

# Selected applications of LLL in number theory

Denis SIMON ([simon@math.unicaen.fr](mailto:simon@math.unicaen.fr))  
LMNO - UMR 6139  
Université de Caen – France  
Campus II – Boulevard Mal Juin  
BP 5186 – 14032 Caen Cedex

June 14, 2007

## Abstract

In this survey, I describe some applications of LLL in number theory. I show in particular how it can be used to solve many different linear problems, to solve quadratic equations, to compute efficiently in number fields...

This survey is submitted to the LLL+25 Conference.

## 1 Introduction

The LLL algorithm has really many applications (on MathSciNet, it is cited in the references of at least 118 papers and in at least 50 reviews !!)

Among the most famous ones are of course those in lattice theory (the shortest vector problem : [FinPoh83] and [FinPoh85], [Die85], [Kan84] ; the closest vector problem : [Bab86], [AgrEriVarZeg02] ...) and also those for factoring polynomials (for example in [Klu07]), since this was precisely the application Lenstra, Lenstra, and Lovász presented in their original paper [LLL82]. At least as famous is the application to the knapsack problem : [Sha82], [Lag83], [FinPoh83] or [Sma98, §VI.2].

In this survey, I would like to present other selected applications in number theory, all of them leading to revolutionary results.

1. for linear problems : computing gcd's, kernels, Hermite normal forms, Smith normal forms, integral relations, linear dependence, algebraic dependence ...
2. solving quadratic equations : Gauss reduction in dimension 3, Shanks' algorithm for the 2-primary part of the class group  $Cl(\sqrt{D})$ , reduction of indefinite quadratic forms, quadratic equations in dimension 4 and more...
3. number fields : polynomial reduction, ideal reduction, computing the class group and the unit group, solving the principal ideal problem ...
4. testing conjectures (Hall, abc, Mertens, ...)

## Warnings

In most of the applications described in this paper, we only use two properties of the LLL algorithm. The first is that, when it is given a lattice  $L$  of dimension  $n$  and determinant  $d(L)$ , then LLL outputs a short vector  $\mathbf{b}_1$  bounded by

$$|\mathbf{b}_1| \leq 2^{(n-1)/4} d(L)^{1/n} .$$

The geometry of numbers would give better bounds. The second one is that LLL finds this vector in polynomial time, hence it gives a very efficient algorithm to solve the different problems.

As noticed in [Coh95, algo 2.6.3, rem 2], LLL only needs to know the Gram matrix of the lattice. This remark implies that it is equivalent to describe the lattice as embedded in  $\mathbb{R}^n$  with the euclidean norm or as  $\mathbb{Z}^n$  equipped with a positive definite quadratic form  $q$ . The result of LLL is then an integral unimodular transformation matrix, or just an  $n$ -tuple  $(x_1, \dots, x_n) \neq (0, \dots, 0)$  of integers such that

$$q(x_1, \dots, x_n) \leq 2^{(n-1)/2} \det(q)^{1/n} .$$

In this paper, LLL will be used mainly in small dimension : almost always  $n \leq 30$ , and very often  $n \leq 6$ . However, the coefficients may have hundreds or thousands of digits.

## 2 Reducing Linear Forms

A significative part of the material of this section comes from [Coh95, §2.7] and [Sma98, §IV.3 and IV.4].

• The best **approximations of a real number  $\alpha$  by rational numbers** are usually obtained by the continued fraction algorithm. As suggested in [LLL82], another way to obtain good approximations is to reduce the quadratic form

$$q(x, y) = M(\bar{\alpha}x - y)^2 + \frac{1}{M}x^2 ,$$

where  $\bar{\alpha}$  is usually a decimal approximation of  $\alpha$  to precision  $\frac{1}{M}$ . Indeed, when  $M$  is large and  $(x, y)$  is a short vector for the quadratic form  $q$ , then  $q(x, y) = O(1)$ , which implies  $x = O(\sqrt{M})$  and  $\alpha x - y = O\left(\frac{1}{\sqrt{M}}\right)$ . Typically, this implies  $|x| \approx |y| \approx \sqrt{M}$  and  $|\alpha - \frac{y}{x}| \approx \frac{1}{M}$ .

More explicitly, it consists of reducing the lattice  $\mathbb{Z}^2$  equipped with the quadratic form  $q(x, y) = M(\bar{\alpha}x - y)^2 + \frac{1}{M}x^2$ , or of applying the LLL algorithm with the 2-dimensional Gram matrix

$$\begin{pmatrix} \bar{\alpha}^2 M + \frac{1}{M} & -\bar{\alpha} M \\ -\bar{\alpha} M & M \end{pmatrix} .$$

This Gram matrix has determinant equal to 1, hence corresponds to a lattice of determinant 1. The underlying lattice in the euclidean plane  $\mathbb{R}^2$  is given by the matrix

$$\begin{pmatrix} \frac{1}{\sqrt{M}} & 0 \\ \bar{\alpha}\sqrt{M} & -\sqrt{M} \end{pmatrix} .$$

The result of LLL is then a unimodular integral transformation matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and the desired short vector  $(x, y)$  is just  $(a, c)$ . Indeed, the bound given by LLL asserts that  $q(x, y) \leq \sqrt{2}$ . This

inequality implies two others, namely

$$\begin{cases} |\bar{\alpha}x - y| \leq \frac{2^{1/4}}{\sqrt{M}} \\ |x| \leq 2^{1/4}\sqrt{M} . \end{cases}$$

Using now the inequality  $|\alpha - \bar{\alpha}| \leq \frac{1}{M}$ , we find

$$|\alpha x - y| \leq \frac{2^{5/4}}{\sqrt{M}} .$$

Example : Assume that we want to find a good rational approximation of  $\alpha = \pi$ , using the decimal approximation  $\bar{\alpha} = 3.1415926536$ . We have ten correct decimals, so we choose  $M = 10^{10}$ . The shortest vector found by LLL is then  $(x, y) = (99532, 312689)$ . We indeed see that  $|x| \approx |y| \approx 10^5 \approx \sqrt{M}$  and  $|\pi - \frac{y}{x}| \approx 0.3 \times 10^{-10} \approx \frac{1}{M}$ . This rational approximation is exactly the same as the one given by the continued fraction expansion of  $\pi$ , corresponding to the eight first coefficients  $[3, 7, 15, 1, 292, 1, 1, 1]$ .

If  $\alpha$  is close to 1, it might also be interesting to consider the more symmetrical quadratic form

$$q(x, y) = M(\bar{\alpha}x - y)^2 + \frac{1}{M}(x^2 + y^2) .$$

• There is an analog of this algorithm for **p-adic approximation** (for example in [Sma98, §VI.4]). If  $p$  is a prime number and  $\alpha$  is a  $p$ -adic unit, approximated modulo  $p^m$  by a rational integer  $\bar{\alpha}$ , then we can look for a short vector for the quadratic form

$$q(x, y, z) = M^2(\bar{\alpha}x - y - p^m z)^2 + \frac{1}{M}(x^2 + y^2) .$$

The Gram matrix of  $q$  is

$$\begin{pmatrix} \bar{\alpha}^2 M^2 + \frac{1}{M} & -\bar{\alpha} M^2 & -\bar{\alpha} M^2 p^m \\ -\bar{\alpha} M^2 & M^2 + \frac{1}{M} & M^2 p^m \\ -\bar{\alpha} M^2 p^m & M^2 p^m & M^2 p^{2m} \end{pmatrix}$$

and its determinant is  $p^{2m}$ . It corresponds to the lattice in  $\mathbb{R}^3$  generated by

$$\begin{pmatrix} \frac{1}{\sqrt{M}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{M}} & 0 \\ \bar{\alpha} M & -M & -p^m M \end{pmatrix}$$

of determinant  $p^m$ . Applied to this 3-dimensional Gram matrix, LLL returns a short integral vector  $(x, y, z)$  satisfying the inequality

$$q(x, y, z) \leq 2^{3/2} p^{2m/3} ,$$

from which we deduce in particular

$$|\bar{\alpha}x - y - p^m z| \leq 2^{3/4} p^{m/3} M^{-1} .$$

If we choose  $M$  such that  $2^{3/4} p^{m/3} < M < 2p^{m/3}$ , we have  $|\bar{\alpha}x - y - p^m z| < 1$  which implies that  $\bar{\alpha}x - y - p^m z = 0$ , since this is an integer. It now remains

$$x^2 + y^2 \leq 2^{5/2} p^m ,$$

whence

$$\begin{cases} |x| & \leq 2^{5/4}p^{m/2} \\ |y| & \leq 2^{5/4}p^{m/2}. \end{cases}$$

In summary, we have found rational integers  $x$  and  $y$  such that  $|x|$  and  $|y|$  are both  $O(p^{m/2})$ . Furthermore, when  $\alpha$  is a  $p$ -adic unit,  $x$  is also a  $p$ -adic unit, and we have a  $p$ -adic approximation  $|\alpha - \frac{y}{x}|_p \approx p^{-m}$  with the real bounds  $|x| \approx |y| \approx p^{m/2}$ .

When  $m = 1$ , this result proves that any element in  $\mathbb{F}_p^*$  can be represented by a fraction  $\frac{y}{x}$  with  $|x| = O(p^{1/2})$  and  $|y| = O(p^{1/2})$ . The corresponding algorithm is just an application of LLL in dimension 3.

Example : Consider the prime number  $p = 10^{10} + 19$  and the  $p$ -adic number  $\alpha = \frac{16}{17}$ . Its  $p$ -adic expansion is  $\alpha = 7647058839 + 9411764723p + 2352941180p^2 + \dots$ . Using the described algorithm, with  $m = 3$ ,  $\bar{\alpha} = 7647058839 + 9411764723p + 2352941180p^2 = 235294118988235296665882354556$ , LLL quickly finds the short vector  $(x, y, z) = (17, 16, 4)$ , hence recovers the original fraction.

- The previous approach (either real or  $p$ -adic) easily generalizes to obtain small values of a linear form  $L(x_1, \dots, x_n) = x_n + \sum_{i=1}^{n-1} \alpha_i x_i$  in dimension  $n$ , evaluated at small integers  $x_1, \dots, x_n$ . In the real case, we just have to reduce the quadratic form

$$M^{n-1}L(x_1, \dots, x_n)^2 + \frac{1}{M} \sum_{i=1}^{n-1} x_i^2$$

(this also appears in [LLL82]).

Even more generally, if we are given  $n$  linear forms  $L_1, \dots, L_n$  in  $n + m$  variables  $x_1, \dots, x_{n+m}$ , then we will have a **simultaneous approximation** if we reduce the single quadratic form

$$W_1 L_1(x_1, \dots, x_{n+m})^2 + \dots + W_n L_n(x_1, \dots, x_{n+m})^2 + W_{n+1} x_{n+1}^2 + \dots + W_{n+m} x_{n+m}^2$$

where the  $W_i$  are weights that are to be chosen depending on how much the linear forms and the coefficients have to be reduced compared to each other. This application to Diophantine approximation is described for example in [Lag85]. Many other applications of LLL applied to linear forms in logarithms are given in [Sma98, part 2] or in [Han07].

- For example, if the coefficients of the  $L_i$  are integers and if we want to insist on having exactly  $L_i(x_1, \dots, x_{n+m}) = 0$  for all  $i = 1, \dots, n$ , we will choose very large weights  $W_i$ ,  $i = 1, \dots, n$  and the other weights very small. This approach is used by [Poh87] to **compute the kernel of an integral matrix** and to give a modified version of LLL, called MLLL, applicable not only on a basis of a lattice, but also on a generating set of vectors  $\mathbf{b}_1, \dots, \mathbf{b}_{n+m}$  of a lattice of dimension  $n$ . The result of this algorithm is then a reduced basis of the lattice together with a matrix containing  $m$  independent relations among the  $\mathbf{b}_i$ . See also [Coh95, §2.7.1].

Example : Consider the matrix

$$M = \begin{pmatrix} 2491 & 5293 & 1032 & 5357 & 9956 \\ 6891 & 4280 & 3637 & 3768 & 4370 \\ 5007 & 4660 & 5712 & 7743 & 4715 \end{pmatrix},$$

which has been chosen randomly with coefficients less than  $10^4$ . Its kernel has dimension 2, and using gaussian elimination, we find that this kernel is generated by

$$\begin{pmatrix} \frac{59229512635}{82248101629} & \frac{33495205035}{82248101629} \\ -\frac{94247651922}{82248101629} & -\frac{180166533113}{82248101629} \\ -\frac{86522262381}{82248101629} & \frac{49731399425}{82248101629} \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Consider now the quadratic form  $A^4(2491v + 5293w + 1032x + 5357y + 9956z)^2 + A^4(6891v + 4280w + 3637x + 3768y + 4370z)^2 + A^4(5007v + 4660w + 5712x + 7743y + 4715z)^2 + A^{-6}y^2 + A^{-6}z^2$  or equivalently the lattice

$$\begin{pmatrix} 2491A^2 & 5293A^2 & 1032A^2 & 5357A^2 & 9956A^2 \\ 6891A^2 & 4280A^2 & 3637A^2 & 3768A^2 & 4370A^2 \\ 5007A^2 & 4660A^2 & 5712A^2 & 7743A^2 & 4715A^2 \\ 0 & 0 & 0 & A^{-3} & 0 \\ 0 & 0 & 0 & 0 & A^{-3} \end{pmatrix}.$$

This lattice has determinant  $c$ , with  $c = 82248101629$ . We now apply LLL to this quadratic form. If  $A$  is large enough (here  $A > 13$  works) then the values of the quadratic form are so small that the first two columns of the unimodular transformation matrix

$$U = \begin{pmatrix} 6845 & -300730 & -53974 & 121395 & -138794 \\ 285983 & 782775 & 114176 & -446636 & 387087 \\ -240869 & 202704 & 56844 & 19781 & 73475 \\ 118346 & -306061 & -64578 & 75646 & -131789 \\ -192463 & -197241 & -18341 & 164323 & -107769 \end{pmatrix}$$

are the coordinates of kernel. We can see that the coefficients are much smaller (6 digits) than with the other method (11 digits) Here, we have

$$MU = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

In [HavMajMat98], this idea is used to solve the **extended gcd problem** : given integers  $s_1, \dots, s_m$ , find a vector  $x = (x_1, \dots, x_m)$  with integral coefficients and small euclidean norm such that  $x_1s_1 + \dots + x_ms_m = \gcd(s_1, \dots, s_m)$ . The method is generalized to the problem of producing small unimodular transformation matrices for **computing the Hermite Normal Form** of an integer matrix (in [HavMajMat98]) and for **computing the Smith Normal Form** (in [Matwww] and [Jag05]).

- We can also want to **find  $\mathbb{Z}$ -linear relations among real numbers**. In a computer, an integer relation between real numbers can not of course be tested to be exactly 0, but only if it is small. This means that if an integer relation really exists, then LLL will probably find it. But LLL can also find other  $\mathbb{Z}$ -linear combinations that are not 0 but just small. In fact, if the relation is not

exactly 0, it is usually possible to prove it just by computing it with enough precision. However, it is the responsibility of the mathematician to prove that a relation found by LLL is exactly 0.

Example : We are aware of Machin's formula

$$a \arctan(1) + b \arctan\left(\frac{1}{5}\right) + c \arctan\left(\frac{1}{239}\right) = 0,$$

where  $a$ ,  $b$ , and  $c$  are small integers, but we do not know their values. We apply LLL to the quadratic form

$$A^2 \left( a \arctan(1) + b \arctan\left(\frac{1}{5}\right) + c \arctan\left(\frac{1}{239}\right) \right)^2 + (b^2 + c^2)$$

or to the lattice

$$\begin{pmatrix} \arctan(1)A & \arctan\left(\frac{1}{5}\right)A & \arctan\left(\frac{1}{239}\right)A \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

with a large value of  $A$ . If  $A$  is not large enough, LLL suggests that  $\arctan\left(\frac{1}{239}\right) \approx 0$ . It is clearly true, but not exactly 0. If  $A > 1000$ , LLL suggests the relation

$$\arctan(1) - 4 \arctan\left(\frac{1}{5}\right) + \arctan\left(\frac{1}{239}\right) \approx 0.$$

Now a rigorous proof that this is exactly 0 comes with the observation that through the transformation  $\exp(2i \arctan t) = \frac{1+it}{1-it}$  the relation is equivalent to

$$\frac{(1+i)(1+5i)^{-4}(1+239i)}{(1-i)(1-5i)^{-4}(1-239i)} = 1.$$

Other algorithms for detecting integer relations between reals are given in [FerFor79] and [FerBaiArn99] (without LLL) and [HasJusLagSchHel89] (with LLL). See also the `linddep` function in GP/PARI, described in [Coh95, §2.7.2].

Using these algorithms, Borwein and Bradley [BorBra97] have for example tried to generalize Apéry's formula

$$\zeta(3) = \frac{5}{2} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^3 \binom{2k}{k}}.$$

After an extensive search they suggested that there is no formula of the type

$$\zeta(5) = \frac{a}{b} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^5 \binom{2k}{k}}$$

at least as long as  $a$  and  $b$  are not astronomically large. However, they found

$$\zeta(7) = \frac{5}{2} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^7 \binom{2k}{k}} + \frac{25}{2} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^3 \binom{2k}{k}} \sum_{j=1}^{k-1} \frac{1}{j^4}$$

and similar expressions for  $\zeta(9)$ ,  $\zeta(11)$ , and proposed the following conjecture

$$\sum_{s=0}^{\infty} \zeta(4s+3)x^{4s} = \frac{1}{2} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{\binom{2k}{k} k^3} \frac{5k}{k^4 - x^4} \prod_{n=1}^{k-1} \left( \frac{n^4 + 4x^4}{n^4 - x^4} \right).$$

This was later proved to be true by [AlmGra99]. Similar methods and results are also obtained about  $\zeta(2s+2)$  in [BorBra06].

- A special case of integer relations between real (or complex) numbers is the case when the real numbers are powers of the same real number. In this case, a linear relation  $\sum_{i=1}^n x_i \alpha^i = 0$  proves that  $\alpha$  is an algebraic number of degree at most  $n$  and the given polynomial  $\sum_{i=1}^n x_i X^i \in \mathbb{Z}[X]$  is a multiple of its minimal polynomial. In some sense, LLL is able to **recover the minimal polynomial of an algebraic number**. It is important to remark that in this algorithm, the degree  $n$  is fixed, so that it can only find a polynomial if we have a bound on its degree. See for example the `algdep` function in `GP/PARI`, described in [Coh95, §2.7.2].

In practice, since we only work with real approximations of  $\alpha$ , the polynomials found are only candidates. However, it is quite common that checking the vanishing of a polynomial at  $\alpha$  is easy. Hence, the algorithm can be used in both ways: either to give evidence that  $\alpha$  is a transcendental number, or to build a polynomial taking such a small value at  $\alpha$ , that there is a high chance that it in fact vanishes exactly at  $\alpha$ .

This method has been used in [KanMcG86] to give evidence that the numbers  $e \pm \pi$  and some other numbers are transcendental. It is described in more details in [KanLenLov88], where a surprising application is given for the **factorization of polynomials in  $\mathbb{Z}[X]$** : Start with a polynomial  $P \in \mathbb{Z}[X]$  of degree  $n$  and compute sufficiently many digits of the real and imaginary parts of a root  $\alpha$  (using your preferred method, for example by Newton's method) ; then use the algorithm to look for an integral polynomial  $Q$  vanishing at  $\alpha$  ; if  $Q$  divides  $P$ , we are done, otherwise  $P$  has no proper factor. See also [Len84]. Other polynomial factorization algorithms using LLL are given in [Sch84] or [Klu07].

Example : Imagine we would like to prove that  $\alpha = e + \pi$  is an algebraic number of degree 4. This would mean that there are integers  $a_4, a_3, a_2, a_1$ , and  $a_0$ , not all 0, such that  $a_0\alpha^4 + a_1\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = 0$ . Using an approximation of  $\alpha$  to 20 decimals, LLL suggests the relation

$$127\alpha^4 - 399\alpha^3 - 2268\alpha^2 + 1849\alpha - 2417 \approx 0.$$

In order to verify this relation, we increase the precision of  $\alpha$  to 40 decimals and observe that the expression is not 0, but close to  $-4.6 \cdot 10^{-13}$ . Using this new precision, LLL now suggests a new relation

$$3498343\alpha^4 - 940388\alpha^3 - 116624179\alpha^2 + 761230\alpha + 64496487 \approx 0.$$

Repeating this procedure always gives a tentative polynomial with growing coefficients, but never vanishing exactly at  $\alpha$ . Of course, this does not prove that  $\alpha$  is transcendental, and it does even not prove that is not algebraic of degree 4. However, it proves that there is no quartic polynomial with small coefficients vanishing at  $\alpha$ .

Another illustration of this application of LLL is given in [KalYui91]. See also [Coh00, §6.3.2]. For an imaginary quadratic field  $K$  of discriminant  $d$ , the Hilbert class field of  $K$  is of relative degree  $h = \#Cl(K)$  over  $K$ . If  $(\alpha_k)_{1 \leq k \leq h}$  are the roots of  $h$  inequivalent binary quadratic forms

of discriminant  $d$ , then  $j_k = j(\alpha_k)$  (where the function  $j$  is the modular function) are the roots of a degree  $h$  polynomial  $H_d \in Z[X]$  defining exactly the **Hilbert class field** of  $K$ . Instead of computing each of the  $h$  values  $j_k$ , it is possible to compute just one such value and to recover the whole polynomial using the previous algorithm. However, since the coefficients of  $H_d$  are usually quite large, it is preferable to use the Weber function  $f(z)$  instead of the modular function  $j(z)$ . The corresponding polynomial  $h_d$  still defines the Hilbert class field, but the coefficients can be 12 times smaller.

Example : For the discriminant  $d = -32$ , the class number is 3 and the class group is cyclic of order 3, generated by  $P = 2x^2 + x + 3$ . Its roots in the upper half plane is

$$\alpha_1 = \frac{-1 + i\sqrt{23}}{4} \approx -0.25 + 1.19895788082817988539935951604i .$$

We can now compute

$$j(\alpha_1) \approx 737.849984966684102752369273665 + 1764.01893861274614164378642717i .$$

This should be an algebraic integer of degree 6 (and in fact of degree 3). Now, LLL suggests that the minimal polynomial of  $j$  could be  $P = x^3 + 3491750x^2 - 5151296875x + 12771880859375$ . It only remains to prove that this polynomial indeed defines an unramified extension of  $\mathbb{Q}(\sqrt{-23})$ , but this is a different story !

### 3 Solving quadratic equations over the rationals

In this section, we consider the problem of solving quadratic equations over  $\mathbb{Q}$ . Since testing the solvability of these equations is usually easy, we can always assume that they are indeed solvable.

The first nontrivial family of quadratic equations that are interesting to solve are the ternary quadratic equations  $q(x, y, z) = 0$ , with rational coefficients and unknowns. Among them is the diagonal equation, also called Legendre's equation :  $ax^2 + by^2 + cz^2 = 0$ . Usually the general nondiagonal equation  $q(x, y, z) = 0$  is transformed into a diagonal one of Legendre type. For Legendre's equation, a great deal of algorithms exist.

For example, in [Ser88, Ch. IV §3] or [Sma98, Ch. IV §3.3], the solution of  $ax^2 + by^2 + cz^2 = 0$  is deduced from the solution of  $a'x^2 + b'y^2 + c'z^2 = 0$  where the new coefficients are smaller than the old ones. However, this reduction depends on the possibility of extracting square roots modulo  $a$ ,  $b$  or  $c$ , which is only possible if we know the factorization of  $abc$ . During the whole algorithm, the total number of factorizations is quite large. The worst drawback is certainly that the numbers that have to be factored may also be quite large. Solving quadratic equations with these algorithms uses only a few lines in theory, but is extremely slow in practice.

Fortunately, a couple of algorithms exist, which do not factor any other integers than  $a$ ,  $b$ , and  $c$ . It seems impossible in general to avoid these three factorizations. Such an algorithm is given in [CreRus03]. In practice it indeed runs fast.

Other algorithms exist, which use the reduction theory of lattices. They all share the same property of using no other factorization than that of  $abc$ . Since the LLL algorithm can reduce quadratic forms, it is not surprising that it can be used to solve quadratic equations over the rationals. However, if a quadratic equation has a solution, it is certainly not positive definite. The problem is that LLL can a priori only handle positive definite quadratic forms. There are two ways to go around this problem :

- either build a new quadratic form, which is positive definite and the reduction of which can help us in solving the initial quadratic equation,
- or adapt LLL to indefinite quadratic forms.

A positive definite quadratic form attached to the problem is of course  $q = |a|x^2 + |b|y^2 + |c|z^2$ . However, reducing  $\mathbb{Z}^3$  with this quadratic form will not give anything, since it is already orthogonal hence reduced. According to [CocMit98], if  $a$ ,  $b$ , and  $c$  are coprime squarefree integers, some integral solutions of  $ax^2 + by^2 + cz^2 = 0$  lie in a sublattice of  $\mathbb{Z}^3$  of index  $2|abc|$  defined by the congruences

$$\begin{aligned} by - \lambda_1 z &\equiv 0 \pmod{a} \\ ax - \lambda_2 z &\equiv 0 \pmod{b} \\ ax - \lambda_3 z &\equiv 0 \pmod{c} \end{aligned}$$

plus another condition modulo a power of 2, where  $\lambda_1$ ,  $\lambda_2$ , and  $\lambda_3$  are any choice of squareroots of  $-bc$ ,  $-ac$ ,  $-ab$  modulo  $a$ ,  $b$ , and  $c$  respectively. A smallest vector of this lattice (equipped with the positive definite quadratic form  $|a|x^2 + |b|y^2 + |c|z^2$ ) will give a solution. Using this algorithm, we see that LLL (in dimension 3) can be used to **solve Legendre's equation**.

The method of Gauss himself in [Gauss, sections 272, 274, 294] in 1801, was already similar, since he builds the same lattice, using the same congruences. But Gauss reduces directly the corresponding indefinite quadratic form. We can summarize his method in two steps : 1) compute square roots modulo  $a$ ,  $b$ , and  $c$ , and build another quadratic form with determinant  $-1$  ; 2) Reduce and solve this new quadratic form. The reduction of the indefinite quadratic form suggested by Gauss works simultaneously on the quadratic form and its dual. It is quite different from any version of LLL. This reduction algorithm is analyzed in [Lag80] and proved to run in polynomial time. It is interesting to note that the algorithm is used in [Sha71] and [BosSte96] to compute in polynomial time the 2-Sylow subgroup of the class group  $Cl(\sqrt{D})$ .

The algorithms described up to now are quite specific to solve Legendre equations, that is diagonal ternary quadratic equations over  $\mathbb{Q}$ . Some of them can also solve semi-diagonal equations (of the form  $ax^2 + bxy + cy^2 = dz^2$ , but are not able to solve general ternary quadratic equations. Of course, it is always possible to diagonalize any quadratic equation, but if we do so, the integers that are to be factored may be huge (hence impossible to factor in a reasonable amount of time) compared to the determinant of the original equation. An example is given in [Sim05] of an equation with determinant equal to  $-1$  and coefficients having more than 1300 decimal digits : reducing the equation to a diagonal one would require the factorization of integers of that size !

In [Sim05] an algorithm is given to solve general ternary quadratic equations, without requiring other factorizations than that of the determinant. The main strategy follows Gauss :

- compute first an integral quadratic form, equivalent to the initial one, which has determinant  $-1$  (this is the *minimization* step);
- then reduce this indefinite quadratic form (this is the *reduction* step).

The minimization step only uses linear algebra modulo the prime divisors of the determinant. The reduction step could certainly use the reduction of Gauss, but another reduction algorithm is proposed. In fact when we apply LLL to a quadratic form which is indefinite, without changing

LLL, the algorithm may enter into infinite loops. Indeed, the swap condition in the algorithm (also called the Lovász condition) is just

$$|\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*|^2 < c|\mathbf{b}_{i-1}^*|^2,$$

which tests whether the norm of the vector  $\mathbf{b}_{k-1}^*$  decreases when we interchange  $\mathbf{b}_{k-1}$  and  $\mathbf{b}_k$ . In terms of the underlying quadratic form  $q$ , this test is equivalent to

$$q(\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*) < cq(\mathbf{b}_{i-1}^*).$$

In the case where  $q$  is not positive definite, these quantities may be negative, and a swap may increase their absolute values. If we just add absolute values in this test

$$|q(\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*)| < c|q(\mathbf{b}_{i-1}^*)|,$$

the new algorithm, which we call the **Indefinite LLL**, has the following properties :

**Theorem (IndefiniteLLL).** *Let  $q$  be a quadratic form over  $\mathbb{Z}^n$  defined by  $q(\mathbf{x}) = \mathbf{x}^t Q \mathbf{x}$  with a symmetric matrix  $Q \in \mathcal{M}_n(\mathbb{Z})$  such that  $\det(Q) \neq 0$ . The output of the IndefiniteLLL Algorithm applied with a parameter  $\frac{1}{4} < c < 1$  to a basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  of  $\mathbb{Z}^n$  is*

- either some  $\mathbf{x} \in \mathbb{Z}^n$  such that  $q(\mathbf{x}) = 0$ ,
- or a reduced basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  such that

$$|(\mathbf{b}_{k-1}^*)^2| \leq \gamma |(\mathbf{b}_k^*)^2| \quad \text{for } 1 < k \leq n,$$

and

$$1 \leq |(\mathbf{b}_1)^2|^n \leq \gamma^{n(n-1)/2} |\det(Q)|,$$

where  $\gamma = (c - \frac{1}{4})^{-1} > \frac{4}{3}$ .

If furthermore  $q$  is indefinite, we have

$$1 \leq |(\mathbf{b}_1)^2|^n \leq \frac{3}{4} \gamma^{n(n-1)/2} |\det(Q)|.$$

For a better comparison with the standard properties of LLL-reduced bases, we have used the notation  $(\mathbf{b})^2$  for  $q(\mathbf{b})$ , which needs not to be positive in this situation. In both cases, the algorithm finishes in after a polynomial number of steps. We have now an efficient way to **solve general ternary quadratic equations**. Combining the algorithm of [Sha71] and [BosSte96] with this indefinite LLL, we can now claim that LLL can also **compute the 2-Sylow subgroup of the class group  $Cl(\sqrt{D})$** .

One of the key point of this algorithm is to reduce indefinite quadratic forms. Up to now, we have seen two algorithms for this : one by Gauss, which only works in dimension 3, and one in [Sim05], which also works in higher dimensions. In fact, other algorithms exist. For example, in [IvaSza96] an algorithm very similar to [Sim05] is given. The main difference is in the way it handles isotropic vectors. In one case, the algorithm simply stops, whereas in the other case it applies a complicated subroutine. Because of this small difference, the quality of the reduction proved in [Sim05] is slightly better than LLL, whereas it is worse than LLL in [IvaSza96]. I would like to mention a last algorithm used for the reduction of indefinite quadratic forms. Assume that the indefinite quadratic form  $q$  is diagonal in some basis (typically obtained by a Gram-Schmidt

procedure). Then we can bound  $|q|$  by the quadratic form  $q'$  obtained just by taking the absolute values of the coefficients of  $q$  in this basis! Since these quadratic forms have the same determinant (up to sign), a reduced basis for  $q'$  will also be a reduced basis for  $q$ , and the quality of the reduction will be exactly the same as in LLL. This is precisely what is suggested in [CocMit98], where the diagonal form  $ax^2 + by^2 + cz^2$  is bounded by  $|a|x^2 + |b|y^2 + |c|z^2$ . The only drawback of this method is that during the diagonalization step, we may introduce large denominators, a fact that can slow down the algorithm. No serious comparison has been done between these different algorithms.

A generalization of the previous algorithms has been recently proposed in [Sim06] to **solve quadratic equations in higher dimensions**. The main strategy of minimization/reduction still works, but in a different way. A quadratic form  $q$  in dimension  $n$  is minimizable if we can find an integral quadratic form  $q'$  with determinant  $\pm 1$  and equivalent to  $q$  over  $\mathbb{Q}$ . For an indefinite ternary quadratic form, minimizability is equivalent to solvability. In higher dimension  $n \geq 4$ , this property is not true any more.

When  $n = 4$ , we can use a trick of Cassels [Cas59]: there exists a binary quadratic form  $q_2$  such that  $q \oplus q_2$  is minimizable and is equivalent to  $H \oplus H \oplus H$ , where  $H$  is an hyperbolic plane (the  $\oplus$  notation denotes the direct sum of quadratic modules; in terms of matrices, it just corresponds to taking the larger matrix, which is diagonal by blocks, and the blocks are  $q$  and  $q_2$ ). This binary quadratic form  $q_2$  can be computed explicitly from the local invariants of  $q$  and from the 2-Sylow of the class group  $Cl(\sqrt{D})$  ( $D$  being the determinant of  $q$ ). Hence, using LLL and [BosSte96], we can build this  $q_2$  as soon as we know the factorization of  $D$ ! Now, the indefinite LLL algorithm rapidly gives the equivalence between  $q \oplus q_2$  and  $H \oplus H \oplus H$  (this is the reduction step). The remaining part of the algorithm is just linear algebra: a vector in the intersection of a 3-dimensional isotropic subspace for  $H \oplus H \oplus H$  with another 4-dimensional subspace (in the ambient space of dimension 6) will give a solution for  $q(\mathbf{x}) = 0$ .

When  $n \geq 5$ , a similar trick applies, except that the minimization works either in dimension  $n$ ,  $n + 1$ ,  $n + 2$  or  $n + 3$ .

## 4 Number fields

I see two main reasons why the computation of class groups in imaginary quadratic fields are feasible. The first one is that thanks to the correspondence between ideals and quadratic forms (see [Coh95, §5.2]), we can use Gauss reduction. The second one is McCurley's sub-exponential algorithm described in [HafMcC89]. This algorithm assumes the validity of the Generalized Riemann Hypothesis. It is also described in [BucDul91] or [Coh95, §5.5]. It relies on the notion of *relations*, that is expressions of ideals  $\mathfrak{a}$  in the form

$$\mathfrak{a} = \alpha \prod f_i^{e_i}$$

where  $\alpha$  is an element of  $K^*$  and  $f_i$  are the ideals of the factor basis.

McCurley's algorithm has been extended to general number fields. In [Buc90] and [CohDiaOli93] (see also [Coh95, §6.5] and [Bel04]), it is explained how one can compute simultaneously the class group and the units from the relations between ideals. It is also explained how one can perform the ideal reduction. The idea is the following.

- The  $K$  be a number field of degree  $n$  over  $\mathbb{Q}$  with signature  $(r_1, r_2)$ . Let  $\sigma_1, \dots, \sigma_{r_1}$  be the real embeddings of  $K$  and  $\sigma_{r_1+1}, \dots, \sigma_n$  the complex embeddings. For an element  $x \in K$ , we define the

$T_2$ -norm of  $x$  to be  $\|x\| = \sqrt{T_2(x)}$  where

$$T_2(x) = \sum_{i=1}^n |\sigma_i(x)|^2.$$

This  $T_2$ -norm can immediately be extended to  $\mathbb{R}^n \simeq K \otimes_{\mathbb{Q}} \mathbb{R}$  and defines a positive definite quadratic form. Equipped with this quadratic form, the ring of integers  $\mathbb{Z}_K$  of  $K$  is a lattice of determinant  $\det(\mathbb{Z}_K) = |\text{disc } K|^{1/2}$ . Choosing an LLL-reduced basis  $(w_i)$  of  $\mathbb{Z}_K$  (for the  $T_2$ -norm) will give  $\mathbb{Z}_K$  the property that elements with small coefficients will also have a small (algebraic-)norm. This is just an application of the arithmetic-geometric mean :

$$n|\mathcal{N}_{K/\mathbb{Q}}(x)|^{2/n} \leq T_2 \left( \sum_{i=1}^n x_i w_i \right) \leq \left( \sum_{i=1}^n x_i^2 \right) \left( \sum_{i=1}^n T_2(w_i) \right).$$

Of course the converse is not true since in general there are infinitely many units, that is elements of  $\mathbb{Z}_K$  such that  $\mathcal{N}_{K/\mathbb{Q}}(x) = \pm 1$ , but there are only finitely many elements with bounded  $T_2$ -norm or bounded coefficients. As indicated in [Bel04], choosing an LLL-reduced basis for the  $T_2$ -norm, usually gives a **faster arithmetic in the number field**.

- The **polynomial reduction algorithm** described in [CohDia91] and [Coh95, §4.4.2] is a byproduct of this reduction. Indeed, if we have an irreducible polynomial, with splitting field  $K$ , one can compute an LLL-reduced integral basis of  $\mathbb{Z}_K$ , and look for a primitive element with small coefficients. Its minimal polynomial usually has small coefficients. For example, if we look for a defining polynomial for the field  $\mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5})$  the function `polcompositum` of PARI/GP (which implements the standard idea of the proof of the primitive element theorem) gives

$$x^{16} - 72x^{14} + 1932x^{12} - 22552x^{10} + 154038x^8 - 582456x^6 + 1440748x^4 - 1486824x^2 + 3721041$$

with discriminant  $2^{312}3^{50}5^87^4643^2$ . The function `polredabs` of PARI/GP implements this polynomial reduction algorithm and just finds the polynomial

$$x^{16} - 7x^{12} + 48x^8 - 7x^4 + 1$$

having discriminant  $2^{64}3^{32}5^8$ .

- From my point of view, the most important application of this is the notion of **LLL-reduction of ideals** introduced in [Buc90] and [CohDiaOli93], [Coh95, §6.5.1]. Any integral ideal  $\mathfrak{a}$  of  $\mathbb{Z}_K$  of norm  $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})$  is a sublattice of  $\mathbb{Z}_K$  of index  $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})$ . Hence, we can apply LLL to this sublattice. A short vector for this  $T_2$ -norm is certainly an element of  $\mathfrak{a}$ , that is an element  $a \in \mathbb{Z}_K$  satisfying  $a = \mathfrak{a}\mathfrak{b}$  for some integral ideal  $\mathfrak{b}$  such that  $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{b})$  is bounded independently of  $\mathfrak{a}$  (notice that this claim gives a proof of the finiteness of the class group). If  $\mathfrak{b} = 1$ , we have found a generator of the principal ideal  $\mathfrak{a}$ . If the ideal  $\mathfrak{b}$  can be factored in the factor basis, we have a relation. This is exactly the way relations are found in McCurley's algorithm. Hence, we see that combined with McCurley's algorithm, LLL gives a way to **compute class groups and solve the principal ideal problem**. Furthermore, relations among principal ideals give units. More precisely, a relation of the type  $\alpha\mathbb{Z}_K = \beta\mathbb{Z}_K$  is equivalent to the fact that  $\alpha\beta^{-1}$  is a unit. Hence, the algorithm is also able to **compute the unit group**.

## 5 Conclusion : breaking records

It is a popular belief that when one wants to break records in number theory, one has to use LLL. The applications of LLL given in this section are therefore more isolated, but all serve the same goal : testing conjectures with numerical evidences.

- A revolutionary application was given in 1985 by Odlyzko and te Riele in [OdlRie85], where they **give a disproof of the very old conjecture of Mertens**. This conjecture says that if we consider the Möbius function  $\mu(n)$  and its counting function  $M(x) = \sum_{n \leq x} \mu(n)$ , then we should have  $|M(x)| < \sqrt{x}$ . After having computed the 200 first zeros of the Riemann zeta function and used LLL in dimension 200, they were able to prove that  $\limsup M(x)x^{-1/2} > 1.06$  and  $\liminf M(x)x^{-1/2} < -1.009$ . It has been improved in [KotRie06] using the same technics to  $\limsup M(x)x^{-1/2} > 1.218$  and  $\liminf M(x)x^{-1/2} < -1.229$ .

- In a very surprising paper, [Elk00], Elkies applies LLL, not to compute points *on* curves, but to **compute points near curves with small height**. The naive idea to list points of small height on a curve defined by an homogeneous equation  $F(x, y, z) = 0$  is to loop on all possible values for  $x$  and  $y$  with  $|x| < N$  and  $|y| < N$ , compute the corresponding values of  $z$  and test for their height. If we also want points near the curve, a loop on  $z$  is also needed. If we are looking for points at distance at most  $\delta$  to the curve, the idea of Elkies is to cut the curve into small pieces, each of length  $= O(\delta^{1/2})$ . For each piece, the curve is approximated by a segment, and the search region is approximated by a box  $B$  of height, length and width proportional to  $N, \delta^{1/2}N, \delta N$ . Hence, as soon as  $\delta \gg N^{-2}$ , we can expect that the box  $B$  of volume  $N^3\delta^{3/2}$  will contain  $O(N^3\delta^{3/2})$  integral points. Now, **finding all integral points in a box** is a standard application of LLL : find a reduced basis of  $B$  and loop over all points with small coefficients in this basis. Using this approach, he is able to find the following surprising relations :

$$386692^7 + 411413^7 \approx 441849^7 ,$$

$$2063^\pi + 8093^\pi \approx 8128^\pi .$$

This last example raises the question whether there are infinitely many integral solutions to  $|x^\pi + y^\pi - z^\pi| < 1$ . Using some more tricks leads to the relation

$$5853886516781223^3 - 447884928428402042307918^2 = 1641843$$

which is related to Hall's conjecture, telling that if  $k = x^3 - y^2$ , then  $|k| \gg_\epsilon x^{1/2-\epsilon}$ . This example satisfies  $x^{1/2}/|x^3 - y^2| > 46.6$ , improving the previous record by a factor of almost 10.

- See also [Dok04] for examples related the the abc conjecture and the Szpiro conjecture.

## References

- [AgrEriVarZeg02] E. Agrell, T. Eriksson, A. Vardy, K. Zeger : *Closest point search in lattices*, IEEE Trans. Inf. Theory **48**, No.8, 2201–2214 (2002).
- [AlmGra99] G. Almkvist, A. J. Granville *Borwein and Bradley's Apéry-like formulae for  $\zeta(4n+3)$* , Experiment. Math. **8**, no. 2, 197–203 (1999).

- [Bab86] L. Babai : *On Lovász lattice reduction and the nearest lattice point problem*, *Combinatorica* **6**, 1–13 (1986).
- [Bel04] K. Belabas : *Topics in computational algebraic number theory*, *J. Théor. Nombres Bordeaux* **16** no. 1, 19–63 (2004).
- [BorBra97] J. Borwein, D. Bradley : *Empirically determined Apéry-like formulae for  $\zeta(4n + 3)$* , *Exp. Math.* **6**, No.3, 181–194 (1997).
- [BorBra06] J. Borwein, D. Bradley : *Experimental determination of Apéry-like identities for  $\zeta(2n + 2)$* , *Exp. Math.* **15**, No. 3, 281–289 (2006).
- [BosSte96] W. Bosma, P. Stevenhagen : *On the computation of quadratic 2-class groups* *J. Théor. Nombres Bordeaux.* **8**, No.2, 283–313 (1996); erratum *ibid.* **9**, No.1, 249 (1997).
- [Buc90] J. Buchmann : *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, *Sémin. Théor. Nombres, Paris/Fr. 1988–89*, *Prog. Math.* **91**, 27–41 (1990).
- [BucDul91] J. Buchmann, S. Düllmann : *A probabilistic class group and regulator algorithm and its implementation*, *Computational number theory, Proc. Colloq., Debrecen/Hung. 1989*, 53–72 (1991).
- [Cas59] J.W.S. Cassels : *Note on quadratic forms over the rational field*, *Proc. Cambridge Philos. Soc.* **55**, 267–270 (1959).
- [CocMit98] T. Cochrane, P. Mitchell : *Small solutions of the Legendre equation*, *J. Number Theory* **70**, No.1, 62–66 (1998).
- [Coh95] H. Cohen : *A Course in Computational Algebraic Number Theory*, *Graduate Texts in Math.* **138**, Second corrected printing, Springer–Verlag (1995).
- [Coh00] H. Cohen : *Advanced Topics in Computational Algebraic Number Theory*, *Graduate Texts in Math.* **193**, Springer–Verlag (2000).
- [CohDia91] H. Cohen, F. Diaz y Diaz : *A polynomial reduction algorithm*, *Sémin. Théor. Nombres Bordeaux.*, Sér. II **3**, No.2, 351–360 (1991).
- [CohDiaOli93] H. Cohen, F. Diaz y Diaz, M. Olivier : *Subexponential algorithms for class group and unit computations*, *J. Symbolic Comput.* **24**, No 3–4, 433–441 (1997), *Computational algebra and number theory* (London, 1993).
- [CreRus03] J.E. Cremona, D. Rusin: *Efficient solution of rational conics*, *Math. Comp.* **72**, 1417–1441 (2003).
- [Die85] U. Dieter : *Calculating shortest vectors in a lattice* *Ber. Math.-Stat. Sect. Forschungszent. Graz* **244**, 14 p. (1985).
- [Dok04] T. Dokchitser : *LLL & ABC*, *J. Number Theory* **107**, No.1, 161–167 (2004).

- [Elk00] N.D. Elkies : *Rational points near curves and small nonzero  $|x^3 - y^2|$  via lattice reduction*, W. Bosma (ed.), Algorithmic number theory. 4th international symposium. ANTS-IV, Leiden, the Netherlands, July 2-7, 2000. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. **1838**, 33–63 (2000).
- [FerBaiArn99] H.R.P. Ferguson, D. Bailey, S. Arno : *Analysis of PSLQ, an integer relation finding algorithm*, Math. Comput. **68**, No.225, 351–369 (1999).
- [FerFor79] H.R.P. Ferguson, R.W. Forcade : *Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two*, Bull. Am. Math. Soc., New Ser. **1**, 912–914 (1979).
- [FinPoh83] U. Fincke, M. Pohst : *On reduction algorithms in non-linear integer mathematical programming*, Operations research, Proc. 12th Annu. Meet., Mannheim 1983, 289–295 (1984).
- [FinPoh85] U. Fincke, M. Pohst : *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comput. **44**, 463–471 (1985).
- [Gauss] C.F. Gauss: *Disquisitiones Arithmeticae*, Springer Verlag (1986).
- [HafMcC89] J. Hafner, K. McCurley : *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2**, no. 4, 837–850 (1989).
- [Han07] G. Hanrot : *LLL : A tool for effective diophantine approximation*, this volume.
- [HasJusLagSchHel89] J. Håstad, B. Just, J.C. Lagarias, CP.P Schnorr (B. Helfrich, B.) : *Polynomial time algorithms for finding integer relations among real numbers*, SIAM J. Comput. **18**, No.5, 859–881 (1989).
- [HavMajMat98] G. Havas, B.S. Majewski, K.R. Matthews : *Extended GCD and Hermite normal form algorithms via lattice basis reduction*, Exp. Math. **7**, No.2, 125–136 (1998) ; *Addenda and errata: Extended GCD and Hermite normal form algorithms via lattice basis reduction*, Exp. Math. **8**, No.2, 205 (1999).
- [IvaSza96] G. Ivanyos, A. Szántó : *Lattice basis reduction for indefinite forms and an application*, Discrete Math. **153**, No.1–3, 177–188 (1996).
- [Jag05] G. Jäger. *Reduction of Smith normal form transformation matrices* Computing **74**, No.4, 377–388 (2005).
- [KalYui91] E. Kaltofen, N. Yui : *Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction*, Number theory, Proc. Semin., New York/NY (USA) 1989–1990, 149–202 (1991).
- [Kan84] R. Kannan : *Lattices, basis reduction and the shortest vector problem*, Theory of algorithms, Colloq. Pécs/Hung. 1984, Colloq. Math. Soc. János Bolyai **44**, 283–311 (1986).
- [KanLenLov88] R. Kannan, A.K. Lenstra, L. Lovász : *Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers*, Math. Comput. **50**, No.181, 235–250 (1988).

- [KanMcG86] R. Kannan, L.A. McGeoch : *Basis reduction and evidence for transcendence of certain numbers*, Foundations of software technology and theoretical computer science, Proc. 6th Conf., New Delhi/India 1986, Lect. Notes Comput. Sci. 241, 263–269 (1986).
- [Klu07] J. Klüners : *The van Hoeij algorithm for factoring polynomials*, this volume.
- [KotRie06] T. Kotnik, H. te Riele : *The Mertens Conjecture Revisited*, F. Hes, S. Pauli, M. Pohst (ed.), ANTS 2006 Berlin, Lect. Notes Comput. Sci. **4076**, 156–167 (2006).
- [Lag80] J.C. Lagarias : *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*, J. Algorithms **1**, 142–186 (1980).
- [Lag83] J.C. Lagarias : *Knapsack public key cryptosystems and Diophantine approximation*, in *Advances in cryptology* (Santa Barbara, Calif., 1983), 3–23, Plenum, New York, (1984).
- [Lag85] J.C. Lagarias : *The computational complexity of simultaneous diophantine approximation problems*, SIAM J. Comput. **14**, 196–209 (1985).
- [Len84] A.K. Lenstra : *Polynomial factorization by root approximation*, EUROSAM 84, Symbolic and algebraic computation, Proc. int. Symp., Cambridge/Engl. 1984, Lect. Notes Comput. Sci. **174**, 272–276 (1984).
- [LLL82] A.K. Lenstra, H.W. Lenstra, L. Lovász : *Factoring polynomials with rational coefficients* Math. Ann. **261**, 515–534 (1982).
- [Matwww] K. Matthews : [www.numbertheory.org/111.html](http://www.numbertheory.org/111.html)
- [OdlRie85] A.M. Odlyzko, H. te Riele : *Disproof of the Mertens conjecture* J. Reine Angew. Math. **357**, 138–160 (1985).
- [Poh87] M. Pohst : *A modification of the LLL reduction algorithm*, J. Symb. Comput. **4**, 123–127 (1987).
- [Sch84] A. Schönhage : *Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm*, in *Automata, languages and programming*, 11th Colloq., Antwerp/Belg. 1984, Lect. Notes Comput. Sci. **172**, 436–447 (1984).
- [Ser88] J.-P. Serre: *Cours d'arithmétique*, P.U.F. 3d edition (1988).
- [Sha82] A. Shamir : *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem*, in *23rd annual symposium on foundations of computer science* (Chicago, Ill., 1982), 145–152, IEEE, New York, (1982)
- [Sha71] D. Shanks : *Gauss's ternary form reduction and the 2-Sylow subgroup*, Math. Comput. **25**, 837–853 (1971) ; *Corrigendum: Gauss's ternary form reduction and the 2-Sylow subgroup*, Math. Comput. **32**, 1328–1329 (1978).
- [Sim05] D. Simon : *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comput. **74**, No.251, 1531–1543 (2005).
- [Sim06] D. Simon : *Quadratic equations in dimensions 4, 5, and more*, preprint (2006).

[Sma98] N.P. Smart : *The algorithmic resolution of diophantine equations*, London Mathematical Society Student Texts. **41**. Cambridge: Cambridge University Press. (1998).