# 初等数论

author：一扶苏一

## Gcd

$\gcd(a,b)=\gcd(b,a \bmod b)$。

## Ex-Gcd

裴蜀定理：不定方程 $ax+by=c\,(a,b,c\in Z^+)$有整数解当且仅当 $c \mid \gcd(a,b)$。

解不定方程 $ax+by=\gcd(a,b)$：

$ax+by=\gcd(a,b)=\gcd(b,a \bmod b)=bx'+(a \bmod b)y'$

展开 $a \bmod b$ 后对应系数相等即可。

解不定方程 $ax+by=c$，其中 $c \mid \gcd(a,b)$：

先解 $\frac{a}{\gcd(a,b)}x+\frac{b}{\gcd(a,b)}y=\gcd(a,b)$。然后将 $x,y$ 都乘上 $\frac{c}{\gcd(a,b)}$。

## Euler Theorem

$a^k \equiv a^{k \bmod \varphi(p)} \pmod p$，其中 $a\perp p$。

证明略

## Ex-Euler Theorem

$$a^c \equiv \begin{cases} a^{c \bmod \varphi(p)} & a \perp p \\ a^c & a \not\perp p, c<\varphi(p) \\ a^{c \bmod \varphi(p)+\varphi(p)} & a \not\perp p, c \geq \varphi(p) \end{cases}$$

证明略。需要注意的是当 $c\leq\varphi(p)$ 时需要应用 case2 而不是 case3。

## Wilson Theorem

$p$ 为素数的充要条件是 $(p-1)!\equiv -1 \pmod p$。

~~但是我并不知道这东西在 OI 里有什么高妙的应用~~。

## CRT

求解线性同余方程组：

$$\begin{cases} x\equiv a_1 \ \ (mod \ \ m_1) \\ x\equiv a_2 \ \ (mod \ \ m_2) \\ \cdots\cdots \\ x\equiv a_k \ \ (mod \ \ m_k) \end{cases}$$

其中对于所有的 $i\neq j$，$m_i \perp m_j$。

设 $M=\prod m_i$，$M_i=\frac{M}{m_i}$，$t_i\equiv M_i^{-1}\pmod{m_i}$。

则 $x\equiv\sum_{i=1}^{k}a_iM_it_i\pmod M$。

需要注意的是，$t_i$ 是 $M_i^{-1}$ 在模 $m$ 下的逆元，因此在模 $M$ 下，二者之积不一定为 1。

## ExCRT

考虑同余方程组

$$\begin{cases}x\equiv a_1\pmod{m_1}\\x\equiv a_2\pmod{m_2}\end{cases}$$

其中不保证 $m_1\perp m_2$。

设 $M=\operatorname{lcm}(m_1,m_2)$。

根据第一个式子，有 $x=a_1+km_1$。因此只需要找到 $k$，使得 $a_1+km_1\equiv a_2\pmod{m_2}$。整理得 $km_1\equiv a_2-a_1\pmod{m_2}$。使用 exgcd 可以求出 $k$ 的值。然后有 $x\equiv a_1+km_1\pmod{\operatorname{lcm}(m_1,m_2)}$。

## Lucas Theorem

求 $\binom{n}{m}\pmod p$，其中 $p$ 为质数，$m\le n$。

解：将 $n,m$ 都写成 $p$ 进制数，设 $n=\sum_{i=0}^{x}a_i\times p^i$，$m=\sum_{i=0}^{y}b_i\times p^i$，那么有 $\binom{n}{m}\equiv\prod_{i=1}^{n}\binom{a_i}{b_i}\pmod p$。

当 $a<b$ 时，$\binom{a}{b}=0$。

写成递推式的形式：$\binom{a}{b}\equiv\binom{a\bmod p}{b\bmod p}\binom{\left\lfloor\frac{a}{p}\right\rfloor}{\left\lfloor\frac{b}{p}\right\rfloor}\pmod p$

推论：$\binom{n}{m}$ 不能被质数 $p$ 整除的必要条件是 $n$ 和 $m$ 在 $p$ 进制下的任何一位都有 $a_i\ge b_i$。

## Ex-Lucas Theorem

求 $\binom{n}{m}\pmod p$，不保证 $p$ 为质数，$m\le n$，$p$ 较小。

首先对 $p$ 进行唯一分解，只需要对 $p$ 的每个质因子的幂求出答案，然后 CRT 合并即可。下面考虑 $p$ 是质数时，$\binom{n}{m}\pmod{p^k}$ 的值。

考虑 $\binom{n}{m}=\frac{n!}{m!(n-m)!}$。但是无法求出 $m!(n-m)!$ 在模 $p^k$ 下的逆元，因为不一定存在。考虑设 $f(x)=\frac{x!}{p^{g(x)}}$，其中 $g(x)$是 $x!$ 的唯一分解式中 $p$ 一项的幂。那么答案即为 $\frac{f(n)}{f(m)f(n-m)}p^{g(n)-g(m)-g(n-m)}$。而 $f$ 显然与 $k$ 互质，可以求出逆元。下面考虑求 $f(x)$。

考虑 $x!=1\cdot2\cdot3\cdots x=(1\cdot2\cdot3\dots)(p\cdot2p\cdot3p\dots)$，其中第一个括号是不含因子 $p$ 的整数，第二个括号是 $p$ 的倍数。

考虑 $x$ 范围内有 $\left\lfloor\frac{x}{p}\right\rfloor$ 个 $p$ 的倍数，因此第二个括号显然就是 $(1\cdot2\cdot3\dots\left\lfloor\frac{x}{p}\right\rfloor)(p^{\left\lfloor\frac{x}{p}\right\rfloor})=(\left\lfloor\frac{x}{p}\right\rfloor)!p^{\left\lfloor\frac{x}{p}\right\rfloor}$。

考虑第一个括号为 $\prod_{i=1,i\not\equiv 0 \pmod p}^{x} i$。由于是模 $p^k$ 的，所以这个式子每 $p^k$ 一循环。因此有

$$\prod_{i=1,i\not\equiv 0 \pmod p}^{x} i = (\prod_{i=1,i\not\equiv 0 \pmod p}^{p^k} i)^{\left\lfloor \frac{n}{p^k} \right\rfloor} \times \prod_{i=p^k\left\lfloor \frac{n}{p^k} \right\rfloor+1,i\not\equiv 0 \pmod p}^{x} i。$$

第一个括号没有任何一项是 $p$ 的倍数，因此都会产生贡献。第二个括号中 $p^{\left\lfloor \frac{x}{p} \right\rfloor}$ 显然是 $p$ 的倍数，不对 $f$ 产生贡献，而 $(\left\lfloor \frac{x}{p} \right\rfloor)!$ 中有可能存在 $p$ 的倍数，需要递归求解。

综上，$f(x) = f(\left\lfloor \frac{x}{p} \right\rfloor)(\prod_{i=1,i\not\equiv 0 \pmod p}^{p^k} i)^{\left\lfloor \frac{n}{p^k} \right\rfloor} \times \prod_{i=p^k\left\lfloor \frac{n}{p^k} \right\rfloor+1,i\not\equiv 0 \pmod p}^{x} i$。递归求解即可。

考虑求 $g$：观察 $f$ 的式子，在每一层产生了 $\left\lfloor \frac{x}{p} \right\rfloor$ 个 $p$ 因子，因此 $g(x) = g(\left\lfloor \frac{x}{p} \right\rfloor) + \left\lfloor \frac{x}{p} \right\rfloor$。

边界条件是 $f(0) = 1$ 以及 $g(0) = 0$。

## BSGS Algorithm

解 $a^x \equiv b \pmod p$，其中 $a, b, p$ 是正整常数，$a \perp p$。求 $x$ 的最小非负值。

考虑根据欧拉定理，$a^{\varphi(p)} \equiv 1$，因此如果有解，则 $x < \varphi(p)$。设 $t = \lceil \sqrt{\varphi(p)} \rceil$，考虑暴力求出 $a^0 \sim a^t$ 的值，check $0 \sim t$ 是不是解，如果不是，则存入 hash 表中。

接下来进行 $\left\lceil \frac{\varphi(p)}{t} \right\rceil$ 步，每次给 $b$ 乘上 $a^t$，去 hash 表里 check 有没有对应的 $a$ 值。

时间复杂度 $O(\sqrt{p})$。

## Ex-BSGS Algorithm

解 $a^x \equiv b \pmod p$，不保证 $p$ 是质数。

首先的结论是，如果 $\gcd(a, p) \nmid b$ 且 $b \neq 1$，那么方程无解。

证明上可以考虑把式子改写成 $a \times a^{x-1} + kp = b$。根据裴蜀定理，若 $\gcd(a, p) \nmid b$，方程（这里的未知数是 $a^{x-1}$ 和 $k$）无整数解。特殊情况是，当 $b = 1$ 时，显然 $x = 0$ 是一个合法解（这与裴蜀定理不冲突，因为 $a^{x-1} = a^{-1}$ 是一个分数，不适用裴蜀定理）。

排除无解后并特判 $b = 1$ 的情况后，考虑解方程。注意到如果 $p$ 是质数，则可以用 BSGS 直接解。否则去掉他们的公因数。

设 $k = \gcd(a, p)$，由于 $k \mid b$，因此有 $a^{x-1}\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{p}{k}}$，设 $B = \frac{\frac{b}{k}}{\frac{a}{k}}$，$P = \frac{p}{k}$，则显然有 $a^y \equiv B \pmod P$，其中 $y = x - 1$。递归解这个方程即可。需要注意的是，因为 $a$ 在模 $P$ 意义下不一定存在逆元，所以 $B \neq \frac{b}{a}$。边界情况为，当 $P$ 为质数是，使用 BSGS 求解。

设 $a, b, p$ 同阶，因为每次除以大于 $1$ 的因数，所以递归层数为 $O(\log p)$，每层需要 $O(\log p)$ 求一次因数。进行一次 bsgs 的复杂度为 $O(\sqrt{p})$，因此总复杂度 $O(\log^2 p + \sqrt{p})$。