Lesson 11
Finding the factors of a product of two primes

Can the reader say what two numbers multiplied together will produce the number

8 616 460 799?

I think it is unlikely that anyone but myself will ever know.

William S. Jevons, *The Principles of Science*, 1877

UNIT 1
Trial Division

RSA numbers

Large numbers with exactly two prime factors

https://en.wikipedia.org/wiki/RSA_numbers

number of bits

PROBLEM (RSA-2048) **About 616 decimal digits**

RSA-2048 = 25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357

Find the two factors. Not been factored so far…

Trial Division

PROPOSITION (Trial division)

If $N \geq 2$ is not prime then it has a nontrivial divisor $d \leq \sqrt{N}$.

Proof. **Assume $N = ab$ with $1 < a, b < N$. If $a, b > \sqrt{N}$ then**

$N = ab > \sqrt{N}\sqrt{N} = N$, a contradiction. $\square$

TRIAL DIVISION ALGORITHM **EXPONENTIAL ALGORITHM**

Start dividing N by 2, 3,...up to $[\sqrt{N}]$. If none divide N, it is prime.

EXAMPLE **Jevon's number $J = 8616460799$. $\sqrt{J} \approx 42\,559$.**

If on gets rid of the primes $\leq \sqrt{J}$ it's still 10 000 trials

Trial Division

EXAMPLE

N with 100 digits is the product of two 50 digits numbers. About 10^{50} steps.

On May 30, 2022, the Frontier supercomputer at Oak Ridge National Laboratory earned the top ranking as the world's fastest on the 59th TOP500 list, with 1.1 exaflops of performance. The system is the first to achieve the level of computing performance known as exascale, a threshold of a quintillion calculations per second.

1 quintillion $/s = 10^{18}/s$

It would take 10^{32} seconds $\approx 3 \times 10^{24}$ years.

UNIT 2
Factorization via difference of squares

Factorization via difference of squares

The most powerful factorization methods rely on the identity

$$x^2 - y^2 = (x - y)(x + y)$$

REMARK **Let $N \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $b^2 - N = a^2$.**

Then $N = (b - a)(b + a)$.

EXAMPLE $N = 25217.$

Fermat method

$\sqrt{N} = 158.79...$ $[\sqrt{N}] = 158.$ **We look at $c(b) := b^2 - N, b = [\sqrt{N}] + 1, ...$**

- $b = 158 + 1 = 159$**:**

$$c(159) = 159^2 - N = 159^2 - 25217 = 64 = 8^2.$$

$$N = 159^2 - 8^2 = (159 - 8)(159 + 8) = 167 \cdot 151.$$

Factorization via difference of squares

EXAMPLE $N = 2491.$

Find $b > [\sqrt{N}]$ such that $c(b) := b^2 - N$ is a square. Factorize N.

REMARK **With big numbers the method might take as long as the trial division...**

Factorization via difference of squares

BASIC FACTORIZATION PRINCIPLE (Fermat method)

Let $N \geq 1$ and $a, b \in \mathbb{N}$ be such that $a^2 \equiv b^2[N]$, $a \not\equiv \pm b[N]$.

Then $\gcd(a \pm b, N)$ are nontrivial factors of N, i.e., $1 < \gcd(a \pm b, N) < N$.

Proof. $a^2 - b^2 \equiv 0[N] \Rightarrow (a-b)(a+b) \equiv 0[N]$

$$\begin{cases} a - b \not\equiv 0[N] \\ a + b \not\equiv 0[N] \end{cases} : \text{the conclusion follows from the Lemma. } \square$$

LEMMA Let $\alpha, \beta \in \mathbb{Z}$ with $\alpha\beta \equiv 0[N]$, $\begin{cases} \alpha \not\equiv 0[N], \\ \beta \not\equiv 0[N]. \end{cases}$ Then $\begin{cases} 1 < \gcd(\alpha, N) < N \\ \gcd(\alpha, N) \mid N. \end{cases}$

Proof.

Factorization via difference of squares

EXAMPLE $43^2 \equiv 1^2[77] : 43^2 - 1^2 = 24 \cdot 77, \;\; 43 \not\equiv \pm 1[77]$

Then $\gcd(43+1, 77) = 11$, $\gcd(43-1, 77) = 7$ are nontrivial factors of 77.

EXAMPLE

$N = 203299. \;\; 781^2 - 8^2 = 609897 = 3 \cdot 203299 \equiv 0[N].$

Find a prime factor of N.

Factorization via difference of squares

REMARK In order to find a, b: $a^2 \equiv b^2 [N]$ it is enough to find

a, b, k: $c(k, b) := b^2 + kN$ is a square.

EXAMPLE $N = 143041$. Fix $k = 247$, start with $b = 1$.

$$247 \cdot 143041 + 1^2 = 35331128 \qquad \text{not a square}$$

$$247 \cdot 143041 + 2^2 = 35331131 \qquad \text{not a square}$$

$$247 \cdot 143041 + 3^2 = 35331136 = 5944^2 \qquad ** \text{ square } **$$

Factorization via difference of squares

EQUIVALENCE TO FACTORIZATION

REMARK When $N = pq$ with p, q primes, finding a, b such that $a^2 \equiv b^2[N]$ and $a \not\equiv \pm b[N]$ is equivalent to factoring N.

Indeed, assume $N = pq$ with p, q primes. Then

$$N = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Assume $p \geq q$. $\quad a := \frac{p+q}{2}, \quad b := \frac{p-q}{2}. \quad N = a^2 - b^2 \Rightarrow a^2 \equiv b^2[N].$

If $a \equiv b[N]$ then $\frac{p+q}{2} \equiv \frac{p-q}{2}[N] \Leftrightarrow p \equiv 0[N] \Leftrightarrow N \mid p$, a contradiction.

Similarly $a \not\equiv b[N]$.

UNIT 3
Fermat-Kraitchik algorithm

Fermat-Kraitchik algorithm

Produce $a, b : b^2 \equiv a^2 [N]$.

Step 1. **Find $c \equiv a^2 [N]$ with:**

no need that c is. a square

- **$a \in \mathbb{N}$,**
- **c product of small primes**

Enough that $c = c(a) := a^2 - N$ for $a > [\sqrt{N}]$.

EXAMPLE $N = 2041$ $\sqrt{N} = 45.177\ldots$: **start with $a = 46$.**

$$c(46) = 75 = 3 \cdot 5^2$$
$$c(47) = 168 = 2^3 \cdot 3 \cdot 7$$
$$c(48) = 263 = 263$$
$$c(49) = 360 = 2^3 \cdot 3^2 \cdot 5$$

Remark: the first suitable a such that $c(a)$ is a square is $a = 85$.

Fermat-Kraitchik algorithm

Produce $a, b : b^2 \equiv a^2 [N]$.

Fermat-Kraitchik algorithm

1. **Find many integers $a_1, \ldots, a_r$: $c_i :\equiv a_i^2 [N]$ factors as a product of small primes.**

2. **Take a product $\Pi_{j \in J} c_j$, $J \subseteq \{1, \ldots, r\}$: every prime appears to an even power.**

   Then $\Pi_{j \in J} c_j = b^2$ for some $b \in \mathbb{N}$.

3. **Let $a := \Pi_{j \in J} a_j$. Then $a^2 \equiv \Pi_{j \in J} c_j \equiv b^2 [N]$.**

Fermat-Kraitchik algorithm

EXAMPLE $N = 52907$

$$399^2 \equiv 480[52907], \qquad 480 = 2^5 \cdot 3 \cdot 5,$$

$$763^2 \equiv 192[52907], \qquad 192 = 2^6 \cdot 3,$$

$$773^2 \equiv 15552[52907], \qquad 15552 = 2^6 \cdot 3^5,$$

$$976^2 \equiv 250[52907], \qquad 250 = 2 \cdot 5^3.$$

Fermat-Kraitchik algorithm

EXAMPLE $N = 2041$

Fermat-Kraitchick algorithm.

$$c(x) := x^2 - N,\ x \geq 46.$$

x	$c(x) \equiv x^2[N]$	factorization	marked
46	75	$3 \cdot 5^2$	
47	168	$2^3 \cdot 3 \cdot 7$	
48	263	263	
49	360	$2^3 \cdot 3^2 \cdot 5$	
50	459	$3^3 \cdot 17$	
51	560	$2^4 \cdot 5 \cdot 7$	

Fermat-Kraitchik algorithm

1. Find many integers $a_1, \ldots, a_r$: $c_i :\equiv a_i^2[N]$ factors as a product of small primes.

   In practice we consider the factors of $c(x) := x^2 - N$, $x > [\sqrt{N}]$.

2. Take a product $\Pi_{j \in J} c_j$, $J \subseteq \{1, \ldots, r\}$: every prime appears to an even power.

   Then $\Pi_{j \in J} c_j = b^2$ for some $b \in \mathbb{N}$.

3. Let $a := \Pi_{j \in J} a_j$. Then $a^2 \equiv \Pi_{j \in J} c_j \equiv b^2[N]$.

of N.

Pomerance's quadratic sieve

REMARK **Find numbers whose squares are divisible by small primes.**

$c(x) = x^2 - N$. **Pomerance's trick: if** p **is a prime,**

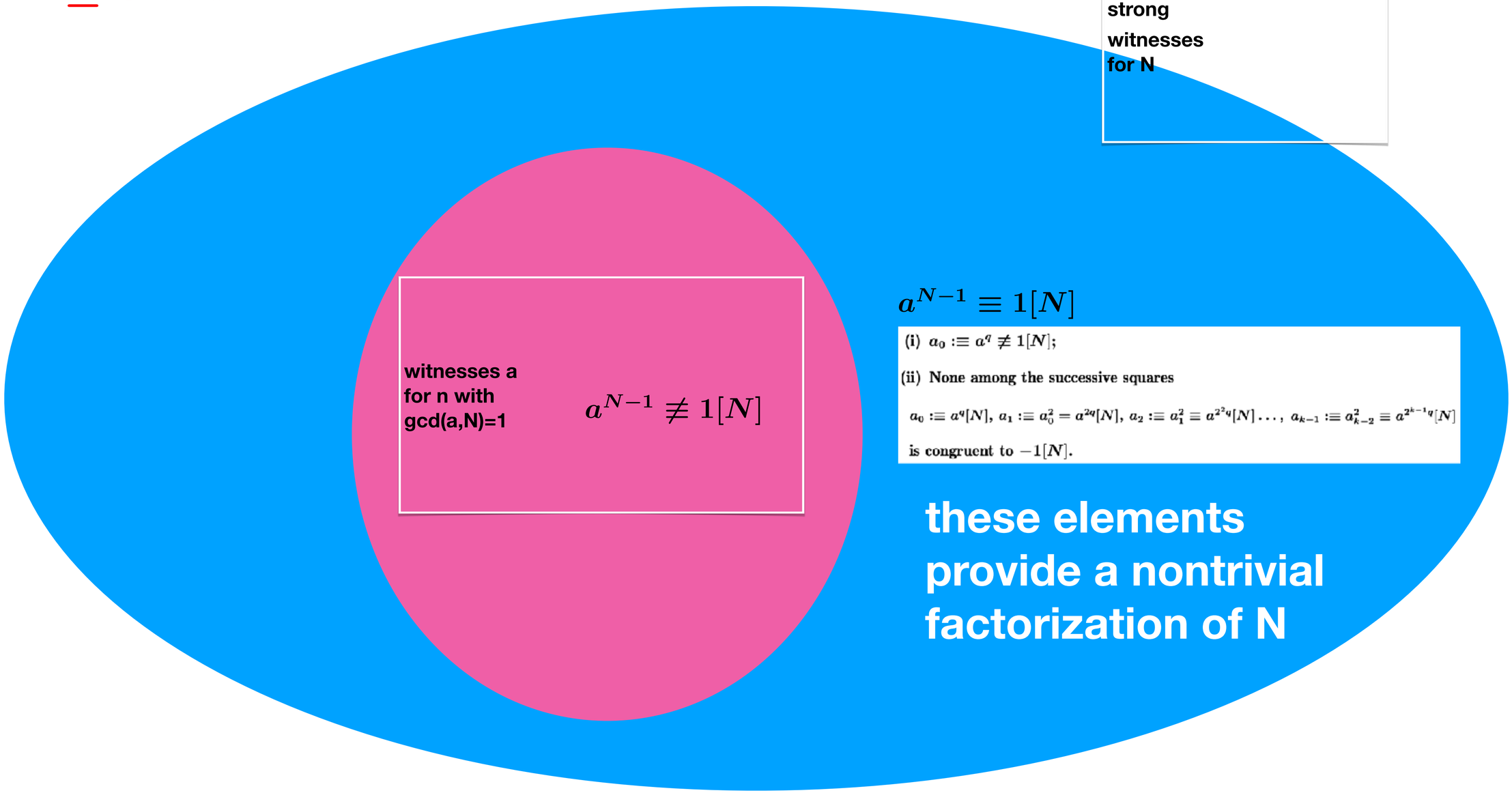
$$p^r \mid c(x) \Rightarrow p^r \mid c(x + p^r), c(x + 2p^r), \ldots$$

Algorithm: quadratic sieve. **RSA-155 was solved using sieving.**

UNIT 4
Strong witnesses and factorization

Factorization through a strong witness that is not a witness

$N \geq 3$ odd



Factorization through a strong witness that is not a witness

Let $N \in \mathbb{N}, N > 2$ be odd.

Let $a \in \mathbb{N}, a \geq 2, \gcd(a, N) = 1$, not a witness for Fermat test: $a^{N-1} \equiv 1[N]$.

$\Rightarrow \gcd(a, N) = 1$

Let's try Strong Fermat test. $N - 1 = 2^k q$, with $2 \nmid q$. a is a strong witness:

(i) $a_0 :\equiv a^q \not\equiv 1[N]$;

(ii) None among the successive squares

$$a_0 :\equiv a^q[N],\ a_1 :\equiv a_0^2 = a^{2q}[N],\ a_2 :\equiv a_1^2 \equiv a^{2^2 q}[N] \ldots,\ a_{k-1} :\equiv a_{k-2}^2 \equiv a^{2^{k-1} q}[N]$$

is congruent to $-1[N]$. Thus, we know that N is not prime.

Guess a nontrivial factor of N? $\gcd(a_{i-1} \pm 1, N)$

Since $a_k = a^{N-1} \equiv 1[N]$, there is $i \in \{1, \ldots, k\} : a_i \equiv 1[N],\ a_{i-1} \not\equiv -1[N]$.

Factorization through a strong witness that is not a witness

PROPOSITION (Factorization via a strong Fermat witness)

Let N odd, $N-1=2^k q, 2\nmid q$ and let $a\in\mathbb{N}$ be such that $a^{N-1}\equiv 1[N]$.

a is not a witness

Let $a_j := a^{2^j q}[N], j=0,\dots,k$. If a is a strong witness

(i) $a_0 :\equiv a^q \not\equiv 1[N]$;

(ii) None among the successive squares

$a_0 :\equiv a^q[N],\ a_1 :\equiv a_0^2 = a^{2q}[N],\ a_2 :\equiv a_1^2 \equiv a^{2^2 q}[N]\dots,\ a_{k-1} :\equiv a_{k-2}^2 \equiv a^{2^{k-1}q}[N]$

is congruent to $-1[N]$.

there is $i\in\{1,\dots,k\}$ such that $a_i\equiv 1[N], a_{i-1}\not\equiv -1[N]$.

Then $\gcd(a_{i-1}\pm 1, N)$ are nontrivial factors of N.

Proof. $a_k\equiv a^{N-1}\equiv 1[N]$: let $i=\min\{j\in\{0,\dots,k\} : a_j\equiv 1[N]\}$.

Since $a_0\not\equiv 1$ then $i\geq 1$. Moreover $a_{i-1}\not\equiv -1$. Thus $\begin{cases} a_{i-1}^2\equiv a_i\equiv 1[N] \\ a_{i-1}\not\equiv \pm 1[N] \end{cases}$

Basic factorization (Fermat method)$\Rightarrow \gcd(a_{i-1}\pm 1, N)$ are nontrivial factors of N. $\square$

Factorization through a strong witness that is not a witness

EXAMPLE (Carmichael 561 passes the Strong test)

$n = 561, n - 1 = 560 = 2^4 \cdot 35$:

$k = 2, q = 35$. Take $a = 2$ (it's not a witness).

(i) $a_0 = a^q = 2^{35} \equiv 263[561]$.

(ii) $a_0 = a^q = 2^{35} \equiv 263[561]$

$a_1 = a_0^2 \equiv 166[561]$

$a_2 = a_1^2 \equiv 166^2 \equiv 67[561]$

$a_3 = a_2^2 \equiv 67^2 \equiv 1[561]$

$a_4 = a_3^2 \equiv a^{n-1} \equiv 1[561]$

Thus $a = 2$ is a strong witness

and 561 is not prime.

PROPOSITION (Factorization via a strong Fermat witness)

Let N odd, $N - 1 = 2^k q, 2 \nmid q$ and let $a \in \mathbb{N}$ be such that $a^{N-1} \equiv 1[N]$.

Let $a_j := a^{2^j q}[N], j = 0, ..., k$. If a is a strong witness

there is $i \in \{1, ..., k\}$ such that $a_i \equiv 1[N], a_{i-1} \not\equiv -1[N]$.

Then $\gcd(a_{i-1} \pm 1, N)$ are nontrivial factors of N.

Factorization through a strong witness that is not a witness

EXAMPLE $N = 1105$ is a Carmichael number.

Thus $a = 2$ is not a witness for N.

1) Prove that $a = 2$ is a strong witness for N.

$$N - 1 = 1104 = 2^4 \cdot 69.$$

2) Deduce a factor of N.

A generalization: factorization via a strong Fermat type test

PROPOSITION (Factorization via a Strong Fermat like test)

Let $N \in \mathbb{N}_{\geq 1}$. Suppose that $L \geq 1$ is even and such that $a^L \equiv 1[N]$.

It might happen that L<N-1

Write $L = 2^k q, 2 \nmid q$. Define the list of successive squares:

$$a_0 :\equiv a^q[N],\ a_1 :\equiv a_0^2 = a^{2q}[N],\ \ldots,\ a_k :\equiv a_{k-1}^2 \equiv a^{2^k q}[N] \equiv 1[N].$$

Assume that:

(i) $a_0 \not\equiv 1[N]$,

(ii) Let $i = \min\{j \in \{1, ..., k\} :\ a_j \equiv 1[N]\}$: then $a_{i-1} \not\equiv -1[N]$.

Then $\gcd(a_{i-1} \pm 1, N)$ are nontrivial factors of N: $1 < \gcd(a_{i-1} \pm 1, N) < N$.

Proof. $a_{i-1}^2 \equiv 1[N], a_{i-1} \not\equiv \pm 1[N] \Rightarrow \gcd(a_{i-1} \pm 1, N)$ are nontrivial factors of N.

BASIC FACTORIZATION PRINCIPLE

□

Factorization via a strong Fermat type test

EXAMPLE $2^{200} \equiv 1[32817151].$

Notice that 200 < N-1

$200 = 2^3 \cdot 25$. Compute:

$$a_0 \equiv 2^{25} \equiv 737281[32817151]$$

$$a_1 \equiv a_0^2 \equiv 32800948[32817151]$$

$$a_2 \equiv a_1^2 \equiv 1[32817151]$$

$2 = \min\{j : a_j \equiv 1[32817151]\}$ and $a_1 \not\equiv -1[32817151]$.

PROPOSITION (Factorization via a Strong Fermat like test)

Let $N \in \mathbb{N}_{\geq 1}$. Suppose that $L \geq 1$ is even and such that $a^L \equiv 1[N]$.

Write $L = 2^k q, 2 \nmid q$. Define the list of successive squares:

$$a_0 :\equiv a^q[N], a_1 :\equiv a_0^2 = a^{2q}[N], \ldots, a_k :\equiv a_{k-1}^2 \equiv a^{2^k q}[N] \equiv 1[N].$$

Assume that:

(i) $a_0 \not\equiv 1[N]$,

(ii) Let $i = \min\{j \in \{1, ..., k\} : a_j \equiv 1[N]\}$: then $a_{i-1} \not\equiv -1[N]$.

UNIT 5
Pollard's p-1 factorization algorithm

The basic idea

Basic idea Let $N = pq$, $p \neq q$ odd primes. Let $p \nmid a$. Then $a^{p-1} \equiv 1[p]$. FERMAT

Thus, if $p-1 \mid L$, $\begin{cases} a^L \equiv 1[p] \\ L \text{ is even.} \end{cases}$

$$\begin{cases} p \nmid a \\ p-1 \mid L \end{cases} \Rightarrow \gcd(a^L - 1, N) = \begin{cases} p \text{ if } q \nmid a^L - 1 \\ N \text{ otherwise: } a^L \equiv 1[N] \end{cases}$$

you find a factor!

Try factorization via a Strong Fermat type test

The moral: chances of factoring if p-1|L

EXAMPLE $N = 143 = pq, p = 13, q = 11.$ $a = 2.$ $p - 1 = 12 = 2^2 \cdot 3.$

Take $L := 4! = 24$ $\quad 2^L \equiv 27[143]$ $\quad \gcd(2^L - 1, N) = \gcd(26, 143) = 13.$

Why? $p - 1 = 12 = 2^2 \cdot 3 \mid L = 4!, 2^L - 1 \equiv 4 \not\equiv 0[q].$

The basic idea

Basic idea Let $N = pq$, $p \neq q$ odd primes.

$$\begin{cases} p-1 \mid L \\ p \nmid a \end{cases} \Rightarrow \gcd(a^L - 1, N) = \begin{cases} p \text{ if } q \nmid a^L - 1 \\ N \text{ otherwise} \end{cases}$$

REMARK $\gcd(a^L - 1, N) = \gcd((a^L - 1)_N, N)$.

QUESTION How to find L without knowing p?

Pollards's observation: if $p-1$ has small factors, then $p - 1 \mid n!$, n "small"

EXAMPLE How to compute $2^{100!}[N]$? $2^{100!}$ has about 10^{157} digits....

$$a^{(n+1)!}[N] \equiv \left(a^{n!}\right)^{n+1}[N].$$

Thus, if $a^{n!} \equiv 1[N]$ then $a^{(n+1)!} \equiv 1[N]$.

Pollard's p-1 factorization algorithm

POLLARD's FACTORIZATION ALGORITHM

Consider $a \in \mathbb{N}$. often a=2

For $n = 2, 3, 4, \ldots$ compute $d = \gcd(a^{n!} - 1, N)$.

- **If $d = 1$ go to the next value of n;**
- **If $d = N$ then use factorization via Strong Fermat like test or change a.**

(no chance to try higher values of n)

- **Otherwise, if $1 < d < N$, d is a nontrivial factor of N.**

Pollard's p-1 factorization algorithm

POLLARD's FACTORIZATION ALGORITHM

Consider $a \in \mathbb{N}$. often a=2

For $n = 2, 3, 4, \ldots$ compute $d = \gcd(a^{n!} - 1, N)$.

- **If $d = 1$ go to the next value of n;**
- **If $d = N$ then use factorization via Strong fermat like test or change a.**
- **Otherwise, if $1 < d < N$, d is a nontrivial factor of N.**

Pollard's p-1 factorization algorithm

EXAMPLE We want to factor $N = 13\,927\,189$.

$$2^{9!} \equiv 13\,867\,884[13\,927\,189] \quad \gcd(2^{9!} - 1, N) = \gcd(13\,867\,884 - 1, N) = 1[N]$$

$$2^{10!} \equiv (2^{9!})^{10}[N] \equiv 13\,867\,884^{10}[N] \equiv 5\,129\,509[13\,927\,189]$$

$$\gcd(2^{10!} - 1, N) = \gcd(5\,129\,508, N) = 1[N]$$

$$\vdots \qquad\qquad \vdots$$

$$2^{13!} \equiv 6\,161\,078[N] \qquad \gcd(2^{13!} - 1, N) = \gcd(6\,161\,077, N) = 1[N]$$

$$2^{14!} \equiv \left(2^{13!}\right)^{14} \equiv 6\,161\,078^{14}[N] \equiv 879\,291[N]$$

$$\gcd(2^{14!} - 1, N) = \gcd(879\,290, N) = 3823[N]$$

Pollard's p-1 factorization algorithm

POLLARD's FACTORIZATION ALGORITHM

Consider $a \in \mathbb{N}$. often a=2

For $n = 2, 3, 4, \ldots$ compute $d = \gcd(a^{n!} - 1, N)$.

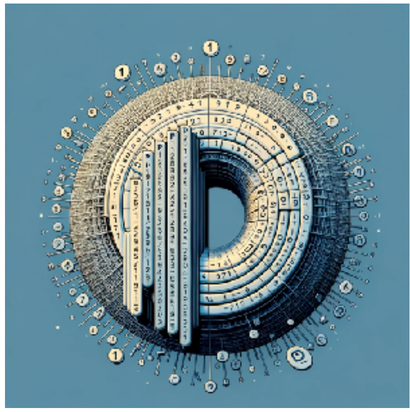
- If $d = 1$ go to the next value of n;
- If $d = N$ then use Strong Fermat type factorization or change a.
- Otherwise, if $1 < d < N$, d is a nontrivial factor of N.

EXAMPLE $N = 1739.$

Successively compute: $2^{n!}[N], \gcd(2^{n!} - 1, N), n = 3, 4, \ldots.$

Deduce the factorization of N and explain why.

Epilogue



It can be shown that, for $B > 0$ fixed, the complexity of Pollard's method for numbers $N = pq$ with $p - 1$ product of primes $\leq B$ (these primes are called B-smooth) is $O\big((\log n)^2\big)$.

For a secure cryptography: avoid primes p such that (p-1) is a product of small primes

In general there are no known polynomial algorithms to factor any number.

The quickest known algorithms (e.g., number field sieve method) has a subexponential complexity: $O(N^{\varepsilon})$ for all $\varepsilon > 0$.

END of
LESSON 11
Finding the factors of a product of two primes

END OF THE COURSE
Cryptography