Integer Factorization and RSA

Maria Eichlseder

Some parts based on slides by Mario Lamberger

Cryptanalysis – ST 2024

SCIENCE
PASSION
TECHNOLOGY

Outline

Introduction to Modern Factoring Algorithms

Factoring with Factor Bases

- Dixon's random squares algorithm
- Quadratic sieve algorithm

Factoring with Continued Fractions

- CFRAC algorithm
- Wiener's attack on RSA

Appendix: Factoring with Elliptic Curves

- Lenstra's ECM algorithm

Introduction to Modern Factoring Algorithms

Motivation: RSA Encryption / Signatures

RSA Key Generation

- Choose 2 large, random primes p, q
- Compute public modulus $n = p \cdot q$
- Choose public exponent e co-prime to $\varphi(n)$
- Compute private exponent $d \equiv e^{-1} \pmod{\varphi(n)}$

public key $= (e, n)$ private key $= (d, n)$

Euler function:
$\varphi(pq) = (p-1)(q-1)$

Euler theorem:
if a, n are coprime, then
$a^{\varphi(n)} \equiv 1 \pmod{n}$

If we can solve the IFP, we can recover p, q from n and thus break RSA:

Integer Factorization Problem (IFP)

Given $n \in \mathbb{N}$, find primes $p_i \in \mathbb{P}$ and $e_i \in \mathbb{N}$ such that $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$.

$\rightarrow$ how large should we choose n for an attack complexity of at least, say, 2^{128}?

Factoring Methods

Fastest general factoring algorithms (take with a grain of salt):

1. General number field sieve
2. Multiple polynomial quadratic sieve
3. Lenstra elliptic curve factorization

You already know two conceptual forerunners of these methods:

- Fermat's difference-of-squares algorithm
- Pollard's $p - 1$ method

Two Ways to Factor n

Difference-of-Squares factorization

Finding p, q : $n = p \cdot q \quad \longleftrightarrow \quad$ finding x, y : $x^2 \equiv y^2 \pmod{n}$

- Century-old idea: Fermat's factoring algorithm ($\rightarrow$ Crypto KU)
- Modern sieving algorithms find x, y much more efficiently
- This lecture: Dixon's random squares, Quadratic sieve, CFRAC

Algebraic Group factorization

Compute in a group $\pmod{n}$ and try to detect identity $\pmod{p}$

- Example: Pollard's $p - 1$ method ($\rightarrow$ Crypto VO)
- This lecture: Lenstra's ECM algorithm

Factoring with Factor Bases

Difference-of-Squares and Factor Bases

The base of modern factoring methods is a century-old idea:

Difference of Squares: $x^2 - y^2 = (x+y)(x-y)$

Find x, y with $x \not\equiv \pm y \pmod{n}$ such that

$$x^2 \equiv y^2 \pmod{n}.$$

Then $(x-y)(x+y) \equiv 0 \pmod{n}$, and if we are lucky,

$$\gcd(x \pm y, n) \in \{p, q\}.$$

Question: How to find such a quadratic congruence?

For random x, it is unlikely that $x^2 \bmod n$ produces a square y^2

Difference-of-Squares and Factor Bases

- **Observation:** When is a number Y a square, i.e., $Y = y^2$?

  Consider the prime factorization $Y = \prod_i p_i^{e_i}$:

  Y is a **square y^2 iff every exponent e_i is even**, and we get $y = \prod_i p_i^{e_i/2}$

- **Idea:** Try many x_i^2 and combine the outputs Y_i to make e_i even:

$$
\begin{aligned}
x_1^2 \quad \bmod n &= Y_1 = 2^3 \cdot 3^2 \cdot 5 \\
x_2^2 \quad \bmod n &= Y_2 = 2 \cdot 5 \\
&\Downarrow \\
(x_1 \cdot x_2)^2 \quad \bmod n &= Y_1 \cdot Y_2 = 2^4 \cdot 3^2 \cdot 5^2 = (2^2 \cdot 3 \cdot 5)^2 = y^2
\end{aligned}
$$

Difference-of-Squares and Factor Bases

- **Obvious problem**: So now we need to factor all Y_i to factor n?
- **Solution:** We use a **factor base** $\mathcal{B} = \{p_1, p_2, \ldots, p_k\}$ containing all prime numbers $\leq B$ (and sometimes -1). We only check if the Y_i can be factored wrt. $\mathcal{B}$.

Definition (B-smooth numbers)

n is **B-smooth** ($\mathcal{B}$-smooth) if every prime factor p of n is $\leq B$ (i.e., $p \in \mathcal{B}$)

Example: $n = 864 = 2^5 \cdot 3^3$ is 3-smooth

Dixon's Random Squares Method

1. Select **factor base** of small prime numbers $\mathcal{B} = \{-1, p_1, p_2, \ldots, p_k\}$
2. Collect **relations** (x_i, Y_i) with $Y_i = x_i^2 \pmod{n}$ and $Y_i = \prod_t p_t^{e_{it}}$
   (select random x_i, test if Y_i is $\mathcal{B}$-smooth)
   (typically $x_i \in [\sqrt{n} - C, \sqrt{n} + C]$, so $Y_i = x_i^2 - n$ is small)
3. **Solve**: select subset of Y_i such that their product is square
   (= all factors p_t occur an even number of times
   $\Rightarrow$ solving a linear equation system $\pmod{2}$: $\mathbf{E} \cdot \mathbf{s} \equiv \mathbf{0}$)
4. $x = \prod x_i$ and $y = \sqrt{\prod Y_i}$
5. Hope that $\gcd(x \pm y, n) \in \{p, q\}$

Factoring with Factor Bases: Example I

Factor $n = 2769$ using factor base $\mathcal{B} = \{2, 3, 5, 7\}$

$x_i = \lfloor \sqrt{n} \rfloor + i$	53	54	55	56	57	58	$\cdots$
$Y_i = x_i^2 - n$	40	147	256	367	480	595	$\cdots$
$\div 2$	2^3		2^8		2^5		
$\div 3$		3			3		
$\div 5$	5				5	5	
$\div 7$		7^2				7	
Rest	1	1	1	367	1	17	$\cdots$

Factoring with Factor Bases: Example II

Factor $n = 2769$ using factor base $\mathcal{B} = \{2, 3, 5, 7\}$

$x_i = \lfloor\sqrt{n}\rfloor + i$	53	54	55	56	57	58	$\cdots$
$Y_i = x_i^2 - n$	40	147	256	367	480	595	$\cdots$
$\div 2$	1	0	0		1		
$\div 3$	0	1	0		1		
$\div 5$	1	0	0		1		
$\div 7$	0	0	0		0		
Rest	✓	✓	✓	✗	✓	✗	$\cdots$

- Solve the linear system (mod 2) $\to \mathbf{s} = (1, 1, 0, 1)$ or $(0, 0, 1, 0)$
- $x = \prod x_i = 53 \cdot 54 \cdot 57 = 163134$
  $y = \sqrt{\prod Y_i} = 2^{(3+5)/2} \cdot 3^{(1+1)/2} \cdot 5^{(1+1)/2} \cdot 7^{2/2} = 1680$
- $\gcd(x + y, n) = \gcd(164814, 2769) = 39$ $\qquad (n = 3 \cdot 13 \cdot 71)$

Quadratic Sieve Method

Observation: If p divides Y, i.e., $x^2 - n \equiv 0 \bmod p$, then $(x+p)^2 - n \equiv 0 \bmod p$.
This is useful to speed up the trial divisions by $\mathcal{B}$ ("**Sieving**"):

1. Select a factor base $\mathcal{B} = \{-1, p_1, p_2, \ldots, p_k\}$.
   For each prime p_j, solve $\alpha_j^2 - n \equiv 0 \pmod{p_j}$ (0 to 2 solutions)
   (if there are 0 solutions, remove p_j from factor base)

2. Set up table of x_i, Y_i for x_i in some interval $[\sqrt{n} - C, \sqrt{n} + C]$.
   For each α_j, divide only Y_i with $x_i = \alpha_j + k \cdot p_j$ for some $k \in \mathbb{N}$ by powers of p_j

3. …(continue from step 3 of Dixon's Random Squares)

Factoring with Continued Fractions

%

And now for something completely different…

You may or may not celebrate π day in a few days (3.14)

But did you know about π approximation day in July: 22/7

$$\frac{22}{7} = 3.1428\ldots$$

is a useful approximation for

$$\pi = 3.1415\ldots$$

Which raises a number of questions:

- How do we approximate irrational numbers?
- Would there be any better π approximation dates to celebrate?
- And what the heck does this have to do with factorization?

Continued fractions to represent real numbers

Definition (Continued fraction expansion)

The continued fraction expansion of $\alpha \in \mathbb{R}$ is

$$\alpha = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}} = [c_0; c_1, c_2, c_3, \ldots]$$

with $c_0 \in \mathbb{Z}$ and $c_i \in \mathbb{N}$ for $i \geq 1$.

The values c_i can be successively computed via:

$$\begin{aligned} c_0 &= \lfloor \alpha \rfloor & \varepsilon_0 &= \alpha - c_0 \\ c_1 &= \lfloor 1/\varepsilon_0 \rfloor & \varepsilon_1 &= 1/\varepsilon_0 - c_1 \\ c_2 &= \lfloor 1/\varepsilon_1 \rfloor & \varepsilon_2 &= 1/\varepsilon_1 - c_2 \\ &\vdots & &\vdots \end{aligned}$$

Continued fractions: Example

Finding the continued fraction expansion of $\alpha = \frac{45}{89}$:

$$c_0 = \lfloor \alpha \rfloor = \left\lfloor \frac{45}{89} \right\rfloor = 0 \qquad \varepsilon_0 = \alpha - c_0 = \frac{45}{89} - 0 = \frac{45}{89}$$

$$c_1 = \left\lfloor \frac{1}{\varepsilon_0} \right\rfloor = \left\lfloor \frac{89}{45} \right\rfloor = 1 \qquad \varepsilon_1 = \frac{1}{\varepsilon_0} - c_1 = \frac{89}{45} - 1 = \frac{44}{45}$$

$$c_2 = \left\lfloor \frac{1}{\varepsilon_1} \right\rfloor = \left\lfloor \frac{45}{44} \right\rfloor = 1 \qquad \varepsilon_2 = \frac{1}{\varepsilon_1} - c_2 = \frac{45}{44} - 1 = \frac{1}{44}$$

$$c_3 = \left\lfloor \frac{1}{\varepsilon_2} \right\rfloor = \left\lfloor \frac{44}{1} \right\rfloor = 44 \qquad \varepsilon_3 = \frac{1}{\varepsilon_2} - c_3 = \frac{44}{1} - 44 = 0$$

$$\Rightarrow \quad \frac{45}{89} = [0; 1, 1, 44] = 0 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{44}}}$$

Continued fractions: Examples for irrational numbers

$$
\begin{aligned}
\varphi &= [1; 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots] \\
\sqrt{2} &= [1; 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, \ldots] \\
\sqrt{19} &= [4; 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, \ldots] \\
e &= [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots] \\
\pi &= [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, \ldots]
\end{aligned}
$$

$$\pi = 3 + \cfrac{1}{7 + \frac{1}{\cdots}} \approx \frac{21 + 1}{7}$$

Continued fractions to approximate real numbers

Definition (n-th convergent)

The n-th convergent of $\alpha = [c_0; c_1, c_2, \ldots] \in \mathbb{R}^+$ is

$$\frac{a_n}{b_n} = [c_0; c_1, c_2, \ldots, c_n]$$

- Convergents can be computed by recursion:

$$\frac{a_0}{b_0} = \frac{c_0}{1}, \quad \frac{a_1}{b_1} = \frac{c_0 c_1 + 1}{c_1}, \quad \ldots, \quad \frac{a_n}{b_n} = \frac{c_n a_{n-1} + a_{n-2}}{c_n b_{n-1} + b_{n-2}}$$

- Convergents are in a sense the “best” approximation of α:

$$\left|\frac{a_n}{b_n} - \alpha\right| < \left|\frac{a}{b} - \alpha\right| \qquad \text{for all } \frac{a}{b} \in \mathbb{Q} \text{ with } \frac{a}{b} \neq \frac{a_n}{b_n} \text{ and } b \leq b_n.$$

Factoring with continued fractions

Remember factoring of n via factor bases:

- Use a factor base $\mathcal{B} = \{-1, p_1, \ldots, p_L\}$
- Collect squares that are $\mathcal{B}$-smooth: $x_k^2 \bmod n = Y_k = \prod_t p_t^{e_{kt}}$
- If Y_k is small, it is more likely to factor over $\mathcal{B}$ successfully!

Continued fraction factoring

Let $\frac{a_k}{b_k}$ be the k-th convergent of $\sqrt{n}$. Consider the square candidates $x_k := a_k$, so $Y_k := a_k^2 \bmod n = a_k^2 - nb_k^2$.

- This choice of x_k asserts that $Y_k = a_k^2 - \sqrt{n}^2 b_k^2 \approx a_k^2 - \frac{a_k^2}{b_k^2} b_k^2 = 0$ is fairly small
- There's an easy algorithm to compute the expansion of $\sqrt{n}$ accurately

Factoring with continued fractions: Example I

Factor $n = 9073$ with the continued fraction method.

- **Compute convergents** for $\sqrt{9073} = 95.2523\ldots$:

$$\frac{a_0}{b_0} = \frac{95}{1}, \quad \frac{a_1}{b_1} = \frac{286}{3}, \quad \frac{a_2}{b_2} = \frac{381}{4}, \quad \frac{a_3}{b_3} = \frac{10192}{107}, \quad \frac{a_4}{b_4} = \frac{20765}{218}$$

- **Smallest absolute residue** Y_i of $a_i^2 \bmod 9073$:

i	0	1	2	3	4	$\cdots$
$x_i = a_i$	95	286	381	10192	20765	$\cdots$
$Y_i = a_i^2 \bmod n$	-48	139	-7	87	-27	$\cdots$

Factoring with continued fractions: Example II

- **Choose factor base** $\mathcal{B} = \{-1, 2, 3, 5, 7\}$
- **Check smoothness** of the Y_i and factorize to get exponents wrt. $\mathcal{B}$:

$$Y_0 = (1, 4, 1, 0, 0), \quad Y_2 = (1, 0, 0, 0, 1), \quad Y_4 = (1, 0, 3, 0, 0).$$

- **Combine** to get squares x and y:

$$y^2 = Y_0 \cdot Y_4 = (-1 \cdot 2^2 \cdot 3^2)^2 = (-36)^2$$
$$x = x_0 \cdot x_4 = 95 \cdot 20765 \equiv 3834 \pmod{9073}$$

  with $(-36)^2 \equiv 3834^2 \pmod{9073}$.

- **Factor** n: $\gcd(3834 + 36, 9073) = 43 \quad \Rightarrow \quad 9073 = 43 \cdot 211$

Wiener's attack on RSA

RSA private key:
primes p, q, exp. d

RSA public key:
mod $N = pq$,
exp. $e \cdot d \equiv 1 \bmod \varphi(N)$

Wiener's attack

- **Goal**: Find private d in RSA with $N = p \cdot q$.
- **Wiener's Theorem**: d appears in convergents of $\frac{e}{N}$ if
  - primes $q < p < 2q$,
  - public exponent $e < \varphi(N)$,
  - small private exponent $d < \frac{1}{3}\sqrt[4]{N}$.

Useful property of continued fractions

Assume $\alpha \in \mathbb{R}$ and $a, b \in \mathbb{Z}$, such that $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$.
Then $\frac{a}{b}$ is a convergent of the continued fraction expansion of α.

Wiener's attack on RSA: Proof of Wiener's theorem

- **Idea**: there exists some $k \in \mathbb{Z}$ with $ed - k\varphi(N) = 1$, so $\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \frac{1}{d\varphi(N)}$; that means, $\frac{e}{\varphi(N)}$ **approximates** $\frac{k}{d}$.

- $\varphi(N)$ is private, but we can **approximate $\varphi(N)$ by N**:
  $|N - \varphi(N)| = |N - (p-1)(q-1)| = |p + q - 1| < 3\sqrt{N}$, so

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \cdots \leq \frac{3k}{d\sqrt{N}} < \frac{1}{2d^2}. \qquad \text{(using } k < d < \tfrac{1}{3}\sqrt[4]{N}\text{)}$$

- The property now says that $\frac{a}{b} = \frac{k}{d}$ **is a convergent of $\alpha = \frac{e}{N}$**.

- **Attack**: Compute continued fraction convergents of $\frac{e}{N}$ and test all candidates d for $(m^e)^d \equiv m \pmod{N}$ with some m.

Wiener's attack on RSA: Example

- Public: $N = 9449868410449$ and $e = 6792605526025$.
  Assume that d satisfies $d < \frac{1}{3}\sqrt[4]{N} \approx 584$.

- Perform Wiener's attack by computing convergents $\frac{a_i}{b_i}$ of $\frac{e}{N}$:

$$\frac{a_0}{b_0} = \frac{1}{1}, \quad \frac{a_1}{b_1} = \frac{2}{3}, \quad \frac{a_2}{b_2} = \frac{3}{4}, \quad \frac{a_3}{b_3} = \frac{5}{7},$$

$$\frac{a_4}{b_4} = \frac{18}{25} \quad \frac{a_5}{b_5} = \frac{23}{32}, \quad \frac{a_6}{b_6} = \frac{409}{569}, \quad \frac{a_7}{b_7} = \frac{1659}{2308}, \ldots$$

- Testing each denominator as possible d reveals $d = 569$.

Runtime comparison

Using **L-Notation**: $L_n[\alpha, c] = \exp\left[(c + o(1))(\ln n)^\alpha (\ln \ln n)^{1-\alpha}\right]$

$0 \leq \alpha \leq 1$: $\alpha = 0$ is **polynomial**; $\alpha = 1$ is **exponential** (wrt. input size $\ln n$)

Dixon's random squares	$L_n[\frac{1}{2}, 2\sqrt{2}]$
CFRAC	$L_n[\frac{1}{2}, \sqrt{2}]$
Lenstra's ECM	$L_p[\frac{1}{2}, \sqrt{2}]$ (p = smallest factor of n)
Quadratic sieve	$L_n[\frac{1}{2}, 1]$
General number field sieve	$L_n[\frac{1}{3}, 1.923]$

Example: 1024-bit RSA n (ca. 80-bit security): $\begin{cases} L_n[\frac{1}{3}, 1.923] \approx 2^{101} \\ L_n[\frac{1}{2}, 1] \approx 2^{122} \end{cases}$

Factoring records

Current records were set using the General Number Field Sieve (GNFS) on numbers from the RSA Factoring Challenge:

- 768-bit RSA using 2000 CPU core years set in 2009
- 795-bit RSA using 900 CPU core years set in 2019
- 829-bit RSA using 2700 CPU core years set in 2020
- See `https://eprint.iacr.org/2020/697`

Conclusion

- Interesting links between algorithms for IFP and DLP (over $\mathbb{Z}_p$)
- For both, the best algorithms are subexponential, but superpolynomial
  - 3072-bit keys needed for 128-bit security

- Two important groups of factoring algorithms:
  - Difference-of-squares factorization using factor bases
    (Dixon's random squares, Quadratic sieve, CFRAC, GNFS)
  - Algebraic group factorization
    (Pollard $p-1$, Lenstra's ECM)

Questions you should be able to answer

1. Explain factoring with factor bases. What is the underlying idea? How are the relations collected in Dixon's Random Square algorithm? How are the relations combined to get a factorization of N?
2. Explain the Quadratic Sieve algorithm. What is the main difference compared to Dixon's algorithm?
3. What is a continued fraction of a number? What is the n-th convergent of a number? How can continued fractions be applied to factoring?
4. Explain the idea of Wiener's attack on RSA.

Appendix: Factoring with Elliptic Curves

Pollard's $p-1$ Method, Revisited

Recall Pollard's $p-1$ method to factor $n = p \cdot q$:

1. Pick $a \in \mathbb{Z}_n^*$ and $k \in \mathbb{N}$, e.g., $k = B!$ for bound B
2. If k is such that $p-1 \mid k$ and $p \nmid a$, then

$$a^k \equiv 1 \pmod{p}.$$

3. Consequently, p divides both n and $a^k - 1$. If

$$d = \gcd(a^k - 1, n) \neq 1, n$$

Success! Else, adapt B (larger if $d = 1$, smaller if $d = n$)

Fermat's theorem:
for $a \in$ group G,

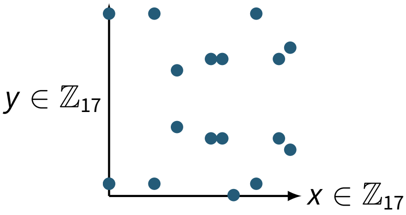
$$a^{|G|} = 1$$

Using different groups

Pollard's $p - 1$ operates in subgroup mod p (of structure mod n).
It only works if group order $|\mathbb{Z}_p^*| = p - 1$ is smooth.

Idea: $\mathbb{Z}_p^*$ isn't the only group we know $\rightarrow$ Elliptic Curve Group!

Modular group $\mathbb{Z}_{17}^*$
(order 16)

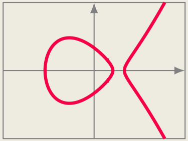


Elliptic curve group $E(\mathbb{Z}_{17})$
$y^2 = x^3 + x + 1$ (order 18)

Elliptic Curve Group

Elliptic curve

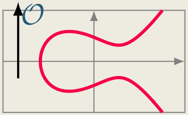
= solutions (x, y) of equation in Weierstrass Form



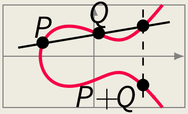
$$y^2 = x^3 + ax + b$$

where $\Delta = -16(4a^3 + 27b^2) \neq 0.$

Elliptic Curve Group



Neutral element $\mathcal{O}$: Special point "$(0, \infty)$"



Addition $P + Q$: Chord rule

How many points are in an EC group?

Order of the group E

The number of points (x, y) on E (incl. $\mathcal{O}$) is its order $|E|$.

Hasse's Theorem

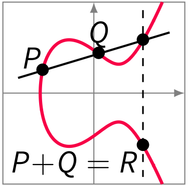
The order of $E(\mathbb{Z}_p)$ is $|E| = p + 1 - t$ for some $|t| \leq 2\sqrt{p}$.

In other words: $|E(\mathbb{Z}_p)| \approx |\mathbb{Z}_p^*|$, but exact value depends on curve!

By trying different curve equations, we get different orders!

This gives us many "candidate orders" that might be smooth.

Addition in $E(\mathbb{Z}_p)$



Points $P = \begin{pmatrix} x_P \\ y_P \end{pmatrix}, \quad Q = \begin{pmatrix} x_Q \\ y_Q \end{pmatrix}, \quad R = \begin{pmatrix} x_R \\ y_R \end{pmatrix}$

$$P + Q = \begin{cases} Q & \text{if } P = \mathcal{O} \\ P & \text{if } Q = \mathcal{O} \\ \mathcal{O} & \text{if } P = -Q \ (x_P = x_Q, y_P = -y_Q) \\ \begin{pmatrix} \left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P \\ \left(\frac{3x_P^2+a}{2y_P}\right)(x_P - x_R) - y_P \end{pmatrix} & \text{if } P = Q \ (x_P = x_Q, y_P = Y_Q) \\ \begin{pmatrix} \left(\frac{y_Q-y_P}{x_Q-x_P}\right)^2 - x_P - x_Q \\ \left(\frac{y_Q-y_P}{x_Q-x_P}\right)(x_P - x_R) - y_P \end{pmatrix} & \text{else} \end{cases}$$

Addition involves computing inverses $\frac{u}{v} \pmod{p}$ (=Euclid)!

Addition in $E(\mathbb{Z}_n)$, $n = p \cdot q$

Idea: Simply perform the same computations $\bmod n$ (if possible).

What can go wrong when computing $\frac{u}{v} \pmod{n}$?

- If $\gcd(v, n) = 1$: everything ok
- If $\gcd(v, n) = n$ (and $\gcd(u, n) = 1$): Means $P = -Q$, result $\mathcal{O}$
- If $\gcd(v, n) \neq n, 1$: Addition failed, but…

We've found a factor of n!

Lenstra's Elliptic Curve Method for Factorization

Repeat until successful:

1. Pick random curve $E(\mathbb{Z}_n) : y^2 = x^3 + ax + b$, point $P = (x_0, y_0)$
   Hint: First pick $x_0, y_0, a \in \mathbb{Z}_n$, compute $b = y_0^2 - x_0^3 - ax_0 \pmod{n}$
2. Pick number k with many small prime factors, e.g., $k = B!$
3. Compute $k \cdot P = P + P + \ldots + P$
   Hint: Step by step: $2P$, then $3(2P)$, then $4(3!P)$, …
   - If all computations successful…bad luck, next curve
   - If intermediate result $\mathcal{O}$…bad luck, next curve
   - If addition fails with $\gcd(v, n) = p \neq n, 1$: Success!

Bibliography

[Dix81] John D. Dixon. **Asymptotically Fast Factorization of Integers.** Mathematics of Computation 36.153 (1981), pp. 255–260. DOI: 10.2307/2007743.

[Len87] H. W. Lenstra. **Factoring Integers with Elliptic Curves.** Annals of Mathematics 126.3 (1987), pp. 649–673. ISSN: 0003486X. DOI: 10.2307/1971363.

[MB75] Michael A. Morrison and John Brillhart. **A Method of Factoring and the Factorization of F_7.** Mathematics of Computation 29.129 (1975), pp. 183–205. DOI: 10.2307/2005475.

[Pom84] Carl Pomerance. **The Quadratic Sieve Factoring Algorithm.** EUROCRYPT. Vol. 209. LNCS. Springer, 1984, pp. 169–182. DOI: 10.1007/3-540-39757-4_17.

[Wie90] Michael J. Wiener. **Cryptanalysis of short RSA secret exponents.** IEEE Transactions on Information Theory 36.3 (1990), pp. 553–558. DOI: 10.1109/18.54902.