简单数学选讲 Preview

4182_543_731

温馨提示

这是一个只保留了题目的预览版。

约定：课件中 p, q 表示指数，其它部分默认表示可以是合数。没有范围的数默认 10^9 或者 10^{18} 级别。

- 质因数分解相关
- 欧拉定理
- exgcd
- CRT/同余方程
- 离散对数/bsgs
- 特征根方程
- 原根
- 单位根
- 二次剩余相关
- 组合数取模/Lucas
- 类欧几里得算法
- Stern-Brocot Tree
-

质因数分解

欧拉定理

Problem 1

求 $2^{2^{2^{2^{\cdots}}}} \pmod{m}$，$m \leq 10^9$，可以证明它良定义。

exgcd

经典问题

给定正整数 x, y，求一组整数 a, b 使得 $ax + by = \gcd(x, y)$，可以证明一定有解。

欧几里得算法的思想在之后的某些部分中也有体现。

综合练习

Problem 2

求 $a^n \equiv n \pmod{m}$ 的一个解，$m \leq 10^9$

CRT

CRT

给定若干两两互质的 $b_1, \cdots, b_k$。每一种可能的 $(r_1, r_2, \cdots, r_k) = (x \bmod b_1, x \bmod b_2, \cdots, x \bmod b_k)$ 都可能出现，且每一种可能的 r 和 $[0, \prod b_i)$ 中的 x 可以一一对应。

同余方程/exCRT

经典问题 (exCRT)

给定若干形如 $x \equiv a_i \pmod{b_i}$ 的同余方程，求解 x，保证 b_i 的 lcm 在合理范围（10^{18}）内。

同余方程/exCRT

Problem 2

找到最小的正整数 x 满足如下 n 个限制：

$a_i x \geq b_i$ 且 $c_i | a_i x - b_i$

$n \leq 10^5$

离散对数/bsgs

经典问题

求解模意义方程 $a^x \equiv b \pmod{p}$

$p \leq 10^{10}$，10^5 次询问

特征根方程

经典问题

给一个 k 阶常系数线性递推 $a_n = \sum_{i=1}^{k} v_i a_{n-i}$，其中前 k 项给定，求通项公式。

特征根方程

Problem 2

定义 f_i 为第 i 个斐波那契数。给定 n，有 n 个未知的整数 a_i，它们生成了一个序列 $p_i = \sum_{j=1}^{n} a_j * (f_j)^i$。

现在给出 p 的前 n 项，求下一项。所有数对某个给定的数取模。

$n \leq 5000$

原根与阶

定义

可以证明，对于任意质数 p，存在 $g \in [1, p-1]$ 使得 $g^0, g^1, g^2, \cdots, g^{\varphi(p)-1}$ 在模 p 下两两不同。

事实上，原根对于 $2, 4, q^r, 2q^r$ 存在，其中 q 是奇质数。

原根

Problem 1

令 $p = 200003$，给定 n 个整数 $a_1, \cdots, a_n$，求 $\sum_{1 \le i < j \le n} (a_i a_j \pmod p)$

Problem 2

给定集合 S 和质数 p，从 S 中选 n 次数（可以重复选同一个），求 n 次选出的数乘积模 p 余 r 的方案数。$p \le 8000$

单位根

定义

称 ω_k 是 k 次单位根，当且仅当 $\omega_k^k = 1$ 且 $\forall i \in [1, k-1], \omega_k^i \neq 1$。

可以证明，模质数意义下 k 次单位根存在当且仅当 $k|p-1$，也可以换为 $\varphi(m)$

单位根

定义

称 ω_k 是 k 次单位根，当且仅当 $\omega_k^k = 1$ 且 $\forall i \in [1, k-1], \omega_k^i \neq 1$。
可以证明，模质数意义下 k 次单位根存在当且仅当 $k|p-1$，也可以换为 $\varphi(m)$

Problem 1

求 $x^3 \equiv 1 \pmod{m}$ 的解数量。

单位根反演

定义 2

$\frac{1}{d}\sum_{i=0}^{d-1}\omega_d^{in}=[d|n]$

单位根反演

Problem 2

求 $\sum_{i=0}^{+\infty} \binom{n}{id}$

当然，如果只有一个序列，或者没有单位根，也可以从生成函数的角度大力做：

$$(1+x)^n \pmod{x^d-1}$$

单位根反演

Problem 3

有 m 个人，进行 n 次操作，每次选一个人。求有多少种操作方式使得每个人被选出的次数为 d 的倍数。

$m \leq 5 \times 10^5, d = 2$ 或者 $m \leq 1000, d = 3$，答案对一个模 6 余 1 且 $> m$ 的质数取模。

二次剩余

经典问题

求解模意义方程 $x^2 \equiv a \pmod{p}$，为了简便只考虑奇质数。

Cipolla

Problem 2

给一棵有根树，点有点权 a。给定质数 p 和常数 A, B。求有多少点对 u, v 满足 u 是 v 的祖先且 $a_u^2 + Aa_ua_v + Ba_v^2 \equiv 0 \pmod{p}$

$n \leq 10^5, 3 \leq p \leq 10^{16}$

勒让德符号

定义

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \ \exists b \ s.\ t.\ b^2 \equiv a \pmod{p} \\ 0, \ p|a \\ -1, \ otherwise \end{cases}$$

根据之前的推导，$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

勒让德符号

有一些结论：

- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$
- $\left(\frac{a^2}{p}\right)=\begin{cases}0, & p|a\\ 1, & otherwise\end{cases}$
- 对于奇质数 p,q，$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$
- $\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)=0$

勒让德符号

Problem 1

求 $x^2 + y^2 \equiv r \pmod{p}$ 的解数量

综合练习

Problem

考虑一种二阶递推：$a_0 = 0, a_1 = 1, a_n = Aa_{n-1} + a_{n-2} (n \geq 2)$

给出 x, p, l, r，求 $\sum_{i=l}^{r} [a_i \equiv x \pmod{p}]$

$l, r \leq 10^{18}, p \leq 10^9$

Lucas

Case 1

求 $\binom{n}{m} \pmod{p}$，$n, m \leq 10^{18}, p \leq 10^6$，$p$ 是质数。

Lucas

Problem 1

给一个序列 $a_1, \cdots, a_n$，求它有多少个子序列 b 满足 $|b| \geq 2$ 且 $\prod_{i=1}^{l-1} \binom{b_i}{b_{i+1}}$ 是奇数

Case 2

求 $\binom{n}{m} \pmod{p^k}$，$n, m \leq 10^{18}, p^k \leq 10^6$，$p$ 是质数。

Problem 3

给定 p, k, A，求有多少对 n, m 满足 $0 \le m \le n \le A$ 且 $p^k | \binom{n}{m}$

$p \le 10^9, A \le 10^{1000}$

Case 3

求 $\binom{n}{m} \pmod{p^k}$，$n, m \leq 10^{18}, p \leq 10^6$，$p$ 是质数。

类欧几里得算法

欧几里得算法的思想：
对于一个以 a, b 作为参数的问题，如果可以递归到 $(a \bmod b, b)$（取模）和 (b, a)（交换），则可以使用 gcd 的过程，在 $O(\log n)$ 步递归内解决问题。

类欧几里得算法

Case 1

求 $\sum_{i=0}^{n} \lfloor \frac{ai+c}{b} \rfloor$, 或者说线段下数点。

$n \leq 10^9$

类欧几里得算法

Case 2

给定 a, p, l, r，找到最小的非负整数 b 使得 $ab \bmod p \in [l, r]$

$p \leq 10^9$

类欧几里得算法

Problem 1

给定互质的 a, b，有 $0, 1, 2, \cdots, n$ 共 $n+1$ 个点，你初始在 x_0，每一步可以选择从当前位置 x 走到 $x \pm a, x \pm b$ 中的一个位置。求能到达多少个位置。

类欧几里得算法

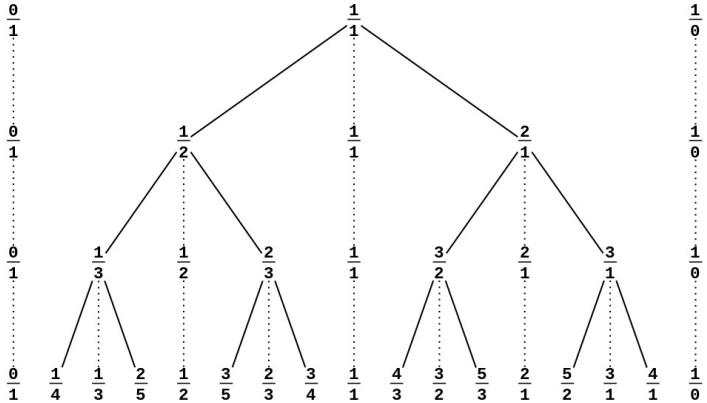
Problem 2

交互。有一个未知的有理数 $\frac{a}{b}$，保证 $a, b \leq 10^9$。你每次可以问一个 $[10^9 + 1, 10^{12}]$ 的质数 p，交互库返回有理数对质数取模的结果。

在 5 次操作内猜出 $\frac{a}{b}$。

万能欧几里得

Stern-Brocot Tree



Stern-Brocot Tree/有理逼近

Problem 1

求 $\sum_{i=1}^{n} \lfloor i\sqrt{d} \rfloor$， $n \leq 10^9$

Stern-Brocot Tree/有理数逼近

Problem 2

给出有理数，求最小的 n 使得 $[an, bn]$ 间存在整数。

Stern-Brocot Tree/有理数二分

Problem 1

考虑所有 $[0,1]$ 之间分母不超过 n 的既约分数，求出第 k 大，$n \leq 10^6$

Extra

Problem

给定 n 个非负整数的三元组 (x_i, a_i, b_i)，选出一个子集满足选择的 x_i 的任意非空子集异或和非零（即异或下线性无关），最大化选出部分的 $(\sum a) * (\sum b)$，$n \leq 100$