

Combinatorics

Sums

$$\begin{aligned}
 \sum_{k=0}^n k &= n(n+1)/2 & \sum_{k=a}^b k &= (a+b)(b-a+1)/2 \\
 \sum_{k=0}^n k^2 &= n(n+1)(2n+1)/6 & \sum_{k=0}^n k^3 &= n^2(n+1)^2/4 \\
 \sum_{k=0}^n k^4 &= (6n^5 + 15n^4 + 10n^3 - n)/30 & \sum_{k=0}^n k^5 &= (2n^6 + 6n^5 + 5n^4 - n^2)/12 \\
 \sum_{k=0}^n x^k &= (x^{n+1} - 1)/(x - 1) & \sum_{k=0}^n kx^k &= (x - (n+1)x^{n+1} + nx^{n+2})/(x-1)^2 \\
 1 + x + x^2 + \dots &= 1/(1-x)
 \end{aligned}$$

Binomial coefficients

	0	1	2	3	4	5	6	7	8	9	10	11	12	$\binom{n}{k} = \frac{n!}{(n-k)!k!}$
0	1													$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
1	1	1												$\binom{n+1}{k} = \frac{n+1}{n-k+1} \binom{n}{k}$
2	1	2	1											$\binom{n}{k+1} = \frac{n-k}{k+1} \binom{n}{k}$
3	1	3	3	1										$\binom{n}{k} = \frac{n}{n-k} \binom{n-1}{k}$
4	1	4	6	4	1									$\binom{n}{k} = \frac{n-k+1}{k} \binom{n}{k-1}$
5	1	5	10	10	5	1								$12! \approx 2^{28.8}$
6	1	6	15	20	15	6	1							$20! \approx 2^{61.1}$
7	1	7	21	35	35	21	7	1						
8	1	8	28	56	70	56	28	8	1					
9	1	9	36	84	126	126	84	36	9	1				
10	1	10	45	120	210	252	210	120	45	10	1			
11	1	11	55	165	330	462	462	330	165	55	11	1		
12	1	12	66	220	495	792	924	792	495	220	66	12	1	
	0	1	2	3	4	5	6	7	8	9	10	11	12	

Number of ways to pick a multiset of size k from n elements: $\binom{n+k-1}{k}$

Number of n -tuples of non-negative integers with sum s : $\binom{s+n-1}{n-1}$, at most s : $\binom{s+n}{n}$

Number of n -tuples of positive integers with sum s : $\binom{s-1}{n-1}$

Number of lattice paths from $(0,0)$ to (a,b) , restricted to east and north steps: $\binom{a+b}{a}$

Multinomial theorem. $(a_1 + \dots + a_k)^n = \sum \binom{n}{n_1, \dots, n_k} a_1^{n_1} \dots a_k^{n_k}$, where $n_i \geq 0$ and $\sum n_i = n$.

$$\binom{n}{n_1, \dots, n_k} = M(n_1, \dots, n_k) = \frac{n!}{n_1! \dots n_k!}. \quad M(a, \dots, b, c, \dots) = M(a + \dots + b, c, \dots) M(a, \dots, b)$$

Catalan numbers. $C_n = \frac{1}{n+1} \binom{2n}{n}$. $C_0 = 1$, $C_n = \sum_{i=0}^{n-1} C_i C_{n-1-i}$. $C_{n+1} = C_n \frac{4n+2}{n+2}$.

$C_0, C_1, \dots = 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900, \dots$

C_n is the number of: properly nested sequences of n pairs of parentheses; rooted ordered binary trees with $n+1$ leaves; triangulations of a convex $(n+2)$ -gon.

Derangements. Number of permutations of $n = 0, 1, 2, \dots$ elements without fixed points is $1, 0, 1, 2, 9, 44, 265, 1854, 14833, \dots$ Recurrence: $D_n = (n-1)(D_{n-1} + D_{n-2}) = nD_{n-1} + (-1)^n$. Corollary: number of permutations with exactly k fixed points is $\binom{n}{k} D_{n-k}$.

Stirling numbers of 1st kind. $s_{n,k}$ is $(-1)^{n-k}$ times the number of permutations of n elements with exactly k permutation cycles. $|s_{n,k}| = |s_{n-1,k-1}| + (n-1)|s_{n-1,k}|$. $\sum_{k=0}^n s_{n,k} x^k = x^n$

Stirling numbers of 2nd kind. $S_{n,k}$ is the number of ways to partition a set of n elements into exactly k non-empty subsets. $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$. $S_{n,1} = S_{n,n} = 1$. $x^n = \sum_{k=0}^n S_{n,k} x^k$

Bell numbers. B_n is the number of partitions of n elements. $B_0, \dots = 1, 1, 2, 5, 15, 52, 203, \dots$ $B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k = \sum_{k=1}^n S_{n,k}$. Bell triangle: $B_r = a_{r,1} = a_{r-1,r-1}$, $a_{r,c} = a_{r-1,c-1} + a_{r,c-1}$.

Bernoulli numbers. $\sum_{k=0}^{m-1} k^n = \frac{1}{n+1} \sum_{k=0}^n \binom{n+1}{k} B_k m^{n+1-k}$.
 $\sum_{j=0}^m \binom{m+1}{j} B_j = 0$. $B_0 = 1$, $B_1 = -\frac{1}{2}$. $B_n = 0$, for all odd $n \neq 1$.

Eulerian numbers. $E(n, k)$ is the number of permutations with exactly k descents ($i : \pi_i < \pi_{i+1}$) / ascents ($\pi_i > \pi_{i+1}$) / excedances ($\pi_i > i$) / $k+1$ weak excedances ($\pi_i \geq i$).
 Formula: $E(n, k) = (k+1)E(n-1, k) + (n-k)E(n-1, k-1)$. $x^n = \sum_{k=0}^{n-1} E(n, k) \binom{x+k}{n}$.

Burnside's lemma. The number of orbits under group G 's action on set X :

$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X_g|$, where $X_g = \{x \in X : g(x) = x\}$. ("Average number of fixed points.")

Let $w(x)$ be weight of x 's orbit. Sum of all orbits' weights: $\sum_{o \in X/G} w(o) = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in X_g} w(x)$.

Number Theory

Linear diophantine equation. $ax + by = c$. Let $d = \gcd(a, b)$. A solution exists iff $d|c$. If (x_0, y_0) is any solution, then all solutions are given by $(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$, $t \in \mathbb{Z}$. To find some solution (x_0, y_0) , use extended GCD to solve $ax_0 + by_0 = d = \gcd(a, b)$, and multiply its solutions by $\frac{c}{d}$.

Linear diophantine equation in n variables: $a_1x_1 + \dots + a_nx_n = c$ has solutions iff $\gcd(a_1, \dots, a_n)|c$. To find some solution, let $b = \gcd(a_2, \dots, a_n)$, solve $a_1x_1 + by = c$, and iterate with $a_2x_2 + \dots = y$.

Extended GCD

```
// Finds g = gcd(a,b) and x, y such that ax+by=g. Bounds: |x|<=b+1, |y|<=a+1.
void gcdext(int &g, int &x, int &y, int a, int b)
{ if (b == 0) { g = a; x = 1; y = 0; }
  else      { gcdext(g, y, x, b, a % b); y = y - (a / b) * x; } }
```

Multiplicative inverse of a modulo m : x in $ax + my = 1$, or $a^{\phi(m)-1} \pmod{m}$.

Chinese Remainder Theorem. System $x \equiv a_i \pmod{m_i}$ for $i = 1, \dots, n$, with pairwise relatively-prime m_i has a unique solution modulo $M = m_1m_2 \dots m_n$: $x = a_1b_1\frac{M}{m_1} + \dots + a_nb_n\frac{M}{m_n} \pmod{M}$, where b_i is modular inverse of $\frac{M}{m_i}$ modulo m_i .

System $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ has solutions iff $a \equiv b \pmod{g}$, where $g = \gcd(m, n)$. The solution is unique modulo $L = \frac{mn}{g}$, and equals: $x \equiv a + T(b-a)m/g \equiv b + S(a-b)n/g \pmod{L}$, where S and T are integer solutions of $mT + nS = \gcd(m, n)$.

Prime-counting function. $\pi(n) = |\{p \leq n : p \text{ is prime}\}|$. $n/\ln(n) < \pi(n) < 1.3n/\ln(n)$.
 $\pi(1000) = 168$, $\pi(10^6) = 78498$, $\pi(10^9) = 50\,847\,534$. n -th prime $\approx n \ln n$.

Miller-Rabin's primality test. Given $n = 2^r s + 1$ with odd s , and a random integer $1 < a < n$. If $a^s \equiv 1 \pmod{n}$ or $a^{2^j s} \equiv -1 \pmod{n}$ for some $0 \leq j \leq r-1$, then n is a probable prime. With bases 2, 7 and 61, the test identifies all composites below 2^{32} . Probability of failure for a random a is at most $1/4$.

Pollard- ρ . Choose random x_1 , and let $x_{i+1} = x_i^2 - 1 \pmod{n}$. Test $\gcd(n, x_{2k+i} - x_{2k})$ as possible n 's factors for $k = 0, 1, \dots$. Expected time to find a factor: $O(\sqrt{m})$, where m is smallest prime power in n 's factorization. That's $O(n^{1/4})$ if you check $n = p^k$ as a special case before factorization.

Fermat primes. A Fermat prime is a prime of form $2^{2^n} + 1$. The only known Fermat primes are 3, 5, 17, 257, 65537. A number of form $2^n + 1$ is prime only if it is a Fermat prime.

Perfect numbers. $n > 1$ is called perfect if it equals sum of its proper divisors and 1. Even n is perfect iff $n = 2^{p-1}(2^p - 1)$ and $2^p - 1$ is prime (Mersenne's). No odd perfect numbers are yet found.

Carmichael numbers. A positive composite n is a Carmichael number ($a^{n-1} \equiv 1 \pmod{n}$ for all a : $\gcd(a, n) = 1$), iff n is square-free, and for all prime divisors p of n , $p - 1$ divides $n - 1$.

Number/sum of divisors. $\tau(p_1^{a_1} \dots p_k^{a_k}) = \prod_{j=1}^k (a_j + 1)$. $\sigma(p_1^{a_1} \dots p_k^{a_k}) = \prod_{j=1}^k \frac{p_j^{a_j+1} - 1}{p_j - 1}$.

Euler's phi function. $\phi(n) = |\{m \in \mathbb{N}, m \leq n, \gcd(m, n) = 1\}|$.
 $\phi(mn) = \frac{\phi(m)\phi(n)\gcd(m,n)}{\phi(\gcd(m,n))}$. $\phi(p^a) = p^{a-1}(p-1)$. $\sum_{d|n} \phi(d) = \sum_{d|n} \phi(\frac{n}{d}) = n$.

Euler's theorem. $a^{\phi(n)} \equiv 1 \pmod{n}$, if $\gcd(a, n) = 1$.

Wilson's theorem. p is prime iff $(p-1)! \equiv -1 \pmod{p}$.

Mobius function. $\mu(1) = 1$. $\mu(n) = 0$, if n is not squarefree. $\mu(n) = (-1)^s$, if n is the product of s distinct primes. Let f, F be functions on positive integers. If for all $n \in \mathbb{N}$, $F(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d})$, and vice versa. $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$. $\sum_{d|n} \mu(d) = 1$.
 If f is multiplicative, then $\sum_{d|n} \mu(d)f(d) = \prod_{p|n} (1 - f(p))$, $\sum_{d|n} \mu(d)^2 f(d) = \prod_{p|n} (1 + f(p))$.

Legendre symbol. If p is an odd prime, $a \in \mathbb{Z}$, then $\left(\frac{a}{p}\right)$ equals 0, if $p|a$; 1 if a is a quadratic residue modulo p ; and -1 otherwise. Euler's criterion: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$.

Jacobi symbol. If $n = p_1^{a_1} \dots p_k^{a_k}$ is odd, then $\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{k_i}$.

Primitive roots. If the order of g modulo m ($\min n > 0: g^n \equiv 1 \pmod{m}$) is $\phi(m)$, then g is called a primitive root. If Z_m has a primitive root, then it has $\phi(\phi(m))$ distinct primitive roots. Z_m has a primitive root iff m is one of $2, 4, p^k, 2p^k$, where p is an odd prime. If Z_m has a primitive root g , then for all a coprime to m , there exists unique integer $i = \text{ind}_g(a)$ modulo $\phi(m)$, such that $g^i \equiv a \pmod{m}$. $\text{ind}_g(a)$ has logarithm-like properties: $\text{ind}(1) = 0$, $\text{ind}(ab) = \text{ind}(a) + \text{ind}(b)$.

If p is prime and a is not divisible by p , then congruence $x^n \equiv a \pmod{p}$ has $\gcd(n, p-1)$ solutions if $a^{(p-1)/\gcd(n, p-1)} \equiv 1 \pmod{p}$, and no solutions otherwise. (Proof sketch: let g be a primitive root, and $g^i \equiv a \pmod{p}$, $g^u \equiv x \pmod{p}$. $x^n \equiv a \pmod{p}$ iff $g^{nu} \equiv g^i \pmod{p}$ iff $nu \equiv i \pmod{p}$.)

Discrete logarithm problem. Find x from $a^x \equiv b \pmod{m}$. Can be solved in $O(\sqrt{m})$ time and space with a meet-in-the-middle trick. Let $n = \lceil \sqrt{m} \rceil$, and $x = ny - z$. Equation becomes $a^{ny} \equiv ba^z \pmod{m}$. Precompute all values that the RHS can take for $z = 0, 1, \dots, n-1$, and brute force y on the LHS, each time checking whether there's a corresponding value for RHS.

Pythagorean triples. Integer solutions of $x^2 + y^2 = z^2$. All relatively prime triples are given by: $x = 2mn, y = m^2 - n^2, z = m^2 + n^2$ where $m > n, \gcd(m, n) = 1$ and $m \not\equiv n \pmod{2}$. All other triples are multiples of these. Equation $x^2 + y^2 = 2z^2$ is equivalent to $(\frac{x+y}{2})^2 + (\frac{x-y}{2})^2 = z^2$.

Postage stamps/McNuggets problem. Let a, b be relatively-prime integers. There are exactly $\frac{1}{2}(a-1)(b-1)$ numbers *not* of form $ax + by$ ($x, y \geq 0$), and the largest is $(a-1)(b-1) - 1 = ab - a - b$.

Fermat's two-squares theorem. Odd prime p can be represented as a sum of two squares iff $p \equiv 1 \pmod{4}$. A product of two sums of two squares is a sum of two squares. Thus, n is a sum of two squares iff every prime of form $p = 4k + 3$ occurs an even number of times in n 's factorization.

RSA. Let p and q be random distinct large primes, $n = pq$. Choose a small odd integer e , relatively prime to $\phi(n) = (p-1)(q-1)$, and let $d = e^{-1} \pmod{\phi(n)}$. Pairs (e, n) and (d, n) are the public and secret keys, respectively. Encryption is done by raising a message $M \in Z_n$ to the power e or d , modulo n .