1 Pollard $p-1$ method

Idea: We know by Fermat that $\forall c \in \mathbb{Z}/p\mathbb{Z} : c^{p-1} \equiv 1 \mod p$ and thus

$$\forall M \in \mathbb{Z} \text{ and } p-1 \mid M : c^M \equiv 1 \mod p \implies p \mid c^M - 1$$

Now if $p \mid n$ then $p \mid \gcd(c^M - 1, n)$.

Algorithm Basic Pollard $p-1$ method

Require: odd number n, search bound B
  [Establish prime-power base]
    Find the sequence of primes $p_1 < p_2 < \cdots < p_m \le B$ and
    for each such prime p_i, the maximum integer a_i s.t. $p_i^{a_i} \le B$
  [Perform power ladders]
    $c = 2$; ▷ Actually, a random c can be tried
    for $(1 \le i \le m)$ **do**
      for $(1 \le j \le a_i)$ **do** $c = c^{p_i} \mod n$;
      end for
    end for
  [Test gcd]
    $g = \gcd(c-1, n)$;
    return g; ▷ We hope for a success $1 < g < n$

Remark.
- We set $M = \mathrm{lcm}(B, B-1, \dots, 1) = \prod_{p_i^{a_i} \le B} p_i^{a_i}$.
- The algorithm is successful if the group order $\#\mathbb{Z}/p\mathbb{Z} = p-1$ is $B-$smooth.
- The algorithm fails if $\gcd(c-1, n) = 1$ or n. Then we can replace $c = 2$ with some other integer and increase or lower the search bound B.

2 Basic ECM

2.1 Pseudocurves

Definition 2.1. Let $a, b \in \mathbb{Z}/n\mathbb{Z}, \gcd(n, 6) = 1$ and $\gcd(4a^3 + 27b^2, n) = 1$. An elliptic pseudocurve (EP) over the ring $\mathbb{Z}/n\mathbb{Z}$ is a set

$$E_{a,b}(\mathbb{Z}/n\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}_n\}$$

where $\mathcal{O}_n$ is the point at infinity and $a, b \in \mathbb{Z}/n\mathbb{Z}$.

Remark.
- If $p \mid n$ then there exists a mapping
$$(-)_p : E(\mathbb{Z}/n\mathbb{Z}) \to E(\mathbb{F}_p)$$
$$P = (x \bmod n, y \bmod n) \mapsto (x \bmod p, y \bmod n) = P_p \text{ and } \mathcal{O}_n \mapsto \mathcal{O}_p$$
We notice that $\ker(-)_p = \mathcal{O}_n$
- If n is composite, $E(\mathbb{Z}/n\mathbb{Z})$ fails to form a group since inverse elements are needed for the slope m giving rise to Lenstra's ECM.

2.2 The algorithm

Algorithm Lenstra elliptic curve method (ECM)

Require: Composite number n
Ensure: $\gcd(n, 6) = 1, n$ not a proper power
  [Choose B_1 limit]
    $B_1 = 1000$ ▷ Or whatever is a practical initial 'stage-one limit' B_1
  [Find curve $E_{a,b}(\mathbb{Z}/n\mathbb{Z})$ and point $(x, y) \in E$]
    Choose random $x, y, a \in [0, n-1]$;
    $b = (y^2 - x^3 - ax) \mod n$;
    $g = \gcd(4a^3 + 27b^2, n)$;
    if $(g == n)$ **then** goto [Find curve ...];
    end if
    if $(g > 1)$ **then** return g;
    end if ▷ Factor is found
    $E = E_{a,b}(\mathbb{Z}/n\mathbb{Z}); P = (x, y)$; ▷ Elliptic pseudocurve and point on it
  [Prime-power multipliers]
    for $(1 \le i \le \pi(B_1))$ **do** ▷ Loop over primes p_i
      Find largest integer a_i such that $p_i^{a_i} \le B_1$;
      for $(1 \le j \le a_i)$ **do**
        $P = [p_i]P$, halting the elliptic algebra if the computation
        of some d^{-1} for addition-slope denominator d signals
        a nontrivial $g = \gcd(n, d)$, in which case return g; ▷ Factor is found
      end for
    end for
  [Failure]
    Possibly increment B_1;
    goto [Find curve ...];

Proposition 2.1. *Let $n \in \mathbb{Z}, p \in \mathbb{P}$ the least prime with $p \mid n$ and $q \in \mathbb{P}$ another prime with $q \mid n$, $P \in E(\mathbb{Z}/n\mathbb{Z})$*

(i) If $\exists k \in \mathbb{Z}$ s.t.
$$[k]P_p = \mathcal{O}_p \text{ on } E(\mathbb{F}_p), \quad [k]P_q \ne \mathcal{O}_q \text{ on } E(\mathbb{F}_q)$$
then $[k]P \notin E(\mathbb{Z}/n\mathbb{Z})$

(ii) If $\#E(\mathbb{F}_p)$ is B_1 powersmooth then ECM finds a $k \in \mathbb{Z}$ s.t. $[k]P_p = \mathcal{O}_p$

Proof. (i) Assume for contradiction that $[k]P \in E(\mathbb{Z}/n\mathbb{Z})$. Then since $\ker((-)_p) = \mathscr{O}_n \implies [k]P = \mathscr{O}_n$, but then $([k]P)_q = (\mathscr{O}_n)_q = \mathscr{O}_q$ a contradiction.

(ii) In the algo we set

$$k = \prod_{p_i^{a_i} \leq B_1} p_i^{a_i}$$

Then if $\#E(\mathbb{F}_p)$ is B_1-powersmooth $\implies \#E(\mathbb{F}_p) \mid k$ and since $\text{ord}(P_p) \mid \#E(\mathbb{F}_p)$ (by Lagrange's theorem) we are finished.

□

2.3 Complexity analysis

Let p be the least prime factor of n. Let

$$\mathscr{S} = \#\{n \in [p+1-\sqrt{2}p, p+1+\sqrt{2}p] \mid n \text{ is } B_1-\text{smooth}\}$$
$$N_2(\mathscr{S}) = \#\{(a, x_0, y_0) \in \mathbb{F}_p^3 \mid b = y_0^2 - x_0^3 - ax_0 : 4a^3 + 27b^2 \neq 0,\ \#E_{a,b}(\mathbb{F}_p) \in \mathscr{S}\}$$

So $N_2(\mathscr{S})$ contains all the triples creating an EC which will give us an successful algorithm. Then from Lenstra's Theorem the probability $prob(B_1)$ of success is given by

$$prob(B_1) = \frac{N_2(\mathscr{S})}{p^3} > c\frac{\mathscr{S}}{\sqrt{p}\ln p}$$

The expected numbers of applying the step [Prime-power multipliers] until we are successful can be modelled by a geometric random variable and thus the expected number of such steps is given by $\frac{1}{prob(B_1)}$ and since it takes about B_1 arithmetic steps to perform [Prime-power multipliers] we get that the expected arithmetic operations until the algorithm is successful is given by

$$\frac{B_1}{prob(B_1)} < C\frac{\sqrt{p}\ln pB_1}{\mathscr{S}}$$

yielding to a complexity estimate $\frac{B_1}{prob(B_1)}$ that is given by

$$\exp\left(\sqrt{2}+o(1)\right)\sqrt{\ln p \ln\ln p}$$

Remark.
- We do not know p to begin with so we start with a low B_1 value of 1000 and then possibly raise this value in Step [Failure]
- the larger the least prime factor of n, the more arithmetic steps are expected
- worst case: n is the product of two roughly equal primes, then the complexity is $L(n)^{1+o(1)}$ the same as QS (quadratic sieve) where $L(n) = \exp\sqrt{\ln n \ln\ln n}$.

3 Elliptic curve primality proving (ECPP)

Theorem 3.1 (Goldwasser-Kilian ECPP theorem)**.** *Let $n \in \mathbb{Z}_{>1}$ and $\gcd(n,6) = 1$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a PC and $s, m \in \mathbb{Z}$ s.t. $s \mid m$. Assume that $\exists P \in E(\mathbb{Z}/n\mathbb{Z})$ s.t.*

(i) $[m]P = \mathscr{O}$

(ii) $\forall q \in \mathbb{P}$ and $q \mid s$ we have $[m/q]P \neq \mathscr{O}$

Then $\forall p \in \mathbb{P}$ and $p \mid n$ we have

$$\#E(\mathbb{F}_p) \equiv 0 \mod s$$

Moveover, if $s > (n^{1/4}+1)^2 \implies n \in \mathbb{P}$.

3.1 Goldwasser-Kilian primality test

Algorithm Goldwasser-Kilian primality test

Require: nonsquare integer $n > 2^{32}$
Ensure: $\gcd(n,6) = 1$

[Choose a pseudocuve over $\mathbb{Z}/p\mathbb{Z}$]
  Choose random $(a,b) \in [0, n-1]^2$ s.t. $\gcd(4a^3 + 27b^2, n) = 1$;
[Assess curve order]
  $m = \#E_{a,b}(\mathbb{Z}/n\mathbb{Z})$ ▷ if n is prime
[Attempt to factor]
  Attempt to factor $m = kq$ s.t. $k > 1$ and $q > (n^{1/4}+1)^2$ a probable prime
  but if this cannot be done according to some time-limit criterion,
  goto [Choose a pseudocurve ...];
[Choose point on $E_{a,b}(\mathbb{Z}/n\mathbb{Z})$]
  Choose random $x \in [0, n-1]$ s.t. $Q = (x^3 + ax + b) \mod n$ and $(\frac{Q}{n}) \neq 1$
  Find an integer y s.t. $y \equiv Q(\mod n)$ if n were prime;
  if $(y^2 \mod n \neq Q))$ **then** return 'n is composite';
  end if
  $P = (x, y)$;
[Operator on point]
  Compute the multiple $U = [m/q]P$ (however if any illegal inversions occur, return 'n is composite');
  if $(U == \mathscr{O})$ **then** goto [Choose point ...];
  end if
  Compute $V = [q]U$ (however check the above rule on illegal inversions);
  if $(V \neq \mathscr{O})$ **then** return 'n is composite';
  end if
  return 'If q is prime, then n is prime';

Remark.
- In practice one repeatedly applies the algorithm to obtain a chain of numbers with the last number q so small its primality may be proved by trial division.
- if some intermediate q is composite, then one can retreat one level in the chain and apply the test again.