简单数学选讲

4182_543_731

温馨提示

数学方面的知识点有点杂，所以这里讲的东西也有点杂。
为了双方的身心健康，一些偏组合计数的东西（各种数论函数，筛法）可能不在这个课件包含的范围之内。
因为讲题人还没考虑讲课时间问题，最后可能会加入/删除一部分内容。
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
- 特征根方程
- 原根
- 单位根
- 离散对数/bsgs
- 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

10^{15} 之内都可以暴力试除。

稍微大一点的情况 OI 常见做法是 Miller Rabin 判素数，再用 Pollard's rho，这在 2^{64} 内都没有压力。但它几乎不会出现（我 OI 中用过大概两次），出现也是板子。

~~还有一些可以实现的更快的分解算法 (loj6466)，但是绝对不可能有用~~

基础应用：算一下积性函数，例如 φ。~~事实上求φ 不弱于分解 (loj3657)~~

欧拉定理

Lemma

如果 a, b 互质，则 $a^{\varphi(b)} \equiv 1 \pmod{b}$

经典例子：a^{p-2}。在推导中更常出现。

欧拉定理

Lemma

如果 a, b 互质，则 $a^{\varphi(b)} \equiv 1 \pmod{b}$

经典例子：a^{p-2}。在推导中更常出现。

如果 a, b 不互质则不能直接用，但可以发现乘 $\log_2 b$ 个 a 之后可能出现的 b 的因子已经全部出现了，之后就是互质的情况。因此 $t > \log_2 b$ 时有 $a^t \equiv a^{t+\varphi(b)} \pmod{b}$。

另一种形式（扩展欧拉定理）：

$$a^b \equiv a^{\min(b,b \pmod{\varphi(b)}+\varphi(b))} \pmod{b}$$

欧拉定理

Problem 1

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

欧拉定理

Problem 1

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

根据扩展欧拉定理一直模下去即可。这里每次都应该取指数很大的情况。

因为 $\frac{\varphi(n)}{n} = \prod_{p|n,p\ is\ prime}(1-\frac{1}{p})$，可以发现如果 n 是 >2 的偶数，则 $\varphi(n) \le \frac{n}{2}$，且如果 $n>2$ 则 $2|\varphi(n)$，所以只会递归 $O(\log n)$ 次。但算 φ 需要分解，暴力做的复杂度是 $O(\sqrt{p})$

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。

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。

简单的推导：

$$x = qy + r$$

$$ar + by = g$$

$$ax + (b - aq)y = g$$

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。

简单的推导：

$$x = qy + r$$

$$ar + by = g$$

$$ax + (b - aq)y = g$$

经典应用：如果 x, y 互质，那么 $ax \equiv 1 \bmod y$，因此可以模合数意义下求逆。(虽然 $x^{\varphi(y)-1}$ 也是逆元，但求 φ 和分解等难)

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，$m \leq 10^9$

综合练习

Problem 2

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

如果 a, m 互质，那么 a 每增加 $\varphi(m)$，左侧不变，右侧加 $\varphi(m)$。那么根据 exgcd，可以找到正整数 k 使得 $k\varphi(m) \equiv \gcd(\varphi(m), m) \pmod m$)，那么只要 $\pmod{\gcd}(\varphi(m), m)$ 有解，在这个解的基础上加上若干倍 $k\varphi(m)$ 即可。那么可以直接递归，递归次数不超过每次变为 φ 的复杂度，如果暴力算 φ 复杂度为 $O(\sqrt{m})$。

综合练习

Problem 2

求 $a^n \equiv n \pmod m$ 的一个解，$m \le 10^9$

如果 a, m 互质，那么 a 每增加 $\varphi(m)$，左侧不变，右侧加 $\varphi(m)$。那么根据 exgcd，可以找到正整数 k 使得 $k\varphi(m) \equiv \gcd(\varphi(m), m) \pmod m$)，那么只要 $\pmod{\gcd}(\varphi(m), m)$ 有解，在这个解的基础上加上若干倍 $k\varphi(m)$ 即可。那么可以直接递归，递归次数不超过每次变为 φ 的复杂度，如果暴力算 φ 复杂度为 $O(\sqrt{m})$。

但还可能不互质，此时仍然考虑特殊处理前 $\log_2 m$ 项。当 $n > \log_2 m$ 时，$g = \gcd(a^n, m)$ 会变为定值。此时 n 必须是 g 的倍数，取 kg 为一个大于 $\log_2 m$ 的数，要求变为 $\frac{a^{kg}}{g} * a^{ng} \equiv n + k \pmod{\frac{m}{g}}$。此时循环的性质仍然存在且 $\gcd(a, \frac{m}{g}) = 1$，然后使用之前的做法即可。

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。

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。

解同余方程通常使用下一页的东西，但 CRT 有一些更加常用的推导。

一个应用是将模合数的问题分成模 p^k 的情况求解，最后将模每个 p^k 的解合并。直接的情况是答案对合数取模，然后 CRT 合并解。

另一种情况是给一个对合数取模的方程。对于解方程 $f(x) \equiv 0 \pmod{m}$，根据 CRT，可以将 m 分解为 $\prod p_i^{k_i}$，然后对于每个 $\pmod{p_i^{k_i}}$ 求解，因为每一组 $(r_1, r_2, \cdots, r_k)$ 对应一个 x，最后答案为每一个 $p_i^{k_i}$ 解数量的乘积。

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

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。

比较简单的推导：

考虑两个方程 $(a_1, b_1), (a_2, b_2)$。可以发现 x, y 模 b_1, b_2 同余当且仅当 $lcm(b_1, b_2) | (x - y)$，因此合并后也应当形如 $x \equiv a' \pmod{lcm(b_1, b_2)}$ 或无解。

首先模 $\gcd(b_1, b_2)$，从而如果 $a_1 \not\equiv a_2 \pmod{\gcd(b_1, b_2)}$ 则显然无解。

否则，从 a_1 开始，由 exgcd 可以找到 s, t 使得 $s * b_1 + t * b_2 = \gcd(b_1, b_2)$，从而每加一个 $s * b_1$ 不会改变 $\pmod{b_1}$ 而会使 $\pmod{b_2}$ 增加 $\gcd$，从而答案是 $a_1 + \frac{a_2 - a_1}{g} * s * b_1$.

同余方程/exCRT

应用：板子（部分神必出题人可能会强行加一个 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 $c_i | a_i x - b_i$

$n \leq 10^5$

同余方程/exCRT

应用：板子（部分神必出题人可能会强行加一个 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 $c_i | a_i x - b_i$

$n \leq 10^5$

可以拆成两部分，第一部分相当于 $x \geq$ 某个数，第二部分是同余方程组。因此先解同余方程组得到 $x \equiv a \pmod{b}$，再求第一个大于某个数的即可。

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

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。

考虑方程 $x^k = \sum_{i=1}^{k} v_i x^{k-i}$，如果 r 是方程的一个解，则可以发现 $a_n = r^n$ 满足线性递推关系。根据线性性它们的任意线性组合满足递推。

如果方程有 k 个不同的根 $r_1, \cdots, r_k$，那么 k 个上述序列 $\{r_1^i\}_i, \cdots, \{r_k^i\}_i$ 的前 k 项线性无关，因此它们的线性组合可以凑出前 k 项，从而 $a_n = \sum_{i=1}^{k} w_i r_i^n$ 满足递推和前 k 项，那么它就是答案。

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。

考虑方程 $x^k = \sum_{i=1}^{k} v_i x^{k-i}$，如果 r 是方程的一个解，则可以发现 $a_n = r^n$ 满足线性递推关系。根据线性性它们的任意线性组合满足递推。

如果方程有 k 个不同的根 $r_1, \cdots, r_k$，那么 k 个上述序列 $\{r_1^i\}_i, \cdots, \{r_k^i\}_i$ 的前 k 项线性无关，因此它们的线性组合可以凑出前 k 项，从而 $a_n = \sum_{i=1}^{k} w_i r_i^n$ 满足递推和前 k 项，那么它就是答案。

如果有重根怎么办？可以发现对于二重根，$a_n = nr^n$ 满足递推关系，证明可以手推一下 $(x-r)^2$ 的情况。类似的，高阶重根是 $n^{d-1}r^n$。

因为高阶方程不能求根，这东西 OI 中大概率不实用，但二次还是有用的。

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。

$n \leq 5000$

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。

$n \leq 5000$

给出的序列是一个特征根通项的形式，反向应用特征根的结论可以发现：

设 $f(x) = (x - f_1)(x - f_2) \cdots (x - f_n)$，展开得到 $f(x) = x^n - \sum_{i=1}^{n} v_i x^{n-i}$。考虑递推 $a_n = \sum_{i=1}^{n} v_i a_{n-i}$，根据之前的推导每一个 $\{f_j^i\}_i$ 都满足递推，那么 p 必定满足这个 n 阶递推，从而展开 f 即可。直接做即为 $O(n^2)$

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，但这个结论应该没用。

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，但这个结论应该没用。

a 模 p 的阶定义为最小的正整数 x 使得 $a^x \equiv 1 \pmod{p}$，有结论 $ord\ a | \varphi(p)$，因为如果不是，可以把它和欧拉定理的结论 exgcd 找到一个更小的。

判断一个数是否是原根：由上一条结论，求出并分解 $\varphi(p)$，对每个质因子判断 $x^{\frac{\varphi(p)}{r}}$ 是否模 p 余 1。

找原根：原根的数量是 $\varphi(\varphi(p))$ 的，随机几个试试就行，也可以从小到大。

原根

Problem 1

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

原根

Problem 1

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

令一个原根为 g，考虑将所有非零的数表示为 g^{b_i}，那么相乘相当于指数上相加：$a_i a_j \equiv g^{b_i + b_j}$。

那么问题变为指数上模 $p - 1$ 的循环卷积，FFT 即可。

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。$p \le 8000$

原根

Problem 1

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

令一个原根为 g，考虑将所有非零的数表示为 g^{b_i}，那么相乘相当于指数上相加：$a_i a_j \equiv g^{b_i + b_j}$。

那么问题变为指数上模 $p-1$ 的循环卷积，FFT 即可。

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。$p \le 8000$

取原根后相当于 $f(x)^n \pmod{x^{\varphi(p)-1}}$，然后倍增 +FFT。

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 $\varphi(m)$（前提原根存在）

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 $\varphi(m)$（前提原根存在）

Problem 1

求 $x^3 \equiv 1 \pmod{m}$ 的解数量。

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 $\varphi(m)$（前提原根存在）

Problem 1

求 $x^3 \equiv 1 \pmod{m}$ 的解数量。

首先考虑 CRT，对于 $p^k(p>2)$，$\bmod p^k$ 存在原根，那么可以发现 g^i 是一个解当且仅当 $\varphi(p^k)|3i$。进一步存在三个解当且仅当 $3|\varphi(p^k)$，否则只有一个解。
对于 $\pmod{2^k}$ 的情况，分析一下可以发现，解必须是奇数，如果解不是 1，设解为 $e*2^r+1$ 其中 e 是奇数，那么 $a^3 = 2^{r+1}*(\cdots)+2^r+1$，因此不可能是解。
因此 p^k 有三个解当且仅当 $p \equiv 1 \pmod 3$ 或者 $p=3, q>1$。

单位根反演

定义 2

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

证明：如果 $\omega_d^n\neq 1$，则可以等比数列求和 $\sum_{i=0}^{d-1}\omega_d^{in}=\frac{1-\omega_d^{nd}}{1-\omega_d^n}=0$

单位根反演

定义 2

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

证明：如果 $\omega_d^n\neq 1$，则可以等比数列求和 $\sum_{i=0}^{d-1}\omega_d^{in}=\frac{1-\omega_d^{nd}}{1-\omega_d^n}=0$

典型应用：DFT 与 IDFT，a 到 b 的贡献系数是 $\sum_{i=0}^{l-1}\omega_l^{ai}\omega_l^{-bi}=\sum_{i=0}^{l-1}\omega_l^{(a-b)i}=l[p|(a-b)]$

单位根反演

单位根可以处理许多 $[d|n]$ 相关，或者 $[n \equiv k \pmod d]$ 的问题。(减去 k)

最简单的例子：带入 $d=2$，得到 $[2|n]=\frac{1}{2}(1+(-1)^n), [2|n-1]=\frac{1}{2}(1-(-1)^n)$

Problem 2

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

单位根反演

单位根可以处理许多 $[d|n]$ 相关，或者 $[n \equiv k \pmod d]$ 的问题。(减去 k)

最简单的例子：带入 $d=2$，得到 $[2|n]=\frac{1}{2}(1+(-1)^n), [2|n-1]=\frac{1}{2}(1-(-1)^n)$

Problem 2

求 $\sum_{i=0}^{+\infty}\binom{n}{id}$

相当于 $[d|k]\binom{n}{k}$，将 $[d|k]$ 展开为 $\frac{1}{d}\sum_{i=0}^{d}(\omega_d^i)^k$，可以发现对于一个 i 整体需要求和的项为 $\sum_{k=0}^{n}(\omega_d^i)^k\binom{n}{k}$，根据二项式定理这是 $(1+\omega_d^i)^n$。

单位根反演

单位根可以处理许多 $[d|n]$ 相关，或者 $[n \equiv k \pmod d]$ 的问题。(减去 k)
最简单的例子：带入 $d=2$，得到 $[2|n]=\frac{1}{2}(1+(-1)^n), [2|n-1]=\frac{1}{2}(1-(-1)^n)$

Problem 2

求 $\sum_{i=0}^{+\infty}\binom{n}{id}$

相当于 $[d|k]\binom{n}{k}$，将 $[d|k]$ 展开为 $\frac{1}{d}\sum_{i=0}^{d}(\omega_d^i)^k$，可以发现对于一个 i 整体需要求和的项为 $\sum_{k=0}^{n}(\omega_d^i)^k\binom{n}{k}$，根据二项式定理这是 $(1+\omega_d^i)^n$。
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。

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。

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

使用单位根反演处理每个人被选出的次数为 d 的倍数的限制，每个人对 $\sum_i (\omega_d^i)^k$ 求和相当于每个人先选择一个 i，之后每次选到这个人权值乘以 ω_d^i，对方式求和。

选择了所有 i 后可以发现权值为每个人的 ω_d^i 之和的 n 次方，那么可以枚举选择每个 i 的有多少人。例如对于 $d = 3$ 答案为：

$$\sum_{i=0}^{m} \sum_{j=0}^{m-i} (m - i - j + i\omega_3 + j\omega_3^2)^n * \binom{m}{i, j}$$

复杂度 $O(m^{d-1} \log n)$

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

离散对数/bsgs

经典问题

求解模意义方程 $a^x \equiv b \pmod{p}$

$p \le 10^{10}$，10^5 次询问

bsgs 是一个类似折半的过程：由欧拉定理答案小于 p，因此取 $d = \lceil \sqrt{p} \rceil$，则存在 $x, y < d$ 使得答案是 $xd + y$。因此考虑 $a^0, a^1, \cdots, a^{d-1}$ 和 $a^0, a^d, a^{2d}, \cdots, a^{\lceil \frac{p}{d} \rceil d}$，其中必定存在两个数乘起来是 b。那么枚举一侧（例如枚举 $a^0, a^1, \cdots$），在另一侧 hash 表查找即可。复杂度 $O(\sqrt{p})$

离散对数/bsgs

经典问题

求解模意义方程 $a^x \equiv b \pmod{p}$

$p \le 10^{10}$，10^5 次询问

bsgs 是一个类似折半的过程：由欧拉定理答案小于 p，因此取 $d = \lceil \sqrt{p} \rceil$，则存在 $x, y < d$ 使得答案是 $xd + y$。因此考虑 $a^0, a^1, \cdots, a^{d-1}$ 和 $a^0, a^d, a^{2d}, \cdots, a^{\lceil \frac{p}{d} \rceil d}$，其中必定存在两个数乘起来是 b。那么枚举一侧（例如枚举 $a^0, a^1, \cdots$），在另一侧 hash 表查找即可。复杂度 $O(\sqrt{p})$但对于多组询问，可以进一步平衡复杂度：改变 d 可以调整查找侧和询问侧的大小，T 次询问时取 $d = \sqrt{\frac{p}{T}}$ 即可做到 $O(\sqrt{Tp})$

离散对数/bsgs

如果不是质数但 a, m 互质，则仍然可以求逆元。

如果不互质，则可以使用和欧拉定理部分类似的处理方式：先判前 $\log_2 m$ 次，之后 $\gcd(a^x, m)$ 就固定了。此时如果 b 不被 $\gcd(a^x, m)$ 整除则之后部分无解，否则可以整体除掉 $\gcd(a^x, m)$ 变为互质的情况（exBSGS）

bsgs 的这一折半思想可以有更多的应用，但我一时没找到好的例子。

离散对数/bsgs

如果不是质数但 a, m 互质，则仍然可以求逆元。

如果不互质，则可以使用和欧拉定理部分类似的处理方式：先判前 $\log_2 m$ 次，之后 $\gcd(a^x, m)$ 就固定了。此时如果 b 不被 $\gcd(a^x, m)$ 整除则之后部分无解，否则可以整体除掉 $\gcd(a^x, m)$ 变为互质的情况（exBSGS）

bsgs 的这一折半思想可以有更多的应用，但我一时没找到好的例子。

还可以更快：有一个算法被称为 Pohlig–Hellman，可以做到 sqrt 因子，但是大概率不会有人考（反例：1310f）

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。

首先根据原根的结论，$x^{2*\frac{p-1}{2}} \equiv 1 \pmod{p}$，因此 $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ 时必定无解。

否则，设原根为 g 且 $a \equiv g^k \pmod{p}$，则 k 不能是奇数（否则违反上一条），因此一定存在解 $g^{\frac{k}{2}}$。因此称 a 是二次剩余当且仅当 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$（不考虑 p 倍数的情况），下一部分会讲求解。

同时，对于 p 是奇质数的情况，如果有解则一定正好存在两组解：如果 x 是解则 $p-x$ 也是解。而如果 x, y 是两个解，则 $p|x^2 - y^2 = (x+y)(x-y)$，因此一定有 $x \equiv y$ 或者 $x \equiv -y$。

Cipolla

首先，对于模 p 的非二次剩余 x，考虑 $x^{\frac{p-1}{2}} \pmod p$，它的平方模 p 余 1，但它是非剩余，因此 $x^{\frac{p-1}{2}} \equiv -1 \pmod p$。

那么考虑加入任意一个非二次剩余对应的 $\sqrt{x}$ 进行计算（扩域），有 $(a+\sqrt{x})^p = \sum_{i=0}^{p} \binom{p}{i} a^i \sqrt{x}^{p-i}$，但中间项都被模 p 消掉了，因此 $(a+\sqrt{x})^p \equiv a^p + \sqrt{x}^p \equiv a - \sqrt{x} \pmod p$。从而 $(a+\sqrt{x})^{p+1} \equiv a^2 - x$。

那么随机一个 t 使得 $t^2 - a$ 不是二次剩余，然后 $(t+\sqrt{t^2-a})^{\frac{p+1}{2}}$ 即为答案。根据一些代数定理，在一个域下 k 次方程最多 k 个根，因此结果必定不含 $\sqrt{t^2-a}$。

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 $a_u^2 + Aa_ua_v + Ba_v^2 \equiv 0 \pmod{p}$

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

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 $a_u^2 + Aa_ua_v + Ba_v^2 \equiv 0 \pmod{p}$

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

对于每个 a_v 考虑，可以发现满足条件的 a_u 需要满足一个二次方程，带入求根公式，二次剩余即可解出可能的 a_u。

然后 dfs，在 dfs 中维护当前点到根上每种权值出现的次数即可。

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

可以推一些式子，比如：

Problem 1

求 $x^2 + y^2 \equiv r \pmod{p}$ 的解数量

勒让德符号

可以推一些式子，比如：

Problem 1

求 $x^2 + y^2 \equiv r \pmod{p}$ 的解数量

$x^2 \equiv a \pmod{p}$ 的解数量为 $1 + \left(\frac{a}{p}\right)$，因此有：

$$\begin{aligned}
&\sum_{i=0}^{p-1}\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{r-i}{p}\right)+1\right)\\
&= p + 2\sum_{i=0}^{p-1}\left(\frac{i}{p}\right) + \sum_{i=0}^{p-1}\left(\frac{i(r-i)}{p}\right)\\
&= p + \sum_{i=1}^{p-1}\left(\frac{\frac{r}{i}-1}{p}\right)
\end{aligned}$$

勒让德符号

$$p+\sum_{i=1}^{p-1}\left(\frac{\frac{r}{i}-1}{p}\right)$$

如果 $r=0$，答案为 $p+(p-1)\left(\frac{-1}{p}\right)$，否则 $\frac{r}{i}-1$ 遍历 -1 外的所有数，答案为 $p-\left(\frac{-1}{p}\right)$。

勒让德符号

$$p+\sum_{i=1}^{p-1}\left(\frac{\frac{r}{i}-1}{p}\right)$$

如果 $r=0$，答案为 $p+(p-1)\left(\frac{-1}{p}\right)$，否则 $\frac{r}{i}-1$ 遍历 -1 外的所有数，答案为 $p-\left(\frac{-1}{p}\right)$。但这东西很难记住也不太需要记住，实在不行这种题打表观察极其容易看出规律，例如这题模合数的版本 (gym 104234a)

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

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

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

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

首先考虑特征根方程，有 $x^2 - Ax - 1 = 0$，那么根为 $\frac{1}{2}(A \pm \sqrt{A^2 + 4})$。此时根据 $A^2 + 4$ 的情况考虑：

如果 $A^2 + 4 \equiv 0 \pmod{p}$，则在模 p 下解为重根，因此通项形如 $a_n = (c_1 n + c_2) * \frac{A}{2}^n$，但这个形式没法直接解（形式上是 $a^x \equiv bx$，但之前的做法求的不是通解）。

可以发现此时 $(\frac{A}{2})^2 \equiv -1$，从而 $(\frac{A}{2})^4 \equiv 1$，因此枚举 $n \bmod 4$ 即可。

综合练习

否则，记 $r=\sqrt{A^2+4}$，根为 $\frac{A+r}{2},\frac{A-r}{2}$。

考虑存在二次剩余的情况。比对系数（$a_0=0,a_1=1$）可以发现 $v_1+v_2=0,\frac{A+r}{2}v_1+\frac{A-r}{2}v_2=1$，那么 $v_1=\frac{1}{r},v_2=-\frac{1}{r}$。从而 $a_n=\frac{1}{r}((\frac{A+r}{2})^n-(\frac{A-r}{2})^n)$。

直接的形式还是不能解，但可以发现 $\frac{A+r}{2}*\frac{A-r}{2}=\frac{A^2-r^2}{4}\equiv\frac{A^2-(A^2+4)}{4}\equiv-1$。因此考虑枚举 n 的奇偶性，然后变为关于 $(\frac{A+r}{2})^n$ 的一个形如 $x+c_1x^{-1}\equiv c_2$ 的方程。这可以转成二次方程的形式。那么可以 Cipolla 求出两个根，然后对于每个根求出 $(\frac{A+r}{2})^n\equiv r$ 的满足奇偶性的通解。

综合练习

否则，记 $r=\sqrt{A^2+4}$，根为 $\frac{A+r}{2},\frac{A-r}{2}$。

考虑存在二次剩余的情况。比对系数（$a_0=0,a_1=1$）可以发现 $v_1+v_2=0,\frac{A+r}{2}v_1+\frac{A-r}{2}v_2=1$，那么 $v_1=\frac{1}{r},v_2=-\frac{1}{r}$。从而 $a_n=\frac{1}{r}((\frac{A+r}{2})^n-(\frac{A-r}{2})^n)$。

直接的形式还是不能解，但可以发现 $\frac{A+r}{2}*\frac{A-r}{2}=\frac{A^2-r^2}{4}\equiv\frac{A^2-(A^2+4)}{4}\equiv-1$。因此考虑枚举 n 的奇偶性，然后变为关于 $(\frac{A+r}{2})^n$ 的一个形如 $x+c_1x^{-1}\equiv c_2$ 的方程。这可以转成二次方程的形式。那么可以 Cipolla 求出两个根，然后对于每个根求出 $(\frac{A+r}{2})^n\equiv r$ 的满足奇偶性的通解。

这部分是一个 bsgs，但直接的 bsgs 只求出了最小的解。因此可以在求 bsgs 的时候顺便求 $\frac{A+r}{2}$ 的阶。然后可以发现 bsgs 的通解形如 $n\equiv a\pmod{\varphi(p)}$，和奇偶性方程合并即可（因为 $\varphi(p)$ 是偶数，合并很简单）

综合练习

$\sqrt{A^2+4}$ 不存在怎么办?

之前的推导仍然成立，bsgs 的时候为了避免 $a+b\sqrt{x}$ 的求逆可以变成枚举 $at-b$ 而不是 $at+b$，唯一的问题是复数幂循环节的大小可能是 p^2 的。

令 $B=\frac{A}{2}$，则根变为 $B+\sqrt{B^2+1}$。那么根据之前二次剩余的结论，$\sqrt{B+1}$ 模意义下不存在时，$(B+\sqrt{B^2+1})^{p+1}\equiv B^2-(B^2+1)=-1$，那么循环节不超过 $2p+2$。所以直接用之前的做法就行了。

综合练习

$\sqrt{A^2+4}$ 不存在怎么办?

之前的推导仍然成立，bsgs 的时候为了避免 $a+b\sqrt{x}$ 的求逆可以变成枚举 $at-b$ 而不是 $at+b$，唯一的问题是复数幂循环节的大小可能是 p^2 的。

令 $B=\frac{A}{2}$，则根变为 $B+\sqrt{B^2+1}$。那么根据之前二次剩余的结论，$\sqrt{B+1}$ 模意义下不存在时，$(B+\sqrt{B^2+1})^{p+1}\equiv B^2-(B^2+1)=-1$，那么循环节不超过 $2p+2$。所以直接用之前的做法就行了。

这里可以看出，有些数论向问题除去用已有模板外可能还需要对数直接性质进一步分析。

Case 1

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

Lucas

Case 1

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

对于这种情况，有 Lucas 定理：

$$\binom{n}{m} \equiv \binom{\lfloor \frac{n}{p} \rfloor}{\lfloor \frac{m}{p} \rfloor} * \binom{n \bmod p}{m \bmod p} \pmod p$$

有一个基于生成函数和 $(1+x)^p \equiv 1 + x^p \pmod p$ 的证明，但这里留到 exLucas。

板子题：loj2038

Lucas

一直使用上一个定理可以得到，如果 n, m 的 p 进制表示为 $n_l n_{l-1} \cdots n_1 n_0, m_l m_{l-1} \cdots m_1 m_0$，则 $\binom{n}{m} \equiv \prod \binom{n_i}{m_i} \pmod{p}$。
这相当于结果只和 p 进制下单独的每一位有关。例如，如果 $p = 2$，可以发现 $\binom{n}{m}$ 是奇数当且仅当二进制表示下 m 是 n 的子集。那么可以做一点 FWT 相关。

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

Lucas

一直使用上一个定理可以得到，如果 n, m 的 p 进制表示为 $n_l n_{l-1} \cdots n_1 n_0, m_l m_{l-1} \cdots m_1 m_0$，则 $\binom{n}{m} \equiv \prod \binom{n_i}{m_i} \pmod{p}$。
这相当于结果只和 p 进制下单独的每一位有关。例如，如果 $p = 2$，可以发现 $\binom{n}{m}$ 是奇数当且仅当二进制表示下 m 是 n 的子集。那么可以做一点 FWT 相关。

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

设 dp_i 表示以 i 结尾的序列数量，则顺序考虑每个数，相当于做操作 $dp_i += \sum_{i \subset j} dp_j$。
相当于支持单点修改，查某个子集的子集和。可以使用类似根号平衡的方式：修改同时改前 d 位的子集，询问查剩余位的子集。

Lucas

一般情况下，可以做一些数位 DP。

Problem 2

给出 n 组 l_i, r_i 和 m，求 $\sum_{i_1=l_1}^{r_1} \cdots \sum_{i_n=l_n}^{r_n} \binom{i_1+\cdots+i_n}{m} \pmod p$

$n, p \le 7, m \le 10^{18}$，$p$ 是质数，$10s$

由于篇幅限制，

Case 2

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

Case 2

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

重新考虑这个问题，$\binom{n}{m} = \frac{n!}{m!(n-m)!}$，考虑将 $n!$ 表示为 $p^k * d$ 的形式，其中 d 不被 p 整除。如果能求出这样的形式，则算组合数时可以对 k 部分做一些加减，对 d 部分求一些逆元。考虑如何求这一部分。将 $1, \cdots, n$ 中 p 的倍数和其它部分分开考虑，那么有

$$
\begin{aligned}
n! &= \prod_{i=1}^{\lfloor \frac{n}{p} \rfloor} pi * \prod_{1 \leq i \leq n, i \neq pk} i \\
&= \lfloor \frac{n}{p} \rfloor ! * p^{\lfloor \frac{n}{p} \rfloor} \prod_{1 \leq i \leq n, i \neq pk} i
\end{aligned}
$$

最后一部分关于模 p^k 循环，可以预处理 p^k 中所有和 p 互质的数的前缀乘积。然后即可做到 $O(p^k)$ 预处理，$O(\log n)$ 查询。

这一过程还可以得出，$n!$ 中 p 的次数是 $\sum_{i>0}\lfloor\frac{n}{p^i}\rfloor$，然后有如下结论：

Lemma（库默尔定理）

$\binom{n+m}{m}$ 中 p 的次数等于 n, m 在 p 进制下相加时进位的次数。

简单证明：$n!$ 中 p^k 一位对 p 次数的贡献是 $p^{k-1}+p^{k-2}+\cdots+p+1$，可以发现 p 个 p^k 进位到 p^{k+1} 会使次数增加 1。

这一过程还可以得出，$n!$ 中 p 的次数是 $\sum_{i>0}\lfloor\frac{n}{p^i}\rfloor$，然后有如下结论：

Lemma（库默尔定理）

$\binom{n+m}{m}$ 中 p 的次数等于 n, m 在 p 进制下相加时进位的次数。

简单证明：$n!$ 中 p^k 一位对 p 次数的贡献是 $p^{k-1}+p^{k-2}+\cdots+p+1$，可以发现 p 个 p^k 进位到 p^{k+1} 会使次数增加 1。

这也证明了 Lucas 的第一部分：$\binom{n}{m} \pmod p$ 不为 0 当且仅当 m 的 p 进制表示每一位都不大于 n。然后对之前 $\prod_{1\le i\le n, i\neq pk} i$ 部分分析一下容易得到之后的结论。

Problem 3

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

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

Problem 3

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

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

再分析一下，可以发现 $m + (n - m)$ 的进位次数相当于考虑 p 进制表示的每个后缀，其中 m 的后缀比 n 的后缀大的次数。

然后又是一个数位 DP：从后往前填数，设 $dp_{i,j,0/1,0/1}$ 表示填了后 i 位，后面进位了 j 次，当前 n, m 后缀的大小关系，n, A 后缀的大小关系。

p 很大不能枚举一位的情况转移，但注意到转移只需要知道 n, m 这一位的关系和 n, A 这一位的关系（大于，等于，或小于），每一种可能的情况在复杂的讨论后都可以 $O(1)$ 求出，从而复杂度 $O(\log^2 A)$

Case 3

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

上一个做法的瓶颈在于 $O(p^k)$ 的预处理，只需要重新考虑这部分。最后不完整的 $O(p)$ 项可以处理前缀和，只考虑求前 kp 个数中与 p 互质的数的乘积。从而可以看成

$$\prod_{i=0}^{k} \prod_{j=1}^{p-1} (i * p + j)$$

因为 $p^k \equiv 0$，考虑将这个式子看成 p 的多项式做，这样只需要保留 k 次。然后尝试倍增处理

exLucas

具体来说，设 $f_n(x)=\prod_{i=0}^{n-1}\prod_{j=1}^{p-1}(x+i*p+j)$（为了倍增），则答案为 $f_n(0)$。注意到如果只带入 p 的倍数，则求值时只需要保留 k 项。

然后倍增，显然有 $f_{2n}(x)=f_n(x)*f_n(x+n*p)$。问题是计算 $f_n(x+n*p)$ 时删去的高阶项本来会改变低阶项的值，但可以发现次数每减一值就会乘一个 p，因此只保留 k 项不会改变答案。（对于 i 次项，只有值模 p^{k-i} 的部分是有用的）

那么直接倍增就可以做到单次 $O(k^2\log n)$，总复杂度 $O(k^2\log^2 n)$

例子:

Problem 4

给一棵 n 个点的树，点有非负点权 v_i，边有边权 c_i。称一个点集是好的，当且仅当它是一个连通块且点权和不超过 M。

求有多少种选出 k 个好的点集的方式，使得存在一个点 x 满足对于每一个选出的点集 S，都有 $\sum_{u \in S} dis(u, x) * v_u \leq S$。答案对 $\mathbf{5^{23}}$ 取模。

$n \leq 60, M \leq 10^4, k \leq 10^{18}$

类欧几里得算法

欧几里得算法的思想：

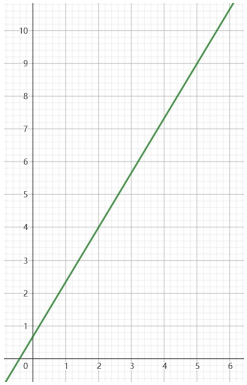
对于一个以 a, b 作为参数的问题，如果可以递归到 $(a \bmod b, b)$（取模）和 (b, a)（交换），则可以使用 gcd 的过程，在 $O(\log n)$ 步递归内解决问题。

类欧几里得算法

Case 1

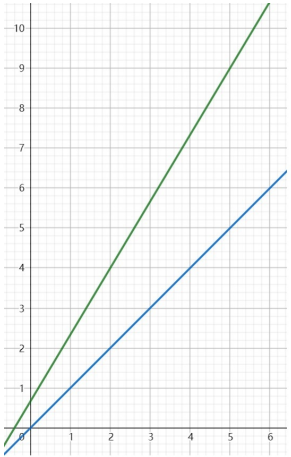
求 $\sum_{i=0}^{n} \lfloor \frac{ai+c}{b} \rfloor$，或者说线段下数点。

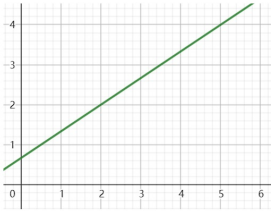
$n \leq 10^9$



类欧几里得算法

首先如果 $c \geq b$，可以简单处理。如果 $a \geq b$，则可以提出 $\lfloor \frac{a}{b} \rfloor * b$ 的部分，即：





类欧几里得算法

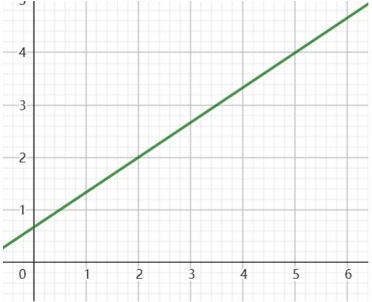
从推式子的角度：

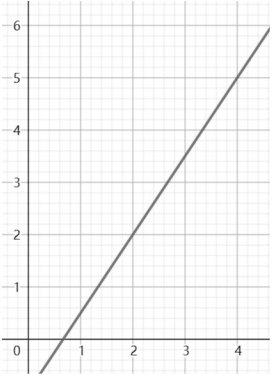
$$\sum_{i=0}^{n}\lfloor\frac{ai+c}{b}\rfloor$$

$$=\lfloor\frac{a}{b}\rfloor\sum_{i=0}^{n}i+\sum_{i=0}^{n}\lfloor\frac{(a \bmod b)i+c}{b}\rfloor$$

类欧几里得算法

然后考虑交换的操作。想法是翻转 x, y 轴，变为减去左上的部分。





需要注意的是线上的部分需要减去。

类欧几里得算法

从推式子的角度：

$$\begin{aligned}\sum_{i=0}^{n}\lfloor\frac{ai+c}{b}\rfloor &= \sum_{i=0}^{n}\sum_{d=1}^{\lfloor\frac{an+c}{b}\rfloor}\left[\lfloor\frac{ai+c}{b}\rfloor \geq d\right]\\ &= \sum_{i=0}^{n}\sum_{d=1}^{\lfloor\frac{an+c}{b}\rfloor}[ai+c \geq bd]\\ &= \sum_{d=1}^{\lfloor\frac{an+c}{b}\rfloor}\sum_{i=0}^{n}[bd-c-1 < ai]\\ &= \sum_{d=1}^{\lfloor\frac{an+c}{b}\rfloor} n+1-\lfloor\frac{bd+a-c-1}{a}\rfloor\end{aligned}$$

类欧几里得算法

因此复杂度可以做到 $O(\log n)$。

稍微极端一点的例子：对线段下的点 (x, y) 求和 $x^a y^b$。

从之前两张图的角度容易分析：b 的变换相当于 $(x, y) \to (x, y + c)$，取模相当于 $(x, y) \to (x, y + cx)$，交换相当于 $(x, y) \to (y, x)$，所以可以递归同时维护所有需要的 $x^a y^b$。

细节有亿点多。（P5170 是一个一次的情况）

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

a 对 p 取模是显然的，考虑如何交换。

可以发现问题相当于找到最小的 b，使得存在非负整数 q 满足 $ab - pq \in [l, r]$。转换得到 $pq - ab \in [-r, -l]$，同时可以发现最小的 b 一定对应最小的 q。

因此问题可以转换为找到最小的非负整数 q 使得 $pq \bmod a \in [-r, -l]$，对 $[-r, -l]$ 进行一些操作后即可变回之前的区间问题。

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 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。

考虑如下策略：能 $-a$ 就减，否则 $+b$。这样如果 $a+b-1 \geq n$，则可以经过 $[0, a+b-1]$ 的所有点，从而答案显然是 $n+1$。

否则可以发现，$a+b-1 < n$ 说明一个点不可能有 $+a, -b$ 两种合法操作，因此可以发现一个点最多有两种操作，那么可以到达的点构成一条链（如果成环就变为了上一种情况）

如果沿着链走，不掉头，则可以发现操作一定形如：能 $-a$ 就减，否则 $+b$ 或者能 $-b$ 就减，否则 $+a$。那么只需要考虑每一侧能走多远。

类欧几里得算法

考虑能 $-a$ 就减，否则 $+b$ 的过程，考虑能加几次 b，不能加 b 的情况是走到了一个 $(n-b,a)$ 之间的点。那么第一次不能加 b 的情况对应最小的 k 使得 $x+kb \bmod a \in (n-b,a)$。

然后就是上一个问题，这里多出的 $+c$ 也容易处理。复杂度 $O(\log n)$

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 $\frac{a}{b}$。

类欧几里得算法

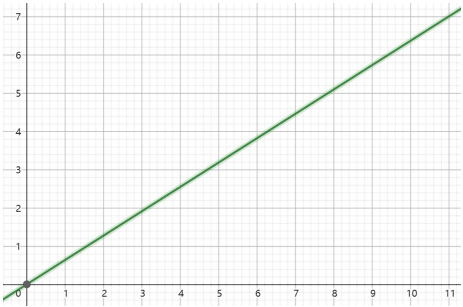
Problem 2

交互。有一个未知的有理数 $\frac{a}{b}$，保证 $a, b \le 10^9$。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 $\frac{a}{b}$。

考虑任取两个质数询问，CRT 得到 $\frac{p}{q} \equiv r \pmod m$，其中 $r \ge 10^{18}$。
如果 $\frac{a}{b} \equiv \frac{c}{d} \pmod m$，则可以发现 $m | ad-bc$，但 $m \ge (10^9)^2$，所以这不可能。因此只需要求出任意一组 $p, q \le 10^9$ 使得 $pq \equiv r \pmod m$ 即可。
可以发现对于一个 q，合法的条件是 $qr \pmod m \le 10^9$，那么找到最小的这样的 q 即可。
也可以用 S-B Tree，逼近 $\frac{r}{m}$

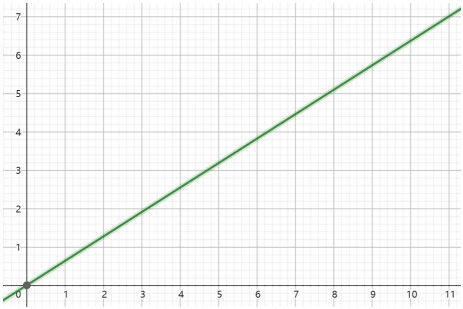
万能欧几里得

我不会细节，只能大概讲一下思路。



考虑从 $(0,0)$ 走到 (a,b)，其中 a,b 互质。每经过一条纵向线段 $x=i$ 做一次操作 A，每经过一条横向线段做一次操作 B。例如，在线段数点的过程中，可以看成记录当前下方点数 c，A 操作让答案加 c，B 操作让 c 加一，那么两种操作都可以写成矩阵乘法。

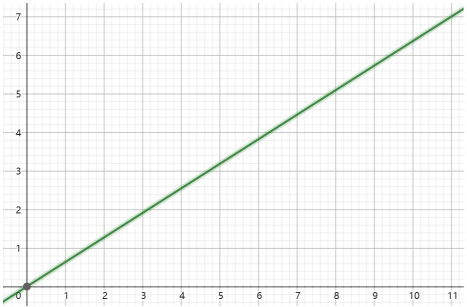
万能欧几里得

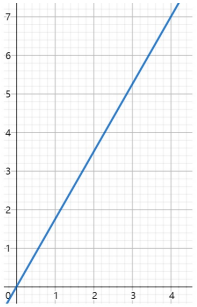


考虑 $a \geq b$ 的情况。可以发现，每两次 B 操作中间一定间隔了一次 A 操作。

进一步可以发现，如果将 B 换成 AB，然后考虑 $(a-b, b)$ 的情况，则：

万能欧几里得



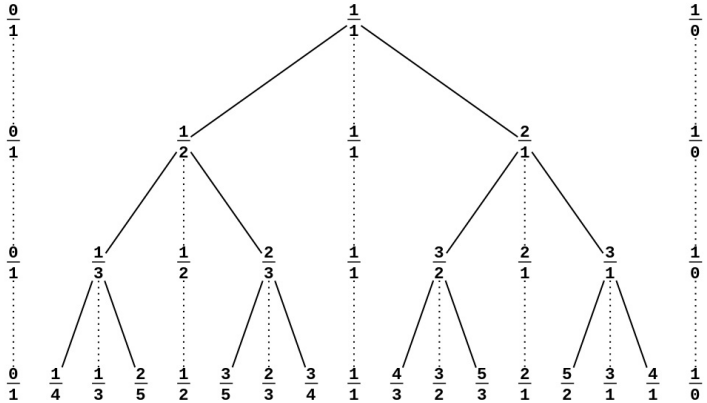


可以发现变换后与原问题等价，那么自然得到了欧几里得的过程：取模将 B 变为 $A^{\lfloor \frac{a}{b} \rfloor} B$，交换直接交换 A, B。

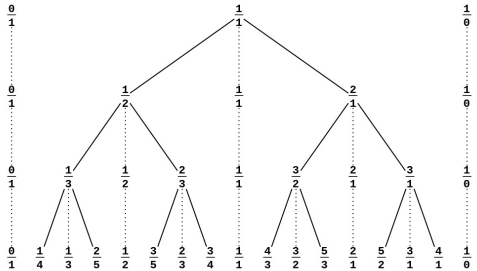
但问题是这东西的边界情况极其复杂，我完全不会，然后我 CTT2021 D4T3 的 60 就没过。

大概是需要讨论一下边界上的一些 A 和 B。

Stern-Brocot Tree



Stern-Brocot Tree



从层的角度考虑：第 0 层有两个“分数” $\frac{0}{1}, \frac{1}{0}$，之后每一层使用如下方式扩展：将上一层及之前的数按照中序遍历排成一列，在每相邻两个分数 $\frac{a}{b}, \frac{c}{d}$ 间加入 $\frac{a+c}{b+d}$

另一种理解方式：每个点可以表示为两个分数 $\left(\frac{a}{b}, \frac{c}{d}\right)$，它的值为 $\frac{a+c}{b+d}$，它的左右儿子为 $\left(\frac{a}{b}, \frac{a+c}{b+d}\right), \left(\frac{a+c}{b+d}, \frac{c}{d}\right)$

Stern-Brocot Tree

一些有用的性质：

- 树中出现的数均为既约分数，且它满足二叉搜索树的性质，即左儿子子树中的所有值小于父亲，小于右子树中的所有值。
- 任意既约分数都在树中出现。

前者的证明考虑 $\frac{a}{b}, \frac{c}{d}$ 推出 $\frac{a+c}{b+d}$ 的过程即可，后半部分可以考虑生成分数 $\frac{p}{q}$ 的 $p - q * \frac{c}{d}$。
后者证明忘了。

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/有理逼近

Problem 1

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

考虑逼近 $\sqrt{d}$。可以根据二叉树的性质，在 S-B Tree 上进行搜索：判断当前有理数与 $\sqrt{d}$ 的大小关系，然后向一侧走。

考虑二分到分母大于 n 停止，记录此时二分过程中左侧的最后一个数 $\frac{p}{q}$。那么根据二叉搜索树以及向下分母递增的性质，可以发现 $(\frac{p}{q}, \sqrt{d})$ 间不可能存在分母小于 n 的有理数。

Stern-Brocot Tree/有理逼近

Problem 1

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

考虑逼近 $\sqrt{d}$。可以根据二叉树的性质，在 S-B Tree 上进行搜索：判断当前有理数与 $\sqrt{d}$ 的大小关系，然后向一侧走。

考虑二分到分母大于 n 停止，记录此时二分过程中左侧的最后一个数 $\frac{p}{q}$。那么根据二叉搜索树以及向下分母递增的性质，可以发现 $(\frac{p}{q}, \sqrt{d})$ 间不可能存在分母小于 n 的有理数。

问题是一个有理数出现的深度可能是 $O(v)$ 的，例如 $\frac{1}{10^9}$。正确的结论是转向两次分母一定翻倍，因此考虑二分每次走的长度，可以在 $O(\log^2 v)$ 内完成查找。事实上如果精细实现(先倍增走的距离)，复杂度也可以是 $O(\log v)$ 的。

那么可以直接将 $\sqrt{d}$ 换成 $\frac{p}{q}$ 使得答案不变，然后是一个类欧。

Stern-Brocot Tree/有理逼近

Problem 1

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

考虑逼近 $\sqrt{d}$。可以根据二叉树的性质，在 S-B Tree 上进行搜索：判断当前有理数与 $\sqrt{d}$ 的大小关系，然后向一侧走。

考虑二分到分母大于 n 停止，记录此时二分过程中左侧的最后一个数 $\frac{p}{q}$。那么根据二叉搜索树以及向下分母递增的性质，可以发现 $(\frac{p}{q}, \sqrt{d})$ 间不可能存在分母小于 n 的有理数。

问题是一个有理数出现的深度可能是 $O(v)$ 的，例如 $\frac{1}{10^9}$。正确的结论是转向两次分母一定翻倍，因此考虑二分每次走的长度，可以在 $O(\log^2 v)$ 内完成查找。事实上如果精细实现(先倍增走的距离)，复杂度也可以是 $O(\log v)$ 的。

那么可以直接将 $\sqrt{d}$ 换成 $\frac{p}{q}$ 使得答案不变，然后是一个类欧。

其实也可以直接类欧，推一下 $\frac{a+b\sqrt{d}}{c}$ 啥的。

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/有理数逼近

Problem 2

给出有理数，求最小的 n 使得 $[an, bn]$ 间存在整数。

相当于存在一个有理数 $\frac{k}{n}$，它在 a, b 之间。
显然在 S-B Tree 上从上往下二分，找到第一个能分开 a, b 的数的分母即可。
但还是可以类欧：二分答案，求 $\sum_{i=1}^{n} \lfloor bn \rfloor - \sum_{i=1}^{n} \lfloor an - \epsilon \rfloor$ 是否非零。

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。

相当于存在一个有理数 $\frac{k}{n}$，它在 a, b 之间。
显然在 S-B Tree 上从上往下二分，找到第一个能分开 a, b 的数的分母即可。
但还是可以类欧：二分答案，求 $\sum_{i=1}^{n} \lfloor bn \rfloor - \sum_{i=1}^{n} \lfloor an - \epsilon \rfloor$ 是否非零。
有理逼近还可以推出一些非常难的结论，例如 AGC051F

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，$n \leq 10^6$

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，$n \le 10^6$

考虑直接的二分，问题在于需要求一个子树内分母不超过 n 的点数。

可以发现 S-B Tree 中子树的结构和整体相同，那么 $\frac{a}{b}, \frac{c}{d}$ 可以生成出所有满足 $\gcd(p,q)=1$ 的 $\frac{pa+qc}{pb+qd}$。然后相当于求 $\sum_{p,q\ge 1}[\gcd(p,q)=1][pb+qd\le n]$。根据经典方法，先莫比乌斯反演去掉 gcd 的限制，然后可以发现问题是一个类欧，可以 $O(n\log n)$。如果数论分块甚至能做到 $O(\sqrt{n}\log n)$，因为向下 p,q 会增加，加上外层二分的复杂度也是这个。

Stern-Brocot Tree/有理数二分

也有一些可能的替代方式。

如果可能的分母不多（例如给 10^5 个 $\frac{ai+b}{c}$ 序列）且分母不大，可以考虑如下方式：

取 M 为最大分母，可以发现任意两个限制内的既约分数差不小于 $\frac{1}{M^2}$，那么乘以 M^2 后，所有既约分数下取整两两不同。因此可以二分 $\frac{i}{M^2}$，变成普通的二分。但这样不能求出具体结果，因此可能需要枚举分母得到结果。

为啥这里全是数论?

~~因为 OI 也几乎不考连续的东西~~

但还有一个有趣的离散例子。

Extra

Problem

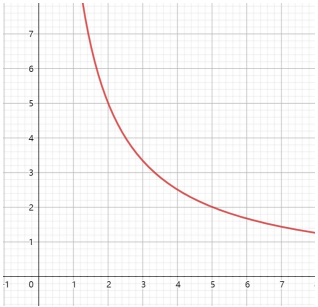
给定 n 个非负整数的三元组 (x_i, a_i, b_i)，选出一个子集满足选择的 x_i 的任意非空子集异或和非零（即异或下线性无关），最大化选出部分的 $(\sum a) * (\sum b)$，$n \leq 100$

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 $(\sum a) * (\sum b)$，$n \leq 100$

在二维上看这个问题，考虑 $xy = k$ 的图像（只看 $x, y \geq 0$）：



Extra

可以发现它是上凸的，那么 $xy = k$ 上任意点存在切线，使得整个 $xy \geq k$ 都在切线上方。
然后考虑最优解，使用上述结论可以发现，存在一个 k 使得最优解的 $\sum(a + bk)$ 最小。而一维情况下最大权线性基可以直接贪心：从大到小尝试加入即可。
但最优解对应的 k 并不是已知的，因此考虑遍历可能的 k。一个 k 的问题相当于平面上有 n 个点，然后用一条 $y = -kx$ 的线从上往下扫，得到的顺序就是 $y + xk$ 从大到小排序的结果。枚举 k 相当于这条线转 90 度，由计算几何知识可以发现这一过程中顺序只会变化 $O(n^2)$ 次，可以通过维护相邻点对改变顺序的时间 $O(n^2 \log n)$ 维护。
然后对于每个顺序暴力插入即可做到 $O(n^3 \log v)$，根据一些拟阵性质，交换也可以贪心做到 $O(\log v)$。

Extra

可以发现这个例子只用到了两点：子集满足的限制可以贪心选（即它是一个拟阵），最大化的东西形如 $f(\sum x, \sum y)$，其中 $f(x,y)=k$ 的图像是上凸的。

一些例子：

拟阵部分：选不超过 k 个 (Uniform)(abc257ex)，线性无关 (Linear)(tc11676)，构成森林 (Graph)(loj3412)，$\cdots$（当然拟阵应该 NOI 范围内不会直接出现）

函数部分：$f=xy$，$f=x^2+y$(abc257ex)，$f=xe^y$(tc14118)，$f=x^2/y$(loj3677)，$\cdots$

Thanks!

Sources：

欧拉定理：bzoj3884

exgcd：一个模拟赛题

CRT：loj2719

特征根：gym 100299j

原根：agc047c，loj2183

单位根：loj3403（的第一步），uoj450

二次剩余：SCOI2018 D1T2，gym 104234a，一个模拟赛题

Lucas：loj2264，一个模拟赛题，cf582d，loj2462（的最后一步）

类欧：Luogu P5170，arc127f，gym 102354i

S-B Tree：Luogu P5172,?，arc123f（稍微转化一下）

Extra：agc257ex，tc11676，tc14118，~~loj3412，loj3677~~