MPRI – Cours 2.12.2

F. Morain

The Number Field Sieve

2019/10/22

The slides are available on `http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI/2019`

I. Quadratic fields as examples of number fields.

II. Factorization in (euclidean) quadratic fields.

III. NFS.

Bibliography

Z. I. Borevitch and I. R. Chafarevitch.
Théorie des nombres. Gauthiers-Villars, Paris, 1967.

I. N. Stewart and D. O. Tall.
Algebraic number theory.
Chapman and Hall, London, New-York, 2nd edition, 1987.

M. Pohst and H. Zassenhaus.
Algorithmic algebraic number theory.
Cambridge Univ. Press, 1989.

H. Cohen.
A course in algorithmic algebraic number theory, volume 138 of *Graduate Texts in Mathematics*.
Springer–Verlag, 1996. Third printing.

H. Cohen.
Advanced topics in computational number theory, volume 193 of *Graduate Texts in Mathematics*.
Springer-Verlag, 2000.

I. Quadratic fields as examples of number fields

A) Definitions and properties

$d \in \mathbb{Z} - \{1\}$ **squarefree**

Def. $K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d}, a, b \in \mathbb{Q}\}$.

Prop. K is a field extension of degree 2 of $\mathbb{Q}$, i.e., a vector space of dimension 2 over $\mathbb{Q}$.

Proof: since $\sqrt{d} \notin \mathbb{Z}$, $a + b\sqrt{d}$ is invertible for $(a, b) \neq (0, 0)$.
A basis of $K/\mathbb{Q}$ is $\{1, \sqrt{d}\}$. Addition/subtraction is done componentwise, multiplication by scalar easy. $\square$

Rem. More generally, a number field is $\mathbb{Q}[X]/(f(X))$ with $f(X) \in \mathbb{Z}[X]$, $f(X)$ irreducible. Here, $f(X) = X^2 - d$.

Conjugates, etc.

Def. Conjugate of $\alpha = a + b\sqrt{d}$ is $\alpha' = a - b\sqrt{d}$;
norm: $\mathrm{N}(\alpha) = \alpha\alpha' = a^2 - db^2$
trace: $\mathrm{Tr}(\alpha) = \alpha + \alpha' = 2a$).

Prop.
(i) $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$;
(ii) $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$;
(iii) $\mathrm{N}(x) = 0 \Leftrightarrow x = 0$.

Prop. K has two $\mathbb{Q}$-automorphisms, Id and conjugation $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.

Minimal polynomial

Def. Minimal polynmial $M_\alpha(X)$ of $\alpha = a + b\sqrt{d}$ is the monic P of minimal degree s.t. $P(a + b\sqrt{d}) = 0$.
Prop. Let $\alpha = a + b\sqrt{d}$.
(i) If $b = 0$, $M_\alpha(X) = X - a$; if $b \neq 0$, then

$$M_\alpha(X) = X^2 - 2aX + a^2 - db^2.$$

(ii) All $Q(X) \in \mathbb{Q}[X]$ s.t. $Q(\alpha) = 0$ is a multiple of M_α in $\mathbb{Q}[X]$.
Proof.
(i) For $b \neq 0$, $\alpha \notin \mathbb{Q}$, hence $\deg(M_\alpha(X)) > 1$.
Let's try $P(X) = AX^2 + BX + C$:

$$A(a^2 + db^2) + Ba + C = 0, \quad 2Aab + Bb = 0$$

from which

$$P(X) = A(X^2 - 2aX + a^2 - db^2).$$

(ii) use euclidean division of polynomials (classical).□

Algebraic integers

Def. An element of $K = \mathbb{Q}(\sqrt{d})$ is an algebraic integer iff it satisfies a monic algebraic equation with coeffcients in $\mathbb{Z}$. These numbers form $\mathcal{O}_K$.

Rem. Generalizes the concept of integers in $\mathbb{Q}$.

Thm. $\mathcal{O}_K$ is a commutative ring with unit.

Thm. $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ iff $M_\alpha(X) = X^2 - 2aX + a^2 - db^2 \in \mathbb{Z}[X]$, equivalently $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}$.

Rem. Very general results for any number field.

A basis for $\mathcal{O}_K$ (1/2)

Thm. $\mathcal{O}_K = \mathbb{Z}[\omega] = \{a + b\omega; a \in \mathbb{Z}, b \in \mathbb{Z}\}$ where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \bmod 4, \\ \dfrac{1 + \sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Ex.
1. $d = -1 : K = \mathbb{Q}(i)$; $\mathcal{O}_K = \mathbb{Z}[i]$;
2. $d = 2 : \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$;
3. $d = 5 : \mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{5})/2]$.

Rem. Not all number fields have integral power basis. For instance, this is almost never the case for $\mathbb{Q}(\sqrt[3]{d})$.

A basis for $\mathcal{O}_K$ (2/2)

Proof: let $x = a + b\sqrt{d} \in \mathcal{O}_K$. $\exists u, h$ in $\mathbb{Z}$. s.t.

$$\mathrm{Tr}(x) = 2a = u, \quad \mathrm{N}(x) = a^2 - db^2 = h.$$

$\Rightarrow 4db^2 = u^2 - 4h$, or $d(2b)^2 \in \mathbb{Z}$.
$\Rightarrow 2b = v$ with $v \in \mathbb{Z}$, from which

$$u^2 - dv^2 = 4h \equiv 0 \pmod 4.$$

u is even $\Rightarrow$ v even, since $d \not\equiv 0 \pmod 4$.
u is odd $\Rightarrow$ v odd, only if $d \equiv 1 \bmod 4$. If yes, $u = 2u' + 1$, $v = 2v' + 1$ and

$$a + b\sqrt{d} = \frac{2u'+1}{2} + \sqrt{d}\frac{2v'+1}{2} = (u' - v') + (2v' + 1)\omega.$$

Converse true using elementary calculations. $\square$

Discriminant

Def. The *discriminant* of $[\alpha_1, \alpha_2] = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z}$ with $\alpha_i \in \mathcal{O}_K$ is

$$\mathrm{Disc}([\alpha_1, \alpha_2]) = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \sigma(\alpha_1) & \sigma(\alpha_2) \end{vmatrix}^2.$$

Prop. The *discriminant* D of K is the discriminant of $[1, \omega]$, i.e., $D = d$ if $d \equiv 1 \bmod 4$ and $D = 4d$ otherwise.

B) Units

Def. unit $=$ invertible element in $\mathcal{O}_K$.

Prop. $\mathcal{U} = \{x \text{ unit}\} = \{x \in \mathcal{O}_K, \mathrm{N}(x) = \pm 1\}$; $\mathcal{U}$ is a multiplicative group.

Proof: If x is invertible in $\mathcal{O}_K$: $xy = 1$ and

$$\mathrm{N}(xy) = 1 = \mathrm{N}(x)\mathrm{N}(y)$$

and $\mathrm{N}(x)$ is in $\mathbb{Z}$.
If $x = a + b\sqrt{d}$ has norm $\epsilon = \pm 1$, its inverse is $\epsilon(a - b\sqrt{d})$. $\square$

Thm. (Dirichlet) Let $f(X) \in \mathbb{Q}(X)$ with r_1 real roots and $2r_2$ complex roots. Then $\mathcal{U} = \{\pm 1\} \times \mathbb{Z}^{r_1 + r_2 - 1}$.

Rem. All units can be of norm 1, or not; $\mathcal{U}^+$ is either the full $\mathcal{U}$, or a subgroup of index 2.

The case of imaginary quadratic fields ($d < 0$)

Thm. If $d = -1$, $\#\mathcal{U} = 4$; if $d = -3$, $\#\mathcal{U} = 6$; otherwise $\#\mathcal{U} = 2$.
Proof: Write $d = -d' < 0$; $\varepsilon = a + b\omega$ is a unit iff

$$\mathrm{N}(\varepsilon) = \mathrm{N}(a + b\omega) = \pm 1, \text{ with } a, b \in \mathbb{Z}.$$

If $d \equiv 2, 3 \pmod 4$, $d' \equiv 2, 1 \pmod 4$ and $\mathrm{N}(a + b\omega) = a^2 - db^2 = a^2 + d'b^2 = \pm 1$. Only $+1$ is possible and as soon as $d' \geq 2$, the only solution is $\varepsilon = \pm 1$. If $d' = 1$, $\mathcal{U} = \{\pm 1, \pm i\}$.
If $d \equiv 1 \pmod 4$, $d' \equiv 3 \pmod 4$ and $\mathrm{N}(a + b\omega) = (a + \frac{b}{2})^2 + \frac{b^2}{4}d' = +1$. If $d' = 3$, solutions are $b = 0$, $a = \pm 1$ and $b = \pm 1$, $a = \pm\frac{1}{2} - \frac{b}{2}$, and $\mathcal{U} = \left\{\left(\frac{1+i\sqrt{3}}{2}\right)^m, 0 \leq m \leq 5\right\}$. If $d' > 3$ (i.r., $d' \geq 7$), the only solution is $a = \pm 1$, $b = 0$. $\square$

The case of real quadratic fields ($d > 0$)

Thm. $\mathcal{U} = \{\pm 1\} \times \mathbb{Z}$. There exists a unit $\varepsilon > 1$, the fundamental unit, s.t. all $\eta \in \mathcal{U}$ can be written $\eta = \pm\varepsilon^m$ with $m \in \mathbb{Z}$.

Rem. in fact, $\varepsilon = \min\{u \in \mathcal{U}, u > 1\}$.

Rem. the fundamental unit is computed using the Pell Fermat equation, or $x^2 - dy^2 = \pm 1$ or ± 4. It can be solved using continued fractions.

C) Factoring in $\mathcal{O}_K$

Goal: generalize factorization over $\mathbb{Z}$.

Be careful: units are trouble shooters and deserve a special treatment. Unique factorization is rather rare.

Def. $x \in \mathcal{O}_K$ is irreducible iff x is not a unit and $x = yz$ implies y or z is a unit.

Ex. In $K = \mathbb{Q}(\sqrt{-5})$, let us prove that 2 is irreducible.
If $2 = yz$, we get $4 = \mathrm{N}(y)\mathrm{N}(z)$, therefore $\mathrm{N}(y) \mid 4$. Write $y = u + v\sqrt{-5}$, of norm

$$\mathrm{N}(u + v\sqrt{-5}) = u^2 + 5v^2.$$

The number 2 cannot be a norm and the only possible solution are ± 2 of norm 4. Therefore $\mathrm{N}(y) = 1$ (and y is a unit) or $\mathrm{N}(y) = 4$ (and z is a unit).

Associates

Def. $x, x' \in \mathcal{A}$ are associate iff there is some unit u s.t. $x' = ux$. Association is an equivalence relation.

Prop. If x is irreducible in $\mathcal{A}$ and x' associate of x, then x' is irreducible in $\mathcal{A}$.

Def. π in $\mathcal{A}$ is prime iff $\pi \mid \alpha\beta$ implies $\pi \mid \alpha$ or $\pi \mid \beta$.

Thm. A prime number is irreducible.

Proof: let x be prime, written as $x = ab$. We have $x \mid a$ or $x \mid b$. If $x \mid a$, one has $a = xc$ with c in $\mathcal{A}$. We get $a(1 - bc) = 0$ and since $a \neq 0$, $1 = bc$ and b is a unit. $\square$

Ex. (cont'd) One has

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

2 is irreducible, but not prime, because 2 doesn't divide any of $1 \pm \sqrt{-5}$: $\mathrm{N}(2) = 4$, but $\mathrm{N}(1 \pm \sqrt{-5}) = 6$.

Factoring over a number field: general theorems

The integer ring of a number field has the so-called Noetherian property.

Thm. If $\mathcal{A}$ is Noetherian, all elements can be written as a finite product of irreducible elements.

Thm. The Noetherian ring $\mathcal{A}$ has unique factorization iff irreducible implies prime.

Thm. If $\mathcal{A}$ is principal, factorization is unique.

Thm. If $\mathcal{A}$ is euclidean, it is principal (copy the proof for $\mathbb{Z}$).

Euclidean rings

Def. $\mathcal{A}$ is euclidean iff there exists $\phi : \mathcal{A}^\times \to \mathbb{N}$ s.t. for $x, y \in \mathcal{A}^\times$:

- $x \mid y \Rightarrow \phi(x) \leq \phi(y)$;
- $\exists q, r \in \mathcal{A}^\times, x = yq + r$, with $r = 0$ or $\phi(r) < \phi(y)$.

This is rather rare.

Thm. If $d < 0$, $\mathcal{O}_K$ is euclidean iff $d \in \{-1, -2, -3, -7, -11\}$.

Thm. If $d > 0$, $\mathcal{O}_K$ is euclidean iff

$$d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

II. Factorization in (euclidean) quadratic fields

We consider the case where $\mathbb{Q}(\sqrt{d})$ is euclidean.

Thm. Let d be such that $\mathbb{Q}(\sqrt{d})$ is euclidean and p be a rational prime.

(a) If $\left(\frac{d}{p}\right) = -1$, p is irreducible in $\mathcal{O}_K$ and p is unramified.

(b) If $\left(\frac{d}{p}\right) = 1$, $p = u\pi_p\pi_p'$ with $u \in \mathcal{U}$, $\pi_p = x - y\sqrt{d}$ and $\pi_p' = x + y\sqrt{d}$ are two irreducible non associate factors in $\mathcal{O}_K$; p splits.

(c) If $\left(\frac{d}{p}\right) = 0$, $p = u(x + y\sqrt{d})^2$ where $x + y\sqrt{d}$ is irreducible in $\mathcal{O}_K$ and $u \in \mathcal{U}$; p is ramified.

Rem. For small p's, any trivial algorithm will work.

A numerical example: $\mathbb{Q}(\sqrt{6})$

Fundamental unit: $\varepsilon = 5 + 2\sqrt{6}$.

$$2 = -(2+\sqrt{6})(2-\sqrt{6}) = (5-2\sqrt{6})(2+\sqrt{6})^2 = \varepsilon^{-1}(2+\sqrt{6})^2.$$

Let's factor $\xi = 1010 + 490\sqrt{6}$. We first have

$$\mathrm{N}(\xi) = 1010^2 - 6 \cdot 490^2 = -420500 = -2^2 \cdot 5^3 \cdot 29^2,$$

$5 = -(1+\sqrt{6})(1-\sqrt{6})$, $29 = -(5+3\sqrt{6})(5-3\sqrt{6})$; therefore

$$\xi = u(2+\sqrt{6})^{\alpha}(1+\sqrt{6})^{\gamma_1}(1-\sqrt{6})^{\delta_1}(5+3\sqrt{6})^{\gamma_2}(5-3\sqrt{6})^{\delta_2}.$$

$$\begin{array}{ll}
\alpha = 2, & \xi_1 = \frac{\xi}{(2+\sqrt{6})^2} = -415 + 215\sqrt{6} \\
\gamma_1 = 1, & \xi_2 = \frac{\xi_1}{1+\sqrt{6}} = 341 - 126\sqrt{6} \\
\delta_1 = 2, & \xi_3 = \frac{\xi_2}{(1-\sqrt{6})^2} = 35 - 8\sqrt{6} \\
\gamma_2 = 2, & \xi_4 = \frac{\xi_3}{(5+3\sqrt{6})^2} = 5 - 2\sqrt{6} \\
\gamma_3 = 0, & u = \xi_4 = \varepsilon^{-1}
\end{array}$$

$$\xi = \varepsilon^{-1}(2+\sqrt{6})^2(1+\sqrt{6})(1-\sqrt{6})^2(5+3\sqrt{6})^2.$$

III. NFS

Pollard's idea: let $f(X) \in \mathbb{Z}[X]$ and m s.t.

$$f(m) \equiv 0 \bmod N.$$

Let θ be a root of f in $\mathbb{C}$ and $K = \mathbb{Q}[X]/(f(X)) = \mathbb{Q}(\theta)$.
To simplify things: $\mathcal{O}_{\mathbf{K}}$ is supposed to be $\mathbb{Z}[\theta]$ and euclidean. Let

$$\begin{array}{rccc}
\phi : & \mathbb{Z}[\theta] & \to & \mathbb{Z}/N\mathbb{Z} \\
 & \theta & \mapsto & m \bmod N.
\end{array}$$

ϕ is a ring homomorphism.
Look for algebraic integers of the form $a - b\theta$ s.t.

$$a - b\theta = \prod_{\pi \in \mathcal{B}_K} \pi^{v_\pi(a-b\theta)}$$

where $v_\pi(a - b\theta) \in \mathbb{Z}$ and

$$a - bm = \prod_{p \in \mathcal{B}} p^{w_p(a-bm)}$$

with $\mathcal{B}$ a prime basis and $w_p(a - bm) \in \mathbb{Z}$.

NFS: basic idea (cont'd)

We then look for $\mathcal{A}$ s.t.

$$\prod_{(a,b)\in\mathcal{A}} (a - b\theta)$$

is a square in $\mathcal{O}_K$ and at the same time

$$\prod_{(a,b)\in\mathcal{A}} (a - bm)$$

is a square in $\mathbb{Z}$. Then

$$\prod_{(a,b)\in\mathcal{A}} (a - bm) = Z^2, \quad \prod_{(a,b)\in\mathcal{A}} (a - b\theta) = (A - B\theta)^2.$$

Applying ϕ, we get:

$$\phi((A - B\theta)^2) \equiv (A - Bm)^2 \equiv Z^2 \bmod N$$

and $\gcd(A - Bm \pm Z, N)$ might factor N.

Numerical example

Let's factor $N = 5^8 - 6 = 390619 = m^2 - 6$ (surprise!) with $m = 5^4 = 625$, hence we will work in $\mathbb{Q}(\theta) = \mathbb{Q}[X]/(f(X))$ with $f(X) = X^2 - 6$ and $\theta = \sqrt{6}$.

Rational basis: $\mathcal{B} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$.

Algebraic basis: $\mathcal{B}_K$ given as

p	c_p	π, π'
2	0	$2 + \theta = \pi_2$
3	0	$3 + \theta = \pi_3$
5	± 1	$1 + \theta = \pi_5, 1 - \theta = \pi'_5$
19	± 5	$5 + \theta = \pi_{19}, 5 - \theta = \pi'_{19}$
23	± 11	$1 + 2\theta = \pi_{23}, 1 - 2\theta = \pi'_{23}$
29	± 8	$5 + 3\theta = \pi_{29}, 5 - 3\theta = \pi'_{29}$

with c_p s.t. $f(c_p) \equiv 0 \bmod p$. All these obtained via factoring of $\mathrm{N}(a - b\theta)$ for small a's and b's.

Free relations: $2 = \varepsilon^{-1}(2 + \theta)^2$, or $5 = -\pi_5\pi'_5$.

Sieving

$\mathrm{N}(a - b\theta) = a^2 - 6b^2 = b^2 f(a/b)$.

Function *Sieve*(F, A, B)
- **for** $b = 1$ **to** B **do**
  - **for** $a = -A$ **to** $A - 1$ **do**
    - $T[a] \leftarrow a^2 - 6b^2$;
  - **for** $p \in \mathcal{B}$ **do**
    - **for** c_p *root of* $f \bmod p$ **do**
      - $x \leftarrow$ smallest $z \equiv bc_p \bmod p$ and $z \geq -A$;
      - **while** $x \leq A$ **do**
        - $T[x] \leftarrow T[x]/p$;
        - $x \leftarrow x + p$;
  - **for** $a = -A$ **to** $A - 1$ **do**
    - **if** $T[a] = \pm 1$ **then**
      - refactor $a^2 - 6b^2$ over $\mathcal{B}$;
      - store relation if needed;

Results for $|a| \leq 60$, $1 \leq b \leq 30$

rel	a	b	$N(a - b\theta)$	$a - b\theta$	$a - bm$
L_1	2	0	2^2	$\varepsilon^{-1} \cdot \pi_2^2$	2
L_2	3	0	3^2	$\varepsilon^{-1} \cdot \pi_3^2$	3
L_3	5	0	5^2	$-\pi_5 \cdot \pi'_5$	5
L_4	19	0	19^2	$\pi_{19} \cdot \pi'_{19}$	19
L_5	23	0	23^2	$-\pi_{23} \cdot \pi'_{23}$	23
L_6	29	0	29^2	$-\pi_{29} \cdot \pi'_{29}$	29
L_7	-21	1	$3 \cdot 5 \cdot 29$	$-\varepsilon^{-1} \cdot \pi_3 \cdot \pi_5 \cdot \pi_{29}$	$-2 \cdot 17 \cdot 19$
L_8	-12	1	$2 \cdot 3 \cdot 23$	$-\varepsilon^{-1} \cdot \pi_2 \cdot \pi_3 \cdot \pi_{23}$	$-7^2 \cdot 13$
L_9	-5	1	19	$-\pi_{19}$	$-2 \cdot 3^2 \cdot 5 \cdot 7$
L_{10}	-2	1	-2	$-\pi_2$	$-3 \cdot 11 \cdot 19$
L_{11}	0	1	$-2 \cdot 3$	$-\varepsilon^{-1} \cdot \pi_2 \cdot \pi_3$	-5^4
L_{12}	1	1	-5	π'_5	$-2^4 \cdot 3 \cdot 13$
L_{13}	4	1	$2 \cdot 5$	$\varepsilon^{-1} \cdot \pi_2 \cdot \pi_5$	$-3^3 \cdot 23$

More results

rel	a	b	$N(a-b\theta)$	$a-b\theta$	$a-bm$
L_{14}	9	1	$3\cdot 5^2$	$\varepsilon^{-1}\cdot\pi_3\cdot\pi_5^2$	$-2^3\cdot 7\cdot 11$
L_{15}	16	1	$2\cdot 5^3$	$-\pi_2\cdot\pi_5'^3$	$-3\cdot 7\cdot 29$
L_{16}	-10	3	$2\cdot 23$	$\pi_2\cdot\pi'_{23}$	$-5\cdot 13\cdot 29$
L_{17}	5	3	-29	π'_{29}	$-2\cdot 5\cdot 11\cdot 17$
L_{18}	13	3	$5\cdot 23$	$\pi'_5\cdot\pi'_{23}$	$-2\cdot 7^2\cdot 19$
L_{19}	1	4	$-5\cdot 19$	$-\pi_5\cdot\pi'_{19}$	$-3\cdot 7^2\cdot 17$
L_{20}	25	4	23^2	$\pi_{23}'^2$	$-3^2\cdot 5^2\cdot 11$
L_{21}	-11	5	-29	$\varepsilon\cdot\pi'_{29}$	$-2^6\cdot 7^2$
L_{22}	-7	9	$-19\cdot 23$	$\pi_{19}\cdot\pi'_{23}$	$-2^9\cdot 11$
L_{23}	-27	11	3	$-\varepsilon\cdot\pi_3$	$-2\cdot 7\cdot 17\cdot 29$
L_{24}	-2	11	$-2\cdot 19^2$	$-\pi_2\cdot\pi_{19}'^2$	$-13\cdot 23^2$
L_{25}	33	13	$3\cdot 5^2$	$\varepsilon^{-1}\cdot\pi_3\cdot\pi_5'^2$	$-2^2\cdot 7\cdot 17^2$

The associated matrix

	u_0	ε	π_2	π_3	π_5	π'_5	π_{19}	π'_{19}	π_{23}	π'_{23}	π_{29}	π'_{29}	2	3	5	7	11	13	17	19	23	29
L_1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
L_2	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
L_3	1	0	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
L_4	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0
L_5	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0
L_6	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1
L_7	0	1	0	1	1	0	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	0
L_8	0	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0
L_9	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0
L_{10}	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0
L_{11}	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L_{12}	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
L_{13}	1	1	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0

$\ldots$

Some dependency relation

$L_3\cdot L_6\cdot L_7\cdot L_{10}\cdot L_{15}\cdot L_{17}\cdot L_{25}$ yields

$$\phi\left((5+2\theta)^{-1}(2+\theta)(3+\theta)(1+\theta)(1-\theta)^3(5+3\theta)(5-3\theta)\right)^2$$

$$\equiv\left(2^2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 17^2\cdot 19\cdot 29\right)^2 \pmod{N}$$

and

$$2^2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 17^2\cdot 19\cdot 29\equiv 148603 \pmod{N},$$

gives $242016^2\equiv 148603^2 \bmod N$ and $\gcd(242016-148603,N)=1$,
$L_1\cdot L_2\cdot L_3\cdot L_4\cdot L_9\cdot L_{10}\cdot L_{14}\cdot L_{15}\cdot L_{19}\cdot L_{23}$ leads to

$$\phi\left((5+2\theta)^{-1}(2+\theta)^2(3+\theta)^2(1+\theta)^2(1-\theta)^2(5+\theta)(5-\theta)\right)^2$$

$$\equiv\left(2^3\cdot 3^3\cdot 5\cdot 7^3\cdot 11\cdot 17\cdot 19\cdot 29\right)^2 \pmod{N}$$

or $61179^2\equiv 81314^2 \bmod N$, $\gcd(61179-81314,N)=4027$.

Working without units

We can use factorization modulo units. We will end up with relations

$$\mathrm{N}(A+B\sqrt{6})=\varepsilon^m=1$$

and hope to get a square.

If we don't know ε, we can try to extract a squareroot of

$$\eta=A+B\sqrt{6}$$

using brute force: $\eta=\xi^2=(x+y\sqrt{6})^2$, or:

$$\begin{cases} x^2-6y^2 &= \pm 1\\ x^2+6y^2 &= A\end{cases}$$

which readily gives $x^2=(A\pm 1)/2$ which is easily solved over $\mathbb{Z}$.

Over a general number field, computing units is in general difficult, and some workaround has been found.

A bit of complexity

SNFS: $N = r^e \pm s$ with r and s small.
Choose an extension of degree d. Put $k = \lceil e/d \rceil$, $m = r^k$ and $c = sr^{kd-e}$ s.t. $m^d \equiv c \bmod N$. Put $f(X) = X^d - c$ and use $K = \mathbb{Q}(X)/(f(X)) = \mathbb{Q}(\theta)$.

$$\mathrm{N}(a - b\theta) = b^d f(a/b).$$

For $0 \leq \alpha \leq 1$ and $\beta > 0$, we define $L_N[\alpha, \beta] = \exp((\beta + o(1))(\log n)^\alpha (\log\log n)^{1-\alpha})$, sometimes simplified to $L_N[\alpha]$.

Thm. The computing time is $L_N[1/2, \sqrt{2/d}]$.

Thm. Let d vary with N as:

$$d = K(\log N)^\varepsilon (\log\log N)^{1-\varepsilon}.$$

Optimal values are $\varepsilon = 1/3$, $K = (2/3)^{-1/3}$

$$L_N[1/3, \exp(2(2/3)^{2/3})].$$

GNFS

For a general N, we need $f(X)$ representing N and f is not sparse, nor “small”.
Basic thing is to write N in base m for $m \approx N^{1/d}$ and

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0.$$

Conj. GNFS has cost $L_N[1/3, (64/9)^{1/3}]$ for optimal d as function of N.

Some problems:

- A lot of effort was put in searching for

$$f(X) = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_0$$

  with $a_i \approx N^{1/(d+1)}$ and a_i “small” with many properties.
- Properties related to units and/or factorization solved using characters (Adleman). See LNM 1554 for details.
- As usual, linear algebra causes some trouble.

RSA-768 with NFS

- **Who?** Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann.
- **Sieving:** August 2007 til April 2009 (about 1500 AMD64 years), several countries/continents. 64 334 489 730 relations (38% INRIA, 30% EPFL, 15% NTT, 8% Bonn, 3.5% CWI, 5.5% others).
- **Linear algebra** (after filtering): $192\,796\,550 \times 192\,795\,550$ (total weight 27 797 115 920) using 155 core years in 119 calendar days (block Wiedemann in parallel).

Conclusions

- A broad view of integer factorization.
- Programs are now available (cado-nfs, GMP-ECM).
- discrete log algorithms as companions to integer factorization.