Pollard p-1 Algorithm

Fermat's Little Theorem
\[ a^{p-1} \equiv 1 \mod p \]

1. Choose random \( a \).
2. Compute \( N(k) = \text{lcm}(1, \ldots, k) \).
3. Compute \( b = a^{N(k)} \mod N \).
4. Compute \( \gcd(b, N) \).
5. If \( \gcd(b, N) \neq 1 \) or \( N \)
   return \( \gcd(b, N) \).

Facts:
- If \( p-1 \mid N(k) \) then \( p \) has all small factors.
- A "strong prime": \( p-1 \) has some big prime factor \( p = 2q + 1 \).

Computational Notes:
- To compute \( N(k) \):
  1. Use the Eratosthenes sieve to find primes \( p \leq k \).
  2. \( N(k) = \prod p_i^{a_i} \) where \( p_i^{a_i} \leq k \).

To compute \( a^{N(k)} \mod N \):
- Square and multiply.

Elliptic Curve Method

Weierstrass Form
\[ y^2 = x^3 + ax + b \]

Edwards Curve
\[ x^2 + y^2 = 1 + dx^2 y^2 \]

Cycle Group:
\[ 1 = 0 \] "point at infinity"
\[ g = pt \text{ on curve} \]
\[ + : p + g = -r \]
Alphee Curve Method for Factoring
(Lenstra)

1. Choose curve $E$ and point $P$ on $E$.
2. $Q = P \cdot M(k)$
3. Return gcd $(x(Q), N)$

Finds $N$ if order of $P$ in $E(1Fp)$ divides $M(k)$

Hess

Order $\#E(1Fp)$.

$p - 2 \cdot \sqrt{p} < \#E < p + 2 \cdot \sqrt{p}$

In $p-1$ method, only 1 group $\mathbb{Z}/(p - 1)^{\#}$

ECM: Randomly choose new groups with different orders

with $\#E(1Fp)$ is smooth.

Logarithm:

$L_n(x, e) = e^{(\log(n))(\ln x)^x(\ln \ln n^{-2a})}$

Optimize $k$, # times:

$L_p \left( \frac{e}{2}, \frac{2}{1} \right) = e^{\left( \frac{e^{2p}(1-\log p)}{\log \log p} \right)}$

(Depends on prob. $\#E(1Fp)$ is k-smooth.)

Fermat Factorization

Write $N = a^2 - b^2 = (a + b)(a - b)$

$N = uv \Rightarrow N = a^2 - b^2 \Rightarrow a = \frac{1}{2}(uv)$

$b = \frac{1}{2}(u - v)$

1. For $\sqrt{uv} \leq a \leq \frac{N}{b}$
2. If $b = \sqrt{a^2 - N} \in \mathbb{Z}$
   return $a - b$
**Quadratic Sieve**

1. Start at \( \lceil \sqrt{N} \rceil = x \)
2. Sieve \( x^2 - N \)
3. Save decomposition if \( B \)-smooth.
   \[
   \begin{align*}
   x_1^2 - N &= 2e_1 \varepsilon_1 \ldots \varepsilon_1 \ldots = y_1 \\
   x_2^2 - N &= 2e_2 \varepsilon_2 \ldots \varepsilon_2 \ldots = y_2
   \end{align*}
   \]

4. Linear Algebra
   - Try to find \( \Pi y \); a square
     \[
     \Rightarrow \Pi p_i e_i \text{ even}
     \Rightarrow \text{Linear Algebra, over-exponent checks mod 2}
     \Rightarrow \# p \in B \text{ Lindappency } \Rightarrow p \in B \text{ (x,y) pair.}
     \]

5. Compute square root \( b = \sqrt{\Pi y} \)
   \[
   (a = \Pi x_i \mod N)
   \]

6. \( d = \gcd(a-b,N) \)

**Implementation Issues**

Sieving over polynomials:

We're sieving \( f(x) = x^2 - N \)

1. Construct table \( \rightarrow f(1) \)
   \[
   M \rightarrow f(M)
   \]

2. For each prime \( p \in B \):
   - Solve \( f(x) \mod p \).
   - \( p = 2 \): 1 solution
   - \( p = 1 \mod 4 \): 2 solutions
   - \( p = 3 \mod 4 \): 0 solutions

Sieving residue class \( atkp \) for each solution,
\[
(f(a) \equiv 0 \mod p \Rightarrow f(atkp) \equiv 0 \mod p) \quad M \lfloor a \rfloor B \text{ war}
Choosing $B$

$$ \Pr(X \sim B \text{-smooth}) \sim u^{-u} \quad u = \frac{\ln x}{\ln B} $$

**Steps:**
- $\ln \ln B \propto u$
- $3$ values to solve for $B$-smooth $B: u^u$
- $\# \text{primes } \leq B: \frac{B}{\ln B} = \# \text{B-smooth numbers}$ and

Work: $u^u \cdot \frac{B}{\ln B}, \ln \ln B = T(B)$

$$ \ln (T(B)) \propto u \ln u + \ln B $$

$$ = u \ln u + \ln B $$

$$ \ln B = \ln \frac{N}{u} $$

$$ \frac{d \ln (T)}{du} : u \cdot \frac{1}{u} \ln u - \ln \frac{N}{u^2} = 0 $$

$$ u^2 (\ln u + 1) = \ln N $$

$$ 2 \ln u + \ln u = \ln \ln N $$

$$ \ln u \sim \ln \ln \frac{N}{u} $$

$$ \ln u \sim (\ln N)^{1/2} $$

$$ u^u \sim (\ln N)^{1/2} (\ln N)^{1/2} $$

$$ \sim e^{\frac{1}{2} \ln \ln N \cdot \ln \ln N} $$

$$ \frac{B}{\ln B} \sim e^{-\ln N} $$

$$ \ln \ln B = \ln \ln N \sim \ln \ln N $$

**Right Answer:** $L(\frac{1}{2}, 1) = e^{-\ln N \ln \ln N}$