

Theorem (Chinese Reminder Theorem)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then, the system:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ \ldots & \quad \ldots \\ x &\equiv a_n \pmod{m_n}, \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution).

$x \equiv 3 \pmod 5$

$x \equiv 1 \pmod 7$

$x \equiv 6 \pmod 8$

$x \equiv b_1 \pmod{n_1}$

$x \equiv b_2 \pmod{n_2}$

$x \equiv b_3 \pmod{n_3}$

b_i	N_i	x_i	$b_i N_i x_i$
b_1	$N_1 = n_2 n_3$	x_1	$b_1 N_1 x_1$
b_2	$N_2 = n_1 n_3$	x_2	$b_2 N_2 x_2$
b_3	$N_3 = n_1 n_2$	x_3	$b_3 N_3 x_3$

$$x = \sum_{i=1}^{3} b_i N_i x_i \pmod N$$

$N = n_1 n_2 n_3$

$N_i = \frac{N}{n_i}$

$x \equiv 3 \pmod 5$

$x \equiv 1 \pmod 7$

$x \equiv 6 \pmod 8$

b_i	$N_i = \frac{N}{N_i}$	x_i	$b_i N_i x_i$
b_1	$N_1 = n_2 n_3$	x_1	$b_1 N_1 x_1$
b_2	$N_2 = n_1 n_3$	x_2	$b_2 N_2 x_2$
b_3	$N_3 = n_1 n_2$	x_3	$b_3 N_3 x_3$

Remainders

Inverse of N_i

$N = n_1 n_2 n_3$

$N_i = \frac{N}{n_i}$

$$\boxed{x = \sum_{i=1}^{3} b_i N_i x_i \pmod N}$$

$N = 5 \times 7 \times 8$
$= 280$

b_i	N_i	x_i	$b_i N_i x_i$
3	56	1	168
1	40	3	120
6	35	3	630

$x = 168 + 120 + 630 = 918$

$x \equiv 918 \pmod{280}$

$x \equiv 78 \pmod{280}$

$$a \equiv b \pmod m \quad \Rightarrow \quad a^k \equiv b^k \pmod m \text{ for any positive integer } k.$$

Euler's phi (or totient) function of a positive integer n is the number of integers in $\{1,2,3,\ldots,n\}$ which are relatively prime to n. This is usually denoted $\varphi(n)$.

integer n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

Clearly for primes p, $\varphi(p)=p-1$. Since $\varphi(x)$ is a multiplicative function, its value can be determined from its value at the prime powers:

$$\phi(p^a) = p^a - p^{a-1}$$

Example 3.8.10

$$\phi(2^3 3^4 7^2) = \phi(2^3)\phi(3^4 7^2) = \phi(2^3)\phi(3^4)\phi(7^2) = (2^3 - 2^2)(3^4 - 3^3)(7^2 - 7)$$

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

$$2^{17-1} \equiv 1 \pmod{17}$$

$$4^{532} = 4^{10 \times 53 + 2}$$
$$= (4^{10})^{53} \times 4^{2}$$
$$\equiv 1^{53} \times 16 \pmod{11}$$
$$\equiv 1 \times 5 \pmod{11}$$
$$\equiv 5 \pmod{11}$$

$$a^{p-1} \equiv 1 \pmod{p}$$
$$4^{11-1} \equiv 1 \pmod{11}$$
$$4^{10} \equiv 1 \pmod{11}$$

$$532 = 10 \times 53 + 2$$

FERMAT'S LITTLE THEOREM If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer a we have

$$a^{p} \equiv a \pmod{p}.$$

Let b be a positive integer. If n is a composite positive integer, and $b^{n-1} \equiv 1 \pmod{n}$, then n is called a *pseudoprime to the base b*.

A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b with $\gcd(b, n) = 1$ is called a *Carmichael number*. (These numbers are named after Robert Carmichael, who studied them in the early twentieth century.)

$p=23 \quad g=5$

You	Friend
$a=6$	$b=4$
$5^6 \pmod{23} = 8$	$5^4 \pmod{23} = 4$
$4^6 \pmod{23} = 2$	$8^4 \pmod{23} = 2$

THE PRODUCT RULE Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Combinations

- Definition: $\binom{n}{k}$: number of k-element subsets of a given n-element set $\boxed{= \dfrac{n!}{k!(n-k)!}}$

Binomial coefficient $\binom{n}{k}$ $\longrightarrow$ **Binomial probabilities**

- $n \geq 1$ independent coin tosses; $\mathbf{P}(H) = p$ $\boxed{\mathbf{P}(k \text{ heads}) = \binom{n}{k} p^k (1-p)^{n-k}}$

THE SUM RULE If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

THE SUBTRACTION RULE If a task can be done in either n_1 ways or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.

THE DIVISION RULE There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.

The Binomial Formula

$$(X+Y)^n =$$

$$\binom{n}{0}Y^n + \binom{n}{1}XY^{n-1} + \binom{n}{2}X^2Y^{n-2} + \dots + \binom{n}{k}X^kY^{n-k} + \dots + \binom{n}{n}X^n$$

The Binomial Formula

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

THE BINOMIAL THEOREM Let x and y be variables, and let n be a nonnegative integer. Then

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

There are $C(n+r-1, r) = C(n+r-1, n-1)$ r-combinations from a set with n elements when repetition of elements is allowed.

A *linear homogeneous recurrence relation of degree k with constant coefficients* is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

THEOREM 1 Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n = 0, 1, 2, \ldots$, where α_1 and α_2 are constants.

THEOREM 2

Let c_1 and c_2 be real numbers with $c_2 \neq 0$. Suppose that $r^2 - c_1 r - c_2 = 0$ has only one root r_0. A sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$, for $n = 0, 1, 2, \ldots,$ where α_1 and α_2 are constants.

THEOREM 3

Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has k distinct roots $r_1, r_2, \ldots, r_k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

for $n = 0, 1, 2, \ldots,$ where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are constants.

We illustrate the use of the theorem with Example 6.

THEOREM 4

Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has t distinct roots $r_1, r_2, \ldots, r_t$ with multiplicities $m_1, m_2, \ldots, m_t$, respectively, so that $m_i \geq 1$ for $i = 1, 2, \ldots, t$ and $m_1 + m_2 + \cdots + m_t = k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$\begin{aligned} a_n = {} & (\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n \\ & + (\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{2,m_2-1} n^{m_2-1}) r_2^n \\ & + \cdots + (\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n \end{aligned}$$

for $n = 0, 1, 2, \ldots,$ where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_i - 1$.

THEOREM 1 Let f be an increasing function that satisfies the recurrence relation

$$f(n) = af(n/b) + c$$

whenever n is divisible by b, where $a \geq 1$, b is an integer greater than 1, and c is a positive real number. Then

$$f(n) \text{ is } \begin{cases} O(n^{\log_b a}) & \text{if } a > 1, \\ O(\log n) & \text{if } a = 1. \end{cases}$$

Furthermore, when $n = b^k$ and $a \neq 1$, where k is a positive integer,

$$f(n) = C_1 n^{\log_b a} + C_2,$$

where $C_1 = f(1) + c/(a-1)$ and $C_2 = -c/(a-1)$.

MASTER THEOREM Let f be an increasing function that satisfies the recurrence relation

$$f(n) = af(n/b) + cn^d$$

whenever $n = b^k$, where k is a positive integer, $a \geq 1$, b is an integer greater than 1, and c and d are real numbers with c positive and d nonnegative. Then

$$f(n) \text{ is } \begin{cases} O(n^d) & \text{if } a < b^d, \\ O(n^d \log n) & \text{if } a = b^d, \\ O(n^{\log_b a}) & \text{if } a > b^d. \end{cases}$$

DEFINITION 1 The *generating function for the sequence* $a_0, a_1, \ldots, a_k, \ldots$ of real numbers is the infinite series

$$G(x) = a_0 + a_1 x + \cdots + a_k x^k + \cdots = \sum_{k=0}^{\infty} a_k x^k.$$

DEFINITION 1 The *generating function for the sequence* $a_0, a_1, \ldots, a_k, \ldots$ of real numbers is the infinite series

$$G(x) = a_0 + a_1 x + \cdots + a_k x^k + \cdots = \sum_{k=0}^{\infty} a_k x^k.$$

THEOREM 1 Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$. Then

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k \quad \text{and} \quad f(x)g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k.$$

DEFINITION 2 Let u be a real number and k a nonnegative integer. Then the *extended binomial coefficient* $\binom{u}{k}$ is defined by

$$\binom{u}{k} = \begin{cases} u(u-1)\cdots(u-k+1)/k! & \text{if } k > 0, \\ 1 & \text{if } k = 0. \end{cases}$$

THEOREM 2 **THE EXTENDED BINOMIAL THEOREM** Let x be a real number with $|x| < 1$ and let u be a real number. Then

$$(1 + x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k.$$

TABLE 1 **Useful Generating Functions.**

$G(x)$	a_k
$(1+x)^n = \sum_{k=0}^{n} C(n,k)x^k$ $= 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	$C(n,k)$
$(1+ax)^n = \sum_{k=0}^{n} C(n,k)a^k x^k$ $= 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^n x^n$	$C(n,k)a^k$
$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)x^{rk}$ $= 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	$C(n,k/r)$ if $r \mid k$; 0 otherwise
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	1 if $k \le n$; 0 otherwise
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k = 1 + ax + a^2x^2 + \cdots$	a^k
$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	1 if $r \mid k$; 0 otherwise
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	$k+1$
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k$ $= 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n+k-1,k) = C(n+k-1,n-1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^k x^k$ $= 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^k C(n+k-1,k) = (-1)^k C(n+k-1,n-1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)a^k x^k$ $= 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n+k-1,k)a^k = C(n+k-1,n-1)a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$1/k!$
$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$(-1)^{k+1}/k$

Note: The series for the last two generating functions can be found in most calculus books when power series are discussed.