p is prime

generating functions example problem: count solutions of $x_1 + \ldots + x_k = n$ with constraints on x_i.

construction: inductive construction

1 Number Theory

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

- Euler's totient function

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

- Mobius function

$$\sum_{d|n} \mu(d) = [n == 1]$$

$$n \sum_{d|n} \frac{\mu(d)}{d} = \phi(n)$$

$$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$$

$$\forall n, g(n) = \sum_{d|n} f(d) \to \forall n, f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$$

- 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

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

- Derangement: $D_n = nD_{n-1} + (-1)^n$
- Index of r-subset $a_1 \ldots a_r$ in lex-order is
$$\binom{n}{r} - \binom{n-a_1}{r} - \ldots - \binom{n-a_r}{1}$$
- Gray sequence: $G[i] = i \text{ xor } (i >> 1)$
- Burnside Lemma + Polya enumeration theorem
Counts the number of 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 the count of 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 algorithm: 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

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

4 Game theory

- Nim: Lose iff XOR sum is zero