Lenstra's Elliptic Curve Factorization Method

Leo Lai

University of Cambridge

Churchill College Compsci Talk Series, 2016

Integer factorization

Problem

Given an integer N, compute its prime factorization.

Integer factorization

Problem

Given an integer N, find a non-trivial proper factor of N.

Integer factorization

Problem

Given an integer N, find a non-trivial proper factor of N.

Current fastest algorithm: the general number field sieve

Run time:

$$O\left(\exp\left((64/9)^{1/3}(\log N)^{1/3}(\log\log N)^{2/3}\right)\right)$$

Special purpose factorization algorithms

Special purpose algorithms: run time depends on structure of N.

Special purpose factorization algorithms

Special purpose algorithms: run time depends on structure of N.

- Trial division: favours small prime factors of N.

Special purpose factorization algorithms

Special purpose algorithms: run time depends on structure of N.

- Trial division: favours small prime factors of N.
- Fermat factorization: suitable for factors close to $\sqrt{N}$.

Special purpose factorization algorithms

Special purpose algorithms: run time depends on structure of N.

- Trial division: favours small prime factors of N.
- Fermat factorization: suitable for factors close to $\sqrt{N}$.
- Special number field sieve: applies to $r^e \pm s$ for small $r,\ s$.

Special purpose factorization algorithms

Special purpose algorithms: run time depends on structure of N.

- Trial division: favours small prime factors of N.
- Fermat factorization: suitable for factors close to $\sqrt{N}$.
- Special number field sieve: applies to $r^e \pm s$ for small r, s.
- Lenstra's elliptic curve method: see later.

Motivational consideration

Theorem

Let p be a prime. If a is coprime to p, then

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

Motivational consideration

Theorem

Let p be a prime. If a is coprime to p, then

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

$$\begin{aligned} p|N \text{ and } p-1|M &\implies p|\gcd(a^M - 1, N)|N \\ &\implies \text{get non-trivial divisor of } N. \end{aligned}$$

Motivational consideration

Theorem

Let p be a prime. If a is coprime to p, then

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

$$\begin{aligned} p|N \text{ and } p-1|M &\implies p|\gcd(a^M - 1, N)|N \\ &\implies \text{get non-trivial divisor of } N. \end{aligned}$$

How do we find M so this is better than trival division?

The $p-1$ algorithm

Try $M = \text{lcm}(1, 2, \cdots, B)$, for some search limit B.

The $p - 1$ algorithm

Try $M = \mathrm{lcm}(1, 2, \cdots, B)$, for some search limit B.

Definition

A number x is *B-smooth* if $q|x \implies q \leq B$.
It is *B-powersmooth* if $q^r|x \implies q^r \leq B$, or equivalently $x|M$.

The $p-1$ algorithm

Try $M = \operatorname{lcm}(1, 2, \cdots, B)$, for some search limit B.

Definition

A number x is *B-smooth* if $q|x \implies q \leq B$.
It is *B-powersmooth* if $q^r|x \implies q^r \leq B$, or equivalently $x|M$.

$p-1$ is B-powersmooth $\implies \gcd(a^M - 1, N)$ non-trivial factor.

The $p-1$ algorithm

Try $M = \text{lcm}(1, 2, \cdots, B)$, for some search limit B.

Definition

A number x is *B-smooth* if $q | x \implies q \leq B$.
It is *B-powersmooth* if $q^r | x \implies q^r \leq B$, or equivalently $x | M$.

$p-1$ is B-powersmooth $\implies$ $\gcd(a^M - 1, N)$ non-trivial factor.

Example

Take $N = 3^{136} + 1$ (with 64 digits), then it has a factor

$$\begin{aligned} p &= 2670091735108484737 \\ &= 2^7 \cdot 3^2 \cdot 7^2 \cdot 17^2 \cdot 19 \cdot 569 \cdot 631 \cdot 23993 + 1 \end{aligned}$$

which can be easily found using this algorithm.

Observations

- $\mathbb{F}_p^\times = \{1, \cdots, p-1\}$ is a *group* under multiplication.
- Operation mod N compatible with operation mod p.
- Reaching identity mod p gives non-trivial divisor of N.
- $a^{\mathrm{lcm}(1,2,\cdots,B)} = 1$ in $\mathbb{F}_p^\times$ for all a, if $p-1$ is powersmooth.

Extension

Theorem (Lagrange)

If G is a group with n elements and $x \in G$, then $x^n = 1$.

Extension

Theorem (Lagrange)

If G is a group with n elements and $x \in G$, then $x^n = 1$.

Corollary

$|G|$ is B-powersmooth $\implies x^{\mathrm{lcm}(1,2,\cdots,B)} = 1$ for all x.

Extension

Theorem (Lagrange)

If G is a group with n elements and $x \in G$, then $x^n = 1$.

Corollary

$|G|$ is B-powersmooth $\implies x^{\text{lcm}(1,2,\cdots,B)} = 1$ for all x.

Seek groups G such that

- Reaching identity gives non-trivial divisor
- $|G|$ is smooth.

Extension

Theorem (Lagrange)

If G is a group with n elements and $x \in G$, then $x^n = 1$.

Corollary

$|G|$ is B-powersmooth $\implies x^{\text{lcm}(1,2,\cdots,B)} = 1$ for all x.

Seek family of groups G such that

- Reaching identity gives non-trivial divisor
- One $|G|$ in the family is smooth.

Elliptic curves

Definition

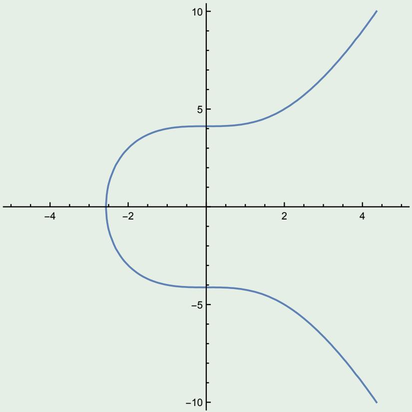
Given two integers a and b such that $4a^3 + 27b^2 \neq 0$, an *elliptic curve* is the set of all solutions to the equation

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

plus an additional point $\mathcal{O}$, thought of as the point at infinity.

Example

The elliptic curve $y^2 = x^3 + 17$ over $\mathbb{R}$

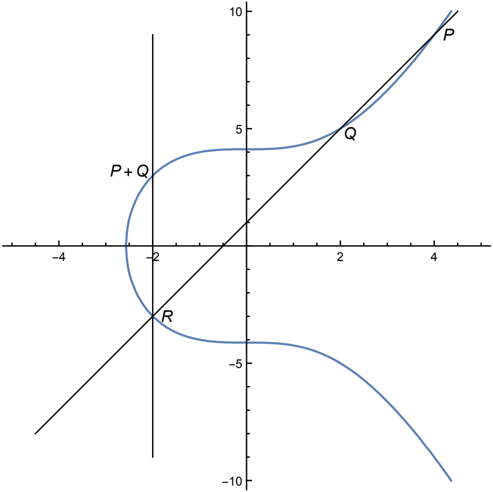


Group law

$P = (4, 9)$, $Q = (2, 5)$.

Line PQ intersects curve at $R = (-2, -3)$.

$P + Q = -R = (-2, 3)$.



Group law

Definition

Given $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on $E : y^2 = x^3 + ax + b$, let

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

then define their *sum* to be $P + Q = (x, y)$, where

$$x = \lambda^2 - x_1 - x_2, \quad y = -y_1 + \lambda(x_1 - x)$$

If $\lambda = \infty$, which occurs when $x_1 = x_2$ and $y_1 = -y_2$, then $P + Q = \mathcal{O}$. Further define $P + \mathcal{O} = \mathcal{O} + P = P$ for all P.

Group law

Theorem

For all P, Q, R on E, the following equations hold:

1. $P + \mathcal{O} = \mathcal{O} + P = P$
2. $P + Q = Q + P$
3. $P + (-P) = \mathcal{O}$, *where* $-(x, y) = (x, -y)$.

Group law

Theorem

For all P, Q, R on E, the following equations hold:

1. $P + \mathcal{O} = \mathcal{O} + P = P$
2. $P + Q = Q + P$
3. $P + (-P) = \mathcal{O}$, *where* $-(x, y) = (x, -y)$.

Proof.

The first three are easy consequences of the definition.

Group law

Theorem

For all P, Q, R *on* E, *the following equations hold:*

1. $P + \mathcal{O} = \mathcal{O} + P = P$
2. $P + Q = Q + P$
3. $P + (-P) = \mathcal{O}$, *where* $-(x, y) = (x, -y)$.
4. $P + (Q + R) = (P + Q) + R$

Proof.

The first three are easy consequences of the definition.

Group law

Theorem

For all P, Q, R on E, the following equations hold:

1. $P + \mathcal{O} = \mathcal{O} + P = P$
2. $P + Q = Q + P$
3. $P + (-P) = \mathcal{O}$, *where* $-(x, y) = (x, -y)$.
4. $P + (Q + R) = (P + Q) + R$

Proof.

The first three are easy consequences of the definition.
The fourth equation follows after a while from the formula for addition defined above. □

Reduction mod p

Everything still works if we work mod p.

Reduction mod p

Everything still works if we work mod p.

Now have group

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

Reduction mod p

Everything still works if we work mod p.

Now have group

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

Question

How many points are there?

Reduction mod p

Everything still works if we work mod p.

Now have group

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

Question

How many points are there?

Heuristically, we expect $p + 1$ points.

Point count

Theorem (Hasse)

Let $|E(\mathbb{F}_p)| = p + 1 - a_p$, *then* $|a_p| < 2\sqrt{p}$.

Point count

Theorem (Hasse)

Let $|E(\mathbb{F}_p)| = p + 1 - a_p$*, then* $|a_p| < 2\sqrt{p}$.

Theorem (Lenstra)

Let S *be a set of* s *integers in the range* $(-\sqrt{p}, \sqrt{p})$*. Let* P *be the probability that the elliptic curve* E *defined by a pair* $(a, b) \in \mathbb{F}_p^2 \backslash \{4a^3 + 27b^2 = 0\}$ *selected uniformly satisfies* $p + 1 - |E(\mathbb{F}_p)| \in S$*, then*

$$c \frac{s-2}{\sqrt{p} \log p} \leq P \leq c' \frac{s}{\sqrt{p}} \log p \log \log p$$

for some absolute constants c *and* c'.

Point count

Theorem (Hasse)

Let $|E(\mathbb{F}_p)| = p + 1 - a_p$*, then* $|a_p| < 2\sqrt{p}$.

Heuristics

For a random elliptic curve, $|E(\mathbb{F}_p)|$ is nearly uniformly distributed in the Hasse range.

Idea

Want to replace multiplication by elliptic curve addition

- $|E(\mathbb{F}_p)|$ is smooth for some E.

Idea

Want to replace multiplication by elliptic curve addition

- $|E(\mathbb{F}_p)|$ is smooth for some E.
- $P + Q = \mathcal{O}$ yields non-trivial divisor.

Idea

Want to replace multiplication by elliptic curve addition

- $|E(\mathbb{F}_p)|$ is smooth for some E.
- $P + Q = \mathcal{O} \implies$ trying to divide by 0 in $\mathbb{F}_p$.

Idea

Want to replace multiplication by elliptic curve addition

- $|E(\mathbb{F}_p)|$ is smooth for some E.
- $P + Q = \mathcal{O} \implies$ trying to divide by 0 in $\mathbb{F}_p$.
  $\implies$ found a non-invertible element mod N.

Idea

Want to replace multiplication by elliptic curve addition

- $|E(\mathbb{F}_p)|$ is smooth for some E.
- $P + Q = \mathcal{O} \implies$ trying to divide by 0 in $\mathbb{F}_p$.
  $\implies$ found a non-invertible element mod N.
  $\implies$ take GCD with N gives non-trivial divisor.

Basic algorithm

0. Select a search limit B.

Basic algorithm

0. Select a search limit B.
1. Choose random elliptic curve $E : y^2 = x^3 + ax + b$ and $P = (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$.

Basic algorithm

0. Select a search limit B.
1. Choose random elliptic curve $E : y^2 = x^3 + ax + b$ and $P = (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$.
2. Try to compute $\operatorname{lcm}(1, 2, \cdots, B)P \pmod{N}$

Basic algorithm

0. Select a search limit B.
1. Choose random elliptic curve $E : y^2 = x^3 + ax + b$ and $P = (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$.
2. Try to compute $\operatorname{lcm}(1, 2, \cdots, B)P \pmod{N}$
    - If successful, go back to step 1.

Basic algorithm

0. Select a search limit B.
1. Choose random elliptic curve $E : y^2 = x^3 + ax + b$ and $P = (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$.
2. Try to compute $\text{lcm}(1, 2, \cdots, B)P \pmod{N}$
   - If successful, go back to step 1.
   - If failed, then we have a non-trivial divisor.

Basic algorithm

0. Select a search limit B.
1. Choose random elliptic curve $E : y^2 = x^3 + ax + b$ and $P = (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$.
2. Try to compute $\text{lcm}(1, 2, \cdots, B)P \pmod N$
   - If successful, go back to step 1.
   - If failed, then we have a non-trivial divisor.
     - If not N, done!

Basic algorithm

0. Select a search limit B.
1. Choose random elliptic curve $E : y^2 = x^3 + ax + b$ and $P = (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$.
2. Try to compute $\operatorname{lcm}(1, 2, \cdots, B)P \pmod{N}$
   - If successful, go back to step 1.
   - If failed, then we have a non-trivial divisor.
     - If not N, done!
     - If we get N, go back to step 1.

Complexity analysis

Let $r_B = \mathbb{P}[|E(\mathbb{F}_p)| \text{ is } B\text{-smooth}]$

Complexity analysis

Let $r_B = \mathbb{P}[|E(\mathbb{F}_p)|$ is B-smooth$]$

- Expect $1/r_B$ curves for factorization.

Complexity analysis

Let $r_B = \mathbb{P}[|E(\mathbb{F}_p)| \text{ is } B\text{-smooth}]$

- Expect $1/r_B$ curves for factorization.
- Each curve takes $O(B \log\log B (\log N)^2)$ operations to check

Complexity analysis

Let $r_B = \mathbb{P}[|E(\mathbb{F}_p)| \text{ is } B\text{-smooth}]$

- Expect $1/r_B$ curves for factorization.
- Each curve takes $O(B \log\log B (\log N)^2)$ operations to check

Now need to minimize

$$\frac{\mathbf{B}}{\mathbf{r_B}}(\log N)^{O(1)}$$

with respect to B.

Estimation of r_B

Theorem (Canfield, Erdös, Pomerance)

Let α be a non-negative real number, then the probability that a random number less than x is $L(x)^{\alpha}$-smooth is $L(x)^{-1/(2\alpha)+o(1)}$, where we define

$$L(x) = \exp(\sqrt{\log x \log \log x})$$

Estimation of r_B

Theorem (Canfield, Erdös, Pomerance)

Let α be a non-negative real number, then the probability that a random number less than x is $L(x)^\alpha$-smooth is $L(x)^{-1/(2\alpha)+o(1)}$, where we define

$$L(x) = \exp(\sqrt{\log x \log \log x})$$

Assumption

If $B = L(p)^\alpha$, then

$$r_B = \mathbb{P}[|E(\mathbb{F}_p)| \text{ is } B\text{-smooth}] = L(p)^{-1/(2\alpha)+o(1)}$$

Choice of B

Take $B = L(p)^{\alpha}$, then

$$\frac{B}{r_B} = L(p)^{\alpha + \frac{1}{2\alpha} + o(1)}$$

Choice of B

Take $B = L(p)^{\alpha}$, then

$$\frac{B}{r_B} = L(p)^{\alpha + \frac{1}{2\alpha} + o(1)}$$

This is optimized at $\alpha = \frac{1}{\sqrt{2}}$.

Choice of B

Take $B = L(p)^\alpha$, then

$$\frac{B}{r_B} = L(p)^{\alpha + \frac{1}{2\alpha} + o(1)}$$

This is optimized at $\alpha = \frac{1}{\sqrt{2}}$.

Final complexity:

$$O\left(\exp\left(\sqrt{(2 + o(1))\log p \log\log p}\right)(\log N)^2\right)$$

Practical considerations

- Choice of elliptic curves:
  - Faster group operations
  - Increases probability of success

Practical considerations

- Choice of elliptic curves:
  - Faster group operations
  - Increases probability of success
- p is not known beforehand: typically specify B first and increase if necessary.

Practical considerations

- Choice of elliptic curves:
  - Faster group operations
  - Increases probability of success
- p is not known beforehand: typically specify B first and increase if necessary.
- Phase two extensions

Practical considerations

- Choice of elliptic curves:
  - Faster group operations
  - Increases probability of success
- p is not known beforehand: typically specify B first and increase if necessary.
- Phase two extensions
- Work over multiple elliptic curves.

Example

The 10th Fermat number F_{10} is

$$2^{2^{10}} + 1 = 45592577 \cdot 6487031809 \cdot c_{291}$$

where c_{291} is a 291 digit composite number.

Example

The 10th Fermat number F_{10} is

$$2^{2^{10}} + 1 = 45592577 \cdot 6487031809 \cdot c_{291}$$

where c_{291} is a 291 digit composite number.

Brent (1999) found a 40 digit prime factor p_{40} of c_{291}.

Example

The 10th Fermat number F_{10} is

$$2^{2^{10}} + 1 = 45592577 \cdot 6487031809 \cdot c_{291}$$

where c_{291} is a 291 digit composite number.

Brent (1999) found a 40 digit prime factor p_{40} of c_{291}.

Curve used: $5y^2 = x^3 + ax^2 + x$, where

$$a = 1597447308290318352284957343172858403618$$

Example

The 10th Fermat number F_{10} is

$$2^{2^{10}} + 1 = 45592577 \cdot 6487031809 \cdot c_{291}$$

where c_{291} is a 291 digit composite number.

Brent (1999) found a 40 digit prime factor p_{40} of c_{291}.

Over $\mathbb{F}_{p_{40}}$, the curve has order

$2^2 \cdot 3^2 \cdot 5 \cdot 149 \cdot 163 \cdot 197 \cdot 7187 \cdot 18311 \cdot 123677 \cdot 226133 \cdot 314263 \cdot 4677853$

Example

The 10th Fermat number F_{10} is

$$2^{2^{10}} + 1 = 45592577 \cdot 6487031809 \cdot c_{291}$$

where c_{291} is a 291 digit composite number.

Brent (1999) found a 40 digit prime factor p_{40} of c_{291}.

Over $\mathbb{F}_{p_{40}}$, the curve has order

$2^2 \cdot 3^2 \cdot 5 \cdot 149 \cdot 163 \cdot 197 \cdot 7187 \cdot 18311 \cdot 123677 \cdot 226133 \cdot 314263 \cdot 4677853$

$p_{40} - 1$ has a 23 digit prime factor

Factorization record

"The purpose of computing is insight, not numbers."

— R. W. Hamming