

## III. Integer factorization – NFS






2007/10/01

- I. Quadratic fields as examples of number fields
- II. NFS using quadratic fields
- III. Some ideas on the general case
- IV. Discrete logarithm
- V. Conclusions

## I. Quadratic fields as examples of number fields

- A) Definitions and properties
- B) Units
- C) Factoring in  $\mathcal{O}_K$

## Good algebraic reading

-  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.

## A) Definitions and properties

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

**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**  $N(\alpha) = \alpha\alpha' = a^2 - db^2$  (resp. **trace**  $\text{Tr}(\alpha) = \alpha + \alpha' = 2a$ ).

**Prop.**

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

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

## Algebraic integers

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

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

**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  $\text{Tr}(\alpha), N(\alpha) \in \mathbb{Z}$ .

**Rem.** Very general results for any number field.

## Minimal polynomial

**Def. Minimal polynomial**  $M_\alpha(X)$  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  $M_\alpha$  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).  $\square$

## Gauss's Lemma

**Lem.** Let  $P(X) \in \mathbb{Z}[X]$  that can be written  $Q(X)R(X)$  with  $Q, R \in \mathbb{Q}[X]$ . There exists  $\lambda \in \mathbb{Q}^*$  s.t.  $\lambda Q, \lambda^{-1}R$  are in  $\mathbb{Z}[X]$ .

**Proof:** multiply by lcm of coefficients of  $Q$  and  $R$  to get

$$nP = Q'R'$$

for integer  $n \in \mathbb{Z}$  and  $Q', R'$  in  $\mathbb{Z}[X]$ .

**Claim:** if the prime  $p \mid n$ , then  $p$  divides all coefficients of  $Q'$  or all coefficients of  $R'$ .

If yes, divide by all primes  $p \mid n$  and end up with  $Q'', R''$  in  $\mathbb{Z}[X]$  s.t.  $P = Q''R''$  and  $Q = \lambda Q'', R = \lambda^{-1}R''$ .

**Proof of the claim:** write  $Q'(X) = q_0 + q_1X + \dots + q_uX^u$ ,  $R'(X) = r_0 + r_1X + \dots + r_vX^v$ .

If  $p$  does not divide all  $q_i$  or all  $r_j$ , let  $q_i$  and  $r_j$  the first two coefficients non divisible by  $p$ .

The coefficient of  $X^{i+j}$  in  $Q'R'$  is

$$q_0r_{i+j} + q_1r_{i+j-1} + \dots + q_{i-1}r_{j+1} + q_i r_j + q_{i+1}r_{j-1} + \dots + q_{i+j}r_0.$$

All terms are divisible by  $p$  except  $q_i r_j$ , contradiction.  $\square$

If  $M_\alpha(X) \in \mathbb{Z}[X]$ ,  $\alpha \in \mathcal{O}_K$ .

Conversely:  $M_\alpha(X) \mid P_\alpha(X)$  in  $\mathbb{Q}[X]$ .

By Gauss: there exists  $\lambda \in \mathbb{Q}^*$  s.t.  $\lambda M_\alpha(X) \in \mathbb{Z}[X]$  and divides  $P_\alpha(X)$  in  $\mathbb{Z}[X]$ .

Since  $M_\alpha$  is monic,  $\lambda M_\alpha(X) \in \mathbb{Z}[X]$  implies  $\lambda \in \mathbb{Z}$ .

Since  $P_\alpha$  is monic, and  $\lambda M_\alpha(X)$  divides  $P_\alpha(X)$  in  $\mathbb{Z}[X]$ , we get  $|\lambda| = 1$  and  $M_\alpha(X) \in \mathbb{Z}[X]$ .  $\square$

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

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

**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  $\mathbb{Q}(\sqrt[3]{d})$ .

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

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

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

$$\Rightarrow 2b = v \text{ with } v \in \mathbb{Z}, \text{ from which}$$

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

$u$  is even  $\Rightarrow v$  even, since  $d \not\equiv 0 \pmod{4}$ .

$u$  is odd  $\Rightarrow v$  odd, only if  $d \equiv 1 \pmod{4}$ . 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.  $\square$

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

**Proof:** let's prove stability. Let  $\alpha = a + b\omega$  and  $\beta = e + f\omega$  with  $a, b, e, f \in \mathbb{Z}$ :

$$\alpha + \beta = (a + e) + (b + f)\omega \in \mathcal{O}_K,$$

$$-\alpha = (-a) + (-b)\omega \in \mathcal{O}_K,$$

if  $d \equiv 2, 3 \pmod{4}$ ,

$$\alpha\beta = (a + b\sqrt{d})(e + f\sqrt{d}) = (ae + bfd) + (af + be)\sqrt{d} \in \mathcal{O}_K$$

and if  $d \equiv 1 \pmod{4}$ ,

$$\alpha\beta = \left(a + b\frac{1 + \sqrt{d}}{2}\right) \left(e + f\frac{1 + \sqrt{d}}{2}\right)$$

$$= \left(ae + bf\frac{d-1}{4}\right) + (af + be + bf)\frac{1 + \sqrt{d}}{2} \in \mathcal{O}_K. \square$$

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

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

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

## 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

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

If  $d \equiv 2, 3 \pmod{4}$ ,  $d' \equiv 2, 1 \pmod{4}$  and

$N(a + b\omega) = a^2 - db^2 = a^2 + d'b^2 = \pm 1$ . 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

$N(a + b\omega) = (a + \frac{b}{2})^2 + \frac{b^2}{4}d' = +1$ . 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.e.,  $d' \geq 7$ ), the only solution is  $a = \pm 1$ ,  $b = 0$ .  $\square$

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

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

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

$$N(xy) = 1 = N(x)N(y)$$

and  $N(x)$  is in  $\mathbb{Z}$ .

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

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

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

## 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 in a random ring  $\mathcal{A}$ .

**Def.**  $x \in \mathcal{A}$  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  $4 = N(y)N(z)$ , therefore  $N(y) \mid 4$ . Write  $y = u + v\sqrt{-5}$ , of norm

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

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

## 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 element 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  $\mathbb{Z}$ ).

## 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.**  $\pi$  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  $1 \pm \sqrt{-5}$ :  $N(2) = 4$ , but  $N(1 \pm \sqrt{-5}) = 6$ .

## Euclidean rings

**Def.**  $\mathcal{A}$  is **euclidean** iff there exists  $\phi : \mathcal{A}^\times \rightarrow \mathbb{N}$  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

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

# Factorization in quadratic fields

**Prop.** Let  $x \in \mathcal{O}_K$  of prime norm in  $\mathbb{Z}$ . Then  $x$  is irreducible.

**Proof:** assume  $x = yz$ . Let  $p = |N(x)|$ .  $p = |N(yz)| = |N(y)| |N(z)|$  implies one of  $y$  or  $z$  has norm 1.  $\square$

**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**.

(b) Admitted without proof (alternatively, use Cornacchia's algorithm, lattice reduction or quadratic form reduction). We do not need it for NFS (see later).

(c) [For  $\mathbb{Q}(\sqrt{6})$ :] by inspection, one finds  $3^2 - 6 \cdot 1^2 = -3$ . Therefore:

$$3 = -(3 + \sqrt{6})(3 - \sqrt{6}).$$

But  $\frac{3+\sqrt{6}}{3-\sqrt{6}} = 5 - 2\sqrt{6} = \varepsilon^{-1}$  and

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

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

**Rem.** To find factorization of the unit  $u = \pm\varepsilon^m$ , compute  $m$  as  $\frac{\log |u|}{\log \varepsilon}$  and check.

**Proof:** (a)

**Lem.**

$$\forall x, y \in \mathbb{Z}, \quad |x^2 - dy^2| \neq p.$$

**Proof:** If not, then  $p \mid y \Rightarrow p \mid x \Rightarrow p^2 \mid x^2 - dy^2 = \pm p$ .  
If  $p \nmid y$ ,  $(xy^{-1})^2 \equiv d \pmod{p}$ , which is impossible.  $\square$

Assume  $p = u\rho_1\rho_2 \dots \rho_k$  for irreducible  $\rho_i$ 's and  $u \in \mathcal{U}$ :

$$p^2 = N(p) = \pm \prod_{i=1}^k N(\rho_i).$$

$\Rightarrow N(\rho_i) = \pm p_i^{\alpha_i}$  with  $\alpha_i \leq 2$ . But  $\alpha_i = 1$  is impossible and  $\alpha_i = 0$  also. Hence  $\alpha_i = 2$ ,  $k = 1$  and  $p = u\rho_1$  is associated with an irreducible element, therefore irreducible.

## II. NFS using quadratic fields

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

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

Let  $\theta$  be a root of  $f$  in  $\mathbb{C}$  and  $K = \mathbb{Q}[X]/(f(X)) = \mathbb{Q}(\theta)$ .

To simplify things:  $\mathcal{O}_K$  is supposed to be  $\mathbb{Z}[\theta]$  and euclidean. Let

$$\begin{aligned} \phi : \mathbb{Z}[\theta] &\rightarrow \mathbb{Z}/N\mathbb{Z} \\ \theta &\mapsto m \pmod{N}. \end{aligned}$$

$\phi$  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  $w_p(a - bm) \in \mathbb{Z}$ .

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  $\phi$ , we get:

$$\phi((A - B\theta)^2) \equiv (A - Bm)^2 \equiv Z^2 \pmod{N}$$

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

We need more than  $\text{Card}(\mathcal{B} \cup \mathcal{B}_K) = 22$  relations.

We need complete simultaneous factorizations of  $a - bm$  and  $N(a - b\theta)$  for  $\gcd(a, b) = 1$ .

**Step 0:** initialize  $T(a, b) = \log |a - bm|$ .

**Step 1:** For fixed  $b$ , subtract from  $T(a, b)$  the  $\log p$  for  $p \mid a - bm$ . Small values of  $T(a, b)$  are  $\mathcal{B}$ -smooth.

**Step 2:** Add  $\log |N(a - b\theta)| = \log |a^2 - 6b^2|$  to  $T(a, b)$ .

If  $p \mid a^2 - 6b^2$ , and  $p \mid b$ , then  $p \mid a$  (impossible); hence  $(ab^{-1})^2 \equiv 6 \pmod{p}$  and  $p \mid N(a - b\theta)$  iff there exists  $c_p$  a root of  $f$  s.t.

$a - bc_p \equiv 0 \pmod{p}$ . We sieve for all  $(p, c_p)$ .

Small values of  $T(a, b)$  are what we are looking for and we just need to factor them.

## 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

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

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

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

## 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	$\pi'_5$	$-2^4 \cdot 3 \cdot 13$
$L_{13}$	4	1	$2 \cdot 5$	$\varepsilon^{-1} \cdot \pi_2 \cdot \pi_5$	$-3^3 \cdot 23$

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	$\pi_{29}'$	$-2 \cdot 5 \cdot 11 \cdot 17$
$L_{18}$	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	$3 \cdot 5^2$	$\varepsilon^{-1} \cdot \pi_3 \cdot \pi_5'^2$	$-2^2 \cdot 7 \cdot 17^2$

	$u_0$	$\varepsilon$	$\pi_2$	$\pi_3$	$\pi_5$	$\pi_5'$	$\pi_{19}$	$\pi_{19}'$	$\pi_{23}$	$\pi_{23}'$	$\pi_{29}$	$\pi_{29}'$	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	1	0	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	1	1	0	0	0
$L_8$	0	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
$L_9$	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0
$L_{10}$	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	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	0	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

## Working without units

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

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

and hope to get a square.

If we don't know  $\varepsilon$ , 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.

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

$$\begin{aligned} &\phi((5 + 2\theta)^{-1}(2 + \theta)(3 + \theta)(1 + \theta)(1 - \theta)^3(5 + 3\theta)(5 - 3\theta))^2 \\ &\equiv (2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17^2 \cdot 19 \cdot 29)^2 \pmod{N} \end{aligned}$$

and

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

gives  $242016^2 \equiv 148603^2 \pmod{N}$  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

$$\begin{aligned} &\phi((5 + 2\theta)^{-1}(2 + \theta)^2(3 + \theta)^2(1 + \theta)^2(1 - \theta)^2(5 + \theta)(5 - \theta))^2 \\ &\equiv (2^3 \cdot 3^3 \cdot 5 \cdot 7^3 \cdot 11 \cdot 17 \cdot 19 \cdot 29)^2 \pmod{N} \end{aligned}$$

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



### III. Some ideas on the general case

- A) General number fields.
- B) SNFS.
- C) GNFS.

#### B) 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.  $m^d \equiv c \pmod N$ . Put  $f(X) = X^d - c$  and use  $K = \mathbb{Q}(X)/(f(X)) = \mathbb{Q}(\theta)$ .

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

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

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

### A) General number fields

$\mathcal{O}_K$  is not always  $\mathbb{Z}[\theta]$  for some algebraic integer  $\theta$ .

$\mathcal{U}$  can be hard to determine.

#### C) 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

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

**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

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

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.

## The current record: 2, 1039–

K. Aoki, J. Franke, T. Kleinjung, A. K. Lenstra, D. A. Osvik,  
2007/05/22.

We are pleased to announce the factorization of  
the 1039th Mersenne number (2,1039- in the  
Cunningham table) by SNFS.

The factorization is:

```
2^1039-1 = p7 * p80 * p227 where
p7      = 5080711
p80     = 55853666619936291260749204658315944968646527018488\
        637648010052346319853288374753
p227    = 20758181946442382764570481370359469516293970800739\
        52098812083870379272909032467938234314388414483488\
        25340533447691122230281583276965253760914101891052\
        41993899334109711624358962065972167481161749004803\
        659735573409253205425523689
```

The factor 5080711 was already known.

Lattice sieving with special-Q on the rational side.  
special-Q:

most of 123M < Q < 911M (about 40M Qs) [...]

factor base bound:

for Q < 300M: 300M on algebraic side,

ca. 0.9 Q on rational side

for Q > 300M: 300M on both sides [...]

large primes:

We accepted large primes up to 2<sup>38</sup>, but the  
parameters were optimised for large primes up  
to 2<sup>36</sup>. Most jobs attempted to split cofactors  
up to 2<sup>105</sup> (both sides), only doing the most  
promising candidates.

sieve area:

2<sup>16</sup> \* 2<sup>15</sup> for most special-Q

Yield:

16 570 808 010 relations

(84.1% NTT, 8.3% EPFL, 7.6% Bonn)

[Polynomial selection]

The following polynomial pair was used:

algebraic side:

$$f(x) = 2 * x^6 - 1$$

rational side:

$$g(x) = x - 2^{173}$$

[Sieving]

We spent 6 month calendar time for sieving.

Environment:

We used various PCs and clusters at EPFL,  
NTT and the University of Bonn.

Time:

Total sieving time is scaled to about 95  
Pentium D [3.0GHz] years. (also scaled to  
about 100 Athlon64/Opteron [2.2GHz] years.)

[Removal of duplicates and singletons, clique  
algorithm and filtering]

Environment:

This was done at PCs and at the cluster at NTT.

Time:

scaled to less than 2 Pentium D [3.0GHz] years  
or less than 7 calendar days

Uniqueness step:

< 10 days on one or two Opteron [2.0GHz] with 4GB  
16 570 808 010 raw relations from sieve  
2 748 064 961 duplicates (16.6%)  
13 822 743 049 unique relations

Removing singletons and clique algorithm:

less than 4 days on up to 113 Pentium D [3.0GHz]

755 746 955 relations

594 150 319 prime ideals

Filtering:

69 hours on 113 Pentium D [3.0GHz]

[Linear algebra]

Input matrix:

66 718 354 \* 66 718 154 (weight 9 538 688 635)

Algorithm:

block Wiedemann with 4\*64-bit block length

Environment:

110 \* Pentium D [3.0GHz], Gb Ethernet (NTT)

36 \* Dual Core2Duo [2.66GHz], Gb Ethernet (EPFL)

Time:

scaled to 59 days on 110 \* Pentium D [3.0GHz]

= 36 core years or 162 days on 32 \* Dual Core2Duo [3.0GHz]

= 56 core years [...]

Calendar time for block Wiedemann was 69 days. Most of the jobs were done at NTT and EPFL in parallel. However, there were some periods where no computation took place. Eliminating these periods the computation could have been done in less than 59 days. Finally, we got 50 solutions which gave via quadratic character tests 47 true solutions.

[Square root]

Algorithm:

Montgomery-Nguyen algorithm

Time and Environment:

2 hours for preparing data for 4 solutions

(Opteron [2.2GHz]) + 1.8 hours per solution

(Opteron [2.2GHz])

We found the factor at the 4th solution.

## IV. Discrete logarithm

Summary:

- Generic algorithms:  $O(\sqrt{\#G})$  (baby steps, giant steps; Pollard's rho).
- Over  $\mathbb{F}_{2^n}$ : Coppersmith's algorithm running in time  $O(\exp(c'n^{1/3}(\log n)^{2/3}))$ ; record by Joux et Lercier (22/09/05) with  $n = 613$ .
- Over  $(\mathbb{Z}/p\mathbb{Z})^*$ :  $L_p[1/2, c]$ ; Gordon/Schirokauer give  $L_p[1/3, c]$  using NFS also. Record of T. Kleinjung (160 decimal digits, 05/02/2007: 3.3 years of PC 3.2 GHz Xeon64 for relations + 2177226 × 2177026 matrix with 289976350 non-zero entries with 14 CPU years).

## V. Conclusions

Primality: easy.

Factoring/Discrete logarithm: hard.

$$L_x[\alpha, c] = \exp(c(\log x)^\alpha (\log \log x)^{1-\alpha})$$

$$L_x[0, c] = (\log x)^c, \quad L_x[1, c] = x^c$$

method	complexity
$\rho$	$\sqrt{p} = L_p[1, 1/2]$
ECM	$L_p[1/2, \sqrt{2}]$
QS	$L_N[1/2, c]$
NFS	$L_N[1/3, c]$

$N$	$\sqrt{N}$	$L_N[1/2, 1]$	$L_N[1/3, 1]$
$2^{128}$	$1.84 \times 10^{19}$	$4.61 \times 10^8$	$1.85 \times 10^5$
$2^{256}$	$3.40 \times 10^{38}$	$1.46 \times 10^{13}$	$2.02 \times 10^7$
$2^{512}$	$1.16 \times 10^{77}$	$6.69 \times 10^{19}$	$1.02 \times 10^{10}$
$2^{768}$	$3.94 \times 10^{115}$	$1.27 \times 10^{25}$	$9.49 \times 10^{11}$
$2^{1024}$	$1.34 \times 10^{154}$	$4.42 \times 10^{29}$	$3.82 \times 10^{13}$

## What next?

P. Gaudry's lectures on algebraic curves and their use in Algorithmic Number Theory and crypto.