ICPC Math Table

* p is prime

1 Number Theory

Fermat's little theorem

$$a^{p-1} \equiv 1 \pmod p$$
$$a^{\phi(n)} \equiv 1 \pmod n \text{ where } \gcd(a,n) = 1$$
$$a^m \equiv a^{m\%\phi(n)+\phi(n)} \pmod n$$

Euler's totient function

$\phi(n) = |\{x \mid 1 \le x \le n, \gcd(x,n) = 1\}|$

$$\phi(n) = n\prod_{p|n}(1 - \frac{1}{p})$$
$$\phi(mn) = \phi(m)\phi(n) \text{ if } \gcd(m,n) = 1$$
$$\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)} \text{ where } d = \gcd(m,n)$$
$$\phi(m)\phi(n) = \phi(lcm(m,n))\phi(\gcd(m,n))$$
$$\sum_{d|n}\phi(d) = n$$
$$\sum_{d|n}\frac{n}{d}\phi(d) = \sum_{k=1..n}\gcd(k,n)$$
$$\phi(n)d(n) = \sum_{k=1..n}^{\gcd(k,n)=1}\gcd(k-1,n) \text{ where } d(n) = \text{ \# of divisors of n}$$
$$\frac{1}{2}n\phi(n) = \sum_{k=1..n}^{\gcd(k,n)=1} k$$
$$a \mid b \to \phi(a) \mid \phi(b)$$
$$n \mid \phi(a^n - 1) \text{ for } a, n > 1$$

Mobius function

$$\mu(n) = \begin{cases} 0 \text{ if } n \text{ has squared prime factor} \\ 1 \text{ if } n \text{ has even \# of prime factors} \\ -1 \text{ if } n \text{ has odd \# of prime factors} \end{cases}$$

$$\sum_{d|n}\mu(d) = [n == 1]$$
$$n\sum_{d|n}\frac{\mu(d)}{d} = \phi(n)$$
$$\sum_{d|n}\frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$$
$$\forall n, g(n) = \sum_{d|n} f(d) \to \forall n, f(n) = \sum_{d|n}\mu(d)g(\frac{n}{d})$$

Primality criteria (p is prime iff)

$$\prod_{1\le k\le p-1}(2^k - 1) \equiv p \mod (2^p - 1)$$
$$(p-1)! \equiv -1 \mod p$$

---

2 Combinatorics

$$\binom{n}{0} + \ldots + \binom{n}{n} = 2^n$$
$$\binom{n}{0} + \binom{n}{2} + \ldots = 2^{n-1}$$
$$\binom{n}{1} + \binom{n}{3} + \ldots = 2^{n-1}$$
$$0\binom{n}{0} + \ldots + n\binom{n}{n} = n2^{n-1}$$
$$0^2\binom{n}{0} + \ldots + n^2\binom{n}{n} = n(n+1)2^{n-2}$$
$$n\binom{n-1}{k-1} = k\binom{n}{k}$$
$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$
$$\binom{k}{k} + \ldots + \binom{n}{k} = \binom{n+1}{k+1}$$
$$\binom{m}{0}\binom{n}{k} + \ldots + \binom{m}{k}\binom{n}{0} = \binom{m+n}{k}$$
$$\binom{n}{0}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$$
$$\text{Lucas: } \binom{m}{n} \equiv \prod\binom{m_i}{n_i} \pmod p$$
$$\text{Wolstenholme: } \binom{2p-1}{p-1} \equiv 1 \pmod{p^3} \text{ where } p > 3$$
$$\text{Wolstenholme: } \binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3} \text{ where } p > 3$$

Derangements $D_n = nD_{n-1} + (-1)^n$

Gray sequence $G_i = i \text{ xor } (i >> 1)$

 # lower-diagonal paths from $(0,0)$ to (n,m) $(n \ge m)$ $= \frac{n-m+1}{n+1}\binom{n+m}{m}$

Lex-order index (1-based) of r-subset $\{a_1..a_r\}$ of $\{1..n\}$ $= \binom{n}{r} - \binom{n-a_1}{r} - \ldots - \binom{n-a_r}{1}$

Enum r-subsets of n-set in lex-order

```
int a[] = {1...r}
while (1) {
        int k;
        for (k = r; k > 0 && !(a[k] < n && a[k]+1 != a[k]); k--);
        if (k == 0) break;
        for (int i = r; i >= k; i--) a[i] = a[k] + (i - k + 1);
}
```

Enum r-subsets of n-set

```
int z = (1 << k) - 1;
while (z < (1 << n)) {
        cout << z;
        int x = z & -z;
        int y = z + x;
        z = (((z & ~y) / x) >> 1) | y;
}
```

Difference table leftmost diagonal $= c_0, \ldots c_p, 0, \ldots \to$ original sequence

$$h_n = c_0\binom{n}{0} + \ldots + c_p\binom{n}{p}$$
$$\sum_{k=0..n} h_k = c_0\binom{n+1}{1} + \ldots + c_p\binom{n+1}{p+1}$$

Catalan number

$C_n = \#\ \pm 1$ sequences with non-negative prefix sum

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$
$$C_n = \frac{4n-2}{n+1}C_{n-1}$$

Stirling-1 number

$s(p,k) = \#\ p$ diff items into k same circular permutations

$$\begin{aligned} s(p,0) &= 0 && (p \geq 1) \\ s(p,p) &= 1 && (p \geq 0) \\ s(p,k) &= (p-1)s(p-1,k) + s(p-1,k-1) && (1 \leq k \leq p-1) \\ A_n^p &= \sum_{k=0..p} (-1)^{p-k} s(p,k) n^k \end{aligned}$$

Stirling-2 number

$S(p,k) = \#\ p$ diff items into k same boxes, no empty box

$$\begin{aligned} S(p,0) &= 0 && (p \geq 1) \\ S(p,p) &= 1 && (p \geq 0) \\ S(p,k) &= kS(p-1,k) + S(p-1,k-1) && (1 \leq k \leq p-1) \\ S(p,k) &= \frac{1}{k!}\sum_{i=0..k}(-1)^i\binom{k}{i}(k-i)^p \\ n^p &= \sum_{k=0..p} S(p,k)A_n^k \end{aligned}$$

$\#\ p$ diff items into k diff boxes $= k!S(p,k)$

Bell number

$B_p = \#\ p$ diff items into same boxes

$$B_p = S(p,0) + \ldots + S(p,p)$$
$$B_p = \binom{p-1}{0}B_0 + \ldots + \binom{p-1}{p-1}B_{p-1}$$
$$B_{p^i+k} \equiv iB_k + B_{k+1} \pmod p$$

Generating function

r-combination: $\prod(1 + x^1 + x^2 + \ldots + x^{f_i})$
r-arrangement: $r!\prod(1 + \frac{x^1}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^{f_i}}{f_i!})$
Integer partition: $\prod_{k=1..n}(1-x^k)^{-1}$

Burnside lemma, Polya enum theorem

$\#$ inequivalent colorings on n-set under a permutation group.

$$N(C,G) = \frac{1}{|G|}\sum_{f\in G}|C(f)| = \frac{1}{|G|}\sum_{f\in G}k^{\#(f)} = \frac{1}{|G|}\sum_{f\in G}k^{\sum e_i}$$

G is the equivalent permutation group
C is all colorings on n-set
$N(C,G)$ is $\#$ inequivalent colorings
$C(f)$ is the stable kernel of permutation f
k is the number of colors available
$\#(f)$ is the number of cycles in permutation f
$e_1 \ldots e_n$ is the type of permutation f - it has e_i i-cycles

---

3 Graph theory

Havel-Hakimi algo

degree sequence $(d_1 \geq \ldots \geq d_n)$ is simple-graphic iff $(d_2 - 1 \ldots d_{d_1+1} - 1, d_{d_1+2} \ldots d_n)$ is simple-graphic. Equivalently, connect largest-degree node with other largest-degree nodes.
Erdos-Gallai theorem: $(d_1 \geq \ldots \geq d_n)$ is simple-graphic iff

$$\forall k \in [1,n] \sum_{i=1}^{k} d_i \leq k(k-1) + \sum_{i=k+1}^{n}\min(d_i,k)$$

Vizing's theorem + Misra-Gries edge coloring algo

adjacent edges cannot have same color, uses $\max(deg(v)) + 1$ colors.

---

4 Game theory

Nim Lose iff XOR sum is zero

SG function

P-position: first lose
N-position: second lose
Final node must be P
N's successors contain at least one P
P's successors contain all N
$SG(x) = mex(\{SG(y) \mid \text{y is successor of x}\})$
$SG(x) = 0$ iff x is P-position
Composite game's SG value is the XOR sum of simple games

---

5 Miscellaneous

Farey sequence sorted $\frac{a}{b}$ $(1 \leq a < b \leq N, \gcd(a,b) = 1)$

$$\frac{a_0}{b_0} = \frac{0}{1}$$
$$\frac{a_1}{b_1} = \frac{1}{N}$$
$$\frac{a_n}{b_n} = \frac{a_{n-1}\lfloor\frac{N+b_{n-2}}{b_{n-1}}\rfloor - a_{n-2}}{b_{n-1}\lfloor\frac{N+b_{n-2}}{b_{n-1}}\rfloor - b_{n-2}}$$

Dilworth theorem fewest chain split = longest reverse chain
