

IMUB

Institut de  
Matemàtica

QUADRATIC FIELDS AND PUBLIC KEY  
CRYPTOGRAPHY

*Teresa Crespo and Elżbieta Sowa*

No. 409  
October 2008

**Mathematics Preprint Series**



UNIVERSITAT DE BARCELONA

U

B

# Quadratic fields and public key cryptography

Teresa Crespo and Elżbieta Sowa

## Abstract

We present a survey on quadratic number fields, their groups of units and classes of ideals as well as some applications of them to public key cryptography.

## 1 Introduction

Cryptography is the art of disguise a message in such a way that only the intended receiver can remove the disguise and read it. The message we want to send is called *plaintext* and the disguised message is called the *ciphertext*. The plaintext and the ciphertext are broken up into message units. We consider the set  $\mathcal{P}$  of all possible plaintext message units and the set  $\mathcal{C}$  of all possible ciphertext message units. An *enciphering transformation* is then a bijective map  $f$  from  $\mathcal{P}$  to  $\mathcal{C}$ , its inverse  $f^{-1}$  is called *deciphering transformation*. The set-up

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

is called a *cryptosystem*. The first step in inventing a cryptosystem is to codify all possible ciphertext message units as an integer in some range, let's say from 0 to a positive integer  $n$ . The enciphering transformation can then be seen as a map defined on  $\mathbb{Z}/n$ . The origins of cryptography go back to ancient times. For classical cryptosystems, security is based on the secrecy of the keys used to build the enciphering transformation as the knowledge of these keys allows also to decipher intercepted messages.

In 1976 W. Diffie and M. Hellmann [D-H] invented an entirely different type of cryptosystem, public key cryptography. In a public key cryptosystem, someone who knows how to encipher cannot use the enciphering key to find the deciphering key without a prohibitively lengthy computation. The enciphering transformation is then called *one-way function*. The best

---

<sup>0</sup>2000 Mathematics Subject Classification: 11R11, 11R27, 11R29, 94A60.

Keywords: Quadratic fields, Unit group, Factorization, Class group, Public key cryptography.

known public key cryptosystem is RSA named after its creators R.L Rivest, A. Shamir and L.M. Adleman [A-R-S]. It is based on the computational difficulty in factoring integers. Let us describe it briefly. Each user chooses two big prime numbers  $p$  and  $q$  (having about 100 decimal digits) and set  $n = pq$ . Knowing the factorization of  $n$ , we can compute the Euler function  $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$ . Then the user chooses at random an integer  $e$  between 1 and  $\varphi(n)$ , coprime to  $\varphi(n)$ . Finally, he computes the inverse  $d$  of  $e$  modulo  $\varphi(n)$ . The user makes public the enciphering key  $K_e = (n, e)$  and keeps secret the deciphering key  $K_d = (n, d)$ . The enciphering transformation is then

$$\begin{aligned} f : \mathbb{Z}/n &\rightarrow \mathbb{Z}/n \\ x &\mapsto x^e \bmod n \end{aligned}$$

and the deciphering transformation is

$$\begin{aligned} f^{-1} : \mathbb{Z}/n &\rightarrow \mathbb{Z}/n \\ y &\mapsto y^d \bmod n. \end{aligned}$$

They are indeed mutually inverses as  $ed \equiv 1 \pmod{\varphi(n)} \Rightarrow x^{ed} \equiv x \pmod{n}$  by Euler's theorem.

In order to compute  $d$  from  $e$  we need to know  $\varphi(n)$ . It can be proved that if we know that  $n$  is the product of two primes then knowing  $\varphi(n)$  is equivalent to knowing the factorization of  $n$ . Also knowing  $d$  gives a probabilistic method to factorize  $n$ .

Other processes in number theory can be used to construct one-way functions. One of the most important is raising to a power in a large finite field  $\mathbb{F}_q$ . If  $b$  is an element of the multiplicative group  $\mathbb{F}_q^*$  and  $y$  is an element of  $\mathbb{F}_q^*$  which is a power of  $b$ , then the *discrete logarithm* of  $y$  to the base  $b$  is any integer  $x$  such that  $b^x = y$ . There are several public key cryptosystems or public key arrangements which are based on the computational difficulty of solving the discrete logarithm problem in finite fields. We shall describe here the Diffie-Hellman key exchange protocol and ElGamal cryptosystem [E].

Because public key cryptosystems are relatively slow compared to classical cryptosystems it is usual to combine both, in particular to use a public cryptosystem to agree on a key for a classical cryptosystem. The first detailed proposal for doing this, due to W. Diffie and M.E. Hellman, was based on the discrete logarithm problem. We suppose that the key for the classical cryptosystem is a large randomly chosen positive integer in some range,

let's say  $< N$ . Choosing a random integer in some interval is equivalent to choosing a random element of a large finite field of roughly the same size. If the finite field is  $\mathbb{F}_{p^f}$ , we first choose an  $\mathbb{F}_p$ -basis of this field, so that each element corresponds to an  $f$ -tuple of elements of  $\mathbb{F}_p$ , we consider then the integer having these coordinates as digits in the base  $p$ . We assume now that  $q$  is public knowledge as well as some fixed element  $g \in \mathbb{F}_q^*$ , ideally a generator of  $\mathbb{F}_q^*$ . Let A and B be two users who want to agree upon a key which they will use to encrypt their subsequent messages to one another. A chooses a random integer  $a$  between 1 and  $q - 1$ , which he keeps secret and compute  $g^a$ , which he makes public. B makes the same, he chooses a random  $b$  and publishes  $g^b$ . The secret key they use is  $g^{ab}$ . Both users can compute this key. A third person knows only  $g^a$  and  $g^b$  and is not able to compute  $g^{ab}$  without solving the discrete logarithm problem.

In ElGamal cryptosystem, we use as well a large finite field  $\mathbb{F}_q$  and an element  $g \in \mathbb{F}_q^*$ , preferably a generator. We suppose that we are using plaintext message units with numerical equivalents  $P \in \mathbb{F}_q$ . Each user  $A$  randomly chooses an integer  $a$ , say in the range  $0 < a < q - 1$ . This integer  $a$  is the secret deciphering key, the public enciphering key is the element  $g^a \in \mathbb{F}_q$ . To send a message  $P$  to the user  $A$ , we choose an integer  $k$  at random and then send  $A$  the pair of elements  $(g^k, Pg^{ak})$ . Notice that we can compute  $g^{ak}$  as  $(g^a)^k$  without knowing  $a$ . Now  $A$ , who knows  $a$ , can recover  $P$  as  $(Pg^{ak})(g^k)^{q-1-a}$ .

N. Koblitz [K2] and V. Miller [M] independently built up a cryptosystem using elliptic curves defined over a finite field  $\mathbb{F}_q$ . The multiplicative group  $\mathbb{F}_q^*$  of the finite field is here substituted by the group  $E(\mathbb{F}_q)$  of points with coordinates in  $\mathbb{F}_q$  of an elliptic curve  $E$  defined over  $\mathbb{F}_q$ . The advantage of elliptic curve cryptography is that we have a big choice for selecting the elliptic curve and this gives that we can use integer numbers of a smaller size.

The reader can consult e.g. [K1] or [B] for more information on the above matters.

Some variants of the public key cryptosystems described above have been proposed which are based on computationally hard problems in quadratic fields. They involve the unit group and the ideal class group of a quadratic field. In this paper, we survey the unit group and the ideal class group of number fields. We show explicit computations for these groups in the case of quadratic number fields. We present two different cryptosystems based on the unit group of a real quadratic field and on the ideal class group of an imaginary quadratic field. Finally we discuss why imaginary quadratic fields

appear to be more suitable for encryption systems based on class groups.

## 2 Quadratic Fields

### 2.1 First topics

We recall in this section the main topics on number fields, units and ideal classes, chiefly in the case of quadratic fields. The reader can consult e.g. [N] for more details on these subjects.

**Definition 2.1.** A *number field* is a finite field extension  $K$  of the field  $\mathbb{Q}$  of rational numbers, i.e.  $K$  is a field containing  $\mathbb{Q}$ , such that  $[K : \mathbb{Q}] := \dim_{\mathbb{Q}} K$  is finite.

**Example 2.2.** A *quadratic field* is a number field  $K$  such that  $[K : \mathbb{Q}] = 2$ . It is easy to see that a quadratic field  $K$  can be given as  $K = \mathbb{Q}(\sqrt{d})$ , for  $d$  a square free integer, where  $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ . If  $d > 0$ ,  $K$  can be embedded in the field  $\mathbb{R}$  of real numbers. In this case we say that  $K$  is a *real quadratic field*. If  $d < 0$ , we say that  $K$  is an *imaginary quadratic field*.

**Definition 2.3.** An element in a number field  $K$  is *integer* (over  $\mathbb{Z}$ ) if it is a root of a monic polynomial with coefficients in  $\mathbb{Z}$ . It can be seen that an element in  $K$  is integer if and only if its irreducible polynomial over  $\mathbb{Q}$  has coefficients in  $\mathbb{Z}$ . The set of integer elements in  $K$  form a ring, which is called the *ring of integers* of the number field  $K$  and denoted by  $\mathcal{O}_K$ .

For an element in a number field  $K$  we can define the (absolute) norm and trace. We give here the definition in the particular case of quadratic fields.

**Definition 2.4.** Let  $z = a + b\sqrt{d}$  be an element in the quadratic field  $K = \mathbb{Q}(\sqrt{d})$ . The *conjugate* of  $z$  is the element  $\bar{z} = a - b\sqrt{d}$ . The *trace* of  $z$  is defined by

$$\mathcal{T}_{K|\mathbb{Q}}(z) = z + \bar{z} = 2a,$$

the *norm* of  $z$  is defined by

$$\mathcal{N}_{K|\mathbb{Q}}(z) = z\bar{z} = a^2 - b^2d.$$

The following properties of trace and norm are satisfied for every number field. In the case of quadratic fields, they are proved straightforwardly from our definitions.

**Proposition 2.5.** *Let  $K$  be a number field. The map*

$$\begin{aligned} \mathcal{T}_{K|\mathbb{Q}} : K &\rightarrow \mathbb{Q} \\ z &\mapsto \mathcal{T}_{K|\mathbb{Q}}(z) \end{aligned}$$

*is a morphism of additive groups. The map*

$$\begin{aligned} \mathcal{N}_{K|\mathbb{Q}} : K^* &\rightarrow \mathbb{Q}^* \\ z &\mapsto \mathcal{N}_{K|\mathbb{Q}}(z) \end{aligned}$$

*is a morphism of multiplicative groups.*

For an element  $z$  in the quadratic field  $K = \mathbb{Q}(\sqrt{d})$ , the irreducible polynomial over  $\mathbb{Q}$  is  $X^2 - \mathcal{T}_{K|\mathbb{Q}}(z)X + \mathcal{N}_{K|\mathbb{Q}}(z)$ . From this fact, we obtain

$$z \in \mathcal{O}_K \Leftrightarrow \mathcal{T}_{K|\mathbb{Q}}(z) \in \mathbb{Z} \quad \text{and} \quad \mathcal{N}_{K|\mathbb{Q}}(z) \in \mathbb{Z}.$$

By using this characterization, the ring of integers of a quadratic field is easily determined. If  $K = \mathbb{Q}(\sqrt{d})$ , with  $d$  a squarefree integer, we have

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, \text{ if } d \equiv 2, 3 \pmod{4},$$

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2} : a, b \in \mathbb{Z}\right\}, \text{ if } d \equiv 1 \pmod{4}.$$

The invertible elements of the ring  $\mathcal{O}_K$  are called *units*. They can be characterized by using the norm, namely

$$z \in \mathcal{O}_K^* \Leftrightarrow \mathcal{N}(z) = \pm 1.$$

Using this characterization, we can determine the units of an imaginary quadratic field  $K$ .

**Proposition 2.6.** *Let  $K = \mathbb{Q}(\sqrt{d})$  with  $d$  a negative squarefree integer.*

a)  $\mathcal{O}_{\mathbb{Q}(i)}^* = \{\pm 1, \pm i\},$

b)  $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}^* = \{\pm 1, \pm \rho, \pm \rho^2\},$  where  $\rho = \frac{-1+\sqrt{-3}}{2},$

c)  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}^* = \{\pm 1\},$  in all other cases.

*Proof.*

- a) The ring of integers of  $\mathbb{Q}(i)$  is  $\mathbb{Z}[i]$ . An element  $z = a + bi \in \mathbb{Z}[i]$  is a unit if and only if  $\mathcal{N}(z) = a^2 + b^2 = 1$  and the only solutions in  $\mathbb{Z}$  are  $(a, b) = (\pm 1, 0), (0, \pm 1)$ .
- b) The ring of integers of  $\mathbb{Q}(\sqrt{-3})$  is  $\mathbb{Z}[\alpha]$ , where  $\alpha = \frac{1+\sqrt{-3}}{2}$ . An element in  $\mathbb{Z}[\alpha]$ ,  $z = a + b\alpha = (a + \frac{b}{2}) + \frac{b}{2}\sqrt{-3}$  is a unit if and only if  $\mathcal{N}(z) = (a + \frac{b}{2})^2 + 3(\frac{b}{2})^2 = a^2 + b^2 + ab = 1$  and the only solutions in  $\mathbb{Z}$  are  $(a, b) = (\pm 1, 0), (0, \pm 1), (-1, 1), (1, -1)$ .
- c) If  $d \equiv 2, 3 \pmod{4}$ , the ring of integers of  $K$  is  $\mathbb{Z}[\sqrt{d}]$ . An element  $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$  is a unit if and only if  $\mathcal{N}(z) = a^2 - db^2 = 1$  and the only solution in  $\mathbb{Z}$  is  $(a, b) = (\pm 1, 0)$  for  $d \leq -2$ .

If  $d \equiv 1 \pmod{4}$ , the ring of integers of  $\mathbb{Q}(\sqrt{d})$  is  $\mathbb{Z}[\alpha]$ , where  $\alpha = \frac{1+\sqrt{d}}{2}$ . An element in  $\mathbb{Z}[\alpha]$ ,  $z = a + b\alpha = (a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}$  is a unit if and only if  $\mathcal{N}(z) = (a + \frac{b}{2})^2 - d(\frac{b}{2})^2 = 1$  and the only solution in  $\mathbb{Z}$  is  $(a, b) = (\pm 1, 0)$  if  $d \leq -7$ .

We note that the ring of integers  $\mathcal{O}_K$  of a number field is not in general a unique factorization domain.

**Example 2.7.** We consider the number field  $K = \mathbb{Q}(\sqrt{-5})$ . Its ring of integers is  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$  and  $\mathcal{O}_K^* = \{\pm 1\}$ . The following equalities

$$21 = 3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

are two different factorizations of 21 into a product of irreducible elements. Indeed, let us check that the factors are non equivalent irreducible elements in  $(\mathbb{Z}[\sqrt{-5}])$ . If for elements  $z, z_1, z_2 \in \mathcal{O}_K$ , we have  $z = z_1 z_2$ , then  $\mathcal{N}(z) = \mathcal{N}(z_1)\mathcal{N}(z_2)$ . Now for the factors of the above factorizations, we have  $\mathcal{N}(3) = 9, \mathcal{N}(7) = 49, \mathcal{N}(1 \pm 2\sqrt{-5}) = 21$  and  $\mathcal{N}(a + b\sqrt{-5}) = a^2 + 5b^2$  cannot be equal to 3 or 7 for  $a, b$  integer numbers, so the factors are irreducible. As  $\mathcal{O}_K^* = \{\pm 1\}$ , they are non equivalent.

This lack of unique factorization led Kummer (1810-1893) to introduce ideal elements. His idea was that there should be a further factorization

which fulfill unicity. It is known that the ring  $\mathcal{O}_K$  is a Dedekind domain (i.e. a noetherian, integrally closed domain in which every nonzero prime ideal is maximal) and that Dedekind domains have unique factorization for ideals.

If  $I, J$  are two ideals in a ring  $A$ , we can define its *product* by

$$IJ := \left\{ \sum_i (a_i b_i) : a_i \in I, b_i \in J \right\}.$$

An ideal  $I$  of a ring  $A$  is *prime* if it satisfies

$$ab \in I \Rightarrow a \in I \quad \text{or} \quad b \in I \quad \text{for all} \quad a, b \in A.$$

If  $A$  is a Dedekind domain,  $I$  an ideal of  $A$ ,  $I \neq (0), (1)$ , we have a factorization

$$I = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

for  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  prime ideals, unique up to order.

**Example 2.8.** Turning back to example 2.7, we can consider the principal ideal (21) in  $\mathbb{Z}[\sqrt{-5}]$ . Its factorization in prime ideals is

$$(21) = \underbrace{(3, \sqrt{-5} + 1)}_{\mathfrak{p}_1} \cdot \underbrace{(3, \sqrt{-5} - 1)}_{\mathfrak{p}_2} \cdot \underbrace{(7, \sqrt{-5} + 3)}_{\mathfrak{p}_3} \cdot \underbrace{(7, \sqrt{-5} - 3)}_{\mathfrak{p}_4}.$$

We have  $\mathfrak{p}_1 \mathfrak{p}_2 = (3)$ ,  $\mathfrak{p}_3 \mathfrak{p}_4 = (7)$ ,  $\mathfrak{p}_1 \mathfrak{p}_3 = (1 - 2\sqrt{-5})$ ,  $\mathfrak{p}_2 \mathfrak{p}_4 = (1 + 2\sqrt{-5})$ . We obtain then a further factorization in (non principal) prime ideals and this factorization is unique up to order.

**Definition 2.9.** The ring of integers  $\mathcal{O}_K$  of a number field  $K$  is a free  $\mathbb{Z}$ -module of rank  $n = [K : \mathbb{Q}]$ . A  $\mathbb{Z}$ -basis of  $\mathcal{O}_K$  is called an *integral basis* of  $K$ . As  $\mathbb{Z}$  is a principal ideal ring, a subring of  $\mathcal{O}_K$  is also a free  $\mathbb{Z}$ -module. An *order* of  $K$  is a subring  $\mathcal{O}$  of  $\mathcal{O}_K$  having rank  $n$  as a free  $\mathbb{Z}$ -module.

In particular, the ring of integers  $\mathcal{O}_K$  is an order of  $K$ . It is the maximal order of  $K$ . For example,  $\mathbb{Z}[\sqrt{-3}]$  is an order of  $\mathbb{Q}(\sqrt{-3})$ .

**Definition 2.10.** The *discriminant* of a number field  $K$  (over  $\mathbb{Q}$ ) is defined by

$$\text{disc}(K) = \det(\mathcal{T}_{K|\mathbb{Q}}(\alpha_i \alpha_j))$$

for  $(\alpha_1, \dots, \alpha_n)$  an integral basis of  $K$ . It is independent of the basis choice.

For a quadratic field  $\mathbb{Q}(\sqrt{d})$ , we have

1. If  $d \equiv 2, 3 \pmod{4}$ , we can take  $(1, \sqrt{d})$  as an integral basis of  $K$  and obtain

$$\text{disc}(K) = \det \begin{pmatrix} \mathcal{T}(1) & \mathcal{T}(\sqrt{d}) \\ \mathcal{T}(\sqrt{d}) & \mathcal{T}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & d \end{pmatrix} = 4d.$$

2. If  $d \equiv 1 \pmod{4}$ , we can take  $(1, \frac{1+\sqrt{d}}{2})$  as an integral basis of  $K$  and obtain

$$\text{disc}(K) = \det \begin{pmatrix} \mathcal{T}(1) & \mathcal{T}(\frac{1+\sqrt{d}}{2}) \\ \mathcal{T}(\frac{1+\sqrt{d}}{2}) & \mathcal{T}(\frac{1+d+2\sqrt{d}}{4}) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

## 2.2 The class number

In order to obtain a group structure for the set of ideals of the ring of integers of a number field, we introduce the concept of fractional ideal.

**Definition 2.11.** A *fractional ideal* of a number field  $K$  is a non zero finitely generated  $\mathcal{O}_K$ -submodule of  $K$ .

Since  $\mathcal{O}_K$  is noetherian, an  $\mathcal{O}_K$ -submodule  $\mathfrak{a} \neq \mathcal{O}$  of  $K$  is a fractional ideal if and only if there exists  $c \in \mathcal{O}_K, c \neq 0$  such that  $c\mathfrak{a} \subset \mathcal{O}_K$  is an (integral) ideal of  $\mathcal{O}_K$ .

For  $a \in K, (a) := \{ax | x \in \mathcal{O}_K\}$  is a principal fractional ideal. For fractional ideals, the product is defined in the same way as for ideals in  $\mathcal{O}_K$ . With this product, the set of fractional ideals is an abelian group, *the ideal group*  $I_K$  of  $K$ . The identity element is  $(1) = \mathcal{O}_K$  and the inverse of an ideal  $\mathfrak{a}$  is  $\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subset \mathcal{O}_K\}$ .

Every fractional ideal admits a unique representation as a product

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

where the product is taken over all prime ideals  $\mathfrak{p}$  of the ring  $\mathcal{O}_K$ , with  $\nu_{\mathfrak{p}} \in \mathbb{Z}$  and  $\nu_{\mathfrak{p}} = 0$  for almost all  $\mathfrak{p}$ . The principal fractional ideals form a subgroup

$P_K$  of  $I_K$ . The quotient group  $\mathcal{C}_K = I_K/P_K$  is called *the ideal class group* of the number field  $K$ .

**Theorem 2.12.** *The ideal class group  $\mathcal{C}_K = I_K/P_K$  is finite. Its order  $h_K$  is called the class number of  $K$ .*

If  $[K : \mathbb{Q}] = n$ , there are  $n$  different embeddings of  $K$  in the field  $\mathbb{C}$  of complex numbers. Let  $r$  be the number of real embeddings (i.e. with image contained in  $\mathbb{R}$ ). The non real ones are  $s$  pairs of conjugate embeddings. We have then  $n = r + 2s$ . In order to prove theorem 2.12 we define a map

$$j : K \rightarrow \mathbb{R}^{r+2s}$$

by

$$j(x) = (\rho_1(x), \dots, \rho_r(x), \operatorname{Re}(\sigma_1(x)), \operatorname{Im}(\sigma_1(x)), \dots, \operatorname{Re}(\sigma_s(x)), \operatorname{Im}(\sigma_s(x)))$$

for  $\rho_1, \dots, \rho_r$  real embeddings,  $\sigma_1, \dots, \sigma_s$  non real embeddings, one from each pair of conjugate embeddings. For an ideal  $\mathfrak{a}$ ,  $j(\mathfrak{a})$  is a full lattice in  $\mathbb{R}^n$ , i.e. a discrete subgroup of  $\mathbb{R}^n$  with  $\mathbb{Z}$ -rank equal to  $n$ . We apply then Minkowski's theorem on convex bodies.

The class number of the number field  $K$  measures how far is the integer ring  $\mathcal{O}_K$  from being a principal ideal ring. If  $K = \mathbb{Q}(\sqrt{d})$ ,  $h_K$  can be computed by using the correspondence between the class group of  $K$  and binary quadratic forms established by Gauss (cf. [Bu], [Z]). We have  $h_K = 1$  for  $K = \mathbb{Q}(\sqrt{d})$  ( $d$  square free integer), when

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

and no other negative  $d$ . Gauss had already computed all these values of negative  $d$ 's for which  $h_{\mathbb{Q}(\sqrt{d})} = 1$  and Stark and Baker (late 1960's) proved that there are no more.

For  $d > 0$ , we have  $h_{\mathbb{Q}(\sqrt{d})} = 1$  for the following values of  $d < 100$ :

$$d = 2, 3, 5, 6, 7, 11, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, \\ 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97.$$

It is conjectured that there are infinitely many quadratic fields of class number 1. But it is not even known yet whether there are infinitely many algebraic numbers (of arbitrary degree) with class number 1.

## 2.3 The unit group

For an order in a number field, the structure of its group of units is given by the following Dirichlet's theorem.

**Theorem 2.13 (Dirichlet's theorem).** *Let  $K$  be a number field of degree  $n$ ,  $r$  be the number of real embeddings of  $K$  in  $\mathbb{C}$ ,  $s$  one half of the number of non real embeddings of  $K$  in  $\mathbb{C}$ . Let  $\mathcal{O}$  be any order of  $K$ . Then there exist units  $\varepsilon_1, \dots, \varepsilon_t$ ,  $t = r + s - 1$  such that every unit  $\varepsilon \in \mathcal{O}$  has a unique representation in the form*

$$\varepsilon = \zeta \varepsilon_1^{a_1} \dots \varepsilon_k^{a_k}$$

where  $a_1, \dots, a_k \in \mathbb{Z}$  and  $\zeta$  is a root of unity contained in  $\mathcal{O}$ . We call  $\varepsilon_1, \dots, \varepsilon_t$  a system of fundamental units of  $\mathcal{O}$ .

To prove Dirichlet's theorem, we use the multiplicative embedding

$$\delta : K^* \rightarrow \mathbb{R}^{r+s}$$

$$x \mapsto (\log|\rho_1(x)|, \dots, \log|\rho_r(x)|, \log|\sigma_1(x)|^2, \dots, \log|\sigma_s(x)|^2)$$

for  $\rho_1, \dots, \rho_r$  real embeddings,  $\sigma_1, \dots, \sigma_s$  pairwise nonequivalent non real embeddings. The image of the unit group by  $\delta$  is a full lattice in the hyperplane  $x_1 + \dots + x_{r+s} = 1$ . We can then apply Minkowski's theorem on convex bodies.

If  $L$  is a lattice in  $\mathbb{R}^n$ ,  $e_1, \dots, e_m$  a basis of  $L$ , the set  $T = \{x_1 e_1 + \dots + x_m e_m : 0 \leq x_i < 1\}$  is called a *fundamental parallelepiped* of the lattice  $L$ . If we take the maximal order  $\mathcal{O}_K$ , the volume of the fundamental parallelepiped of  $\delta(\mathcal{O}_K^*)$  is  $\sqrt{r+s}R$ , where  $R$  is, by definition, the *regulator* of the field  $K$ .

By applying Dirichlet's theorem to an order  $\mathcal{O}$  of a quadratic field  $K$ , we obtain

1. For  $K = \mathbb{Q}(\sqrt{d})$  with  $d < 0$ , we have  $r = 0, s = 1$  and so  $t = 0$ . We obtain then that  $\mathcal{O}^*$  is reduced to the roots of unity in  $K$ , as we saw above for  $\mathcal{O}_K^*$ .
2. For  $K = \mathbb{Q}(\sqrt{d})$  with  $d > 0$ , we have  $r = 2, s = 0$  and so  $t = 1$ . We obtain then  $\mathcal{O}^* = \{\pm 1\} \times \langle \varepsilon \rangle$ , with  $\langle \varepsilon \rangle \simeq \mathbb{Z}$ . We call  $\varepsilon$  *the fundamental unit* of  $\mathcal{O}$ .

If we take  $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ ,  $d > 0$ ,  $\varepsilon = a + b\sqrt{d}$ , then  $\mathcal{N}(\varepsilon) = a^2 - b^2d = \pm 1$ . Determining explicitly the fundamental unit  $\varepsilon$  amounts to solving the diophantine equation  $a^2 - b^2d = \pm 1$ , known as *Pell equation*. The solutions to Pell equation may be computed by means of continued fractions (see e.g. [L]).

## 2.4 Continued fractions

If  $x$  is a real number, we define a sequence of integer numbers  $\{a_n\}$  and a sequence of real numbers  $\{x_n\}$  in the following way

$$a_0 = [x], \quad x_0 = x - a_0$$

where  $[ \ ]$  denotes integer part. If  $x_0 \neq 0$

$$a_1 = \left[ \frac{1}{x_0} \right], \quad x_1 = \frac{1}{x_0} - a_1.$$

Inductively, if  $a_k, x_k$  are defined and  $x_k \neq 0$

$$a_{k+1} = \left[ \frac{1}{x_k} \right], \quad x_{k+1} = \frac{1}{x_k} - a_{k+1}.$$

If  $x_k = 0$ , the sequences  $\{a_n\}$  and  $\{x_n\}$  end with the terms  $a_k, x_k$ . The sequence  $\{a_n\}$  is called *continued fraction of  $x$* .

For each integer  $k \geq 0$  we have the equality

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_k + x_k}}}}$$

We write  $x = [a_0, a_1, \dots, a_k + x_k]$ .

**Example 2.14.** If  $x = \frac{m}{n} \in \mathbb{Q}$ , the continued fraction of  $x$  is obtained by successive euclidean divisions:

$$\text{If } m = nq_1 + r_1 \quad \text{then } a_0 = q_1, \quad x_0 = \frac{r_1}{n}$$

$$\text{If } n = r_1q_2 + r_2 \quad \text{then } a_1 = q_2, \quad x_1 = \frac{r_2}{r_1},$$

$$\text{If } r_1 = r_2q_3 + r_3 \quad \text{then } a_2 = q_3, \quad x_2 = \frac{r_3}{r_2} \dots$$

The residues form a decreasing sequence of positive integers numbers, so the continued fraction of a rational number is finite.

**Example 2.15.** We compute the continued fraction of  $x = \sqrt{3}$ .

$$1 < \sqrt{3} < 2 \quad \Rightarrow \quad a_0 = 1, x_0 = \sqrt{3} - 1$$

$$\frac{1}{x_0} = \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2}, \quad 1 < \frac{\sqrt{3} + 1}{2} < 2 \quad \Rightarrow \quad a_1 = 1, x_1 = \frac{\sqrt{3} - 1}{2}$$

$$\frac{1}{x_1} = \sqrt{3} + 1 \quad \Rightarrow \quad a_2 = 2, x_2 = \sqrt{3} - 1 = x_0.$$

So, from here on, the terms  $a_n, x_n$  are repeating and we have

$$\begin{aligned} a_{2k-1} &= 1, & x_{2k-1} &= (\sqrt{3} - 1)/2 \\ a_{2k} &= 2, & x_{2k} &= \sqrt{3} - 1, \quad k \geq 1 \end{aligned}$$

We write  $\sqrt{3} = [1, \overline{1, 2}]$ .

We note that the continued fraction of an irrational quadratic number is always periodic.

**Remark 2.16.** Continued fractions are used in the Brillhart-Morrison factorization method [B-M] to produce factor bases.

**Definition 2.17.** If  $x$  is a real irrational number, *the  $k$ -th convergent* of the continued fraction of  $x$  is the rational number  $[a_0, a_1, \dots, a_k]$ .

**Example 2.18.** The convergents of the continued fraction of  $\sqrt{3}$  are:

$$[a_0] = [1] = 1$$

$$\begin{aligned}
[a_0, a_1] &= [1, 1] = 1 + \frac{1}{1} = 2 \\
[a_0, a_1, a_2] &= [1, 1, 2] = 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3} \sim 1,66\dots \\
[a_0, a_1, a_2, a_3] &= [1, 1, 2, 1] = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = \frac{7}{4} \sim 1,75\dots \\
[a_0, a_1, a_2, a_3, a_4] &= \frac{19}{11} \sim 1,7272\dots \\
[a_0, a_1, a_2, a_3, a_4, a_5] &= \frac{26}{15} \sim 1,733\dots
\end{aligned}$$

As we can observe in the particular case of our example, it can be proved that the convergents of the continued fraction of a real number  $x$  are given by irreducible fractions and converge to  $x$ . The  $k$ -th convergent gives an approximation of  $x$  by excess (resp. by defect) if  $k$  is odd (resp. even).

The following theorem provides the fundamental unit of  $\mathbb{Z}[\sqrt{d}]$  and the solutions to the corresponding Pell equation.

**Theorem 2.19.** *Let  $d$  be a positive integer, which is not a perfect square. Let  $p$  be the period of the continued fraction of  $\sqrt{d}$  and let  $\frac{b_k}{c_k}$  be the  $k$ -th convergent. The fundamental unit of  $\mathbb{Z}[\sqrt{d}]$  is  $b_{p-1} + c_{p-1}\sqrt{d}$ . Its norm is 1 (resp. -1) if the period of the continued fraction of  $\sqrt{d}$  is even (resp. odd)*

**Corollary 2.20.** *Let  $d$  be a positive integer, which is not a perfect square. Let  $p$  be the period of the continued fraction of  $\sqrt{d}$  and let  $\frac{b_k}{c_k}$  be the  $k$ -th convergent.*

a) *If  $p$  is even, the smallest positive solution of the diophantine equation*

$$X^2 - dY^2 = 1$$

*is  $X_1 = b_{p-1}, Y_1 = c_{p-1}$  and all positive solutions of this equation are the integer pairs  $(X_k, Y_k)$  given by*

$$X_k + Y_k \sqrt{d} = (X_1 + Y_1 \sqrt{d})^k, \quad k \geq 1.$$

The diophantine equation

$$X^2 - dY^2 = -1$$

has no solutions.

b) If  $p$  is odd, the smallest positive solution of the diophantine equation

$$X^2 - dY^2 = -1$$

is  $X_1 = b_{p-1}, Y_1 = c_{p-1}$  and all positive solutions of this equation are the integer pairs  $(X_k, Y_k)$  given by

$$X_k + Y_k \sqrt{d} = (X_1 + Y_1 \sqrt{d})^k, \quad k \text{ odd } \geq 1.$$

All positive solutions of the diophantine equation

$$X^2 - dY^2 = 1$$

are the integer pairs  $(X_k, Y_k)$  given by

$$X_k + Y_k \sqrt{d} = (X_1 + Y_1 \sqrt{d})^k, \quad k \text{ even } \geq 1.$$

**Example 2.21.** We had  $\sqrt{3} = [1, \overline{1, 2}]$ , so the fundamental unit of  $\mathbb{Q}(\sqrt{3})$  is  $2 + \sqrt{3}$ . The integer solutions to  $x^2 - 3y^2 = 1$  are given by:

$$\begin{aligned} (2 + \sqrt{3})^2 &= 7 + 4\sqrt{3} &\rightarrow (x, y) &= (7, 4) \\ (2 + \sqrt{3})^3 &= 26 + 15\sqrt{3} &\rightarrow (x, y) &= (26, 15) \dots \end{aligned}$$

The equation  $x^2 - 3y^2 = -1$  has no integer solutions.

**Example 2.22.** We compute now the continued fraction of  $\sqrt{5}$ .

$$\begin{aligned} a_0 &= \sqrt{5}, x_0 = \sqrt{5} - 2 \\ a_1 &= \left[ \frac{1}{\sqrt{5} - 2} \right] = [\sqrt{5} + 2] = 4, x_1 = \sqrt{5} - 2 = x_0 \end{aligned}$$

We obtain then  $\sqrt{5} = [2; \overline{4}]$  and  $p = 1$ . The 0-th convergent is  $2 = \frac{2}{1}$  so the fundamental unit of  $\mathbb{Z}(\sqrt{5})$  is  $2 + \sqrt{5}$ , which has norm equal to  $-1$ .

The integer solutions to  $x^2 - 5y^2 = 1$  are given by:

$$\begin{aligned} (2 + \sqrt{5})^2 = 9 + 4\sqrt{5} &\rightarrow (x, y) = (9, 4) \\ (2 + \sqrt{5})^4 = 161 + 72\sqrt{5} &\rightarrow (x, y) = (161, 72) \dots \end{aligned}$$

The integer solutions to  $x^2 - 5y^2 = -1$  are given by:

$$\begin{aligned} (2 + \sqrt{5}) &\rightarrow (x, y) = (2, 1) \\ (2 + \sqrt{5})^3 = 38 + 17\sqrt{5} &\rightarrow (x, y) = (38, 17) \dots \end{aligned}$$

In general, the explicit determination of a system of fundamental units for an order  $\mathcal{O}$  of a number field  $K$  is not so direct. It is possible to find explicitly a number  $\rho$  such that the ball of radius  $\rho$  in the space  $\mathbb{R}^{s+t}$  must contain a basis for the lattice  $\delta(\mathcal{O}^*)$ . Moreover, it can be proved that there is a finite number of units in  $\mathcal{O}^*$  such that its image by  $\delta$  is contained in such a ball. From this collection of units, we can form all possible systems  $\varepsilon_1, \dots, \varepsilon_t$ ,  $t = r + s$ , for which the vectors  $\delta(\varepsilon_1), \dots, \delta(\varepsilon_t)$  are linearly independent. For each such system we compute the volume of the fundamental parallelepiped determined by the vectors  $\delta(\varepsilon_1), \dots, \delta(\varepsilon_t)$ . That system for which this volume is smallest will be a system of fundamental units (cf. [B-S]). The reader can consult [N] for information on algorithms for computation of units in cubic and quartic fields as well as the determination of units in cyclotomic fields.

## 3 Cryptosystems

### 3.1 A cryptosystem based on the unit group

H.C. Williams proposed in [W] a public key cryptosystem based on the unit group of the order  $\mathbb{Z}[\sqrt{C}]$  of the real quadratic field  $\mathbb{Q}(\sqrt{C})$  (see also [S]).

Let  $\varepsilon = a_1 + b_1\sqrt{C}$  be a unit with  $\mathcal{N}(\varepsilon) = a_1^2 - b_1^2 C = 1$ . We define functions  $X_n, Y_n$  by

$$X_n(a_1, b_1) + \sqrt{C} Y_n(a_1, b_1) = \varepsilon^n, \quad X_n(a_1, b_1) - \sqrt{C} Y_n(a_1, b_1) = \bar{\varepsilon}^n,$$

that is

$$X_n(a, b) = \frac{\varepsilon_n + \bar{\varepsilon}^n}{2}, \quad Y_n(a, b) = \frac{\varepsilon_n - \bar{\varepsilon}^n}{\varepsilon - \bar{\varepsilon}} b$$

We point out that

$$X_n^2 - C Y_n^2 = (\varepsilon\bar{\varepsilon})^n = 1.$$

Also

$$X_{n+m} = 2X_m X_n - X_{n-m},$$

which implies that  $X_n$  depends only on  $a_1$ . We obtain as well

$$X_{nm}(a_1) = X_n(X_m(a_1)).$$

We assume now that  $a_1, b_1, C$  are integers satisfying

$$(1) \quad a_1^2 - C b_1^2 \equiv 1 \pmod{R}$$

for some integer  $R$  and define similarly functions  $X_n, Y_n$  which are now determined modulo  $R$ . The preceding equalities are then now congruencies modulo  $R$ . The cryptosystem is based on the following result.

**Theorem 3.1.** *Let  $a_1, b_1, C, R$  be integers satisfying (1) and suppose  $R = pq$ , where  $p, q$  are primes. We assume the following conditions for the values of the Jacobi symbols.*

$$\varepsilon_p := \left(\frac{C}{p}\right) \equiv -p \pmod{4}, \varepsilon_q := \left(\frac{C}{q}\right) \equiv -q \pmod{4}, \left(\frac{2(a_1 + 1)}{R}\right) = 1,$$

and  $\gcd(Cb_1, R) = 1$ . Let  $e, d$  be integers satisfying

$$(2) \quad ed \equiv \frac{(w+1)}{2} \pmod{w}$$

for

$$(3) \quad w = (p - \varepsilon_p)(q - \varepsilon_q)/4.$$

Then

$$\begin{aligned} X_{2ed}(a_1, b_1) &\equiv \pm a_1 \\ Y_{2ed}(a_1, b_1) &\equiv \pm b_1 \pmod{R}. \end{aligned}$$

To build the public cryptosystem, the designer must select two large primes  $p, q$  and a value of  $C$  such that  $p \equiv -\left(\frac{C}{p}\right) \pmod{4}$  and  $q \equiv -\left(\frac{C}{q}\right) \pmod{4}$ .

Since there are  $(p-1)/2$  values  $\pmod{p}$  which have a prescribed quadratic character  $(1 \text{ or } -1) \pmod{p}$ , there must, by the Chinese remainder theorem, be  $(p-1)(q-1)/4$  values of  $C \pmod{R}$  such that  $p \equiv -\left(\frac{C}{p}\right) \pmod{4}$ ,  $q \equiv -\left(\frac{C}{q}\right) \pmod{4}$ . Thus roughly one quarter of all integers possess this property.

The designer must also determine, by trial, a value of  $A$  such that the Jacobi symbol  $\left(\frac{A^2 - C}{R}\right) = -1$  and  $\gcd(A, R) = 1$ . Finally, he selects a value for  $e$  and solves the congruence (2) for  $d$ , where  $w$  is given by (3). He makes the value of  $R, e, A, C$  public but keeps  $d$  secret.

We assume that the message  $M$  being sent is numerically encoded and less than  $R$ . If this is not the case,  $M$  must be blocked in pieces that are less than  $R$ . To  $M$  we associate integers  $T(M), S(M)$  defined modulo  $R$ , given by

$$T(M) + S(M)\sqrt{C} \equiv \begin{cases} \frac{(A + \sqrt{C})^2 (M + \sqrt{C})^2}{A^2 - C} \pmod{R} & \text{when } \left(\frac{M^2 - C}{R}\right) = -1 \\ \frac{(M + \sqrt{C})^2}{M^2 - C} \pmod{R} & \text{when } \left(\frac{M^2 - C}{R}\right) = +1 \end{cases}$$

The encryption and decryption functions are then based on the functions  $X_e$  and  $X_d$  but they are built in such a way that the original message is recovered when decrypted without the ambiguity in sign appearing in theorem (3.1). It can be proved that breaking the system is equivalent in difficulty to factoring the integer  $R$ .

### 3.2 A cryptosystem based on the class group

Buchmann and Williams [B-W1] have constructed a key-exchange system, of the type of Diffie and Hellman scheme, which uses the class group of an imaginary quadratic field (see also [B-W2])

We consider a quadratic field  $K = \mathbb{Q}(\sqrt{d})$  and its ring of integers  $\mathcal{O}_K$ . Let

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

so that  $\mathcal{O}_K = \mathbb{Z}[\omega]$ .

We recall that for  $\Delta$  the discriminant of  $K$  we have

$$\begin{aligned}\Delta &= 4d & \text{if } d \equiv 2, 3 \pmod{4} \\ \Delta &= d & \text{if } d \equiv 1 \pmod{4}.\end{aligned}$$

An ideal  $\mathfrak{a}$  of  $\mathcal{O}_K$  is a free  $\mathbb{Z}$ -module of rank 2. If  $\alpha, \beta \in K$  is a basis of  $\mathfrak{a}$ , we write  $\mathfrak{a} = [\alpha, \beta]$ . For an ideal  $\mathfrak{a}$  in  $\mathcal{O}_K$  we can choose a basis in a canonical way.

**Theorem 3.2.** *If  $\mathfrak{a}$  is any ideal of  $\mathcal{O}_K$ , then*

$$\mathfrak{a} = [a, b + c\omega]$$

where  $a, b, c \in \mathbb{Z}$  and  $a > 0, c > 0, |b| < a$ . Moreover  $c|a, c|b$  and  $ac|\mathcal{N}(b + c\omega)$ .

The basis with these properties is unique. It is called the *canonical basis of the ideal  $\mathfrak{a}$* . As  $(a) = \mathbb{Z} \cap \mathfrak{a}$ , the element  $a$  is determined by  $\mathfrak{a}$ , we put  $a = L(\mathfrak{a})$ .

The ideal  $\mathfrak{a}$  is called *primitive* when it has  $c = 1$  in its canonical basis.

**Lemma 3.3.** *If  $\mathfrak{a}$  is primitive, then  $\exists \alpha \in \mathfrak{a}$  such that*

$$\mathfrak{a} = [L(\mathfrak{a}), \alpha] \quad \text{and} \quad |Tr(\alpha)| \leq L(\mathfrak{a}).$$

Moreover the value of  $|Tr(\alpha)|$  is unique.

The ideal  $\mathfrak{a}$  is called *reduced* if it is primitive and there does not exist a nonzero  $\beta \in \mathfrak{a}$  such that  $|\beta| < L(\mathfrak{a})$ . Reduced ideals are characterized by the following proposition.

**Proposition 3.4.** *a) If  $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$  is a primitive ideal of  $\mathcal{O}_K$  with  $|Tr(\alpha)| \leq L(\mathfrak{a})$ , then  $\mathfrak{a}$  is reduced if and only if  $|\alpha| \geq L(\mathfrak{a})$ ,*

*b) If  $\mathfrak{a}$  is a reduced ideal of  $\mathcal{O}_K$ , then  $L(\mathfrak{a}) < \sqrt{\frac{|\Delta|}{3}}$ ,*

c) Is  $\mathfrak{a}$  is a primitive ideal of  $\mathcal{O}_K$  and  $L(\mathfrak{a}) < \frac{\sqrt{|\Delta|}}{2}$ , then  $\mathfrak{a}$  is a reduced ideal.

All these results can be proved by using the correspondence between ideals of the integer ring of a quadratic field and binary quadratic forms.

**Proposition 3.5.** *Let  $\mathfrak{a}, \mathfrak{b}$  primitive ideals of  $\mathcal{O}_K$  such that  $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$ ,  $\mathfrak{b} = [L(\mathfrak{b}), \beta]$  with  $|Tr(\alpha)| \leq L(\mathfrak{a})$ ,  $|Tr(\beta)| \leq L(\mathfrak{b})$ . If  $\mathfrak{a} \sim \mathfrak{b}$ , then  $L(\mathfrak{a}) = L(\mathfrak{b})$  and  $|Tr(\alpha)| = |Tr(\beta)|$ .*

**Corollary 3.6.** *There are at most two reduced ideals in any given equivalence class of ideals.*

It can be proved that each equivalence class of  $\mathcal{C}_K$  contains a reduced ideal.

### 3.3 Key-exchange method

In order to use the ideal class group for cryptographic applications, we need to compute effectively the product of two reduced ideals of a quadratic field and also a reduced ideal equivalent to the product. This computation can be made more efficiently in a single step by using Shanks' algorithm which he called NUCOMP [Sh], see also [C].

The scheme of the key-exchange method is the following.

Two users A and B select a value of  $d$  such that  $|d|$  is large, and an ideal  $\mathfrak{a}$  in  $\mathcal{O}_K$  ( $K = \mathbb{Q}(\sqrt{d})$ ). The value of  $d$  and  $\mathfrak{a}$  can be made public.

1. A selects at random an integer  $x$  and computes a reduced ideal  $\mathfrak{b} \sim \mathfrak{a}^x$ .  
A sends  $\mathfrak{b}$  to B.
2. B selects at random an integer  $y$  and computes a reduced ideal  $\mathfrak{c} \sim \mathfrak{a}^y$ .  
B sends  $\mathfrak{c}$  to A.
3. A computes a reduced ideal  $\mathfrak{f}_1 \sim \mathfrak{c}^x$ , B computes a reduced ideal  $\mathfrak{f}_2 \sim \mathfrak{b}^y$ .

Then  $\mathfrak{f}_1 \sim \mathfrak{f}_2 \Rightarrow L(\mathfrak{f}_1) = L(\mathfrak{f}_2)$  and  $|Tr(\alpha_1)| = |Tr(\alpha_2)|$  for  $\mathfrak{f}_1 = [L(\mathfrak{f}_1), \alpha_1]$ ,  $\mathfrak{f}_2 = [L(\mathfrak{f}_2), \alpha_2]$ . Thus A and B can either use  $L(\mathfrak{f}_1) = L(\mathfrak{f}_2)$  or  $|Tr(\alpha_1)| = |Tr(\alpha_2)|$  or parts of them as their common secret key.

The same idea can be used as a public key cryptosystem similar to El Gamal's. Then  $\mathfrak{c} \sim \mathfrak{a}^y$  will be B's public key and if A wants to send  $M$  to

B, he sends  $(M + L(\mathfrak{f}), \mathfrak{b})$  where  $\mathfrak{f} \sim \mathfrak{c}^x$  and  $\mathfrak{b} \sim \mathfrak{a}^x$ . Then B can compute  $\mathfrak{f} \sim \mathfrak{b}^y$ , determine  $L(\mathfrak{f})$  and recover  $M$ .

One problem that may arise in this scheme is that the order of the class of  $\mathfrak{a}$  in  $\mathcal{C}_K$  is small. This is however unlikely due to heuristic results by Cohen and Lenstra. We can write the abelian group  $\mathcal{C}_K$  as the direct product of its 2-Sylow subgroup and its odd part. Cohen and Lenstra found that the probability that the odd part of the class group is cyclic is 97.7575%. Some other results give that the most probable form of  $\mathcal{C}_K$  is the product of some small group by a cyclic group of a big prime order. So the chance of selecting  $\mathfrak{a}$  of small order in  $\mathcal{C}_K$  is very small when  $h$  is large.

Another question is the relation between the size of the class number  $h$  of the quadratic field  $\mathbb{Q}(\sqrt{d})$  and the size of  $d$ . The Brauer-Siegel Theorem states that

$$\ln\sqrt{\Delta} \sim \ln(h_K \text{reg}(K))$$

and empirical data even suggest

$$\sqrt{\Delta} \sim h_K \text{reg}(K).$$

We have  $\text{reg}(K) = 1$  for  $K$  imaginary quadratic field, and  $\text{reg}(K) = \log \varepsilon_1$ , where  $\varepsilon_1$  is the fundamental unity, for  $K$  real quadratic field. So in the case of a real quadratic field the size of the fundamental unity has to be considered.

Moreover for real quadratic fields the situation is different that the one in proposition 3.5. There is a larger number of reduced ideals in every class, arranged in cycles. If  $k$  is the number of reduced ideals in an ideal class, we have the bounds

$$\frac{2\text{reg}(K)}{\ln\Delta} \leq k \leq \frac{2\text{reg}(K)}{\ln 2}.$$

However in [P-S] a family of real quadratic fields with small regulator is presented which appear to be adequate for cryptography.

Department d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain, e-mail: teresa.crespo@ub.edu

Institute of Mathematics, Jagiellonian University, Reymonta 4, 30-059 Kraków, Poland, e-mail: elzbieta.sowa@im.uj.edu.pl

## 4 Bibliography

- [A-R-S] L.M. Adleman, R.L. Rivest, A. Shamir, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* 21 (1978), no. 2, 120–126.
- [B-S] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, 1966.
- [B-M] J. Brillhart, M.A. Morrison, A Method of Factoring and the Factorization of  $F_7$ , *Mathematics of Computation* 29 (1975), 183-205.
- [B] J. Buchmann, *Introduction to cryptography*, Springer-Verlag, 2004.
- [B-W1] J. Buchmann, H.C. Williams, A Key-Exchange System Based on Imaginary Quadratic Fields, *J. Cryptology* 1 (1988), 107-118.
- [B-W2] J. Buchmann, H.C. Williams, Quadratic fields and cryptography, in: *Number theory and cryptography*, J.H. Loxton (ed.), Cambridge University Press, 1990.
- [Bu] D.A. Buell, *Binary Quadratic Forms. Classical Theory and Modern Computations*, Springer-Verlag, 1989.
- [C] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 2000.
- [D-H] W. Diffie, M.E. Hellman, New directions in cryptography, *IEEE Trans. Information Theory* IT-22 (1976), no. 6, 644-654.
- [E] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Information Theory* 31 (1985), no. 4, 469–472.
- [K1] N. Koblitz, *A course in Number Theory and Cryptography*, Springer-Verlag, 1987.
- [K2] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, vol. 48 (1987), no. 177, 203–209.
- [L] H. W. Lenstra Jr., Solving the Pell Equation, *Notices of the AMS* 49 n.2 (2002), 182-192.

- [M] V. Miller, Use of elliptic curves in cryptography, in: Advances in cryptography–CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., 218, Springer, Berlin, 1986, 417–426.
- [N] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Springer-Verlag 1990.
- [P-S] D. Schielzeth, M. E. Pohst, On real quadratic number fields suitable for cryptography, Experimental Mathematics 14 (2005), 198-197.
- [S] A. Salomaa, Public-Key Cryptography, Springer-Verlag, 1996.
- [Sh] D. Shanks, On Gauss and composition I and II, in: Number theory and applications, R. Mollin (ed.), Kluwer Academic Publishers, 1989, 163-204.
- [W] H.C. Williams, Some public-key crypto-functions as intractable as factorization, Cryptologia 9 n.3 (1985), 223-237.
- [Z] D.B. Zagier, Zetafunktionen und quadratische Körper. Eine einföhrung in die höhere Zahlentheorie, Springer-Verlag, 1981.

## Relació dels últims Preprints publicats:

- **390** *A geometric introduction to forking and thorn-forking.* Hans Adler. AMS Subject Classification (2000): 03C45. February 2007.
- **391** *Thorn-forking as local forking.* Hans Adler. AMS Subject Classification (2000): 03C45. February 2007.
- **392** *Epireflections and supercompact cardinals.* Joan Bagaria, Carles Casacuberta, and Adrian R.D. Mathias. AMS Subject Classification (2000): 03E55, 03C55, 18A40, 18C35, 55P60. March 2007.
- **393** *Dynamic complex hedging in additive markets.* José M. Corcuera and João M.E. Guerra. AMS Subject Classification (2000): 60G46, 60H30, 91B28. July 2007.
- **394** *Coverings for function fields over  $\mathbb{F}_3$ .* Teresa Crespo and Zbigniew Hajto. AMS Subject Classification (2000): 12F12. Septiembre 2007.
- **395** *Optimal investment in non-homogeneous Lévy markets.* José M. Corcuera and João M.E. Guerra. AMS Subject Classification: 91B28, 60G51. October 2007.
- **396** *Power variation for Gaussian processes with stationary increments.* Ole E. Barndorff-Nielsen, José M. Corcuera and Mark Podolskij. AMS Subject Classification: 60F05, 60G15, 60G18, 62M99. November 2007.
- **397** *Convergence of certain functionals of integral fractional processes.* José M. Corcuera, David Nualart and Jeannette H.C. Woerner. AMS Subject Classification: 60F05, 60G15, 60G18, 62M99. December 2007.
- **398** *A model of continuous time polymer on the lattice.* David Márquez-Carreras, Carles Rovira and Samy Tindel. AMS Subject Classification: 82D60, 60K37, 60G15. February 2008.
- **399** *Logics preserving degrees of truth from varieties of residuated lattices.* F. Bou, F. Esteva, J.M. Font, A. Gil, L. Godo, A. Torrens, and V. Verdú. AMS Subject Classification (2000): 03B47, 03B50, 03B22, 03G25, 06B99. April 2008.
- **400** *The flow cytometric scatters of bacterial axenic cultures fit the skew-Laplace distribution pattern: biological consequences.* Josep Vives-Rego, Olga Julià, Jaume Vidal-Mas, and Nicolai S. Panikov. AMS Subject Classification: 62E15, 62F03, 62F10. April 2008.
- **401** *Bipower variation for Gaussian processes with stationary increments.* Ole E. Barndorff-Nielsen, José Manuel Corcuera, Mark Podolskij and Jeannette H.C. Woerner. AMS Subject Classification (2000): 60G15, 60F17. May 2008.
- **402** *Insider trading and weak equilibrium.* A. Kohatsu-Higa and S. Ortiz-Latorre. AMS Subject Classification (2000): 49J40, 60G48, 93E20. May 2008.
- **403** *Groups definable in linear  $o$ -minimal structures.* Pantelis E. Eleftheriou. AMS Subject Classification (2000): 03C64, 46A40. June 2008.
- **404** *Definable group extensions in semi-bounded  $o$ -minimal structures.* Mário J. Edmundo and Pantelis E. Eleftheriou. AMS Subject Classification (2000): 03C64, 20K35. June 2008.
- **405** *A semi-linear group which is not affine.* Pantelis E. Eleftheriou. AMS Subject Classification (2000): 03C64, 57Q35. June 2008.
- **406** *Notions of bisimulation for Heyting-valued modal languages.* Pantelis E. Eleftheriou, Costas D. Koutras, and Christos Nomikos. AMS Subject Classification (2000): 03B45, 03B50, 68Q85. June 2008.
- **407** *Brown representability does not come for free.* Carles Casacuberta and Amnon Neeman. AMS Subject Classification (2000): 18E30, 55U35. July 2008.
- **408** *Localization of algebras over coloured operads.* Carles Casacuberta, Javier J. Gutiérrez, Ieke Moerdijk, and Rainer M. Vogt. AMS Subject Classification (2000): Primary: 55P43; Secondary: 18D50, 55P60. July 2008.