Factoring and Continued Fractions

Maria Eichlseder **Florian Mendel**

Applied Cryptography 2 – ST 2016

Parts based on slides by Mario Lamberger

Outline

1. Preliminaries
   - Connections between RSA and Factoring
   - Pollard's $p - 1$ Method
   - Dixon's Random Squares Method

2. Factoring with Continued Fractions
   - Continued Fractions
   - CFRAC factoring
   - Wiener's attack on RSA

3. Factoring with Elliptic Curves
   - Elliptic Curve Group
   - Lenstra's ECM

Outline

1. Preliminaries
   - Connections between RSA and Factoring
   - Pollard's $p-1$ Method
   - Dixon's Random Squares Method
2. Factoring with Continued Fractions
   - Continued Fractions
   - CFRAC factoring
   - Wiener's attack on RSA
3. Factoring with Elliptic Curves
   - Elliptic Curve Group
   - Lenstra's ECM

RSA and Factoring I

Integer Factorization Problem (IFP)

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

- IFP is believed to be intractable (no proof).
- If we can solve IFP, we can break RSA.

RSA Problem (RSAP)

Given modulus $n = p \cdot q$ with $p, q \in \mathbb{P}$, exponent $e \in \mathbb{N}$ with $\gcd(e, (p-1)(q-1)) = 1$, and ciphertext $c \in \mathbb{Z}$, find $m \in \mathbb{Z}$ such that $m^e \equiv c \pmod{n}$ (“the e-th root of $c \pmod{n}$”).

- RSAP is believed to be intractable (no proof).
- RSAP is believed to be computationally equivalent to IFP.

RSA and Factoring II

Theorem

Finding $\varphi(n)$ is equivalent to factoring $n = p \cdot q$.

Proof:

- $\Leftarrow$ If we know $n = p \cdot q$ then $\varphi(n) = (p-1)(q-1)$.
- $\Rightarrow$ If we know $\varphi(n)$ and n, then we can compute p and q:
  Set $q = n/p$ and substitute this in the formula for $\varphi(n)$.
  Then, we get a quadratic equation:

$$p^2 - (n + 1 - \varphi(n))p + n = 0.$$

Solving this equation gives p and thus also q.

RSA and Factoring III

Theorem

Finding $d = e^{-1} \bmod \varphi(n)$ is equivalent to factoring $n = p \cdot q$.

Proof $\Rightarrow$:

- Choose a random value x. Fermat: $x^{\varphi(n)} \equiv 1 \pmod{n}$.
- Since $\varphi(n) | ed - 1$, we also get $x^{ed-1} \equiv 1 \pmod{n}$.
- The exponent is an even number, write $ed - 1 = 2^s \cdot k$.
- Compute $y_1 = \sqrt{x^{ed-1}} = x^{(ed-1)/2}$, so ${y_1}^2 - 1 \equiv 0 \pmod{n}$:
  - If $y_1 \not\equiv \pm 1 \pmod{n}$, factor n by computing $\gcd(y_1 - 1, n)$.
  - If $y_1 = -1$, we have to choose another x.
  - If $y_1 = 1$, we can compute another root: $y_2 = \sqrt{y_1} = x^{(ed-1)/4}$.
- Repeat until a factor is found.

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 the conceptual forerunners of these methods:

- Dixon's random squares method
- Pollard's $p - 1$ method

Pollard's $p - 1$ Method

B-Smooth Numbers

n is B-(power-)smooth if every prime factor p^e of n is $\leq B$.

Example: The number $n = 2^5 \cdot 3^3$ is 33-power-smooth.

Pollard's $p - 1$ Method to factor $n = p \cdot q$

- Suppose that we have guessed a number B such that $p - 1$ is B-power-smooth (but $q - 1$ is not)
- Then, $p - 1$ divides $k = B!$ (but $q - 1$ does not)
- Pick some a. Fermat: $a^k \equiv 1 \pmod{p}$.
- Since $p \mid n$ and $p \mid a^k - 1 \to p \mid \gcd(a^k - 1, n)$.
- If $\gcd(a^k - 1, n) \neq 1, n$: Success!

But: for large prime p, the probability that $p - 1$ is B-smooth is too small.

Dixon's Random Squares Method

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

Difference of Squares

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

Question: How to find such a quadratic congruence?

Random Squares Method:

1. Select factor base $\mathcal{B} = \{p_1, p_2, \ldots, p_k\}$
2. Collect relations (a_i, b_i) with $a_i^2 = b_i \pmod{n}$ and $b_i = \prod_t p_t^{e_{it}}$
   (select random a_i, test if b_i is smooth wrt. $\mathcal{B}$)
3. Solve: select subset of b_i's such that their product is square
   (all factors p_t occur an even number of times)
4. $x = \prod a_i$ and $y = \sqrt{\prod b_i}$

Outline

1. Preliminaries
   - Connections between RSA and Factoring
   - Pollard's $p - 1$ Method
   - Dixon's Random Squares Method

2. Factoring with Continued Fractions
   - Continued Fractions
   - CFRAC factoring
   - Wiener's attack on RSA

3. Factoring with Elliptic Curves
   - Elliptic Curve Group
   - Lenstra's ECM

Continued fractions to represent real numbers

Definition: Continued fraction expansion

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

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} = [a_0; a_1, a_2, a_3, \ldots].$$

- The values a_i can be successively computed via:

$$\begin{aligned} a_0 &= \lfloor \alpha \rfloor & \varepsilon_0 &= \alpha - a_0 \\ a_1 &= \lfloor 1/\varepsilon_0 \rfloor & \varepsilon_1 &= 1/\varepsilon_0 - a_1 \\ a_2 &= \lfloor 1/\varepsilon_1 \rfloor & \varepsilon_2 &= 1/\varepsilon_1 - a_2 \\ &\vdots & &\vdots \end{aligned}$$

- If $\alpha \in \mathbb{Q}$, the a_i can also be obtained via Euclid's Algorithm.

Continued fractions: Example I

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

Solution 1

$$
\begin{aligned}
a_0 &= \lfloor \alpha \rfloor = \left\lfloor \tfrac{45}{89} \right\rfloor = 0 & \varepsilon_0 &= \alpha - a_0 = \tfrac{45}{89} - 0 = \tfrac{45}{89} \\
a_1 &= \left\lfloor \tfrac{1}{\varepsilon_0} \right\rfloor = \left\lfloor \tfrac{89}{45} \right\rfloor = 1 & \varepsilon_1 &= \tfrac{1}{\varepsilon_0} - a_1 = \tfrac{89}{45} - 1 = \tfrac{44}{45} \\
a_2 &= \left\lfloor \tfrac{1}{\varepsilon_1} \right\rfloor = \left\lfloor \tfrac{45}{44} \right\rfloor = 1 & \varepsilon_2 &= \tfrac{1}{\varepsilon_1} - a_2 = \tfrac{45}{44} - 1 = \tfrac{1}{44} \\
a_3 &= \left\lfloor \tfrac{1}{\varepsilon_2} \right\rfloor = \left\lfloor \tfrac{44}{1} \right\rfloor = 44 & \varepsilon_3 &= \tfrac{1}{\varepsilon_2} - a_3 = \tfrac{44}{1} - 44 = 0
\end{aligned}
$$

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

Continued fractions: Example II

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

Solution 2 (Euclid's Algorithm)

Apply Euclid's Algorithm to 45, 89 to get the a_i:

$$
\begin{aligned}
45 &= 89 \cdot 0 + 45 && \Rightarrow \quad a_0 = 0 \\
89 &= 45 \cdot 1 + 44 && \Rightarrow \quad a_1 = 1 \\
45 &= 44 \cdot 1 + 1 && \Rightarrow \quad a_2 = 1 \\
44 &= 1 \cdot 44 + 0 && \Rightarrow \quad a_3 = 44
\end{aligned}
$$

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

Continued fractions: Example III

More examples for irrational numbers:

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

Continued fractions to approximate real numbers

Definition: n-th convergent

The *n-th convergent* of $\alpha = [a_0; a_1, a_2, \ldots] \in \mathbb{R}^+$ is

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n]$$

- Convergents can be computed by recursion:

$$\frac{p_0}{q_0} = \frac{a_0}{1}, \quad \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}, \quad \ldots, \quad \frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}$$

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

$$\left|\frac{p_n}{q_n} - \alpha\right| < \left|\frac{p}{q} - \alpha\right| \qquad \text{for all } \tfrac{p}{q} \in \mathbb{Q} \text{ with } \tfrac{p}{q} \neq \tfrac{p_n}{q_n} \text{ and } q \leq q_n.$$

Factoring with continued fractions I

Remember factoring of n via factor bases:

- Goal: Find x, y such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y$.
  Then, $\gcd(x+y, n)$ is a nontrivial divisor of n.
- Use a factor base $\mathcal{B} = -1 \cup \{r_1, \ldots, r_L\}$
- Collect squares that are $\mathcal{B}$-smooth: $a_k^2 \pmod{n} = b_k = \prod_t p_t^{e_{kt}}$
- Use linear algebra to find x and y.

Continued fraction factoring

Consider the square candidates $p_k^2 - nq_k^2 \equiv p_k^2 \pmod{n} \equiv b_k$,
where $\frac{p_k}{q_k}$ is the k-th convergent of $\sqrt{n}$.

Factoring with continued fractions II

This choice is motivated by…

Fact 1

Let p_ℓ/q_ℓ be the convergents of $\alpha \in \mathbb{R}^+$. Then for all ℓ:

$$\left|p_\ell^2 - \alpha^2 q_\ell^2\right| < 2\alpha.$$

…which implies …

Fact 2

If $n \in \mathbb{N}$ is not a square ($\sqrt{n} \notin \mathbb{N}$), and $\sqrt{n}$ has convergents $\frac{p_\ell}{q_\ell}$, then the smallest absolute residue of $(\pm)p_\ell^2 \pmod{n}$ is $< 2\sqrt{n}$.

…which ensures that the candidates b_k are fairly small!

Factoring with continued fractions: Example I

Task

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

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

$$\frac{p_0}{q_0} = \frac{95}{1}, \quad \frac{p_1}{q_1} = \frac{286}{3}, \quad \frac{p_2}{q_2} = \frac{381}{4}, \quad \frac{p_3}{q_3} = \frac{10192}{107}, \quad \frac{p_4}{q_4} = \frac{20765}{218}$$

- Smallest absolute residue b_i of $p_i^2 \bmod 9073$:

$$b_0 = -48,\ b_1 = 139,\ b_2 = -7,\ b_3 = 87,\ b_4 = -27$$

Factoring with continued fractions: Example II

- Choose factor base $\mathcal{B} = \{-1, 2, 3, 5, 7\}$
- Check smoothness of the b_i and factorize:

$$b_0 = (1, 4, 1, 0, 0), \quad b_2 = (1, 0, 0, 0, 1), \quad b_4 = (1, 0, 3, 0, 0).$$

- Combine to get squares x and y:

$$x = b_0 \cdot b_4 = -1 \cdot 2^2 \cdot 3^2 = -36$$
$$y = p_0 \cdot p_4 = 95 \cdot 20765 \equiv 3834 \pmod{9073}$$

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 Reminder:

- Private exponent d and primes p, q,
- Public exponent e, modulus $N = pq$, with $ed \equiv 1 \bmod \varphi(N)$.

Wiener's attack

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

Then, d can be recovered by trying convergent candidates.

Wiener's attack on RSA: Wiener's theorem

Wiener's theorem

Let $N = pq$ with $q < p < 2q$ and $d < \frac{1}{3}\sqrt[4]{N}$.
Given N and e with $ed \equiv 1 \bmod \varphi(N)$, d can be found efficiently.

Based on the following property of continued fractions:

Fact 3

Let $\alpha \in \mathbb{R}$ 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 I

- 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 $\frac{k}{d}$.

- $\varphi(N) = (p-1)(q-1) = N - q - p + 1$ is private, but $|N - \varphi(N)| = |p + q - 1| < 3\sqrt{N}$ (from p and q's property).

- We use N instead of $\varphi(N)$ and estimate

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - kN}{dN}\right| = \left|\frac{ed - k\varphi(N) - kN + k\varphi(N)}{dN}\right| = \left|\frac{1 - k(N - \varphi(N))}{dN}\right| \leq \frac{3k}{d\sqrt{N}}$$

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

- From $ed - k\varphi(N) = 1$ and $e < \varphi(N)$, we know $k < d$.
- With $d < \frac{1}{3}\sqrt[4]{N}$, we get

$$\left|\frac{e}{N} - \frac{k}{d}\right| \leq \frac{3k}{d\sqrt{N}} < \frac{3}{\sqrt{N}} < \frac{3}{9d^2} < \frac{1}{2d^2}.$$

- Fact 3 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 the convergents of $\frac{e}{N}$:

$$\frac{p_0}{q_0} = \frac{1}{1}, \quad \frac{p_1}{q_1} = \frac{2}{3}, \quad \frac{p_2}{q_2} = \frac{3}{4}, \quad \frac{p_3}{q_3} = \frac{5}{7},$$
$$\frac{p_4}{q_4} = \frac{18}{25} \quad \frac{p_5}{q_5} = \frac{23}{32}, \quad \frac{p_6}{q_6} = \frac{409}{569}, \quad \frac{p_7}{q_7} = \frac{1659}{2308}, \ldots$$

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

Outline

Pollard's $p-1$ Method, Revisited

Recall Fermat's theorem for element a of group G:

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

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

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

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

- To detect this, compute

$$p = \gcd(a^k - 1, n).$$

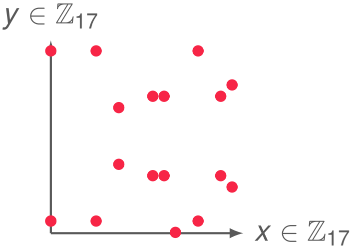
Using different groups

Pollard's $p-1$ operates in subgroup mod p (of structure mod n).

It only works if group order $\left|\mathbb{Z}_p^*\right| = p-1$ is smooth.

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

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

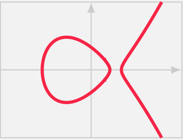


Elliptic curve group $E(\mathbb{Z}_{17})$
$y^2 = x^3 + x + 1$ (order 18)

Elliptic Curve Group

Elliptic curve

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

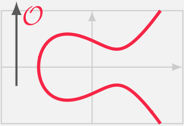


$$y^2 = x^3 + ax + b$$

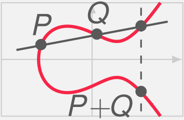
where $\Delta = -16(4a^3 + 27b^2) \neq 0$.

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 $|t| \leq 2\sqrt{p}$.

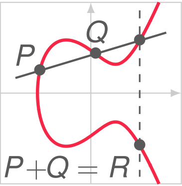
In other words: $|E(\mathbb{Z}_p)| \approx \left|\mathbb{Z}_p^*\right|$, but exact value depends on curve!

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



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

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 mod 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!