题1. 连分数分解 1711

取$k=1,N=1711,FB=\{-1,2,3,5\}$，则有

i	P_i	$W=P_i^2-kNQ_i^2$	factorization
0	41	-30	$(-1)\times 2\times 3\times 5$
1	83	45	$3^2\times 5$
2	124	-23	$(-1)\times 23$
3	331	57	3×19
4	455	-6	$(-1)\times 2\times 3$
5	6246	5	5
6	100391	-38	$(-1)\times 2\times 19$
7	207028	9	3^2
8	1756615	-54	$(-1)\times 2\times 3^3$

当$i=8$的时候，$455^2\times 1756615^2\equiv(2\times 3^2)^2 \pmod N$，此时$(\gcd(799259843,N),(799259807,N))=(59,29)$

题2.

对于N，选择大于 2 的整数 A 构造 lucas 序列

$$V_0=2,V_1=A,V_j=AV_{j-1}-V_{j-2} \pmod N \tag{0.1}$$

对于M，M 是$p-\left(\dfrac{A^2-4}{p}\right)$的倍数，那么任意奇素数$p$一定能除尽$\gcd(N,V_M-2)$

我们需要使$\left(\dfrac{A^2-4}{p}\right)=-1$,即$A^2-4$是模$p$情况下的非二次剩余。

为了找到p，我们不断找M使得$\gcd(N,V_M-2)$不等于1或者N，就得到N的非平凡因子，所使用的M是$k!,k=1,2,3\cdots$，我们有

$$V_{k!}(A)=V_k\left(V_{k-1!}(A)\right) \tag{0.2}$$

题3. 二次筛法分解 1046603 和 998771

$n=1046603,\lceil\sqrt{1046603}\rceil=1024$时, factor base 为

$$Q(x)=(x+\lceil\sqrt{n}\rceil)^2-n\equiv(x+\lceil\sqrt{n}\rceil)^2 \pmod n \tag{0.3}$$

$P=50$情况下，找到了小于50的素数且素数p满足N是模p情况下的二次剩余，这样的p如下:

$$\{2,13,17,19,29,37,41,47\}$$

将这些数作为分解基，去对满足$x\in[0,A=500]$的$Q(x)$进行筛选，最后可以得到形式为$p^2\equiv q \pmod N$的同余方程如下

$$\begin{aligned}
&1030^2\equiv 17\times 29^2 \pmod N\\
&1319^2\equiv 2\times 17\times 19\times 29\times 37 \pmod N\\
&1370^2\equiv 13^2\times 17^3 \pmod N\\
&1493^2\equiv 2\times 19\times 29^2\times 37 \pmod N
\end{aligned} \tag{0.4}$$

从而

$$\big(\gcd(1030 \times 1370 \pm 13 \times 17^2 \times 29)\big) = (557, 1879) \tag{0.5}$$

同理$N = 998771$，得到分解基

$$\{2, 5, 7, 11, 17, 19, 37, 43, 47\} \tag{0.6}$$

最终可以得到

$$(\gcd(1040039 \pm 16150, N)) = (1511, 661) \tag{0.7}$$

题4. rho 算法分解

$f(x) = x^2 + 1, x_1 = 1, N = 8051$情况下（题目给了$x_0 = 1$，为了计算方便，将$x_1$置为1）

$$\begin{aligned} gcd(X[1] - X[1], N) &= 1 \\ gcd(X[3] - X[3], N) &= 1 \\ gcd(X[7] - X[6], N) &= 1 \\ gcd(X[7] - X[7], N) &= 1 \\ gcd(X[15] - X[12], N) &= 1 \\ gcd(X[15] - X[13], N) &= 1 \\ gcd(X[15] - X[14], N) &= 1 \\ gcd(X[15] - X[15], N) &= 1 \\ gcd(X[31] - X[24], N) &= 1 \\ gcd(X[31] - X[25], N) &= 83 \end{aligned} \tag{0.8}$$

所以

$$N = 8051 = 83 \times 97 \tag{0.9}$$

$f(x) = x^3 + x + 1, x_0 = 1, N = 2701$情况下（题目给了$x_0 = 1$，为了计算方便，将$x_1$置为1）

$$\begin{aligned} gcd(X[1] - X[1], N) &= 1 \\ gcd(X[3] - X[3], N) &= 1 \\ gcd(X[7] - X[6], N) &= 37 \end{aligned} \tag{0.10}$$

所以我们有

$$N = 2701 = 37 \times 73 \tag{0.11}$$

题4. 椭圆曲线分解$N = 199843247$

当计算到$9624P$时，求斜率时，分母 dominator 模N逆元不存在，可以得到分母$\gcd(dom, N)$一定是N的一个非平凡因子，可以求得这个结果是 19423，从而

$$N = 199843247 = 19423 \times 10289 \tag{0.12}$$

题5. $BSGS$分解求$x \equiv \log_{37} 15 \pmod{123}$

通过$BSGS$求得的两个列表如下

$$\begin{gathered}\{(15,10),(24,8),(27,9),(63,6),(117,7)\}\\ \{(1,110),(10,99),(16,77),(37,121),(100,88)\}\end{gathered} \tag{0.13}$$

对比两个列表发现找不到满足ba^{is}和a^j满足$ba^{is} \equiv a^j \pmod{N}$，所以判断出$37^x \equiv 15 \pmod{123}$无解