CIS 700 Lecture 17: More Factoring

Pollard P-1 Algorithm

Fermat's Little Theorem

$a^{p-1} \equiv 1 \mod p$

1. Choose random a.
2. Compute $M(k) = \mathrm{lcm}(1, \dots, k)$
3. Compute $b = a^{M(k)} - 1 \mod N$
4. Compute $\gcd(b, N) = g$
5. If $g \neq 1$ or N
   return g

Factors N if $p-1 \mid M(k)$
$\Rightarrow$ $p-1$ has all small factors
"strong primes": $p-1$ has some big prime factor $p = 2q+1$

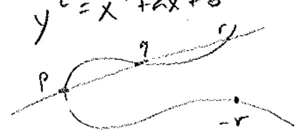
Computational Notes:

To compute $M(k)$:
1. Sieve of Eratosthenes to find primes $p_i < k$
2. $M(k) = \prod p_i^{a_i}$ $\quad p_i^{a_i} < k$

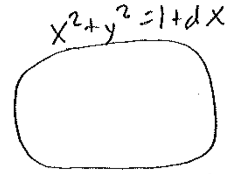
To compute $a^{M(k)} \bmod N$:
square-and-multiply

Elliptic Curve Method

Weierstrass form
$y^2 = x^3 + ax + b$



Edwards Curve
$x^2 + y^2 = 1 + dx^2y^2$



$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$

$\uparrow$
group operation

$E(\mathbb{F}_p) = \{(x, y) \mid x, y \in \mathbb{F}_p, y^2 = x^3 + ax + b\}$

Cyclic group.
$1 = O$ "point at infinity"
g = pt on curve
$+$: $p + q = -r$

Elliptic Curve Method for Factoring

(Lenstra)

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

Factors N if order of P in $E(\mathbb{F}_p)$ divides $M(k)$

Thm (Hasse)

Order $\#E(\mathbb{F}_p)$.

$$p+1-2\sqrt{p} < \#E < p+1+2\sqrt{p}$$

In $p-1$ method, only 1 group $\mathbb{Z}_p^*$ (order $p-1$)

ECM: Randomly choose new groups w/ different orders until $\#E(\mathbb{F}_p)$ is smooth.

L notation:

$$L_n[\alpha, c] = e^{(c+o(1))(\ln n)^{\alpha}(\ln\ln n^{1-\alpha})}$$

Optimize k, # tries:

$$L_p[\tfrac{1}{2}, \sqrt{2}] = e^{(\sqrt{2}+o(1))\sqrt{\ln p \ln\ln p}})$$

(Depends on prob. $\#E(\mathbb{F}_p)$ is k-smooth.)

Fermat Factorization

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

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

1. For $\lceil\sqrt{N}\rceil \le a \le \frac{N+a}{6}$

   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 factorization if B-smooth.

$$\left.\begin{array}{l} x_1^2 - N = 2^{e_{21}} 3^{e_{31}} \cdots = y_1 \\ x_2^2 - N = 2^{e_{22}} 3^{e_{32}} \cdots = y_2 \\ \vdots \end{array}\right\} \text{Relation-Finding}$$

4. Linear Algebra

   Try to find $\prod y_i$ a square

   $\Rightarrow \prod p_i^{e_i}$ e_i even

   $\Rightarrow$ Linear Algebra over exponent vectors mod 2

   $\Rightarrow P_B = \#\text{primes} < B$; Lin. dependency if $> P_B$ (x_i, y_i) pairs.
   $\sim \frac{B}{\ln B}$

5. Compute square root $b = \sqrt{\prod_S y_i}$

   $(a = \prod_S x_i \bmod N)$

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

Computational Issues

Sieving over a Polynomial:

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

1. Construct table $1 \to f(1)$
   $\vdots$
   $M \to f(M)$

2. For each prime $p < B$:

   Solve $f(x) \bmod p$.

   $p = 2$: 1 solution

   $p \equiv 1 \bmod 4$: 2 solutions

   $p \equiv 3 \bmod 4$: 0 solutions

Sieve residue class $a + kp$ for each solution.

$(f(a) \equiv 0 \bmod p \iff f(a+kp) \equiv 0 \bmod p)$ $\quad M \ln\ln B$ work

Choosing B

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

Sieving: $\ln\ln B$ ops per #

$\exists$ values to sieve per B-smooth #: u^u

primes $\leq B$: $\frac{B}{\ln B}$ = # B-smooth numbers to find

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

$\ln(T(B)) \approx u \ln u + \ln B$ $\quad \ln B = \frac{\ln N}{u}$

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

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

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

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

$\ln u \sim \frac{\ln\ln N}{2}$

$u \sim (\ln n)^{\frac{1}{2}}$ $\quad \ln B = (\ln N)^{\frac{1}{2}}$

$B = e^{\sqrt{\ln N}}$

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

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

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

$\ln\ln B = \ln\sqrt{\ln N} \sim \ln\ln N$

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