Sums. Let n be a natural number and x be a real number.

- $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$
- $0 + 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
- $1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}$

Pascal's Rule. Let n be a positive integer and k be a natural number less than n.

- $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

Binomial Theorem. Let n be a a natural number.

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

Divisibility Properties. Let a, b, c, d be integers.

- If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
- If $a \mid b$ and $b \mid c$, then $a \mid c$.
- If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for integers x, y.
- If $a \perp b$, and $a \mid c$ and $b \mid c$, then $ab \mid c$.
- If $a \mid bc$ and $a \perp b$, then $a \mid c$.

Divisors/Multiples. Let a, b be integers w/ $\gcd(a,b) = d$.

- Any common divisor of a and b also divides d.
- There exist integers x and y so $ax + by = d$.
- $(a/d) \perp (b/d)$
- If k is a pos. integer, then $\gcd(ka, kb) = kd$.
- If c is another integer, $\gcd(a,b,c) = \gcd(d,c)$.
- $\operatorname{lcm}(a,b) = (ab)/d$
- $\operatorname{lcm}(a,b)$ divides any common multiple of a and b.
- if $a \perp b$, then the divisors of ab are uniquely of the form d_1d_2 where $d_1 \mid a$ and $d_2 \mid b$

Diophantines. Let a, b, c be integers with $\gcd(a,b) = d$. Consider Diophantine equation $ax + by = c$.

- It admits an integer solution pair iff $d \mid c$.
- If x_0, y_0 is one solution pair, the general solution is:

  $x = x_0 + (b/d)t$

  $y = y_0 - (a/d)t$

  where t is any integer.

Primes. Let p be prime and a, $a_1, \ldots, a_n$ be integers.

- $p \perp a$ iff $p \nmid a$.
- If $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for at least one a_i.

Square–Free. Positive integer n is square–free iff:

- n is not divisible by any perfect square besides 1.
- or equivalently: n is 1 or a prod. of distinct primes.

Primes Under 100.

- from 1 to 20 are: 2, 3, 5, 7, 11, 13, 17, 19
- from 20 to 40 are: 23, 29, 31, 37
- from 40 to 60 are: 41, 43, 47, 53, 59
- from 60 to 80 are: 61, 67, 71, 73, 79
- from 80 to 100 are: 83, 89, 97

Dirichlet's Theorem. Let $a \perp b$ be given.

- There are infinitely many primes of the form $an + b$ where n is a positive integer.

Fixed Modulus. Let n be a positive integer and a, b, c, d be integers. All $\equiv$ below are modulo n.

- $a \equiv a$
- If $a \equiv b$, then $b \equiv a$.
- If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.
- If $a \equiv b$ and $c \equiv d$, then $a + c \equiv b + d$ and $ac \equiv bd$.
- If $a \equiv b$, then $a + c \equiv b + c$ and $ac \equiv bc$.
- If $a \equiv b$, then $a^k \equiv b^k$ for any positive integer k.
- If $a \perp n$, then there exists integer a^{-1} so $aa^{-1} \equiv 1$.
- If $a \perp n$, then $ax \equiv b$ has a unique solution mod n.
- If $a \equiv b$, then $\gcd(a,n) = \gcd(b,n)$.

Changing Moduli. Let k, m, n be positive integers and a, b be integers.

- $a \equiv b \mod n$ iff $ka \equiv kb \mod kn$
- if $a \equiv b \mod n$ and $d \mid n$, then $a \equiv b \mod d$
- if $m \perp n$, then $a \equiv b \mod mn$ if and only if both:

  $a \equiv b \mod m$ and $a \equiv b \mod n$

Chinese Remainder Theorem. Let $n_1, \ldots, n_r$ be relatively prime and $a_1, \ldots, a_r$ be integers. Let $n = n_1 \ldots n_r$. Then:

$x \equiv a_1 \mod n_1, \ldots, x \equiv a_r \mod n_r$

is solved by $x = a_1 x_1 N_1 + \cdots + a_r x_r N_r$ where:

$N_k = n/n_k$ and $N_k x_k \equiv 1 \mod n_k$

This solution is unique modulo n.

Fermat's Theorem. Let p be prime and a an integer.

- $a^p \equiv a \mod p$

Pseudoprimes. Let n be a composite integer.

- n is an absolute pseudoprime iff $a^n \equiv a \mod n$ for all integers a
- absolute pseudoprimes are square–free

Wilson's Theorem. Let n be an integer.

- n prime if and only if $(n-1)! \equiv -1 \mod n$

Square–Root of -1. Let p be an odd prime.

- $x^2 \equiv -1 \mod p$ is solvable iff $p \equiv 1 \mod 4$, in which case a solution is given by $x = ([p-1]/2)!$.

Multiplicative Functions. Let f, g be arithmetic and m, n be positive integers and p be prime.

- multiplicative functions are uniquely determined by their values on powers of primes.
- if f is multiplicative, and r is a real number, f^r is multiplicative
- if f and g are multiplicative, then so is fg
- 1, id, τ, σ, and ϕ are multiplicative.
- $\tau(p^n) = n+1$, $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$, $\phi(p^n) = p^n - p^{n-1}$

Sum Notation. Let f, g arithmetic and n integer.

- $\sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) g(d_2) = \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} g(d_2)$

Convolutions. Let f, g, h arithmetic and n integer.

- $(f * g)(n) = \sum_{d \mid n} f(d) g(n/d)$
- $f * g = g * f$ and $(f * g) * h = f * (g * h)$
- convolutions preserve multiplicativeness.
- $\tau = 1 * 1$, $\sigma = \mathrm{id} * 1$, $f * \epsilon = f$, and $1 * \mu = \epsilon$

Floor Function. Let x be real and m, n integers.

- if $x - 1 < n \leqslant x$ then $\lfloor x \rfloor = n$
- $n \div m$ has quotient $\lfloor n/m \rfloor$ and remainder $m \cdot \{n/m\}$
- the exp. of the max power of prime p dividing $n!$ is:

  $\sum_{k=1}^{\infty} \lfloor n/p^k \rfloor$

  or, if $n = (a_m \cdots a_0)_p$ in base p, this exponent is:

  $(n - [a_m + \cdots + a_0])/(p-1)$
- if f arithmetic and $F = f * 1$, then:

  $\sum_{k=1}^{n} F(k) = \sum_{k=1}^{n} f(k) \lfloor n/k \rfloor$

Properties of Phi. Let n be a positive integer.

- $\sqrt{n}/2 \leqslant \phi(n) \leqslant n$
- if $a \perp n$ then $a^{\phi(n)} \equiv 1 \mod n$
- $\phi * 1 = \mathrm{id}$
- the sum of $\perp n$ integers from $1 \ldots n$ is $n\phi(n)/2$.

Order. Let n be a positive integer and $a \perp n$ with order $\mathrm{ord}(a)$ modulo n. Let k, h be integers.

- $\mathrm{ord}(a) \mid n$
- $\mathrm{ord}(a^k) = \mathrm{ord}(a)/\gcd(\mathrm{ord}(a), k)$
- $a^k \equiv a^h \mod n$ iff $k \equiv h \mod \mathrm{ord}(a)$

Lagrange. Let p prime and $M(x)$ a deg. d monomial.

- $M(x)$ has at most d roots modulo p.
- if $d \mid p-1$, then $x^d - 1$ has d incong. roots mod p.

Primitives. Let p an odd prime and n a pos. integer.

- 2, 4, p^n, and $2p^n$ have primitive roots
- a primitive root of p^2 is a primitive root of p^n
- an odd primitive root of p^n is a primitive root of $2p^n$