BULL. AUSTRAL. MATH. SOC. 11T24, 11T71, 11Y40, 94A60
VOL. 58 (1998) [147–154]

LATTICE BASIS REDUCTION, JACOBI SUMS AND HYPERELLIPTIC CRYPTOSYSTEMS

JOE BUHLER AND NEAL KOBLITZ

Using the LLL-algorithm for finding short vectors in lattices, we show how to compute a Jacobi sum for the prime field $\mathbf{F}_p$ in $\mathbf{Q}\left(e^{2\pi i/n}\right)$ in time $O\left(\log^3 p\right)$, where n is small and fixed, p is large, and $p \equiv 1 \pmod{n}$. This result is useful in the construction of hyperelliptic cryptosystems.

Let $n = 2g + 1$ be an odd prime, and let $p \equiv 1 \pmod{n}$. Consider the hyperelliptic curve

$$C: \ Y^2 + Y = X^n \tag{1}$$

of genus g over $\mathbf{F}_p$. Let N be the number of $\mathbf{F}_p$-points on the jacobian $\mathbf{J}$ of the curve C. Our purpose is to give a fast method to compute N when n is small and p is large — that is, in the cases when the jacobian group might be suitable for the hyperelliptic cryptosystems introduced in [7].

The jacobian $\mathbf{J}$ of the curve C is a quotient of the jacobian of the famous Fermat curve $X^n + Y^n = 1$. Formulas for the number of points on C and on $\mathbf{J}$ go back many years; a detailed treatment can be found, for example, in [6]. We shall state what we need without proof.

Let $\zeta = e^{2\pi i/n}$, and let $\alpha \in \mathbf{F}_p$ be a fixed non-nth-power. There is a unique multiplicative map χ on $\mathbf{F}_p^*$ such that $\chi(\alpha) = \zeta$. We extend this character χ to $\mathbf{F}_p$ by setting $\chi(0) = 0$. Let

$$J(\chi, \chi) = \sum_{y \in \mathbf{F}_p} \chi(y)\chi(1 - y) \tag{2}$$

be the Jacobi sum of the character χ with itself; and for $1 \leqslant i \leqslant n - 1$ let σ_i be the automorphism of the field $K = \mathbf{Q}(\zeta)$ such that $\sigma_i(\zeta) = \zeta^i$. Then an easy counting argument shows that the number of points on the curve (1), including the point at infinity, is equal to

$$M = p + 1 + \sum_{i=1}^{n-1} \sigma_i\Big(J(\chi, \chi)\Big) = p + 1 + \mathbf{T}_{K/\mathbf{Q}}\Big(J(\chi, \chi)\Big)$$

Received 15th January, 1998

where $\mathbf{T}_{K/\mathbf{Q}}$ is the trace from the cyclotomic field K down to the rational numbers. One can also show (see [**6**, **11**]) that $-J(\chi,\chi)$ and its conjugates are the reciprocal roots of the numerator of the zeta-function of this curve. In other words,

$$Z(T; C/\mathbf{F}_p) = \frac{\prod_{i=1}^{n-1}\bigl(1+\sigma_i(J(\chi,\chi))T\bigr)}{(1-T)(1-pT)}.$$

The number N of points on the jacobian J of C is equal to the value at 1 of the numerator of $Z(T; C/\mathbf{F}_p)$; that is,

$$N = \prod_{i=1}^{n-1}\sigma_i\bigl(J(\chi,\chi)+1\bigr) = \mathbf{N}_{K/\mathbf{Q}}\bigl(J(\chi,\chi)+1\bigr), \tag{3}$$

where $\mathbf{N}_{K/\mathbf{Q}}(x)$ denotes the norm of an element x of K.

There are two reasons why we are interested in small n. In the first place, when constructing a hyperelliptic cryptosystem, one usually wants N to be no greater than $\approx 10^{50}$. Since N falls in the interval $\left[\left(\sqrt{p}-1\right)^{n-1}, \left(\sqrt{p}+1\right)^{n-1}\right]$ (by (3)) — that is, it is roughly equal to p^g — we see that if $g \geqslant 8$ we shall be working with primes p of order only about 10^6, and for them the Jacobi sum can be quickly evaluated directly from the definition (2).

In the second place, there is a security consideration that argues against choosing $n > 13$ in the cryptographic applications. In [**1**] a subexponential algorithm is given for the discrete log problem in the jacobian of a hyperelliptic curve of high genus. Although the exact practical meaning of "high genus" has not yet been established, it seems prudent to avoid genus g for which $n = 2g+1 > \log p$. Since we are interested in p such that $g \log p$ is about 100, our restriction $n \leqslant 13$ shall be sufficient for the purpose of ruling out the Adleman-DeMarrais-Huang attack.

A final crucial condition for a hyperelliptic cryptosystem to be secure against all known attacks is that N must be divisible by a large prime (of at least 40 decimal digits). [There is one other attack on hyperelliptic cryptosystems: the generalisation in [**4**] of the method in [**10**] of reducing the elliptic curve discrete logarithm to the discrete logarithm in a finite field. However, that attack is feasible only if the jacobian is supersingular (that is, all of the reciprocal roots of the zeta-function have p-adic ordinal $1/2$), and in the case of the curve (1) with $p \equiv 1 \pmod{n}$ the jacobian in fact is always ordinary (that is, half of the reciprocal roots are p-adic units).]

Along with the curve C given by (1), we also consider its "twists" by non-nth-powers and by non-squares. To do this, let η be a fixed non-square in $\mathbf{F}_p$, and consider the equation

$$\eta^{-i}\left(v+\frac{1}{2}\right)^2 = \alpha^j u^n + \frac{1}{4}$$

https://doi.org/10.1017/S000497270003207X Published online by Cambridge University Press

for $i = 0, 1$ and $j = 0, 1, \ldots, n-1$ (where α is the same fixed non-nth-power that was used to define χ). This equation can be rewritten in the form

$$v^2 + v + \left(1 - \eta^i\right)/4 = \eta^i \alpha^j u^n. \tag{4}$$

By analogy with (3) one finds that the number of points on the jacobian of the curve (4) is given by

$$N_{i,j} = \mathrm{N}_{K/\mathbf{Q}}\left(J(\chi,\chi) + (-1)^i \zeta^j\right), \qquad i = 0, 1, \quad j = 0, 1, \ldots, n-1. \tag{5}$$

When constructing a hyperelliptic cryptosystem we compute the numbers $N_{i,j}$ and hope that some will be prime or almost prime. Actually, some of these numbers are forced to be divisible by n or n^2. It follows from (7) below that $N_{0,0}$ is divisible by n^2 and $N_{0,j}$ is divisible by n for nonzero j. In that case the most one can hope for is that $N_{0,0}/n^2$ or $N_{0,j}/n$ is a prime. When $i = 1$, there is no such obstruction to $N_{1,j}$ itself being prime. Thus, after we compute $J(\chi,\chi)$ for our chosen n and $p \equiv 1 \pmod{n}$, we shall want to compute the numbers (5) and test $n^{-2}N_{0,0}$, $n^{-1}N_{0,j}$, and $N_{1,j}$ for primality. Since $N_{i,j}$ is of order $p^g = p^{(n-1)/2}$, we see that to get jacobians whose order is divisible by a prime of size at least B, we should take primes p larger than $B^{2/(n-1)}$. For instance, if we want $N_{i,j}$ to be divisible by a prime of at least 40 digits, then $B = 10^{40}$ and we should choose p larger than b_n where:

n:	3	5	7	11	13
b_n:	10^{40}	10^{20}	2×10^{13}	10^8	5×10^6

We need a way to compute the Jacobi sum $J(\chi,\chi)$ that is much faster than the definition (2), which clearly takes time $O(p)$. In the case $n = 3$ this was in effect done by Gauss, who found an explicit formula for the number of points on (1) [5]. The calculation boils down to the computation of a greatest common divisor in the ring of integers of the field of third roots of unity. The Euclidean algorithm has been generalised for $n = 5, 7, 11$ [9], and this could presumably be used to calculate Jacobi sums. We prefer to use lattice basis reduction [8], which gives a general solution to the problem that does not depend on special properties of the n-th cyclotomic field. (See also a similar use of LLL in [2].)

We start by considering the prime ideal $P \subset \mathbf{Z}[\zeta]$ of degree one that lies over the rational prime p and is generated by p and $a - \zeta$, where $a = \alpha^{(p-1)/n}$ is a primitive n-th root of unity modulo p that depends on the choice of α. We shall assume that P is a principal ideal; this is always the case if $n < 23$, because the corresponding cyclotomic field has class number one. (We remark that for larger n one could select primes p for which P is principal, or else one could consider the ideal $\prod_{i=1}^{g} \sigma_i^{-1}(P)$, which is guaranteed to be principal since it is generated by the Jacobi sum.)

Our main computational task is to find a generator β of P. Assume for the moment

https://doi.org/10.1017/S000497270003207X Published online by Cambridge University Press

that this has been done. We then set

$$\tilde{J} = \prod_{i=1}^{g} \sigma_i^{-1}(\beta). \tag{6}$$

By standard facts about Jacobi sums, the ideal generated by $\tilde{J}$ is equal to the ideal generated by $J(\chi,\chi)$. Moreover, $\tilde{J}$ also shares with $J(\chi,\chi)$ the property that the different imbeddings in the complex numbers all have the same absolute value. In fact, for any σ_j the product of $\sigma_j\tilde{J}$ and its complex conjugate $\sigma_j\left(\prod_{i=g+1}^{2g}\sigma_i^{-1}(\beta)\right)$ is the norm of β, which is equal to p, so that all archimedean absolute values are equal to $\sqrt{p}$.

It follows from these facts that $\tilde{J}$ is equal to $J(\chi,\chi)$ up to a root of unity. To find the root of unity, we use the congruence

$$J(\chi,\chi) \equiv -1 \pmod{\pi^2} \tag{7}$$

in the ring $\mathbf{Z}[\zeta]$, where $\pi = \zeta - 1$ is a generator of the unique prime ideal lying over n (see [**6**, p.227]).

We know that there exist $r \in \{\pm 1\}$ and s such that $r\zeta^s\tilde{J} = J(\chi,\chi)$. Let $\tilde{J} = \sum_{j=0}^{n-2} a_j\zeta^j$. From the formula

$$\zeta^k = (1+\pi)^k \equiv 1 + k\pi \pmod{\pi^2}$$

we see that the congruence (7) reduces to

$$\begin{aligned} r\zeta^s\tilde{J} &\equiv r(1+s\pi)\sum_{j=0}^{n-2} a_j(1+j\pi) \\ &\equiv r\left(\sum_{j=0}^{n-2} a_j + \left(s\sum_{j=0}^{n-2} a_j + \sum_{j=0}^{n-2} ja_j\right)\pi\right) \\ &\equiv -1 \pmod{\pi^2}. \end{aligned}$$

This congruence is easily solved by choosing $r \in \{\pm 1\}$ such that $r \equiv -\sum a_j \pmod{n}$ and then setting $s \equiv r\sum ja_j \pmod{n}$. We have thereby reduced the problem of finding the exact value of $J(\chi,\chi)$ to the problem of finding a generator β of the ideal P.

To do this, we use the LLL lattice basis reduction algorithm (see [**8**] or [**3**]). Recall that if $L \subset \mathbf{R}^{2g}$ is a lattice of rank $2g$, then the LLL algorithm produces a nonzero vector x in L with norm $\|x\|$ bounded by

$$\|x\| \leqslant \delta^{g/2}(\det L)^{1/2g}.$$

Here $\delta = 1/(a-1/4) > 4/3$ is a constant that depends on the choice of a parameter a satisfying $1/4 < a < 1$. The larger a is, the better the short vectors are and the more slowly the algorithm runs. For fixed g the choice of a only affects constants in the running time.

https://doi.org/10.1017/S000497270003207X Published online by Cambridge University Press

The cyclotomic field $K = \mathbf{Q}(\zeta)$, where $\zeta = e^{2\pi i/n}$, can be imbedded in $\mathbf{C}^g$ in the usual way by taking an element of K and applying each of the g imbeddings (up to complex conjugation) of K into $\mathbf{C}$ to construct a g-tuple of complex numbers. The image of the ring of integers $\mathbf{Z}[\zeta]$ is a lattice whose determinant is $2^{-g}\sqrt{D}$, where $D = D_{K/\mathbf{Q}} = n^{n-2}$ is the discriminant of the field. The prime ideal P of degree one lying over the rational prime p is a sublattice of rank $2g$ and determinant $2^{-g}p\sqrt{D}$. By abuse of notation we shall identify the ideal P with its image under the imbedding into $\mathbf{C}^g$. We now apply LLL to this lattice and get an element

$$x = (x_1, x_2, \ldots, x_{2g-1}, x_{2g}) \in \mathbf{R}^{2g} \simeq \mathbf{C}^g$$

that is bounded in the $\mathbf{R}^{2g}$-norm by

$$\sqrt{x_1^2 + x_2^2 + \ldots + x_{2g-1}^2 + x_{2g}^2} \leqslant \delta^{g/2}(\det P)^{1/2g} = \delta^{g/2}\left(p2^{-g}n^{g-1/2}\right)^{1/2g}.$$

The images of this element of the ideal P under the various imbeddings of K into $\mathbf{C}$ are $x_{2j-1} + ix_{2j}$, $j = 1, \ldots, g$, and the norm of the element is the product of those numbers and their complex conjugates, that is, the product of $x_{2j-1}^2 + x_{2j}^2$ over $j = 1, \ldots, g$. Using the arithmetic-geometric means inequality and the above bound on the Euclidean norm of x, we get

$$\begin{aligned} \mathbf{N}_{K/\mathbf{Q}}(x) &\leqslant \left(\frac{x_1^2 + \cdots + x_{2g}^2}{g}\right)^g \leqslant g^{-g}\delta^{g^2}p2^{-g}(2g+1)^g \cdot \frac{1}{\sqrt{n}} \\ &= \delta^{g^2}p\left(1 + \frac{1}{2g}\right)^g \cdot \frac{1}{\sqrt{n}} < \delta^{g^2}p\sqrt{e/n}. \end{aligned}$$

In other words, LLL returns us an element of P whose norm is bounded by a constant times p.

We consider the ratio $\mathbf{N}_{K/\mathbf{Q}}(x)/p$ and the running time first from a theoretical point of view, and then we describe what happened when we implemented this algorithm.

Since the dimension is fixed, the running time of the LLL algorithm depends only on the size of the numbers describing the lattice. In our context, the size is $O\big(\log(p)\big)$ and the running time is $O\big(\log(p)^3\big)$ (see [8] or [3]).

Now we ask how much larger than p the norm $\mathbf{N}_{K/\mathbf{Q}}(x)$ can be. In the case $n = 5$, $g = 2$, we choose $\delta = 1.99$, so that LLL gives us an element $x \in P$ with $\mathbf{N}_{K/\mathbf{Q}}(x) \leqslant 1.99^4\big(25/(16\sqrt{5})\big)p < 11p$. Since there are no elements of $\mathbf{Z}[\zeta]$ of norm strictly between 1 and 11, it follows that x has norm p, and so is a generator of P. Thus LLL is guaranteed to produce a generator β.

When $n > 5$ the bound on the norm is not sharp enough to guarantee that we shall immediately get a generator. However, the bound tells us that the norm differs from the desired norm p by a constant (that is, $\delta^{g^2}\sqrt{e/n}$) that depends only on n. In theory we could tabulate generators of all ideals of K whose norm is less than that

https://doi.org/10.1017/S000497270003207X Published online by Cambridge University Press

constant, and then divide the element produced by LLL as appropriate. In other words, if $\mathbf{N}_{K/\mathbf{Q}}(x) = cp$, then our table would contain all generators y of ideals of norm c, and for some such y we would find that x/y is an algebraic integer in K of norm p.

For instance, if $n = 7$, then, choosing $\delta = 1.538$, we find that LLL gives us an element $x \in P$ with $\mathbf{N}_{K/\mathbf{Q}}(x) < 29p$. Then the only possibility other than 1 for $\mathbf{N}_{K/\mathbf{Q}}(x)/p$ is 8, and in that case it suffices to try just $y = 1 + \zeta + \zeta^3$ and its complex conjugate. If $n \geqslant 11$, then the number of y of norm less than the theoretical bound $\delta^{g^2}\sqrt{e/n}$ becomes considerably larger.

What happens when we actually implement this algorithm? First, we remark that although the lattice $P \subset \mathbf{R}^{2g}$ is not generated by vectors with integer coordinates, the Gram matrix of the lattice is (almost) integral. This is convenient, because it means that "all-integer" versions of LLL can be employed, so that there are no round-off error concerns (see [3]). For the sake of those wanting to duplicate our experiments, we give the Gram matrix explicitly.

An element ω of the field K is a polynomial $f(\zeta)$ in ζ, and it maps to the element

$$\big(f(\zeta^j) : j = 1, \ldots, g\big) \in \mathbf{C}^g$$

under the usual imbedding. If $f(\zeta^j) = a_j + ib_j$, $a_j, b_j \in \mathbf{R}$ then the image as a real $2g$-tuple is $(a_1, b_1, \ldots, a_g, b_g)$. The Euclidean inner product of two such real vectors $\omega = f(\zeta)$, $\omega' = f'(\zeta)$ is

$$\langle \omega, \omega' \rangle = \sum_{j=1}^{g} a_j a'_j + b_j b'_j = \sum_{j=1}^{g} \mathrm{Re}\big(f(\zeta^j) f'(\zeta^{-j})\big) = (1/2)\mathbf{T}_{K/\mathbf{Q}}(\omega\overline{\omega'}),$$

where $\overline{\omega'}$ denotes the complex conjugate of ω'. To make this inner product an integer when $\omega, \omega' \in \mathbf{Z}[\zeta]$, from now on we replace the standard inner product on $\mathbf{R}^{2g}$ by twice itself. (This artificial device is needed because we considered only half of the complex imbeddings; a more elegant alternative would have been to imbed K into $\mathbf{C}^{2g} \approx \mathbf{R}^{4g}$ and to note that the lattices in question are no longer full lattices, but rather have rank $2g$.) If we now choose a $\mathbf{Z}$-basis $\{\omega_1, \ldots, \omega_{2g}\}$ of the prime ideal P, then the Gram matrix of the corresponding lattice is $\mathbf{T}_{K/\mathbf{Q}}(\omega_i\overline{\omega}_j)$.

Our prime ideal P is generated over $\mathbf{Z}[\zeta]$ by the two elements p and $\zeta - a$ (where $a = \alpha^{(p-1)/n}$ is the same primitive n-th root of 1 modulo p as before). This implies that P has $\mathbf{Z}$-basis

$$\{p, \zeta - a, \zeta^2 - a_2, \ldots, \zeta^{n-2} - a_{n-2}\},$$

where $a_k = \big(a^k \bmod p\big)$. Indeed, these elements are all in P, and the index of the ideal that they generate in $\mathbf{Z}[\zeta]$ is p.

The Gram matrix with respect to this basis is easy to compute:

$$\langle p, p \rangle \quad = \cdot \, \mathbf{T}_{K/\mathbf{Q}}\big(p^2\big) = (n-1)p^2$$

https://doi.org/10.1017/S000497270003207X Published online by Cambridge University Press

$$\begin{aligned}\langle p, \zeta^k - a_k \rangle &= \mathbf{T}_{K/\mathbf{Q}}\big(p(\zeta^{-k} - a_k)\big) = -p - (n-1)pa_k \\ \langle \zeta^k - a_k, \zeta^l - a_l \rangle &= \mathbf{T}_{K/\mathbf{Q}}\big((\zeta^k - a_k)(\zeta^{-l} - a_l)\big) \\ &= \delta_{kl}\, n - 1 + a_k + a_l + (n-1)a_k a_l,\end{aligned}$$

where $\delta_{kl} = 1$ if $k = l$ and $\delta_{kl} = 0$ otherwise.

Our algorithm can be easily implemented in any symbolic algebra system that includes an LLL algorithm. We chose GP/PARI. The program is about 10 lines of code. For $n = 5$ it runs more or less instantaneously on our workstations, even for primes up to 100 digits. For $n = 19$ it takes only a few seconds, even for 50-digit primes. In other words, in an application to hyperelliptic cryptosystems the running time is small, even if we take into account that the program will have to be run many times in order to obtain prime values.

In addition, the shortest vector produced by the algorithm had norm p in all experiments that we tried. In fact, the usual situation was that all $n - 1$ vectors in a reduced basis had norm p, although there were several instances for $n = 19$ where only about half of the vectors had norm p. In other words, the theoretical bounds on the norms of the vectors are much greater than what one seems to get in practice.

References

[1] L.M. Adleman, J. DeMarrais and M. Huang, 'A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields', in *Algorithmic Number Theory*, Lecture Notes Comput. Sci. **877** (Springer-Verlag, Berlin, Heidelberg, New York, 1994), **pp.** 28–40.

[2] J. Buchmann and H.C. Williams, 'On principal ideal testing in algebraic number fields', *J. Symbolic Comput.* **4** (1987), 11–19.

[3] H. Cohen, *A course in computational algebraic number theory* (Springer-Verlag, Berlin, Heidelberg, New York, 1993).

[4] G. Frey and H. Rück, 'A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves', *Math. Comp.* **62** (1994), 865–874.

[5] C.F. Gauss, *Werke* (Zweiter Band, Göttingen, 1976).

[6] K. Ireland and M.I. Rosen, *A classical introduction to modern number theory*, (2nd edition) (Springer-Verlag, Berlin, Heidelberg, New York, 1990).

[7] N. Koblitz, 'Hyperelliptic cryptosystems', *J. Cryptology* **1** (1989), 139–150.

[8] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, 'Factoring polynomials with rational coefficients', *Math. Ann.* **261** (1982), 515–534.

[9] H.W. Lenstra, Jr., 'Euclid's algorithm in cyclotomic fields', *J. London Math. Soc.* **10** (1975), 457–465.

[10] A. Menezes, T. Okamoto and S.A. Vanstone, 'Reducing elliptic curve logarithms to logarithms in a finite field', *IEEE Trans. Inform. Theory* **39** (1993), 1639–1646.

[11] A. Weil, 'Numbers of solutions of equations in finite fields', *Bull. Amer. Math. Soc.* **55** (1949), 497–508.

Department of Mathematics
Reed College
Portland OR 97202-8199
United States of America
e-mail: jpb@reed.edu

Department of Mathematics
Box 354350
University of Washington
Seattle WA 98195
United States of America
e-mail: koblitz@math.washington.edu