1 素数

1. 形如 $M_p = 2^p - 1$ 的数称为梅森数，若M_p为素数，那么称之为梅森素数。

- 若n为合数，则M_n为合数，若M_p为素数，则p为素数
- n为大于 1 的奇数时，M_n的所有因子形式为$8k-1$或$8k+1$（2 一定是p的二次剩余，可以用 Legendre 符号证明）
- p为奇素数时，M_p的所有素因子可以表示为$2kp+1$的所有因子形式

  证明：令q为M_p的任意素因子，由费马小定理得$q \mid 2^{q-1}-1$。所以$q \mid (2^{q-1}, 2^p-1) = 2^{(q-1,p)}-1$，若$(q-1,p)=1$，显然不可能，所以$(q-1,p)=p$，所以$p \mid q-1$，又$q-1$为偶数，所以存在$k$，使$q=2kp+1$

2. 若$n>1$且a^n-1为素数，则$a=2$，且n为素数

3. 若2^m+1为素数，则$m=2^n$。（$F_n = 2^{2^n}+1$ 形式的数叫做费马数，它也不一定是素数）

2 余数

定义

$$\mathbb{Z}/n\mathbb{Z} \text{ or } \mathbb{Z}_n = \{[a]_n : 0 \le a \le n-1\}$$

1. $[a]_n$中有一个元素与n互素，那么$[a]_n$所有元素与n互素；如果n是一个素数，那么它的所有的剩余类都与n互素

2. a 在模 n 情况下的逆元存在当且仅当$gcd(a,n)=1$，所以n是一个素数，1到$n-1$之间的所有数都有逆元；正常情况下有$\phi(n)$个存在逆元的数；

3. $\mathbb{Z}_n$ 是一个域当且仅当 n是一个素数；

4. S是一个完系的充要条件：

- S包含n个元素
- S中任意两个元素不同余

5. 若 $a \equiv b \pmod m$，且 $\gcd(k,m)=1$，k 是一个正整数，那么 $ka \equiv kb \pmod m$，更一般的，$ak \equiv bk \pmod m \Leftrightarrow a \equiv b \pmod{\frac{m}{\gcd(k,m)}}$

6. $a \equiv b \pmod m$且$a \equiv b \pmod n \Leftrightarrow a \equiv b \pmod{lcm(m,n)}$。这个又两种方法证明，第一种唯一素因子分解，第二种$a \equiv b \pmod m$等价于$m \mid a-b$，对于$n\Delta lcm(m,n)$同理。那么，对于一个$a \equiv b \pmod m$，我们就可以把这个拆成模m的所有的素因子的幂的同余式的组。

2.1 完系

1. 若 $a_i(1 \le n)$ 是一个完系，$k, m \in \mathbb{Z}, (m, n) = 1$，则$k + ma_i(1 \le n)$ 也构成一个模 n 的完系

2. 若 $a_i(1 \le n)$ 是一个完系，则$\sum_{i \le n} a_i = n(n+1)/2 \pmod n$，右边这个结果最终要么是$n/2$，要么是0

2.2 缩系

n 是正整数，S 是缩系的充要条件是

- S包含$\varphi(n)$个元素
- S中任意两个元素不同余
- S中任意元素与n互素

1. 设 $a_1, a_2, \cdots, a_{\phi(m)}$ 为一缩系，且$\gcd(m, k) = 1$，那么$ka_1, ka_2, \cdots, ka_{\phi(m)}$也组成一个缩系。否则若$ka_i \equiv ka_j \pmod m$，因为$\gcd(m, k) = 1$，所以$a_i \equiv a_j \pmod m$，矛盾。

2.3 线性同余方程

形如$ax \equiv c \pmod b$的方程被称为线性同余方程(Congruence Equation)。

1. 方程$ax + by = c$ 与方程 $ax \equiv c \pmod b$ 是等价的，有整数解的充要条件为 $\gcd(a, b) \mid c$。

2. 若$d = \gcd(a, b)$,且$d \mid c$, t为原方程的解，则所有的解可以表示为$\{t + k\frac{n}{d} \mid k \in \mathbb{Z}\}$，也是$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$的解。所有这些解模$n$最后会落到$n$的完全剩余系的$d$个元素之上。$t, t + n/d, t+2n/d, \cdots, t+(d-1)n/d$就是$d$个这样的解。其中最小正整数解为$x = (x \bmod t + t) \bmod t$，其中 $t = \dfrac{b}{\gcd(a, b)}$。

2.4 Euler's

1. 若 $(k, m) = 1$，则 $k^{\phi(m)} \equiv 1 \pmod m$，证明：由 $\prod_{i=1}^{\phi(m)}(ka_i) \equiv \prod_{i=1}^{\phi(m)} a_i \pmod m$，由$(a_i, m) = 1$，那么$k^{\phi(m)} \equiv 1 \pmod m$，证毕。

2. 费马小定理：若p为素数，那么对所有整数a有，$a^p \equiv a \pmod p$，或$a^{p-1} \equiv 1 \pmod p$

3. p 是一个素数，$\phi(p^k) = p^k - p^{k-1}$，证明先考虑 0 到 $p^k - 1$，有多少p的倍数，然后减一下

4. 任意整数 n，有 $\sum_{d|n} \phi(n) = n$，因为 $n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$，$\phi(n/d)$ 表示与 n 的最大公因数为 d 的数的个数，关于 $n = \sum_{d|n} \phi(n/d)$，我们想要说明它刚好包括所有 n 个数，

因为没有任意一个数字使得 $gcd(n,a)=d_1, gcd(n,a)=d_2$ 使得这个数字进入两个不同的划分集合 d_1, d_2，所有可以恰好包括所有数字。还需要说明 1 到 n 内的任意一个数字都与 n 有一个公共因子，比较显然，最起码是 1

5. $\neq$

note: 欧拉定理要求$a\Delta p$必须互素，注意到使用缩系证明过程中，给一个缩系乘以一个与p互素的数a，得到的集合依然是一个缩系，如果与p不互素，显然就会出现问题。而费马小定理中要求p是一个素数，更加严格。

2.5 原根

次数为$\varphi(p)$的数称为p的原根，一个推论是次数为$p-1$的数，一定是p的原根（$d \mid \varphi(p) \leq p-1$

1. a模m的次数是l，那么对于正整数n，$l \mid n$的充要条件是$a^n \equiv 1 \pmod{m}$

2. 若 a 与 m 互质，那么 $a^b \equiv a^{b \bmod \varphi(m)} \pmod{m}$，因为

$$a^b = a^{\varphi(m)\lfloor b/\varphi(m)+b \mod \varphi(m)} \equiv a^{b \mod \varphi(m)} \pmod{m}$$

若 a、m 不互素，$a^b \equiv a^{b \bmod \varphi(m)+\varphi(m)} \pmod{m}$

3. 若 a 模 m 的次数是 δ，则 $\{a^0, a^1, \cdots, a^{\delta-1}\}$ 模 m 不同余，注意这个集合可能不包含所有与m互素的元素（但是是一个子集），与m互素的元素数量为$\varphi(m) \geq \delta$，若$\delta = \varphi(m)$也就是说a模m的原根，这是模m的缩系

证明：假如有两个整数 k, l 满足 $a^k \equiv a^l \pmod{m}, 0 \leq k < l < \delta$，由于 $gcd(a,m)=1$，所以 $a^{l-k} \equiv 1 \pmod{m}$，$l-k<\delta$，这与 δ 最小矛盾，原命题成立。

所以如果 a 是一个 m 的原根，那么 $\{a^0, a^1, \cdots, a^{\varphi(m)-1}\}$ 是一个缩系。因为$(a,m)=1$,所以$(a^i, m)=1$.

4. 若 a 模 m 的次数为 r, 设 $\lambda > 0$，a^λ 模 m的次数为$r/gcd(\lambda, r)$（简单的想只需要需要$r \mid \lambda t$，取最小的t）

证明：$r \mid \lambda t$，所以$\frac{r}{(\lambda,r)} \mid \frac{\lambda t}{(\lambda,r)}$，且$(\frac{r}{(\lambda,r)}, \frac{\lambda}{(\lambda,r)}) = 1$，所以$\frac{r}{(\lambda,r)} \mid t$。又$(a^\lambda)^{\frac{r}{(\lambda,r)}} \equiv (a^r)^{\frac{\lambda}{(\lambda,r)}} \pmod{m}$，所以$t \mid \frac{r}{(\lambda,r)}$，所以$t = \frac{r}{(\lambda,r)}$

所以说如果a是m的一个原根（即$r=\varphi(m)$），那么a^λ是模m的原根的充要条件是$(\lambda, \varphi(m)) = 1$。如果找到了一个模$m$的原根$a$，对于任意$k$，只要$k$与$\varphi(m)$互质，那么$a^k$就是模$m$的一个原根。所以只要我们找到一个模$m$的原根，我们就可以找到其他所有原根。

5. a模m的次数是s，b模m的次数是t，若$(s,t)=1$，则ab模m的次数是st

6. a模m的次数是δ，那么满足$(\lambda, \delta)=1, 0<\lambda \leq \delta$，且$a^\lambda$模$m$的次数为$\delta$，这样的$\lambda$有$\varphi(\delta)$个。由4.很容易证。

如果a是模m的原根，那么次数为$\varphi(m)$，那么如果$(\lambda, \varphi(m)) = 1$，那么$a^\lambda$是一个原根，这样的满足$(\lambda, \varphi(m)) = 1$的$\lambda$一共有$\varphi(\varphi(m))$个。

7. 若$\gcd(a, n) = 1$，r是a模n的阶，那么$a^s \equiv a^t \pmod{n}$当且仅当$s \equiv t \pmod{r}$

8. 若g是模n的原根，那么$g^x \equiv g^y \pmod{n}$当且仅当$x \equiv y \pmod{\varphi(n)}$

9. n是一个有原根的正整数，假设$\gcd(a, n) = 1$，则$x^k \equiv a \pmod{n}(k \geq 2)$有解当且仅当

$$a^{\varphi(n)/\gcd(k,\varphi(n))} \equiv 1 \pmod{n} \tag{2.1}$$

10. p是一个素数，$\gcd(a, p) = 1$，a是一个p的k次剩余，当且仅当

$$a^{(p-1)/\gcd(k,(p-1))} \equiv 1 \pmod{p} \tag{2.2}$$

11. 若m为$2, 4, p^k, 2p^k$（p为奇素数）四者之一时，原根才存在。

注：这里还有一些 Jacobi 符号在k次剩余上的拓展

2.6 Carmichael's

1.Carmichael's 定理：对任意的a，a, n为正整数，且互素，那么$a^{\lambda(n)} \equiv 1 \pmod{n}$，$\lambda(n)$为 Carmichael 函数。$\lambda(n)$为满足该同余式的最小正整数，它总是小于等于$\phi(n)$，$\lambda(n)$ 的值称为 a 模 n 的 order.

2.

$$n = p_1^{r_1} p_2^{r_2} \cdots$$

那么$\lambda(n) = lcm(\lambda(p_1^{r_1}), \lambda(p_2^{r_2}), \cdots)$

2.7 中国剩余定理

1. 同余方程$a_1x_1 + \cdots + a_nx_n + b \equiv 0 \pmod{m}$有解的充要条件为$(a_1, \cdots, a_n, m) \mid b$，且模$m$情况下有$m^{n-1}(a_1, \cdots, a_n, m)$组不同的解（解所有的元都在模 m 的剩余系下）。

2. $M = m_1 \cdots m_n$，$m1, \cdots, m_n$两两互素，$f(x) = a_0 + a_1x + \cdots + a_nx^n$。那么$x_0$是$f(x) \equiv 0 \pmod{M}$的解当且仅当$x_0$是下面方程组的解

$$\begin{cases} f(x) & \equiv 0 \pmod{m_1} \\ & \cdots \\ f(x) & \equiv 0 \pmod{m_n} \end{cases} \tag{2.3}$$

充分性比较显然，必要性由中国剩余定理可得（注意和0同余）。

2.8 二次剩余

1. p是一个奇素数，a不能被p整除，那么$x^2 \equiv a \pmod{p}$要么没解，要么有两个解。

证明：若有$x^2 \equiv y^2 \equiv a \pmod{p}$，那么$p \mid (x+y)(x-y)$，所以$x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$，这也是一个比较有意思的结论。

2. 二次剩余和二次非剩余的数量均为$(p-1)/2$

寻找二次剩余最简单的方法就是枚举$1^2, 2^2, \cdots, \frac{(p-1)^2}{2}, \frac{(p+1)^2}{2}, \cdots, (p-1)^2 \pmod{p}$，并且发现如果有解，$x^2 \equiv (p-x)^2 \pmod{p}$，即$x^2 \Delta (p-x)^2$指向同一个二次剩余，所以只需计算$x^2, 1 \leq x \leq (p-1)/2$。另外需要证明不存在$x, y \in [1, (p-1)/2]$指向同一个二次剩余。

3. 欧拉判别条件：p是一个奇素数，$\gcd(a,p) = 1$，那么a是一个二次剩余当且仅当$a^{(p-1)/2} \equiv 1 \pmod{p}$

由欧拉定理有

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv a^{p-1} - 1 \equiv 0 \pmod{0} \tag{2.4}$$

所以$a^{(p-1)/2} \equiv 1 \pmod{p}$或$a^{(p-1)/2} \equiv -1 \pmod{p}$

证明：充分性，a是一个二次剩余，那么存在x_0使$x_0^2 \equiv a \pmod{p}$，又由欧拉定理

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv 1 \pmod{p} \tag{2.5}$$

必要性，假设g是模p的原根，那么存在t使$g^t \equiv a \pmod{p}$（原根构造缩系），那么

$$g^{t(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$$

从而

$$t(p-1)/2 \equiv 0 \pmod{p-1} \tag{2.6}$$

所以t是一个偶数，所以

$$(g^{t/2})^2 \equiv g^t \equiv a \pmod{p} \tag{2.7}$$

所以a是一个模p的二次剩余

4. 令$n = 2^e p_1^{e_1} \cdots p_l^{e_l}$为n的素因子分解，假如$\gcd(a, n) = 1$，那么$x^2 \equiv a \pmod{n}$有解的充要条件为

- 如果$e > 1$（否则不考虑），若$e = 2$，那么$a \equiv 1 \pmod{4}$；若$e \geq 3$，那么$a \equiv 1 \pmod{8}$
- 对任意的$i(1 \leq i \leq k)$，都有$a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$

2.9 Legendre 符号和 Jacobi 符号

p是一个奇素数，a是一个整数，假设$\gcd(a, p) = 1$，那么*Legendre symbol*, $\left(\frac{a}{p}\right)$，定义为

$$\left(\frac{a}{p}\right) = \begin{cases} = 1, & \text{如果}a\text{是模}p\text{的二次剩余} \\ = -1, & \text{如果}a\text{是模}p\text{的非二次剩余} \end{cases} \tag{2.8}$$

需要注意，一般情况下，考虑$\gcd(a, p) = 1$，如果p是a的因子，这个结果等于0，见英文版wiki。

1. 由上面的欧拉判别条件有$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$，所以这是*Legendre symbol*形式的欧拉判别条件。

2. 若$a \equiv b \pmod{p}$，那么$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$，

3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$，由上面性质 1. 可以证明。这也表示这个符号是一个（完全）积性函数。

4. $\left(\frac{a^2}{p}\right) = 1$，$:x^2 \equiv a^2 \pmod{p}$。

由上面四条性质我们可以得到

- 二次剩余的逆元依然是二次剩余，非二次剩余的逆元依然是非二次剩余
- 两个二次剩余或非二次剩余的积是二次剩余
- 二次剩余和非二次剩余的积是非二次剩余

5. p是一个奇素数，那么对所有整数

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases} \tag{2.9}$$

由*Legendre symbol*形式的欧拉判别条件很容易证明。这个结论可以用来判断一些特殊的二次剩余方程是否有解。

2.9.1 高斯引理

1. p为奇素数，假设$\gcd(a,p)=1$，ω为

$$\left\{1a, 2a, 3a, \cdots, \frac{p-1}{2}a\right\}$$

这里面模p为负数（或者大于$p/2$）的数的数量

$$\left(\frac{a}{p}\right) = (-1)^{\omega} \tag{2.10}$$

注：上面那个集合里面，两两不同余，它们模p落到一个完系中，而模p又一个这样的特殊的完系

$$\left\{0, \pm 1, \pm 2, \cdots, \pm\frac{p-1}{2}\right\}$$

但是显然最上面那个集合里面的元素模p不可能等于 0，所以可能的结果会落到这个完系除 0 外的集合上。

2. 若p是奇素数，那么

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

2.9.2 二次互反律

1. 如果p, q是两个不同的奇素数

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, if one of $p, q \equiv 1 \pmod 4$
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, if both $p, q \equiv 3 (\bmod 4)$
- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$，把左边两项中任意一项直接移动到右边，也是成立的

2.9.3 Jacobi 符号

a是一个任意整数，n是一个正奇数，$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，那么*Jacobi*符号定义为

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_!} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

如果$\gcd(a,n)\neq 1$，那么上面的左边等于 0（左边是 Jacobi 符号，右边是 Legendre 符号）。

m,n是任意的正的奇数，$\gcd(a,n)=\gcd(b,n)=1$，那么

- $a\equiv b\pmod n$，那么$\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$
- $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
- $\gcd(m,n)=1$，那么$\left(\frac{a}{mn}\right)\left(\frac{a}{m}\right)=\left(\frac{a}{n}\right)$
- $\left(\frac{1}{n}\right)=1$
- $\left(\frac{-1}{n}\right)=(-1)^{(n-1)/2}$
- $\left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}$
- $\gcd(b,n)=1$，那么$\left(\frac{ab^2}{n}\right)=\left(\frac{a}{n}\right)$
- $\gcd(m,n)=1$，那么$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{(m-1)(n-1)/4}$，或者$\left(\frac{m}{n}\right)=(-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$

对于最后一条性质的后面部分，如果m是偶数不能直接用，需要将 2 的幂提出来，之后再用。

需要注意，与*Legendre*符号不同的是，$\left(\frac{a}{n}\right)$如果结果为-1，那么$a\equiv x^2\pmod n$可以确定无解，但是如果为-1，那么可能无解可能有解。

2.10 连分数

$$[a_0,a_1,\cdots,a_n]=\frac{p_n}{q_n} \tag{2.11}$$

$$\begin{aligned} &p_0=a_0,p_1=a_1a_0+1,p_n=a_np_{n-1}+p_{n-2} && (2\le n\le N)\\ &q_0=1,q_1=a_1,q_n=a_nq_{n-1}+q_{n-2} && (2\le n\le N)\end{aligned}$$

关于这个序列a，比如a/b的连分数序列，就是用欧几里得算法每一步迭代过程中的a/b(商)。

1. 任意有限简单连分数（finite simple continued fraction）一定可以表示为一个有理数。相反，任意有理数一定可以表示为一个有限简单连分数。

2. 任意无理数可以唯一的写成一个无限简单连分数，相反，一个无限简单连分数是一个无理数。

3. 任意具有周期性简单连分数是一个二次无理数（指的是整系数一元二次方程的根），相反，任意二次无理数标识为连分数具有周期性。

4. 一个非完全平方数的平方根的连分数是有周期的，并且若循环节以a_0开始，那么结尾一定是$2a_0$

2.10.1 name

1. $\sqrt{2}=[1,\overline{1}]$, $\sqrt{3}=[1,\overline{1,2}]$, $(\sqrt{5}-1)/2=[0,\overline{1}]$, $(\sqrt{5}+1)/2=[1,\overline{1}]$

2.11 丢番图方程

2.11.1 Pell 方程

设 N 为非平方自然数，那么$x^2-Ny^2=1$有无穷自然整数解

3 大整数分解

3.1 CFRAC, QS and NFS

下面要介绍的几种分解方法基于这样一种重要的事实（起源于Fermat's method）

对于大整数 N，如果有两个整数x,y满足

$$x^2\equiv y^2 \pmod N, 0<x<y<N, x\neq y, x+y\neq N \tag{3.12}$$

那么$\gcd(x-y,N),\gcd(x+y,N)$就可能是N的非平凡因子。要找到上面的同余式，那么就需要找到

$$\left(x_i=\prod p_k^{e_k}\right)\equiv\left(y_i=\prod p_j^{e_j}\right) \pmod N \tag{3.13}$$

这样的同余式的集合，然后用乘法将同余符号两边凑成平方。

CFRAC, QS, NFS 三种方法的出发点都是去寻找

$$x_k^2\equiv(-1)^{e_0}p_1^{e_{1k}}\cdots p_m e_{mk} \pmod N \tag{3.14}$$

p_i 是分解基（FB），通过乘法凑出平方，即

$$\sum_{1\le k\le n} \epsilon_k(e_{0k},\cdots,e_{mk}) \equiv (0,\cdots,0) \pmod 2 \tag{3.15}$$

令$x = \prod_{1\le k\le n} x_k^{\epsilon_k}, y = (-1)^{v_0} p_1^{v_1}\cdots p_m^{v_m}$, 且$\sum_k \epsilon_k(e_{0k},\cdots,e_{mk}) = 2(v_0,\cdots,v_m)$, 那么就有$x^2 \equiv y^2 \pmod N$

3.1.1 CFRAC

$$W_i = P_i^2 - Q_i^2 kN \Rightarrow P_i^2 \equiv W_i \Leftrightarrow x_i^2 \equiv (-1)^{e_0}\cdots p_m^{e_m} \pmod N \tag{3.16}$$

P_i/Q_i是$\sqrt{kN}$的连分数逼近，k是任意选的一个数字，使kN不是一个平方数。

3.1.2 Quadratic sieve

定义

$$Q(x) = (x + \left\lfloor\sqrt{N}\right\rfloor)^2 - N \tag{3.17}$$

那么

$$Q(x) = (x + \left\lfloor\sqrt{N}\right\rfloor)^2 - N \equiv (x + \left\lfloor\sqrt{N}\right\rfloor)^2 \pmod N \tag{3.18}$$

只需要$Q(x)$是一个平方数

二次筛法中，没有直接找$Q(x)$，而是先找一系列能被分解基完全分解的数（能被完全分解就成为光滑）。只需要寻找一系列$Q(x_i)$

$$\sum_i Q(x_i) \equiv \sum_i (x_i + \left\lfloor\sqrt{N}\right\rfloor)^2 \pmod N \tag{3.19}$$

使得上面等式的左边是一个平方数，即在分解基下分解结果每个质因子的幂都是偶数。（本质是一个解线性方程的过程）

假如有个序列$X = \{0,\cdots,n\}$，对于分解基 F，我们想要求出所有关于分解基的光滑的$Q(X_i)$（在这之后在考虑线性组合的问题）。如果$Q(X_i)$是光滑的，对于每个分解基 F 中的质数p，下面的方程都需要满足。

$$Q(X_i) \equiv (X_i + \left\lfloor\sqrt{N}\right\rfloor)^2 - N \equiv 0 \pmod p \text{ for each p} \tag{3.20}$$

由于p都很小，所以方程很好解，得到$X_i \equiv a \pmod{p}$，然后将$Q(X)$中$a, a+p, a+2p, \cdots$位置的数除以p（值得注意的是对于$p > 2$，X_i有两个解）。这样得到的光滑数关于分解基中每个质数的幂都是 0 或者 1。那些$Q(X)$中值为 1 的数就对应一个光滑数。

然后就是一个解线性方程组的问题，即怎么组合这些光滑数分解基表达情况下，幂的组合是偶数。wiki给出了一个很好的例子

3.2 Polland's rho and p - 1 Methods

3.2.1 Polland's p - 1 Method

如果能够找到一个与大合数n不互质的数p，那么可以直接求$\gcd(n, p)$求得n的一个因子。

如果素因子 $p \mid n, n = pq$，那么$a^{p-1} \equiv 1 \mod p$，假如我们有$M = (p-1)x$（这里的M就是下面的k），那么对于满足$\gcd(a, p) = 1$的a，$a^M = (a^{p-1})^x \equiv 1 \pmod{p}$，那么$p \mid a^M - 1$，又$p \mid n$，则有$p \mid \gcd(n, a^{M-1} - 1)$。这样就可能找到一个$n$的平凡因子。一般$a$为2。

比如对于$k = \mathrm{lcm}(1, 2, \cdots, B)$，$B$多大才比较合适呢。我们希望$\gcd(a^k - 1, n) \neq 1$，对于$a^k - 1$它的因子有$k$的所有素因子（不考虑特殊情况），那么如果$k$包含$n$的因子，那就很好。所以我猜测，$B$最好应该大于等于$n$所包含的最小因子。

下面是算法执行的步骤

- 从 1 到 n 中选择一个数 a，选择一个合适的B，B越大找到N因子的可能性越大，但算法需要的时间可能越久
- 计算k，k计算方式很多，比如可以是$\mathrm{lcm}(1, 2, \cdots, B)$，可以是$B!$，又比如可以是

$$k = \prod_{p\ prime, 1 \leq p \leq B} p^{\lfloor \log B / \log p \rfloor} \tag{3.21}$$

  前面两种计算方式好像有缺点，比如$p-1$的分解包含一个素数的高次幂，那么就可能会失败。
- 计算$d = \gcd(a, n)$，$d \neq 1$，返回d
- 计算$e = \gcd(a^k - 1, n)$，若$e = 1$则增大B，若$e = n$，则重新选择a，否则返回e

3.2.2 Polland's rho Method

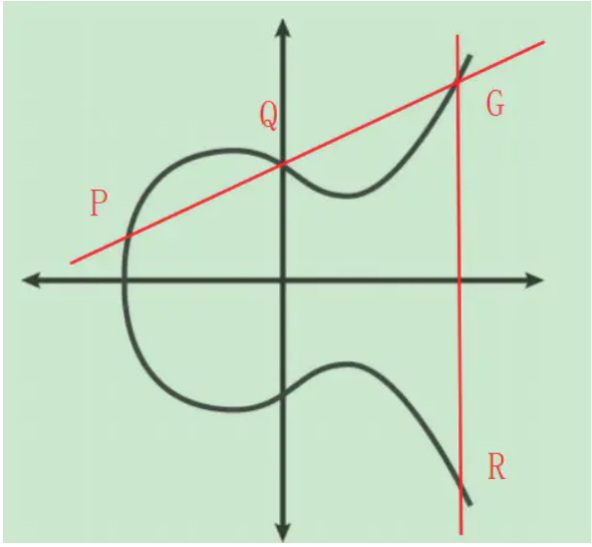
3.3 Elliptic Curve Method

$$y^2 = x^3 + ax + b \pmod{p} \tag{3.22}$$

F_p是一个定义在整数集合$\{0, 1, 2, \cdots, p-1\}$上的域，$a, b \in F_p$

3.3.1 椭圆曲线

对于椭圆曲线$y^2 = x^3 + ax + b$上的点$P = (x_p, y_p), Q = (x_q, y_q)$，定义$P + Q = R = (x_r, y_r)$，如图



$$\begin{cases} \lambda = (y_p - y_q)/(x_p - x_q) & \text{if } P \neq Q \\ \lambda = (3x_p^2 + a)/2y_p & \text{if } P = Q \end{cases} \tag{3.23}$$

可以求得R

$$\begin{cases} x_r = \lambda^2 - x_p - x_q \\ y_r = \lambda(x_p - x_r) - y_p \end{cases} \tag{3.24}$$

如果是在有限域F_p情况下，那么就对所有操作取余。

$$\begin{cases} \lambda = (y_p - y_q)/(x_p - x_q) \pmod p & \text{if } P \neq Q \\ \lambda = (3x_p^2 + a)/2y_p \pmod p & \text{if } P = Q \end{cases} \tag{3.25}$$

$$\begin{cases} x_r = \lambda^2 - x_p - x_q \pmod p \\ y_r = \lambda(x_p - x_r) - y_p \pmod p \end{cases} \tag{3.26}$$

可以求得R

对于乘法$nP = P + (n-1)P$，如此不断递归，$2P = P + P$

- 椭圆曲线上进行$Q - P$的减法运算，只需要将$P(x_p, y_p)$变为$-P(x_p, -y_p)$，然后做Q和$-P$的加法即可

- 在一个有限域F_p的情况下，单位元O_E定义为无穷远点，假设阶为k，那么对任意P，$kP = O_E$，且$P + O_E = P$
- 加法可以视作代数里面的乘法，P乘以常数c，可以视作代数里面对P取幂，$xP = D$可以视作$P^x = D$

3.3.2 Elliptic Curve Method

下面的所有运算都在Z_p中

1. 随机取$k = B!$或$k = \mathrm{lcm}(2, 3, 5, 7, \cdots)$
2. 取$a, x, y \in Z_p$，计算$b = y^2 - x^3 - ax$. 重复 2. 直到$\gcd(4a^3 + 27b^2, n) \neq 1$. 这样就得到椭圆曲线 $E : y^2 = x^3 + ax + b$和其上一点$P(x, y)$
3. 计算kP，每次计算，我们要么会得到一个新的点，要么会得到n的一个因子. 如果$kP \equiv \mathcal{O}_E \pmod n$ (这个的意思就是λ不存在，λ是一个求逆元的过程，所以实际上是逆元不存在)，设此时kP的λ的分母是m，计算$\gcd(m, n)$，这个结果一定是n的非平凡因子
4. 如果 3. 没有得到n的因子那么重复 2. (也可以进一步增大B)

4 离散对数

给定$a, g, p \in \mathbb{N}$，计算满足$a^x \equiv g \pmod p$的x

g是$\mathbb{Z}_p$对应循环群的生成元，也就是原根，其阶数为$\varphi(p)$；$\mathbb{Z}_p$是一个循环群，当且仅当$p = 1, 2, 4, p^k, 2p^k (k > 0)$

最朴素的方法就是

- 计算$g^2 (mod\ p), g^3 (mod\ p) \cdots$
- 如果$g^k (mod\ p) = a$就结束
- 复杂度是$p/2$

4.1 Shanks' Baby-Step Giant-Step Algorithm

令$s = \lfloor \sqrt{n} \rfloor$，令$k = im + j, i, j \in \{0, 1 \cdots, m - 1\}$，由于$a \equiv g^k \pmod p \equiv g^{im+j}$，从而$g^j \equiv ag^{-im} \pmod p$；搜索$i, j$，找到满足$g^j \equiv ag^{-im} \pmod p$的$ifij$,然后就得到$x = im + j$

对于$y \equiv a^x \equiv \bmod n$

- $s = \lfloor n \rfloor$

- y就是给定的g，计算$(ya^r, r), r = 0, \cdots, s-1$，$S = \{(y,0), (ya,1), (ya^2,2), \cdots, (ya^{s-1}, s-1) \bmod n\}$
- 计算$(a^{ts}, ts), t = 1, \cdots, s$，$T = \{(a^s,1), (a^{2s},2), (a^{s^2}, s) \bmod n\}$
- 将S, T按第一项排序，然后寻找$ya^r = a^{ts}$，计算$x = ts - r$即为答案$\log_a y \pmod n$

复杂度$\sqrt{n}\log n$，用 hash 存储 S 然后第二个表边计算边查询则是 $\sqrt{n}$，如果用 map 存储也是$\sqrt{n}\log n$。

4.2 Silver-Pohlig-Hellman Algorithm

假如p是一个大素数，然而$p-1$的素因子都相对较、小。

$$a^x \equiv b \pmod p \tag{4.27}$$

假如$GF(p)$的原根是g，那么$a \equiv g^i \pmod p, b \equiv g^j \pmod p$，其中$i, j \in \{1, p-1\}$，带入上面的方程有$g^{xi} \equiv g^j \pmod p$，那么一定有$xi \equiv j \pmod{\varphi(p) = p-1}$，即$x = i^{-1}j \pmod{\prod_k p_k^{\alpha_k}}$，也就是如何解$i, j$，即$g^i \equiv a \pmod p$。

现在我们考虑$p - 1 = q^n$，假如

$$x \equiv x_0 + x_1 q + \cdots + x_{n-1} q^{n-1} \pmod{q^n} \tag{4.28}$$

$$g^x \equiv a \pmod p \tag{4.29}$$

那么

$$\begin{aligned} a^{q^{n-1}} &\equiv (g^x)^{q^{n-1}} \\ &= (g^{x_0 + x_1 q + \cdots + x_{n-1} q^{n-1}})^{q^{n-1}} \\ &= (g^{q^{n-1}})^{x_0} \pmod p \end{aligned} \tag{4.30}$$

从而转化为一个求x_0的离散对数问题，假如使用大步小步解出x_0后

$$\begin{aligned} a^{q^{n-2}} &\equiv (g^x)^{q^{n-2}} \\ &= (g^{x_0 + x_1 q + \cdots + x_{n-1} q^{n-1}})^{q^{n-2}} \\ &= (g^{x_0 q^{n-2} + x_1 q^{n-1}}) \pmod p \\ \iff (g^{q^{n-1}})^{x_1} &\equiv ((g^{-x_0} a)^{q^{n-2}}) \pmod p \end{aligned} \tag{4.31}$$

这又是一个新的求x_1的离散对数问题，复杂度为$O(n\sqrt{q})$，以此类推求出$x_i (0 \le i < n)$

对于$N=\varphi(p)=p-1=\prod_k p_k^{\alpha_k}$，我们需要求$x\equiv \log_a b \pmod{\varphi(p)=N=p-1}$，可以先求$x\equiv \log_a b \pmod p$，然后用 CRT。所以复杂度大约$\mathcal{O}(\sum_k \alpha_k\sqrt{p_k})$

下面给出解$a^x\equiv b \pmod q$算法的步骤，即解$x\equiv \log_a b \pmod{\varphi(q)}$

- 分解$q-1=\prod_k p_k^{\alpha_k}$
- 对于分解结果中的因子p^α，对于$x\equiv \log_a b \pmod{p^\alpha}$ (为方便，下标k均省略)，假设

$$x\equiv x_0+x_1p+\cdots+x_{\alpha-1}p^{\alpha-1} \pmod{p^{\alpha-1}},\ (0\le x_i<p) \tag{4.32}$$

  - 预处理计算，$r_{p_i,j}=a^{j\cdot\frac{q-1}{p}} \pmod q, 0\le j\le p_i$
  - 计算x
    - $b_0=b$，寻找满足$b_1^{(q-1)/p}\equiv r_{p,j} \pmod q$的$j$，那么$x_0=j$
    - $b_1=b\cdot a^{-x_0}$，寻找满足$b_1^{(q-1)/p^2}\equiv r_{p,j} \pmod q$的$j$，那么$x_1=j$
    - $b_2=b\cdot a^{-x_0-x_1p}$，寻找满足$b_2^{(q-1)/p^2}\equiv r_{p,j} \pmod q$的$j$，那么$x_2=j$
    - 类比，得到x_i
  - 通过 CRT 组合$x\equiv \log_a b \pmod{p_k^{\alpha_k}}$

这里有两个具体的手算的例子，例1、例2

下面给出枚举$r_{p,j}$的理由，假如$x_0,\cdots,x_{i-1}$已知

$$\begin{aligned}(b)^{\frac{q-1}{p^{i+1}}}&\equiv (a^{x_0+\cdots+x_{\alpha-1}p^{\alpha-1}})^{\frac{q-1}{p^i}}\\&=(a^{x_0+\cdots+x_{i-1}p^{i-1}})^{\frac{q-1}{p^{i+1}}}\cdot a^{x_i\cdot\frac{q-1}{p}} \pmod q\\ \iff (b\cdot a^{x_0+\cdots+x_{i-1}p^{i-1}})^{(q-1)/p^{i+1}}&\equiv a^{x_i\cdot\frac{q-1}{p}} \pmod q\end{aligned} \tag{4.33}$$

然后需要用解x_i，所以需要预处理，这里的$a^{(q-1)/p}$相当于上面大步小步法里的a，当然最好使用大步小步解这个，但是看了一些博客包括书里面，预处理计算$r_{p,j}$枚举j都是 0 到 p，这是$\mathcal{O}(p)$的

需要注意，如果模数不是一个素数，可能也是可以的，这里关键的是我们需要使用费马小定理去掉底数a的指数上的多余的多项式

另外上面考虑的是对于$a^x\equiv b \pmod p$，其中a恰好是模p的原根，这是最简单的情况，对于一般的情况下我们需要求出a,b用原根g的多少次幂表示（也就是最上面 4.2 说的i,j）。

4.3 Index Calculus for Discrete Logarithms

Index Calculus Method

这个链接里面的 lecture 21 是讲这个算法的。

需要求$a^x\equiv b \pmod p$，假设有一个平滑参数y，$p_1,\cdots,p_k$是小于y的素数，然后选取一个$\alpha\in[0,p-2]$，计算$a^\alpha \pmod p$，将这个结果用素因子表示，如果它能用小于y的素数完全分解，那就乘a^α是$y-smooth$的，如果它不是$y-smooth$的就重新随机一个α。假设$a^{alpha} \pmod p=\prod p_i^{e_i}$

$$\alpha \equiv e_1 \log_a p_1 + \cdots + e_k \log_a p_k \pmod{p-1} \tag{4.34}$$

$\log_a p_1, \cdots, \log_a p_k$都是不知道的，如果得到足够多这种关于$\log_a p_i$的方程（最好的情况就是刚好$k$个），那么就可以解出来$\log_a p_i$。现在随机选择$\beta \in [0, p-2]$，计算$a^\beta b \pmod{p}$的结果，然后用小于$y$的素数分解得到

$$\beta + \log_a b \equiv f_1 log_a p_1 + \cdots + f_k \log_k p_k \pmod{p-1} \tag{4.35}$$

上面的等式里面只有$\log_a b$未知

4.4 The Elliptic Curve Discrete Logarithm Problem

在P的生成群$< P >$上，阶为n，给定$P \Delta D$，求x使得$xP = D$，相当于解$x = \log_P D$

4.4.1 Shanks' Baby-Step Giant-Step Algorithm

大步小步法一般简写$BSGS$，类似与Z_p中的$BSGS$

设

$$x = s\lfloor n \rfloor + d, (0 < d < \lfloor n \rfloor) \tag{4.36}$$

那么$D - dP = s\lfloor n \rfloor P$，其中$d$是小步，$s$是大步，因为它成了一个关于$n$的系数，然后枚举$ds$即可

4.4.2 Silver-Pohlig-Hellman Algorithm

将$xP = D$视作解$x = \log_P D \pmod{n}$的问题即可，点之间加法视作乘法，乘以常数c视作幂，一样的做法

这里有篇文章讲的比较好 Pohlig-Hellman Applied in Elliptic Curve Cryptography

5 解同余方程

5.1 三次方根

$$x^3 \equiv a \pmod{p} \tag{5.37}$$

1. 当$a=0$，解为$x \equiv 0 \pmod{p}$

2. 当$a \neq 0$

   (a) 若$p=2$，a一定等于 1，则解必定为$x \equiv 1 \pmod{2}$

   (b) 若p为奇素数，则$(a,p)=1$，设p的最小原根为g，则存在$t,s \in [0,\varphi(p)-1]$，满足

$$a \equiv g^t \pmod{p} \tag{5.38}$$

$$x \equiv g^s \pmod{p} \tag{5.39}$$

$$\tag{5.40}$$

   所以$3s \equiv t \pmod{\varphi(p)=p-1}$，该同余式未知数是$s$，$t$是求离散对数，有解的充要条件是$(3,p-1) \mid t$，解得$s$即可

举例

$$x^3 \equiv 26 \pmod{41} \tag{5.41}$$

$g=6,\varphi(41)=40,t=17,s=19 \Rightarrow x \equiv 34 \pmod{41}$

$$x^3 \equiv 1 \pmod{7} \tag{5.42}$$

$g=3,\varphi(7)=6,t=0,s=0,2,4 \Rightarrow x \equiv 1,2,4 \pmod{7}$

这个计算方法适用于n次剩余

5.2 平方根

$$x^2 \equiv a \pmod{p} \tag{5.43}$$

https://chenyangwang.gitbook.io/mathematical-base-for-information-safety/er-ci-tong-yu-shi-he-ping-fang-sheng-yu/mo-ping-fang-gen

https://oi-wiki.org/math/number-theory/quad-residue/

link1

link2

5.2.1 模 4k + 3 平方根

如果$p \equiv 3 \mod 4$

$$\begin{aligned}\left(a^{(p+1)/4}\right)^2 &\equiv a^{(p+1)/2} \\ &\equiv x^{p+1} \\ &\equiv x^2 \cdot x^{p-1} \\ &\equiv x^2 \pmod{p}\end{aligned} \tag{5.44}$$

所以$x \equiv a^{(p+1)/4} \pmod{p}$为一个解

5.3 一些例子

求解

$$\begin{aligned}2x^7 &\equiv 5 \pmod{11} \\ \iff \log_2 2 + 7\log_2 x &\equiv \log_2 5 \pmod{10} \\ \iff 1 + 7\log_2 x &\equiv 4 \pmod{10} \\ \iff \log_2 x &\equiv 9 \pmod{10}\end{aligned}$$

注意我们需要先求出$\log_2 2, \log_2 5$的值，模数很小的话可以直接枚举。

6 超几何式

6.1 离散求和

需要求

$$\sum f(k) = g(k) + C \tag{6.45}$$

如果有$\Delta g(k) = f(k) = g(k+1) - g(k)$

那么

$$\sum f(k) = \sum f(k)\delta k = g(k) + C \tag{6.46}$$

问题是如何求g http://yyy.is-programmer.com/posts/205150.html

7 特殊的数

7.1 斯特林数

https://zhuanlan.zhihu.com/p/350774728

8 裴蜀定理

若 $(a,b)=1$，则存在正整数 x,y 使 $ax+by=1$

1. 若 $(a,b)=1$，则 $(a^i,b^j)=1$，对任意 i,j

8.1 一些其他结论

1. $\gcd(a_m,a_n)=a_{\gcd(m,n)}$

9 一些site

1. https://mathmu.github.io/MTCAS/Doc.html （计算机代数）

10 Reference

1. https://www.luogu.com.cn/blog/luogu/latex

2. [Carmichael function[卡迈克尔函数相关性质]](https://blog.csdn.net/AdijeShen/article/details/108476229)

3. http://gotonsb-numbertheory.blogspot.com/2014/06/primitive-roots.html

4. https://chaoli.club/index.php/2756/0（连分数入门）

5. https://crypto.stanford.edu/pbc/notes/contfrac/pell.html（Pell 方程）

6. https://math.uchicago.edu/ may/VIGRE/VIGRE2008/REUPapers/Yang.pdf （Pell 方程和连分数）

7. https://trizenx.blogspot.com/2018/10/continued-fraction-factorization-method.html（CFRAC code）

8. https://bbs.pediy.com/thread-224471.htm（二次筛法）

9. 整数因子分解

Example 2.3.10. Use the ECM method to factor the number $N = 187$.

[1] Choose $B = 3$, and hence $k = \mathrm{lcm}(1, 2, 3) = 6$. Let $P = (0, 5)$ be a point on the elliptic curve $E: \ y^2 = x^3 + x + 25$ which satisfies $\gcd(N, 4a^3 + 27b^2) = \gcd(187, 16879) = 1$ (note that here $a = 1$ and $b = 25$).

[2] Since $k = 6 = 110_2$, we compute $6P = 2(P + 2P)$ in the following way:

[2-1] Compute $2P = P + P = (0, 5) + (0, 5)$:

$$\begin{cases} \lambda = \dfrac{m_1}{m_2} = \dfrac{1}{10} \equiv 131 \pmod{187} \\ x_3 = 144 \pmod{187} \\ y_3 = 18 \pmod{187}. \end{cases}$$

So, $2P = (144, 18)$ with $m_2 = 10$ and $\lambda = 131$.

[2-2] Compute $3P = P + 2P = (0, 5) + (144, 18)$:

$$\begin{cases} \lambda = \dfrac{m_1}{m_2} = \dfrac{13}{144} \equiv 178 \pmod{187} \\ x_3 = 124 \pmod{187} \\ y_3 = 176 \pmod{187}. \end{cases}$$

So, $3P = (124, 176)$ with $m_2 = 144$ and $\lambda = 178$.

[2-3] Compute $6P = 2(3P) = 3P + 3P = (124, 176) + (124, 176)$:

$$\lambda = \frac{m_1}{m_2} = \frac{46129}{352} \equiv \frac{127}{165} \equiv \ \mathcal{O}_E \pmod{187}.$$

This time $m_1 = 127$ and $m_2 = 165$, so the modular inverse for $127/165$ modulo 187 does not exist; but this is exactly what we want! – this type of failure is called a "pretended failure". We now set $z = m_2 = 165$.

[3] Compute $d = \gcd(N, z) = \gcd(187, 165) = 11$. Since $1 < 11 < 187$, 11 is a (prime) factor of 187. In fact, $187 = 11 \cdot 17$.