a divides b: b=ac; a is a divisor of b and b is a multiple of a
Fundermental Theorem of Arithmetic: every integer greater than 1 can be written uniquely as a product of prime numbers (Proof: Induction)
Divison Algorithm: for any integer a and positive integer b, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$
Ideal: a set of integers that is closed under addition and subtraction(e.g. $d\mathbb{Z} = \{0, \pm d, \pm 2d....\}$) Let I be an ideal of $\mathbb{Z}$, then $\exists d \in \mathbb{Z}$ such that $I = d\mathbb{Z}$
Let I_1, I_2 be ideals of $\mathbb{Z}$, then $I_1 + I_2$ is also an ideal of $\mathbb{Z}$. $a\mathbb{Z} + b\mathbb{Z} = gcd(a,b)\mathbb{Z}$
gcd: there exists integers s and t such that $gcd(a,b) = as + bt$
$[a]_n$: the residue class of a modulo n. Let n be any positive integer, we define $\mathbb{Z}_n$ be set of all residue classes modulo n.
$[s]_n$ is called an inverse of $[a]_n$ if $[a]_n[s]_n = [1]_n$ $[b]_n \in \mathbb{Z}_n$ has an inverse iff gcd(b,n) = 1. (bs + nt = 1)
$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n | gcd(a,n) = 1\}$
Euler's phi function: $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. $\phi(p) = p - 1$ if p is prime. $\phi(p^k) = p^k - p^{k-1}$ if p is prime. $\phi(mn) = \phi(m)\phi(n)$ if m and n are relatively prime.
Euler's Theorem: if a and n are relatively prime, then $a^{\phi(n)} \equiv 1 \pmod{n}$
Fermat's Little Theorem: if p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$
RSA public key cryptosystem: choose two large primes p and q, compute n=pq, $\phi(n) = (p-1)(q-1)$, choose e such that $1 < e < \phi(n)$ and gcd(e,$\phi(n)$)=1, find d such that $ed \equiv 1 \pmod{\phi(n)}$, public key is (n,e), private key is (n,d). Encryption: $c \equiv m^e \pmod{n}$, Decryption: $m \equiv c^d \pmod{n}$ where m is the message.
Complexity of Arithmetic: addition and subtraction: O(k), multiplication: O(k^2), division: O((k-l+1)l)
Complexity of Arithmetic Modulo N: $(a \pm b) \pmod{N}$ can be computed in O(l(N)) bit operations. $ab \pmod{N}$ can be computed in O($l(N)^2$) bit operations. $a^b \pmod{N}$ can be computed in O(l(N)logb) bit operations.
Square and Multiply Algorithm: Convert the exponent to Binary, for the first 1, simply list the number. for each ensuring 0, do Square Operation. For each ensuring 1, do Square and Multiply operations.
$3^5 -> 5 = 101 -> 3 -> (3)^2 -> ((3)^2)^2 * 3$
EA: compute gcd(a,b). EEA: compute d=gcd(a,b),s,t such that as + bt = d: $\begin{pmatrix} s_0 \\ t_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $\begin{pmatrix} s_1 \\ t_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$; $\begin{pmatrix} s_{i+1} \\ t_{i+1} \end{pmatrix} = \begin{pmatrix} s_{i-1} - q_i s_i \\ t_{i-1} - q_i t_i \end{pmatrix}$, where $r_{i-1} = r_i q_i + r_{i+1}$
Linear Congruence Equations: $ax \equiv b \pmod{m}$ has a solution iff $gcd(a,m)|b$. If $d = gcd(a,m)$, then the equation has d solutions modulo m.($x_0 + k\frac{m}{d}$)
Solution to Sun-Tsu's Question: $n = n_1n_2n_3, N_1 = n_2n_3, N_2 = n_1n_3, N_3 = n_1n_2$ Use EEA to find $s_1n_1 + t_1N_1 = 1$, $s_2n_2 + t_2N_2 = 1$, $s_3n_3 + t_3N_3 = 1$. The solution is $x = a_1N_1t_1 + a_2N_2t_2 + a_3N_3t_3$ Then we can use CRT.
CRT Map: $f : \mathbb{Z}_{n_1n_2...n_k} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$, $f(x) = (x \pmod{n_1}, x \pmod{n_2}, ..., x \pmod{n_k})$: a well-defined bijection
Discrete Logarithm Problem: given $g^x \pmod{p}$, find x. Computational Diffie-Hellman Problem: given $g^a \pmod{p}$ and $g^b \pmod{p}$, find $g^{ab} \pmod{p}$
Diffie-Hellman Key Exchange: Alice and Bob agree on a prime p and a generator g. Alice chooses a secret a and sends $g^a \equiv A \pmod{p}$ to Bob. Bob chooses a secret b and sends $g^b \equiv B \pmod{p}$ to Alice. They can compute the shared secret $g^{ab} \pmod{p}$ with B^a A^b
Group Definition: A group G is a set with a binary operation $\star$ that satisfies the following properties: 1. Closure: for all a,b in G, $a \star b$ is in G. 2. Associativity: for all a,b,c in G, $(a \star b) \star c = a \star (b \star c)$. 3. Identity: there exists an element e in G. 4. Inverse: for all a in G, there exists an element a^{-1} in G.
Abelian Group: a group that satisfies the commutative property: $\forall a, b \in G, a \star b = b \star a$. Group $\mathbb{Z}_n^*$ is an abelian group under multiplication modulo n.
Two types of Abelian Groups: 1. Additive Group 2. Multiplicative Group
Field Definition: A field F is a set with two binary operations + and $\cdot$ that satisfies the following properties: 1. F is an abelian group under +. 2. F-0 is an abelian group under $\cdot$. 3. Distributive Law: for all a,b,c in F, $a \cdot (b + c) = a \cdot b + a \cdot c$
Polynomial over $\mathbb{Z}_p$: A polynomial f(X) has $\leq$ deg(f) roots in $\mathbb{Z}_p$.
Order: the order of a group G is the cardinality of G. $|Z_n| = n, |Z_p^*| = p - 1$. The order of an element a in a group G is the smallest positive integer n such that $a^n = e$.
Let G be a multiplicative group of order n. For all a in G, $a^n = 1.(i \neq j, aa_i \neq aa_j$. Then multiply them together)
Subgroup: a subset H of a group G is a subgroup of G if H is a group under the same operation as G.
Cyclic Group: a group G is cyclic if there exists an element g(generator) in G such that every element in G can be written as a power of g. For any prime p, the group $\mathbb{Z}_p^*$ is cyclic.
Theorem $|(0,1)| \neq |\mathbb{Z}^+|$: Cantor's Diagonalization Argument. Construct a new element by considering the diagonal of the list.
Cantor's Theorem: for any set A, $|A| < |\mathbb{P}(A)|$, where $\mathbb{P}(A)$ is the power set of A(set of all subsets).
The Halting Problem: there is no Turing machine that can determine whether an arbitrary Turing machine halts on a given input.
Schroder-Bernstein Theorem: $|A| \leq |B| |B| \leq |A| \to |A| = |B|$.(Use injection)
Construct a bijection: $[0,1] -> (0,1) : f(1) = \frac{1}{2}, f(0) = 2^{-2}, f(2^{-n}) = 2^{-n-2}, f(x) = x$ for all other x.
Difference between permutation and combination: permutation is the arrangement of objects in a specific order, combination is the selection of objects without considering the order.
Multiset: a set in which an element can appear more than once. $A = \{1 \cdot a, 2 \cdot b, 3 \cdot c, 100 \cdot d\}$ a 106-Multiset
Permutations of Multisets: the number of permutations of a multiset A is $\frac{n!}{n_1!n_2!...n_k!}$ where $n = n_1 + n_2 + ... + n_k$
Shortest Path: a p*q grid of shortest path is $\frac{(p+q)!}{p!q!}$: Let $A = \{p \cdot \to, q \cdot \uparrow\}$ be a p+q multiset.
T-Route: There is a T-Route from $A = (a, \alpha)$ to $B = (b, \beta)$ iff $b > a,\ b - a \geq |\beta - \alpha|,\ 2|(b + \beta - a - \alpha)$

The number of T-Route from $A = (a, \alpha)$ to $B = (b, \beta)$ is $\frac{(b-a)!}{(\frac{b-a+\beta-\alpha}{2})!(\frac{b-a-\beta+\alpha}{2})!}$

Andre's Reflection: To find T-Route that intersect with a given line, reflect the starting point across the line

$\star$ Catalan Number: C_n is the number of solutions of the equation system:

$$\begin{cases} x_1 + x_2 + ... + x_{2n} = n \\ x_1 + x_2 + ... + x_i \leq \frac{i}{2} \\ x_i \in \{0, 1\} \end{cases}$$

In particular, $C_n = \frac{(2n)!}{n!(n+1)!}$.

r-combination of A is an r-subset of A. The number of r-combinations of a set with n elements is $\binom{n}{r} = \frac{n!}{r!(n-r)!}$

r-combination of A with repetition is an r-multiset of A. The number of r-combinations of a set with n elements is $\binom{n+r-1}{r} = \frac{(n+r-1)!}{r!(n-1)!}$

Pascal's Identity: $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$

Ways to prove L=R: e.g. 1.$X = \{s \in \{0,1\}^n :$ s contains $r0\}$ 2. Let $U = \{u_1, u_2, u_3....u_n\}$ be a finite set of n elements, $S = \{(A, B) : A \subseteq U, |A| = k, B \subseteq A, |B| = r\}$

$\star$Inverse Bionomial Transform: Form1: n elements in total, f(k) is the number of ways to select with k certain elements selected. g(k) is the number of ways to select exactly k elements. Form2: f(k) is the number of ways satisfy at most k conditions, g(k) is the number of ways to satisfy exactly k conditions.

$f(k) = \sum_{i=k}^{n} \binom{i}{k} g(i), g(k) = \sum_{i=k}^{n} (-1)^{i-k} \binom{i}{k} f(i)$ or $f(n) = \sum_{i=0}^{n} \binom{n}{i} g(i), g(n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(i)$

In the derangement problem(for the permutation of 1-n, how many satisfy that $\forall i, p_i \neq i$), f(n) is at most n derangements, g(n) is exactly n derangements. Of course f(n) = n!, then $g(n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(i) = \sum_{j=0}^{n} (-1)^j \frac{n!}{j!}$

Lemmas used to prove Inverse Bionomial Transform: $\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$, $\sum_{k=r}^{n} (-1)^{n-k} \binom{n}{k}\binom{k}{r} = \begin{cases} 0, r < n \\ 1, r = n \end{cases}$

Distribution Problems: Type1: n labeled objects into k labeled boxed$(n_1, n_2...n_k)$, $\frac{n!}{n_1!n_2!....n_k!}$ permutations. Type2: n labeled objects into k unlabeled boxed, $\binom{n+k-1}{n}$ ways, combinations. Type3: n unlabeled objects into k labeled boxed, $S(n, k)$ ways. Type4: n unlabeled objects into k unlabeled boxed, $p(n, k)$ ways.

$\star$Stirling Number of the Second Kind: $S(n, k)$ is the number of ways to partition n labeled elements into k non-empty unlabeled sets.

$S(n, k) = kS(n-1, k) + S(n-1, k-1)$, $S(n, k) = \sum_{i=0}^{k} \frac{(-1)^{k-i} i^n}{i!(k-i)!}$

$S(n, 2) = 2^{n-1} - 1, S(n, n-1) = \binom{n}{2}, S(n, n-2) = \binom{n}{3} + 3\binom{n}{4}$

Partition of Integers: For $n \in \mathbb{Z}^+, p_j(n+j) = \sum_{k=1}^{j} p_k(n)$ e.g. $p_3(6) = p_1(3) + p_2(3) + p_3(3)$

LHRR: find characteristic polynomial and characteristic roots. If without repeated roots, the general solution is $f_n = \sum_{i=1}^{k} \alpha_i r_i^n$. If there are multiple roots, suppose we have distinct roots $r_1, r_2, ...r_t$ with multiplicity $m_1, m_2, ...m_t$, then the general solution is $f_n = \sum_{i=1}^{t} (\sum_{j=0}^{m_i - 1} \alpha_{ij} n^j) r_i^n$

LNRR: First find the associated LHRR, solve it and we have a general solution named h_n. For the particular solution b_n, We can simply guess it out. e.g $a_n = 2a_{n-1} - a_{n-2} + 2^n, a_0 = 1, a_1 = 2$ guess $b_n = c2^n + d -> b_n = 4 \cdot 2^n, a_n = b_n + h_n$. Note that if s($F(n) = f(n)s^n$) is a root of the LHRR, then we have to multiply n^m, where m is the multiplicity.

$\star$Generating Function: $A(x) = \sum_{r=0}^{\infty} a_r x^r$, $\sum_{r=0}^{\infty} x^r = \frac{1}{1-x}$

All kinds of generating function: $a_n = \binom{m}{n} => A(x) = (1+x)^m$, $a_n = \binom{n+m-1}{n} k^n => A(x) = \frac{1}{(1-kx)^m}$ ($a_n = \binom{n+1}{1} => A(x) = \frac{1}{(1-x)^2}$)

Application of generating function: 4 weights of 1,2,3,4 grams. How many weights can they make up? Each in how many ways? $(1+x)(1+x^2)(1+x^3)(1+x^4)$

Fib(n) $= \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$, $f(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5....$ $f(x) - xf(x) = x + x^2 f(x)$ So $f(x) = \frac{x}{1-x-x^2} = -\frac{1}{\sqrt{5}} \frac{1}{1 - \frac{1-\sqrt{5}}{2}x} + \frac{1}{\sqrt{5}} \frac{1}{1 - \frac{1+\sqrt{5}}{2}x}$

Skill: $a_n <=> A(x)$, $na_n <=> xA^{'}(x)$ Solving RR with Generating Functions: $a_n = 8a_{n-1} + 10^{n-1}, a_0 = 1$: $A(x) = \sum_{n=0}^{\infty} a_n x^n = 1 + \sum_{n=1}^{\infty} (8a_{n-1} + 10^{n-1}) x^n = 1 + 8xA(x) + \frac{x}{1-10x}$, $A(x) = \frac{1-9x}{(1-8x)(1-10x)}$ For A(x) in this kind of form $(\frac{P(x)}{Q(x)})$, we have the following Theorem:

$deg(Q) > deg(P)$, if $Q(x) = (1 - r_1 x)^{m_1}.....(1 - r_t x)^{m_t}$, then $\frac{P(x)}{Q(x)} = \sum_{j=1}^{t} \sum_{u=1}^{m_j} \frac{\alpha_{j,u}}{(1 - r_j x)^u}$

Generating Functions for the Catalan Number: $C_n = C_0 C_{n-1} + C_1 C_{n-2} + ... + C_{n-1} C_0$, $xC(x)^2 = C(x) - 1$

Principle of Inclusion-Exclusion: $|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + ... + (-1)^{n-1} |A_1 \cap A_2 \cap ... \cap A_n|$, $|A_1 \cap A_2 \cap ... \cap A_n| = |A_1| + |A_2| + ... + |A_n| - |A_1 \cup A_2| - |A_1 \cup A_3| - ... - |A_{n-1} \cup A_n| + |A_1 \cup A_2 \cup A_3| + ... + (-1)^{n-1} |A_1 \cup A_2 \cup ... \cup A_n|$

QUESTION: Let $k > 0, N_1, ..., N_k \subseteq \mathbb{N}$. For every $n \geq 0$, let a_n be the number of n-permutations of $[k]$ with repetition where every $i \in [k]$ appears N_i times. (**Distribution problems: Type 1**)

- $a_n = \sum_{n_1 \in N_1, n_2 \in N_2, ..., n_k \in N_k,\, n_1 + n_2 + \cdots + n_k = n} \frac{n!}{n_1! n_2! \cdots n_k!}$
  - This is the number of ways of distributing n labeled objects into k labeled boxes such that N_i objects are sent to box i for all $i \in [k]$

THEOREM: $\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = \prod_{i=1}^{k} \sum_{n_i \in N_i} \frac{x^{n_i}}{n_i!}$.

- $\prod_{i=1}^{k} \sum_{n_i \in N_i} \frac{x^{n_i}}{n_i!} = \sum_{n_1 \in N_1} \frac{x^{n_1}}{n_1!} \cdot \sum_{n_2 \in N_2} \frac{x^{n_2}}{n_2!} \cdots \sum_{n_k \in N_k} \frac{x^{n_k}}{n_k!}$

  $= \sum_{n=0}^{\infty} \left(\sum_{n_1 \in N_1, n_2 \in N_2, ..., n_k \in N_k,\, n_1 + n_2 + \cdots + n_k = n} \frac{n!}{n_1! n_2! \cdots n_k!} \right) \frac{x^n}{n!}$

  $= \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$

QUESTION: Let $k > 0, N_1, ..., N_k \subseteq \mathbb{N}$. For every $n \geq 0$, let a_n be the number of n-combinations of $[k]$ with repetition where every $i \in [k]$ appears N_i times. (**Distribution problems: Type 2**)

- $a_n = |\{(n_1, ..., n_k): n_1 \in N_1, ..., n_k \in N_k, n_1 + \cdots + n_k = n\}|$
  - This is the number of ways of distributing n unlabeled objects into k labeled boxes such that N_i objects are sent to box i

THEOREM: $\sum_{n=0}^{\infty} a_n x^n = \prod_{i=1}^{k} \sum_{n_i \in N_i} x^{n_i}$.

- $\prod_{i=1}^{k} \sum_{n_i \in N_i} x^{n_i} = \sum_{n_1 \in N_1} x^{n_1} \cdot \sum_{n_2 \in N_2} x^{n_2} \cdots \sum_{n_k \in N_k} x^{n_k}$

  $= \sum_{n=0}^{\infty} (\sum_{n_1 \in N_1, ..., n_k \in N_k, n_1 + \cdots + n_k = n} 1) x^n$

  $= \sum_{n=0}^{\infty} a_n x^n$