# RSA Cryptosystem and Factorization

D. J. Guan

Department of Computer Science
National Sun Yat Sen University
Kaoshiung, Taiwan 80424
R. O. C.

guan@cse.nsysu.edu.tw

August 25, 2003

# RSA Cryptosystem

was invented by Rivest, Sharmir, and Adleman in 1978.

$m$: message
$c$: cipher

Encryption

1. choose $n$ and $e$;

2. compute $c = m^e \bmod n$;

Decryption

1. compute $d$, the inverse of $e$ in $\mathbf{Z}^*_{\phi(n)}$
   $d \cdot e \equiv 1 \pmod{\phi(n)}$;

2. compute $m = c^d \bmod n$;

## Example

$n = 143,\ e = 103$

$$m = 2,\quad c = 2^{103} \bmod 143 \ = 63$$
$$m = 3,\quad c = 3^{103} \bmod 143 \ = 16$$
$$m = 4,\quad c = 4^{103} \bmod 143 \ = 108$$
$$m = 5,\quad c = 5^{103} \bmod 143 \ = 125$$
$$m = 6,\quad c = 6^{103} \bmod 143 \ = 7$$
$$m = 7,\quad c = 7^{103} \bmod 143 \ = 123$$

$n = 143,\ \phi(143) = 120,\ e = 103,$
$103^{-1} = 7,\quad (103 \cdot 7 \equiv 1 \pmod{120}).$

$$c = 63,\quad m = 63^{7} \bmod 143 \ = 2$$
$$c = 16,\quad m = 16^{7} \bmod 143 \ = 3$$
$$c = 108,\quad m = 108^{7} \bmod 143 \ = 4$$
$$c = 125,\quad m = 125^{7} \bmod 143 \ = 5$$
$$c = 7,\quad m = 7^{7} \bmod 143 \ = 6$$
$$c = 123,\quad m = 123^{7} \bmod 143 \ = 7$$

# Why RSA Cryptosystem Works?

If $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.

$d \cdot e \equiv 1 \pmod{\phi(n)} \Rightarrow d \cdot e - 1$ is a multiple of $\phi(n)$.

If $(m, n) = 1$, then

$$
\begin{aligned}
c^d \bmod n &= (m^e)^d \bmod n \\
&= m^{(ed)} \bmod n \\
&= m^{(k\phi(n)+1)} \bmod n \\
&= m^{(k\phi(n))} m \bmod n \\
&= ((m^{\phi(n)})^k) m \bmod n \\
&= m
\end{aligned}
$$

If $(m, n) \neq 1$, then ?

# Application of the RSA Cryptosystem

$A$ sends a secret message to $B$.

1. $B$ chooses two large primes $p$ and $q$;

2. $B$ computes $n = p \cdot q$, and
$$\phi(n) = (p - 1)(q - 1);$$

3. $B$ chooses $e$ such that $(e, \phi(n)) = 1$;

4. $B$ sends $n$ and $e$ to $A$;

5. $A$ computes $c = m^e \bmod n$, and sends it to $B$;

6. $B$ computes $d$, the inverse of $e$ in $\mathbf{Z}^*_{\phi(n)}$;

7. $B$ decrypts the message $m$ by computing
$$m = c^d \bmod n;$$

$B$'s public key: $(n, e)$

$B$'s private key: $d$

Using only the public key $n$ and $e$, it is "computationally infeasible" to compute $d$.

It is "easy" to compute $d$, if $\phi(n)$ is known.

## Another Application of the RSA

$A$ signs a message and sends it to $B$.

$A$'s public key: $(n, e)$
$A$'s private key: $d$

1. $A$ computes $s = m^d$ mod $n$;

2. $A$ sends $m$ and $s$ to $B$;

3. $B$ accepts the signature if $m = s^e$ mod $n$;

## Yet Another Application of the RSA

$A$ signs a secret message and sends it to $B$.

$A$'s public key: $(n_A, e_A)$
$A$'s private key: $d_A$

$B$'s public key: $(n_B, e_B)$
$B$'s private key: $d_B$

$n_A > n_B$

1. $A$ encrypts the message $c = m^{e_B} \bmod n_B$;

2. $A$ computes the signature $s = c^{d_A} \bmod n_A$;

3. $A$ sends $c$ and $s$ to $B$;

4. $B$ accepts the signature if $c = s^{e_A} \bmod n_A$;

5. $B$ decrypts the message $m = c^{d_B} \bmod n_B$;

# How to Compute $\phi(n)$?

$\phi(n)$ is the order of the multiplicative group $\mathbf{Z}_n^*$.

$$\text{If } n = \prod_{k=1}^{r} p_k^{e_k}, \text{ then } \phi(n) = \prod_{k=1}^{r} p_k^{e_k-1}(p_k - 1).$$

1. If $n$ is prime, then $\phi(n) = n - 1$.

2. If $n$ is the product of two primes $p \cdot q$, then $\phi(n) = (p-1)(q-1)$.

How to compute $\phi(n)$ without factoring $n$?

The security of the RSA cryptosystem depends on the difficulty of factoring $n$.

# Factorization

In April 1994, an international cooperative group of mathematicians and computer scientists solved a 17-year-old challenge problem, the factoring of a 129-digit number, called RSA-129, into two primes.

1143816257578888676692357997614
6612010218296721242362562 5618429
3570693524573389783059712356 3958
7050589890751475992900268 7954 3541

is the product of

34905295108476509491478496199038
9813341776463849338784 3990820577

and

3276913299326709549961988190834
46141317 64296799429253 97 98288533

by 1600 computers, 8 months, 5000 mips-years.

## Factorization Algorithms

Trial division:

> **for** $k = 2, 3, 5, 7, \ldots, \left\lceil \sqrt{n} \right\rceil$
>     **if** $k \mid n$ **then** $k$ is a factor of $n$;

> $n$ cannot be the products of "small" primes.

## Factorization Algorithms

In RSA, $n$ is a product of two large distinct primes.

Assume that $n = p \cdot q$, $p < q$.

If $q - p$ is too "large", then $p$ may be too small.

If $q - p$ is too "small", then

$$(q + p)^2 - (q - p)^2 = 4pq = 4n$$

$$(q + p)^2 = 4n + (q - p)^2$$

Guess the value of $q - p$,
such that $4n + (q - p)^2$ a perfect square.

$$q + p = \sqrt{4n + (q - p)^2}$$

Computing square root in $\mathbf{R}$ is "easy".

Example:  $n = 221$

| $q - p$ | $4n + (q-p)^2$ | $q + p$ |
|:---:|:---:|:---:|
| 1 | 885 | $29.7489\cdots$ |
| 2 | 888 | $29.7993\cdots$ |
| 3 | 893 | $29.8831\cdots$ |
| 4 | 900 | 30 |

$q - p = 4$, $q + p = 30$,

$p = 13$, $q = 17$,

$n = 13 \times 17$

The difference of $p$ and $q$ should be "large".

In particular, $n$ cannot be the square of a prime.

## Factorization Algorithms

let $x = \left[\sqrt{n}\right]$, $p = x - a$, $q = x + b$

$$
\begin{aligned}
n &= (x - a)(x + b) \\
&= x^2 + (b - a)x - ab \\
&= x^2 + (b - a - 1)x + (x - ab)
\end{aligned}
$$

$x$-radix representation $n = x^2 + \alpha x + \beta$,

$(p + q)/2 > \sqrt{pq} = \sqrt{n} \geq x$

$\left[(x - a) + (x + b)\right]/2 > x$

$b - a > 0$

If $ab \leq x$ then

$0 \leq b - a - 1 < x$

$0 \leq x - ab < x$

If $p - q \leq n^{1/4}$, then the values of $a$ and $b$ can be obtained by solving

$$
\begin{aligned}
b - a - 1 &= \alpha \\
x - ab &= \beta
\end{aligned}
$$

An example: $n = 187$

$$x = \left\lceil \sqrt{187} \right\rceil = 13$$

$$187 = (13)^2 + 1(13) + 5$$

$$\alpha = 1, \ \beta = 5$$

$$
\begin{aligned}
b - a &= 1 + 1 \\
ab &= 13 - 5
\end{aligned}
$$

$$a = 2, \ b = 4$$

$$p = 13 - 2 = 11, \ q = 13 + 4 = 17$$

$$n = 11 \times 17$$

The difference of $p$ and $q$ should be at least $n^{1/4}$.

In other words, if first half of the bits of $p$ and $q$ are equal, then $n$ can be factorized easily.

## $p - 1$ **Factoring Algorithm**

In 1974, Pollard introduced the $p - 1$ Factorization Algorithm.

1. Let $a$ be an integer in $(1, n - 1)$.

2. If $(a, n) \neq 1$ then $(a, n)$ is a factor of $n$.

3. Otherwise, compute $x = a^m \bmod n$, for some $m$ which is a multiple of $p - 1$.

4. $d = \gcd(x - 1, n)$ is a factor of $n$.

# How to compute a multiple of $p - 1$?

If every prime power factor of $p - 1$ is bounded by $B$, then $p - 1$ is $B$-smooth.

Example: $12 = 2^2 \cdot 3$, it is 4-smooth.

Let $m = \displaystyle\prod_{i=1}^{r} p_i^{\alpha_i}$, where
$p_1, p_2, \ldots, p_r$ are the primes $\leq B$,
$\alpha_i$ is the integer such that $p_i^{\alpha_i} \leq B < p_i^{\alpha_i + 1}$.

If $p - 1$ is $B$ smooth, then $m$ must be a multiple of $p - 1$.

$n = p \cdot q$, where $p$ and $q$ are primes.

$a \equiv b \pmod{n}$, if and only if

$a \equiv b \pmod{p}$, and
$a \equiv b \pmod{q}$.

$x = a^m \bmod n = a^{k(p-1)} \bmod n$

$x \equiv a^{k(p-1)} \pmod{p}$

$x \equiv 1 \pmod{p}$

$p \mid (x - 1)$

$x - 1 = kp$

compute $d = (x - 1, n)$

If $1 < d < n$ then $d$ is a nontrivial factor of $n$.

It has been shown that, if $a$ is randomly chosen, the successful rate is 0.5.

$p - 1$ must contain large prime factors.

## $p + 1$ **Factoring Algorithms**

In 1982, Williams introduced the $p + 1$ Factoring
Algorithm.

Use group generated by the Lucas sequence,
instead of $\mathbf{Z}_n^*$.

With proper choice of parameters, the order of the
group is $p + 1$.

If $p + 1$ is $B$-smooth, then $n$ can be factored by the
$p + 1$ method.

$p + 1$ must contain large prime factors.

## Lucas Sequence

Given $a$ and $b$, let $\alpha$ and $\beta$ be the zeros of

$$x^2 - ax + b.$$

Lucas sequence is defined by
$u_k = (\alpha^k - \beta^k)/(\alpha - \beta)$
$v_k = (\alpha^k + \beta^k)$

**Theorem 1 (Lehmer 1978)** *If $p$ is an odd prime and $p \nmid b$ then*
$u_{k(p-\gamma)} \equiv 0 \pmod{p}$
$v_{k(p-\gamma)} \equiv 2b^{k(1-\gamma)} \pmod{p}$
*where* $\gamma = \left( \dfrac{a^2 - 4b}{p} \right)$.

Legendre symbol

$$\left( \frac{x}{p} \right) = \begin{cases} 0 & \text{if } x \equiv 0 \pmod{p} \\ 1 & \text{if } x \text{ is a quadratic residue modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

$$\left( \frac{x}{p} \right) \equiv x^{(p-1)/2} \pmod{p}$$

## Elliptic Curves

Assume that $\mathbf{F}_p$ is a field whose characteristic is not equal to 2 or 3.

An elliptic Curves over $\mathbf{F}_p$ is define by the Weierstrass equation

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

where $a, b \in \mathbf{F}_p$, and $4a^3 + 27b^2 \neq 0$.

$$\mathbf{E}_{a,b}(\mathbf{F}_p)$$
$$= \{(x, y, z) \in \mathbf{P}^2(\mathbf{F}_p) \mid y^2 z = x^3 + axz^2 + bz^3\}$$

The projective plan $\mathbf{P}^2(\mathbf{F}_p)$ over $\mathbf{F}_p$ consists of the equivalence classes of $(x, y, z) \in \mathbf{F}_p \times \mathbf{F}_p \times \mathbf{F}_p$, where $(x, y, z)$ and $(cx, cy, cz)$ are equivalent.

Addition rules:

1. $O = (0, 1, 0)$ is the zero of the group.
   $P + O = O + P = P$.

2. $P = (x_1, y_2, 1)$, $Q = (x_2, y_2, 1)$, $R = (x_3, y_3, z_3)$ be the intersections of the curve and a line then $P + Q + R = O$.

## Elliptic Curve Factoring Algorithm

In 1985, Hendric and Lenstra invented the Elliptic curve method for factoring $n$, by using elliptic curves "over" $\mathbf{Z}_n$.

1. Randomly select $a, b \in \mathbf{Z}_n$ for the Elliptic curve to be used;

2. Randomly select a point $P = (x, y, 1)$ of the curve;

3. Select a bound $B$, and compute
$$m = \prod_{i=1}^{r} p_i^{\alpha_i},$$
where $p_i$, $i = 1, 2, \ldots, r$, are prime numbers bounded by $B$, and $\alpha_i$ is the maximum integer such that $p_i^{\alpha_i}$ is more than $B$;

4. Attempt to compute $mP = \underbrace{P + P + \cdots + P}_{m}$;

**Elliptic Curves modulo** $n$

$\mathbf{E}_{a,b}(\mathbf{Z}_n)$
$= \{(x, y, z) \in \mathbf{P}^2(\mathbf{Z}_n) \mid y^2 z = x^3 + axz^2 + bz^3\}$

The following addition algorithm will either find a factor of $n$, or compute the "sum" of $P = (x_1, y_1, 1)$ and $Q = (x_2, y_2, 1)$.

> **If** $x_1 = x_2$ **and** $y_1 = -y_2$ **then return**$(O)$;
> **If** $x_1 = x_2$ **then**
> > find $s, t,\ s(y_1 + y_2) + tn = (y_1 + y_2, n) = d$;
> > **if** $d > 1$ **then**
> > > $d$ is a factor of $n$; **stop**;
> >
> > **else**
> > > $\lambda = s(3x_1^2 + a)$;
> >
> > **end**
>
> **else**
> > find $s, t,\ s(x_1 - x_2) + tn = (x_1 - x_2, n) = d$;
> > **if** $d > 1$ **then**
> > > $d$ is a factor of $n$; **stop**;
> >
> > **else**
> > > $\lambda = s(y_1 - y_2)$;
> >
> > **end**
>
> **end**
> $x = \lambda^2 - x_1 - x_2;\ y = \lambda(x - x_1) + y_1$;
> **return**$((x, -y, 1))$

The order of the group generated by the elliptic curve $\mathbf{E}_{a,b}(\mathbf{F}_p)$ is $p + 1 - t$, where $|t| \leq 2\sqrt{p}$.

It has been shown that, for any $t$ with $|t| \leq 2\sqrt{p}$, there is an elliptic curve $\mathbf{E}_{a.b}(\mathbf{F}_p)$ with order $p + 1 - t$.

If $p + 1 - t$ is $B$-smooth, then $n$ can be factored by the elliptic curve method.

By using different elliptic curves, the factorization can be done in "parallel".

# Strong Primes and Strong Keys

Strong prime

1. $p$ is large.

2. The largest prime factor of $p - 1$ is large.

3. The largest prime factor of $p + 1$ is large.

4. ...

Strong key

1. The difference of $p$ and $q$ is large.

2. The ratio, $p/q$, is not close to $a/b$, for some "small" integers $a$ and $b$.

3. ...

Are strong primes needed for RSA?

Are there strong primes for RSA?

Is RSA secure?

> The only way to ensure the security of the
> RSA cryptosystem is to increase the size of
> $n$.

According to the estimate of Silverman and
Wagstaff, using 100000000000 MIPS R10000
computers, running for 3750000000 years could
have only 0.63 chance to factor 1024-bit integer.

## Computational Complexity of the Factoring Algorithms

$$L_n[\nu, \lambda] = \exp\left(\lambda(\log n)^\nu (\log \log n)^{1-\nu}\right)$$

$$L_n[1, \lambda] = n^\lambda, \ L_n[0, \lambda] = (\log n)^\lambda$$

$\log \log L_n[\nu, \lambda]$
$= (\nu) \log \log L_n[1, \lambda] + (1 - \nu) \log \log L_n[0, \lambda]$

The most important parameter is $\nu$.

| | |
|---|---|
| trial division: | $L_n[1, \lambda]$ |
| elliptic curve method: | $L_n[1/2, 1]$ |
| quadratic sieve: | $L_n[1/2, 1]$ |
| number field sieve: | $L_n[1/3, \lambda]$ |

## Sieve Factoring Algorithms

Factoring Algorithms whose running time depends mainly on the size of $n$, e.g., quadratic sieve, special number field sieve, general number field sieve, ...

1. find $x$ and $y$ such that $x \not\equiv \pm y \pmod{n}$ and $x^2 \equiv y^2 \pmod{n}$;

2. compute $d = (x - y, n)$;
   if $1 < d < n$ then $d$ is a nontrivial factor of $n$;

$x \not\equiv \pm y \pmod{n} \Rightarrow n \nmid (x - y)$ and $n \nmid (x + y)$

$x^2 \equiv y^2 \pmod{n} \Rightarrow n \mid (x^2 - y^2) \Rightarrow n \mid (x - y)(x + y)$

## Find Congruent Squares

How to find $x$ and $y$ such that $x^2 \equiv y^2 \pmod{n}$?

1. choose a set of primes $B = \{p_1, p_2, \ldots, p_r\}$.

2. find a set of $x$ in $\mathbf{Z}_n$ such that $x^2$ mod $n$ can be factored by using primes in $B$,

$$C = \{x \mid x^2 \equiv \prod_{i=1}^{r} p_i^{e_i} \pmod{n}\}$$

3. select a subset $S$ of $C$ such that

$$\prod_{x \in S} x^2 \equiv \prod_{i=1}^{r} p_i^{\beta_i} \pmod{n}$$

where each $\beta_i$ is even.

For a randomly chosen pair $x$ and $y$ satisfying $x^2 \equiv y^2 \pmod{n}$, at least half of them will also satisfy $x \not\equiv \pm y \pmod{n}$.

# An Example: Quadratic Sieve

$n = 33221, \ B = \{2, 3, 5, 7\}$

$x_i = \left\lceil \sqrt{33221} \right\rceil + i = 182 + i.$

$$
\begin{aligned}
(189)^2 &\equiv 2500 &&\equiv (2)^2 (5)^4 \\
(378)^2 &\equiv 10000 &&\equiv (2)^4 (5)^4 \\
(409)^2 &\equiv 1176 &&\equiv (2)^3 (3)^1 (7)^2 \\
(567)^2 &\equiv 22500 &&\equiv (2)^2 (3)^2 (5)^4 \\
(682)^2 &\equiv 30 &&\equiv (2)^1 (3)^1 (5)^1 \\
(802)^2 &\equiv 12005 &&\equiv (5)^1 (7)^4 \\
(818)^2 &\equiv 4704 &&\equiv (2)^5 (3)^1 (7)^2 \\
(835)^2 &\equiv 32805 &&\equiv (3)^8 (5)^1 \\
(845)^2 &\equiv 16384 &&\equiv (2)^1 4 \\
(983)^2 &\equiv 2880 &&\equiv (2)^6 (3)^2 (5)^1 \\
(1169)^2 &\equiv 4500 &&\equiv (2)^2 (3)^2 (5)^3 \\
(1223)^2 &\equiv 784 &&\equiv (2)^4 (7)^2 \\
(1227)^2 &\equiv 10584 &&\equiv (2)^3 (3)^3 (7)^2 \\
(1327)^2 &\equiv 216 &&\equiv (2)^3 (3)^3 \\
(1364)^2 &\equiv 120 &&\equiv (2)^3 (3)^1 (5)^1 \\
(1568)^2 &\equiv 270 &&\equiv (2)^1 (3)^3 (5)^1 \\
(1589)^2 &\equiv 125 &&\equiv (5)^3 \\
&\ \ \vdots
\end{aligned}
$$

## An Example: Quadratic Sieve

$189^2 \equiv 2^2 5^4$

$189^2 \equiv 2^2 5^4 \equiv 50^2$

$189^2 - 50^2 \equiv 0 \bmod 33221$

$(189 - 50)(189 + 50) \equiv 0 \bmod 33221$

$(139)(239) = k(33221)$

$33221 = 139 \times 239$

$802^2 \equiv 5^1 7^4$

$835^2 \equiv 3^8 5^1$

$(802 \cdot 835)^2 \equiv (3^4 \cdot 5 \cdot 7^2)^2$

$(669670) \overline{\overline{=}} (19845)^2$

$(5250)^2 \equiv (19845)^2$

$(5250 - 19845)(5250 + 19845) = k \cdot 33221$

$(-14595)(20595) = k \cdot 33221$

$(-14595, 33221) = 139$

$(20595, 33221) = 239$

$$409^2 \equiv 2^3 3^1 7^2$$
$$682^2 \equiv 2^1 3^1 5^1$$
$$835^2 \equiv 3^8 5^1$$

$$(409 \cdot 682 \cdot 835)^2 \equiv (2^2 \cdot 3^5 \cdot 5 \cdot 7)^2$$
$$(232913230)^2 \equiv (34020)^2$$
$$(799)^2 \equiv (799)^2$$

The first phase of the sieve algorithm is to find a set of $x$ in $\mathbf{Z}_n$ such that $x^2 \bmod n$ can be factored by using primes in $B = \{p_1, p_2, \ldots, p_r\}$,

$$C = \{x \mid x^2 \equiv \prod_{i=1}^{r} p_i^{e_i} \pmod{n}\}$$

Each $x \in C$ can be represented by a vector in $\mathbf{Z}_2^r$, $(b_1, b_2, \ldots, b_r)$, where each $b_i = e_i \bmod 2$.

Supposed that we have collected more then $r$ such $x$'s in $C$.

The second phase is to find a pair of congruent squares modulo $n$, i.e., $x^2 \equiv y^2 \pmod{n}$.

Let $V$ be the set of vectors constructed from each element in $C$.

Since $|V| = |C| > |B|$, vectors in $V$ cannot be all linearly independent.

Therefore, we can select a subset $S \subseteq C$ such that the sum of the corresponding vectors in $\mathbf{Z}_2^r$ is zero. Hence,

$$\prod_{x \in S} x^2 \equiv \prod_{i=1}^{r} p_i^{\beta_i} \pmod{n}$$

where each $\beta_i$ is even.

The first phase involves searching for "smooth" integers.

The second phase combines these integers into two congruent squares.
This can be done by solving a large systems of linear equations.

## Multiple Polynomial Quadratic Sieve

In searching for the smooth integers,

quadratic sieve:
$$f(t) = \left(t + \left[\sqrt{n}\right]\right)^2, \; t = 1, 2, \ldots.$$

multiple polynomial quadratic sieve:
$$f(t) = (at + b)^2, \; t = 1, 2, \ldots,$$
where $|b| \leq a/2$ and $b^2 \equiv n \pmod{a}$.

In April 1994, a version of multiple polynomial quadratic sieve was used by Arjen Lenstra and Derek Atkins to factor the RSA-129, a 129-digit number that had been given in 1977 by the inventors of the RSA cryptosystem.

## Number Field Sieve

Number field sieve is considered to be the most efficient factoring algorithm for "large" integers (120+ digits).

It was first invented by Pollard to factor integers of the special form $n = r^e + s$ with small $r$ and $|s|$.

Lenstra, Lenstra, Jr., Manasse, Pollard, Buhler, Pomerance, et al. generalized it to factor any integers.

The basic principle of number field sieve is the same for quadratic sieve, namely to find two congruent squares modulo $n$.

The difference is that, in number field sieve, the squares are formed not only from combining smooth *rational integers*, but also by combining smooth *algebraic integers* from carefully chosen algebraic number field.

## Algebraic Numbers

Let $\mathbf{Z}[x]$ be the set of all polynomials with integer coefficients.

A number $z$ is *algebraic* if it is a root of a polynomial $P(x) \in \mathbf{Z}[x]$.

Assume that the polynomial $P(x)$ is *irreducible* over the rationals. The root $z$ of $P(x)$ generates an *algebraic number field*,

$$\mathbf{Q}(z) = \left\{ \sum_{i=0}^{n-1} a_i z^i \mid a_i \in \mathbf{Q} \right\}$$

$x = a_0 + a_1 z + \ldots + a_{n-1} z^{n-1}$ is *rational* if $x = a_0$, otherwise, it is irrational.

$x = a_0 + a_1 z + \ldots + a_{n-1} z^{n-1}$ is an *integer* if $x$ is a root of a monic polynomial in $\mathbf{Z}[x]$.

## An Example: Quadratic Fields

The quadratic polynomial $x^2 - D$ has roots $\pm\sqrt{D}$.

$\sqrt{D}$ generates a quadratic field $\mathbf{Q}(\sqrt{D})$

The elements of $\mathbf{Q}(\sqrt{D})$ can be represented by

$$z = a + b\sqrt{D}.$$

1. $(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$

2. $(a + b\sqrt{D}) - (c + d\sqrt{D}) = (a - c) + (b - d)\sqrt{D}$

3. $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$

4. $\dfrac{a + b\sqrt{D}}{c + d\sqrt{D}} = \dfrac{(a + b\sqrt{D})(c - d\sqrt{D})}{(c + d\sqrt{D})(c - d\sqrt{D})} =$
   $\dfrac{ac - bdD}{c^2 - d^2 D} + \left(\dfrac{ad - bc}{c^2 - d^2 D}\right)\sqrt{D}$

# Integer in a Quadratic Field

$z$ is an integer in $\mathbf{Q}(\sqrt{D})$ if $z^2 + bz + c = 0$ for some "rational" integer $b$ and $c$.

Let $z = r + s\sqrt{D}$ be an integer.

$(z - r)^2 = s^2 D$, thus $z$ is a root of the equation:

$$z^2 - 2rz + r^2 - s^2 D$$

$z$ is an integer iff $-2r \in \mathbf{Z}$ and $r^2 - s^2 D \in \mathbf{Z}$.

$z$ is an integer iff

$$\begin{cases} z = r + s\sqrt{D}, & \text{if } D \equiv 2 \text{ or } 3 \text{ mod } 4 \\ z = r + s\dfrac{-1 + \sqrt{D}}{2}, & \text{if } D \equiv 1 \text{ mod } 4 \end{cases}$$

## Conjugate Numbers

Let $z_1, z_2, \ldots, z_n$ be the roots of $P_n(x) \in \mathbf{Z}[x]$ of degree $n$. The numbers $z_1, z_2, \ldots z_n$ are called *conjugate numbers*.

The *norm* of $z = z_1$ is

$$N(z) = \prod_{i=1}^{n} z_i = (-1)^n d_0/d_n$$

1. $N(x)$ is rational.

2. $N(x) = 0$ iff $x = 0$.

3. $N(x)$ is integer if $x$ is an algebraic integer.

4. The norm $N$ is multiplicative, $N(xy) = N(x)N(y)$.

## Unit

$x$ is a unit of $\mathbf{Q}(z)$ if $N(x) = \pm 1$.

Examples:

There are 4 units in $C$: $\pm 1$, $\pm i$.

There are 6 units in $\mathbf{Q}(\sqrt{-3})$: $\pm 1$, $\pm \dfrac{-1 \pm \sqrt{-3}}{2}$.

There are infinite number of units in $\mathbf{Q}(\sqrt{2})$:
$(1 + \sqrt{2})^n$, $n = 1, 2, \ldots$

## Associate Numbers

$x$ and $y$ are associated numbers if $\dfrac{x}{y}$ is a unit of $\mathbf{Q}(z)$.

Examples:

$\mathbf{Z}$: $x$ and $-x$

$\mathbf{C}$: $2 + 3i$ and $-3 + 2i$

$\mathbf{Q}(\sqrt{2})$: $5 + \sqrt{2}$ and $11 - 7\sqrt{2}$

## Divisibilty, Primes, and Composites

Let $\mathbf{Z}(z)$ be the ring of integers in $\mathbf{Q}(z)$, $a, b, c \in \mathbf{Z}(z)$.

$a \mid b$, if $b = ac$ for some $c \in \mathbf{Z}(z)$.

If $a \mid b$, then $N(a) \mid N(b)$.

If $a = bc$ and both $b$ and $c$ are not units, then $a$ is composite, otherwise $a$ is prime.

Primes in $C$:

1. $1 + i$, $2 \pm i$, $3 \pm 2i$, $4 \pm i$,... i.e., all the factor $a \pm bi$ of $p = a^2 + b^2$, where $p = 2$ or $p$ is a prime of the form $4k + 1$.

2. 3, 7, 11, 19,... i.e., primes of the form $4k - 1$.

3. The associate numbers of the above.

## Factorization

Every integers $z \in \mathbf{Q}(\sqrt{D})$ can be factored into the product of the primes and the units.

For quadratic fields, if $D = -163$, -67, -43, -19, -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, and 73, then the factorization is unique in $\mathbf{Q}(\sqrt{D})$.

The nagative values of $D$ mentioned above are the only fileds for which the factorization is unique.

## Number Field Sieve

1. Construct an algebraic number field $\mathbf{Q}(z)$.

2. Find a nonempty set $S$ of pairs $(a, b)$ of relative prime integers such that:

$$\left( \prod_{(a,b) \in S} a + bm \right) = x^2 \text{ for some } x \in \mathbf{Z}_n$$

$$\left( \prod_{(a,b) \in S} a + bz \right) = y^2 \text{ for some } y \in \mathbf{Q}(z)$$

3. Compute a factor of $n$.

Let $f(x)$ be the polynominal of degree $d$ selected to construct the field $\mathbf{Q}(z)$.

$m$: $f(m) \equiv 0 \pmod{n}$.

Let $\mathbf{Z}(z)$ be the ring of integers in $\mathbf{Q}(z)$.

There is a ring homomorphism $\phi:\ \mathbf{Z}(z) \to \mathbf{Z}_n$,

$$\phi(z) = (m \bmod n).$$

$$\phi\left(\sum_{i=0}^{d-1} a_i z^i\right) = \left(\sum_{i=0}^{d-1} a_i m^i \bmod n\right).$$

$$\phi(y^2) = \prod_{(a,b)\in S} \phi(a+bz) = \prod_{(a,b)\in S} a + bm = x^2 \bmod n.$$

**Find $f(x)$, and $m$**

1. select a degree $d$, $2^{d^2} < n$.

2. let $m = \left[ n^{1/d} \right]$.

3. write $n = \sum_{i=0}^{d} c_i m^i$, $0 \leq c_i < m$.

4. $f(x) = \sum_{i=0}^{d} c_i x^i$.

1. $c_d = 1$, $c_{d-1} \leq d$.

2. $|\Delta(f)| < d^{2d} n^{2-3/d}$, where $\Delta$ is the discriminant of $f$.

## Compute $S$

1. construct a factor basis $B_1$ for $\mathbf{Z}_n$.

2. construct a factor basis $B_2$ for $\mathbf{Q}(z)$.

3. select a range $u$, and let
   $U = \{(a, b) \mid \gcd(a, b) = 1, \ |a| \leq u, \ 0 < b \leq u\}$.

4. find a subset $T = \{(a, b) \in U \mid$
   $a + bm$ is $b_1$-smooth and $a + bz$ is $b_2$-smooth$\}$.

5. find a subset $S = \{(a, b) \in T\}$ such that the
   sum of each exponent is even.

## An Example

$n = 1333$, $d = 3$,
$m = \left[n^{1/d}\right] = \left[1333^{1/3}\right] = [11.00550...] = 11$

$1333 = 11^3 + 2$, $f(x) = x^3 + 2$, $\sqrt[3]{-2}$ is a root of $f(x) = 0$.

factorization is unique in $\mathbf{Q}(\sqrt[3]{-2})$.

units are: $(1 + \sqrt[3]{-2})^k$, $k = 1, 2, \ldots$

$B_1 = \{-1, 2, 3, 5, 7\}$, $B_2 = \{-1, U, A, B, C, D, E, F\}$, where
$U = [1, 1, 0]$, $A = [0, 1, 0]$, $B = [-1, 1, 0]$,
$C = [1, 0, 1]$, $D = [1, 1, -1]$, $E = [1, -2, 0]$,
$F = [3, 0, -1]$

$T =$

| $(a,b)$ | $-1$ | $2$ | $3$ | $5$ | $7$ | $-1$ | $U$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
|---------|------|-----|-----|-----|-----|------|-----|-----|-----|-----|-----|-----|-----|
| $(-7,1)$ | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| $(-4,1)$ | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| $(-1,1)$ | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $(-1,3)$ | 0 | 5 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| $(1,-2)$ | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| $(2,3)$ | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| $(5,4)$ | 0 | 0 | 0 | 0 | 2 | 1 | 3 | 0 | 1 | 0 | 0 | 0 | 0 |
| $(7,3)$ | 0 | 3 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 |

$S = \{(-1,1),(5,4),(7,3)\}$

$$\prod_{(a,b)\in S} a + bm = 2 \cdot 5 \cdot 7^2 \cdot 2^3 \cdot 5 = (2^2 \cdot 5 \cdot 7)^2 = 140^2$$

$$\prod_{(a,b)\in S} a + bz = (U^2 \cdot [-1,1,0] \cdot [1,-2,0])^2 = [1,5,3]^2$$

$\phi([1,5,3]^2) = (\phi()[1,5,3])^2 =$
$(1 + (5)11 + (3)11^2])^2 = 419^2$

$140^2 \equiv 419^2 \bmod 1333$

$d = \mathsf{gcd}(419 - 140, 1333) = 31$ is a factor of 1333