Index form surfaces and construction of elliptic curves over large finite fields

Attila Pethő *
University of Debrecen
Department of Computer Science
H–4010 Debrecen, POB 12
Hungary
e-mail:pethoe@math.klte.hu

November 28, 2009

Abstract

Index form equations play an important role in algebraic number theory especialy in computing all elements with given discriminant. Using geometric ideas Gaál, Pethő and Pohst [4] gave a practical method for the solution of index form equations over quartic number fields. Continuing their investigations we introduce the notion of index form surfaces associated to quartic polynomials and show, that they are either empty or elliptic surfaces.

*Research supported in part by Centre de Recerca Matemática, Bellaterra and also by Hungarian National Foundation for Scientific Research Grant 25157/98.

1 Introduction

Let $\mathbb{K}$ be an algebraic number field of degree n, denote by $\mathbb{Z}_{\mathbb{K}}$ its ring of integers and by $D_{\mathbb{K}}$ its discriminant. Let $1, \omega_1, \ldots, \omega_{n-1}$ be an integral basis of $\mathbb{Z}_{\mathbb{K}}$, $\underline{X} = (X_1, \ldots, X_{n-1})$,

$$L^{(i)}(\underline{X}) = L^{(i)}(X_0, \underline{X}) = X_0 + \omega_1^{(i)} X_1 + \ldots + \omega_{n-1}^{(i)} X_{n-1}, \quad i = 1, \ldots, n.$$

The *discriminant form* of $\mathbb{K}$ /$\mathbb{Q}$ with respect to the basis $1, \omega_1, \ldots, \omega_{n-1}$ or simply the discriminant form of $\mathbb{K}$ /$\mathbb{Q}$ is then defined by

$$D_{\mathbb{K}\ /\mathbb{Q}}(L(\underline{X})) = \prod_{1 \le i < j \le n} \left(L^{(i)}(\underline{X}) - L^{(j)}(\underline{X}) \right)^2 .$$

It is easy to see that

$$D_{\mathbb{K}\ /\mathbb{Q}}(L(\underline{X})) = D_{\mathbb{K}} \left(I_{\mathbb{K}\ /\mathbb{Q}}(\underline{X}) \right)^2 ,$$

where $I_{\mathbb{K}\ /\mathbb{Q}}(\underline{X})$ is a homogenous polynomial of degree $n(n-1)/2$ in $\mathbb{Z}[\underline{X}]$. The polynomial $I_{\mathbb{K}\ /\mathbb{Q}}(\underline{X})$ is called the *index form* of $\mathbb{K}$ /$\mathbb{Q}$ with respect to the basis $1, \omega_1, \ldots, \omega_{n-1}$ or simply the index form of $\mathbb{K}$ /$\mathbb{Q}$.

To find elements with given discriminant in algebraic number fields the index forms are playing an important role. Indeed, the element $\alpha = x_0 + x_1\omega_1 + \ldots + x_{n-1}\omega_{n-1} \in \mathbb{Z}_{\mathbb{K}}$ has discriminant d if and only if

$$I_{\mathbb{K}\ /\mathbb{Q}}(x_1, \ldots, x_{n-1}) = \pm\sqrt{d/D_{\mathbb{K}}} . \tag{1}$$

T. Nagell proved that if $\mathbb{K}$ is a quartic number field, then (1) has only finitely many solutions. His result was extended to arbitrary number fields by K. Győry [5]. It is important that Győry's result is effectiv, i.e. it implies an algorithm for the solution of (1). He generalized this result for relative extensions and even for finitely generated integral domains [6].

The solutions of index form equations for small degree fields are also tabulated. This is not too hard for $n = 3$, because then $I_{\mathbb{K}\ /\mathbb{Q}}(x_1, x_2)$ is a cubic form, thus (1) becomes a Thue equation of degree 3. Gaál and Schulte [3] developed an algorithm in this case and computed all power integral bases in cubic number fields with $|D_{\mathbb{K}}| < 50000$.

Forgetting the arithmetical meaning of equation (1) one can study the geometrical properties of the curve defined by that equation over an extension of $\mathbb{Q}$ or over a finite field. It is well known that this curve is of genus one, hence it is empty or an elliptic curve. (See e.g. [15], Section I.2.)

Already for quartic number fields becomes the computation of integer solutions of (1) much harder. Although Győry's result imply an algorithm for the resolution of (1), but it is not practical. This is because he transforms (1) to finitely many S-unit equations in two unknowns over the normal closure of $\mathbb{K}$, and from the solutions of these unit equations derive the solutions of (1). In the worst, but most frequent, case the Galois group of $\mathbb{K}$ is isomorphic to S_4, the symmetric group of degree 4, and the normal closure of $\mathbb{K}$ has degree 24. Generaly even a system of fundamental units of such a large degree field is very hard to compute. Therefore we must understand better the structure of the index form if we will find the solutions of index form equations. If $\mathbb{K}$ has a qudratic subfield, then $I_{\mathbb{K}\ /\mathbb{Q}}(\underline{X})$ splits in $\mathbb{Q}[\underline{X}]$ and we have to do with a system of equations. Based on this fact Gaál, Pethő and Pohst worked out methods for solving quartic index form equations if the Galois group of $\mathbb{K}\ /\mathbb{Q}$ is isomorphic to C_4, V_4 or D_8. Finally they succeeded to prove, that one can get all integer points lying on $I_{\mathbb{K}\ /\mathbb{Q}}(\underline{X})$ by a simple transformation of the integer solutions of finitely many quartic Thue equations (see [4] and the references therein). You find a collection of recent computational results on index form equations of higher degree number fields in Gaál [1, 2].

We shall show in this note, that if $\mathbb{K}$ is a quartic extension of $\mathbb{Q}$ than the surface defined by the equation

$$I_{\mathbb{K}\ /\mathbb{Q}}(\underline{X}) = m \neq 0$$

has a nice geometric structure: it is either empty or an elliptic surface, i.e. can be uniquely covered by elliptic curves. Exactly this structure makes relativ simple the computation of integer points on such a surface. This observation is behinde of the result of Gaál, Pethő and Pohst. We present the geometrical structure theorem in more general context.

The classification of index form surfaces associated to higher degree number fields should be the topics of further research.

The results of sections 2 and 3 were proved several years ago and circulated in a manuscript. In section 4 we summarize results of F. Leprévost et al. [7]. In those sections the index form surface is studied over a finitely generated integral domain over $\mathbb{Q}$. In the last section we collect some observation of P. Nagy [12], who performed computations concerning index form surfaces over finite fields.

2 Parametrization of the index forms

To formulate our results we generalize the notion of index form and introduce some notation.

Let k be a field (of arbitrary characteristic), a_1, a_2, a_3, a_4 be indeterminates over k and $K = k(a_1, a_2, a_3, a_4)$. Let $p(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 \in K[X]$ of non-zero discriminant. Let $\alpha = \alpha_1, \ldots, \alpha_4$ denote the zeros of $p(X)$ in some algebraic closure of K. Let $L = K(\alpha)$ and denote by $I_p(\underline{X})$ the index form associated to the basis $1, \alpha, \alpha^2, \alpha^3$ of L. Then

$$I_p(\underline{X}) = \prod_{1 \le i < j \le 4} L_{i,j}(\underline{X}),$$

where

$$L_{i,j}(\underline{X}) = X_1 + (\alpha^{(i)} + \alpha^{(j)})X_2 + (\alpha^{(i)2} + \alpha^{(i)}\alpha^{(j)} + \alpha^{(j)2})X_3.$$

for $1 \le i < j \le 4$.

By the fundamental theorem on symmetric polynomials, $I_p(\underline{X})$ is a form of degree 6 in $K[\underline{X}]$. We are given a parametrization of $I_p(\underline{X})$ in Theorem 1 below. But befor it we note, that if one specialises K to $\mathbb{Q}$ and a_1, a_2, a_3, a_4 to fixed integers, then L becomes a number field. If it is quartic and $1, \alpha, \alpha^2, \alpha^3$ is a power integral basis of the ring of integers of L, then $I_p(\underline{X})$ specialises to the classical notion of index forms.

Note, that one can define analogously the index form of higher degree polynomials.

Theorem 1 *Let*

$$\begin{aligned} Q_1(\underline{X}) &= X_1^2 - a_1X_1X_2 + a_2X_2^2 + (a_1^2 - 2a_2)X_1X_3 + (a_3 - a_1a_2)X_2X_3 \\ &\quad +(-a_1a_3 + a_2^2 + a_4)X_3^2 = \underline{X}Q_1\underline{X}^T, \\ Q_2(\underline{X}) &= X_2^2 - X_1X_3 - a_1X_2X_3 + a_2X_3^2 = \underline{X}Q_2\underline{X}^T \quad , \end{aligned} \tag{2}$$

where Q_1 and Q_2 denote the matrix of the quadratic form with the same name and $\underline{X}^T$ denotes the transpose of the vector $\underline{X}$. Let further

$$f_3(X, Y) = X^3 - a_2X^2Y + (a_1a_3 - 4a_4)XY^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)Y^3. \tag{3}$$

Then we have

$$I_p(\underline{X}) = f_3(Q_1(\underline{X}), Q_2(\underline{X})). \tag{4}$$

Note that $f_3(X, 1)$ is the cubic resolvent of $p(X)$.

Proof. Collect the factors in the definition of $I_p(\underline{X})$ as follows:

$$I_p(\underline{X}) = (L_{1,2}(\underline{X})L_{3,4}(\underline{X}))\,(L_{1,3}(\underline{X})L_{2,4}(\underline{X}))\,(L_{1,4}(\underline{X})L_{2,3}(\underline{X}))\,.$$

Putting $\xi_1 = \alpha^{(1)}\alpha^{(2)} + \alpha^{(3)}\alpha^{(4)}, \xi_2 = \alpha^{(1)}\alpha^{(3)} + \alpha^{(2)}\alpha^{(4)}$ and $\xi_3 = \alpha^{(1)}\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)}$ we obtain

$$I_p(\underline{X}) = (Q_1(\underline{X}) - \xi_1 Q_2(\underline{X}))(Q_1(\underline{X}) - \xi_2 Q_2(\underline{X}))(Q_1(\underline{X}) - \xi_3 Q_2(\underline{X}))$$

after a simple, but length computation. A similar simple and similar length computation proves (4). We use in both part of the proof only the well known Vieta's formulae. □

3 Structure of the index form surfaces

Let M be an extension of K and let $0 \neq \mu \in M$. We shall now study the structure of the set

$$\mathcal{F}(M, \mu) = \{P = (x_1, x_2, x_3) \in M^3 : I_p(P) = \mu\},$$

i.e. the set of M-rational points on the *index form surface* $I_p(\underline{X}) - \mu$.

Let call $P_1, P_2 \in \mathcal{F}(M, \mu)$ equivalent, if

$$Q_1(P_1) = Q_1(P_2) \quad \text{and} \quad Q_2(P_1) = Q_2(P_2).$$

This is obviously an equivalence relation on the set $\mathcal{F}(M, \mu)$. Moreover, there exists by Theorem 1 a bijective correspondence between the equivalence classes of $\mathcal{F}(M, \mu)$ and the M-rational points on the curve $f_3(X, Y) = \mu$. It can be defined formally as follows: For $u, v \in M$ such that $f_3(u, v) = \mu$ let

$$\mathcal{F}_{(u,v)} = \mathcal{F}_{(u,v)}(M, \mu) = \{P \in \mathcal{F}(M, \mu) : Q_1(P) = u, Q_2(P) = v\}.$$

Then Theorem 1 implies

$$\mathcal{F}(M, \mu) = \cup_{\substack{u,v,\in M \\ f(u,v)=\mu}} \mathcal{F}_{(u,v)}.$$

It can happen, that $\mathcal{F}(M, \mu) = \emptyset$ and even if $\mathcal{F}(M, \mu) \neq \emptyset$ the set $\mathcal{F}_{(u,v)}$ can be empty for some $(u, v) \in M^2$. Indeed, consider for example the polynomial $p(x) = x^4 + 4a^2$, with $a \in \mathbb{Q}$. The polynomials f_3, Q_1, Q_2 corresponding to the index form $I_p(\underline{X})$ by Theorem 1 are $f_3(X, Y) = X^3 - 16a^2XY^2, Q_1(\underline{X}) = X_1^2 + 4a^2X_3^2, Q_2(\underline{X}) = X_2^2 - X_1X_3$.

The rank of the elliptic curve $X^3 - 16a^2XY^2 = 1$ over $\mathbb{Q}$ is zero, and the only rational points on it are $(1, 0), (-1/2, 3/8a), (-1/2, -3/8a)$. This implies

$$\mathcal{F} = \mathcal{F}_{(1,0)} \cup \mathcal{F}_{(-1/2,3/8a)} \cup \mathcal{F}_{(-1/2,-3/8a)}$$

for

$$\mathcal{F} = \mathcal{F}(\mathbb{Q}, 1) = \{P \in \mathbb{Q}^3 \ : \ I_p(P) = 1\}.$$

Obviously $(1,0,0) \in \mathcal{F}_{(1,0)}$, hence $\mathcal{F}$ is not empty. On the other hand the sets $\mathcal{F}_{(-1/2,\pm 3/8a)}$ are empty because the equation $X_1^2 + 4a^2X_3^3 = -1/2$ is not solvable in $\mathbb{Q}$.

The above example is due to Susanne Schmitt. She also proved that $\mathcal{F}$ from the example is infinite if and only if $a = c_1c_2(c_1 + c_2)(c_1 - c_2)z^2$, where $c_1, c_2 \in \mathbb{Z}, \gcd(c_1, c_2) = 1$ and $z \in \mathbb{Q}$.

If M is algebraicaly closed then $\mathcal{F}_{(u,v)} \neq \emptyset$ for every $u, v \in M$ with $f_3(u, v) = \mu$. Indeed, choosing $x_3 = 0$ we obtain the system of equations $x_1^2 - a_1x_1x_2 + a_2x_2^2 = u, x_2^2 = v$, which is always solvable in $x_1, x_2 \in M$, thus $(x_1, x_2, 0) \in \mathcal{F}_{(u,v)}$.

As the intersection of two conics is an elliptic curve, $\mathcal{F}_{(u,v)}$ is an elliptic curve for every $u, v \in M$ with $f_3(u, v) = \mu$. We will compute a model for these curve more explicitely.

Theorem 2 *Let M be an extension of $K, 0 \neq \mu \in M$. Let $u, v \in M$ be such that $f_3(u, v) = \mu$ and $P = (x_1, x_2, x_3) \in \mathcal{F}_{(u,v)}$. Put $Q_3 = vQ_1 - uQ_2$. Then there exists for every $R \in \mathcal{F}_{(u,v)}$ a vector $S \in M^3$ such that one of the coordinates of S is* 0,

$$\ell(S)R = S\ell(S) - PSQ_3S^T, \quad \textit{with} \quad \ell(S) = 2PQ_3S^T$$

and S satisfies the equation

$$v\ell(S)^2 = (S\ell(S) - PSQ_3S^T)Q_2(S^T\ell(S) - SQ_3S^TP^T), \tag{5}$$

if $v \neq 0$ and

$$4u(PQ_3S^T)^2 = ((SQ_2S^T)P - 2(PQ_2S^T)S)Q_1((SQ_2S^T)P^T - 2(PQ_2S^T)S^T),$$

if $v = 0$.

Proof Assume that $v \neq 0$ and let $P = (x_1, x_2, x_3) \in \mathcal{F}_{(u,v)}$. Then one of the coordinates of P is non-zero. Assume that this is x_3. Let $R \in \mathcal{F}_{(u,v)}$. Then there exist $r, s_1, s_2 \in M$ such that

$$R = rP + S,$$

with $S = (s_1, s_2, 0)$. Using that $R, P \in \mathcal{F}_{(u,v)}$ we obtain the following chain of identities:

$$\begin{aligned} 0 &= vQ_1(R) - uQ_2(R) = vRQ_1R^T - uRQ_2R^T \\ &= v(rP + S)Q_1(rP^T + S^T) - u(rP + S)Q_2(rP^T + S^T) \\ &= r^2(vPQ_1P^T - uPQ_2P^T) + r(P(vQ_1 - uQ_2)S^T + S(vQ_1 - uQ_2)P^T) \\ &\quad + vSQ_1S^T - uSQ_2S^T \end{aligned}$$

We have $vPQ_1P^T - uPQ_2P^T = vQ_1(P) - uQ_2(P) = 0$. As Q_1 and Q_2 are symmetric matrices, Q_3 is symmetric too. Thus $(PQ_3S^T)^T = SQ_3P^T$. Further, as PQ_3S^T is a constant, we obtain $PQ_3S^T + SQ_3P^T = 2PQ_3S^T = \ell(S)$ and

$$r\ell(S) = -SQ_3S^T.$$

This implies the assertion on R at once.

We have further $Q_2(R) = v$. If $v \neq 0$ then by multiplying this equation by $\ell(S)^2$ and inserting the formula for $\ell(S)R$ we obtain (5) immediately.

Finally, if $v = 0$, then as $f_3(u, 0) = u^3 = \mu \neq 0$ we have $u \neq 0$. Working now with the relation $Q_1(R) = u$ we obtain the asserted equation for S. □

One of the coordinates of S is zero by Theorem 2. Denote by s_1 and s_2 the other two coordinates of S. Then the expression staying on the right hand side of (5) is a quartic form in s_1 and s_2. We denote it by $f_4(s_1, s_2)$. The coefficients of $f_4(s_1, s_2)$ belong obviously to M. Redoing the computation of sections 3.2 and 3.3 of [4] one can prove the following theorem.

Theorem 3 *Beside the notations of Theorem 2 let $\alpha_i, i = 1, \ldots, 4$ denote the zeros of $p(X)$ and $f_4(s_1, s_2)$ the quartic form staying on the right hand side of (5). Then we have*

$$f_4(s_1, s_2) = v^2 \prod_{i=1}^{4} \left((x_3\alpha_i - x_2 + a_1x_3)s_1 - (x_3\alpha_i^2 + x_3a_1\alpha_i + x_3a_2 - x_1)s_2\right).$$

4 Elliptic surfaces associated to cubic and quartic polynomials

We are given in this section an overview on results of the paper of F. Leprévost et al [7].

We proved in the last section that in the parametrization of index form surfaces associated to quartic polynomials the curve

$$C: \quad f_3(X, Y) = 1, \tag{6}$$

where $f_3(X, Y)$ is defined by (3), is playing an important role. Observe that the coefficients of f_3 are depending only on the coefficients of the quartic polynomial $p(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$. The point $P = (1, 0)$ is lying obviously on the curve (6). In the sequel we assume that $\mathrm{char}(k) \neq 2, 3$.

Let

$$H(X,Y) = -\frac{1}{4}\left(\frac{\partial^2 f_3}{\partial X^2}\frac{\partial^2 f_3}{\partial Y^2} - \left(\frac{\partial^2 f_3}{\partial X \partial Y}\right)^2\right)$$

denote the quadratic and

$$G(X,Y) = \frac{\partial f_3}{\partial X}\frac{\partial H}{\partial Y} - \frac{\partial f_3}{\partial Y}\frac{\partial H}{\partial X}$$

the cubic covariants of f_3. They satisfy the classical identity

$$4H^3 = G^2 + 27 D_{f_3} f_3^2, \tag{7}$$

where D_{f_3} denotes the discriminant of $f_3(X,1)$. Remark that D_{f_3} is equal to the discriminant of $p(x)$.

We have $f_3(1,0) = 1$. Defining

$$\begin{aligned} A(4) &:= H(1,0) = 12a_4 + a_2^2 - 3a_1a_3 \quad \text{and} \\ B(4) &:= G(1,0) = 27a_1^2a_4 - 9a_1a_2a_3 + 2a_2^3 - 72a_2a_4 + 27a_3^2 \end{aligned}$$

the point $P' = (A(4), B(4))$ is lying on the curve

$$E: \quad y^2 = 4x^3 - 27D_{f_3}.$$

The curve E is 3-isogenous to the curve

$$E_t: \quad X^2 = 4X^3 - 27D_{f_3},$$

where the 3-isogeny is given by the map

$$\varphi: \quad (x,y) \longrightarrow (X,Y) = \left(\frac{4(x^3 - 27D_{f_3})}{9x^2}, \frac{4y(x^3 + 54D_{f_3})}{27x^3}\right).$$

Hence the point

$$P_0 := \varphi(P') = \left(\frac{4(A^3(4) - 27D_{f_3})}{9A^2(4)}, \frac{4B(4)(A^3(4) + 54D_{f_3})}{27A^3(4)}\right)$$

is lying on the elliptic curve E_t.

The main results of F. Leprévost et al [7] are the following.

Theorem 4 *Let $k = \mathbb{Q}$ and assume that the transcendence degree of $K = \mathbb{Q}(a_1, a_2, a_3, a_4)$ is 4. Then the rank of $E_t(K)$ is at least one, P_0 is of infinite order and the group of torsion points of $E_t(K(\sqrt{D_{f_3}}))$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.*

Using the specialization $(a_1, a_2, a_3, a_4) = (-1, -6, 2, 14)$ and the point $P = (1,0)$ they also proved:

Theorem 5 *The surface $I_p(X_1, X_2, X_3) = 1$ is an elliptic surface. Its Kodaira dimension and the dimension of its Albanése variety is one.*

5 Index form surfaces over finite fields

Let $q > 3$ be a rational prime and $k = \mathbb{F}_q$ be the finite field of q elements. If a_1, a_2, a_3, a_4 denote indeterminates over k and $K = k(a_1, a_2, a_3, a_4)$ then the point P_0, defined in the last section, belongs to $E_t(K)$. Specialyzing a_1, a_2, a_3, a_4 to $\tilde{a}_1, \tilde{a}_2, \tilde{a}_3, \tilde{a}_4 \in \mathbb{F}_q$, such that $D_{\tilde{f}_3}\tilde{A}(4) \neq 0$ the curve $\tilde{E}_t(\mathbb{F}_q)$ becomes an elliptic curve and the image $\tilde{P}_0$ of P_0 is a rational point of $\tilde{E}_t(\mathbb{F}_q)$.

If $q \equiv 2 \pmod 3$, then $|\tilde{E}_t(\mathbb{F}_q)| = q + 1$, i.e. the curve is supersingular. (c.f. A. Menezes [8] pp 26,27.) The situation is much more interesting if $q \equiv 1 \pmod 3$, which we shall assume in the sequel.

In his diploma work P. Nagy [12] studied for randomly chosen primes $q \equiv 1 \pmod 3$ and $p(x) \in \mathbb{F}_q[x]$ how offen generates $\tilde{P}_0$ a subgroup of $\tilde{E}_t(\mathbb{F}_q)$ of small index. He used the following algorithm:

1. $q \leftarrow$ random odd prime with $q \equiv 1 \pmod 3$,
   $p(x) \leftarrow x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in \mathbb{F}_q[x]$ random polynomial,
   $t \leftarrow$ discriminant of $p(x)$,
2. if $t = 0$ or $A(4) = 12a_4 + a_2^2 - 3a_1a_3 = 0$ in $\mathbb{F}_q$ then goto 1,
3. $N \leftarrow$ the order of $\tilde{E}_t(\mathbb{F}_q)$,
4. if $N = q + 1$ then goto 1,
5. factorize N. If failed goto 1,
6. compute $\tilde{P}_0$ and its order M,
7. output $q, \tilde{P}_0, N, N/M$.

Remarks *1. The algorithm was tested for 80,100,120 and 200 decimal digit primes.*

2. To compute $N = |\tilde{E}_t(\mathbb{F}_q)|$ Cornacchia's algorithm was used, which complexity is $O(\log^2 q)$. (c.f. R. Schoof [14])

3. To factorize N only trial division with the first 100 000 primes was performed. If N or one of its divisors passed this test and the Miller-Rabin test [10, 13] then it was declared to be prime. We did not used deterministic primality tests.

4. Assume that the prime factorization of N is $N = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ with $p_1 < \ldots < p_r, \alpha_i \geq 1$ is computed. Then the order of $\tilde{P}_0$ is the smallest integer M such that M divides N and $M\tilde{P}_0 = \mathcal{O}$.

The algorithm was implemented in SIMATH 4.3 [16]. The computation were done on a PC with 166 MHz PENTIUM-MMX processor. Our experiences are the following:

- For 100 decimal digit primes the algorithm was performed 4000 times. We were able to compute the order of $\tilde{P}_0$ 440 times. The largest index was 1350. Curves with a point of small index were found in 1.3 minutes.
- For 120 decimal digit primes the algorithm was performed 2200 times. We were able to compute the order of $\tilde{P}_0$ 186 times. The largest index was 1158. Curves with a point of small index were found in 3.2 minutes.
- For 200 decimal digit primes the algorithm was performed 1632 times. We were able to compute the order of $\tilde{P}_0$ 89 times. The largest index was 223. Curves with a point of small index were found in about 30 minutes.

References

[1] I.Gaál, *Power integral bases in algebraic number fields,* in: Number Theory (K. Győry, A. Pethő and V.T. Sós, eds.), Walter de Gruyter, Berlin-New York 1998, 243-254.

[2] I.Gaál, *Power integral bases in algebraic number fields, II.,* in: Algebraic Number Theory and Diophantine Analysis (F. Halter-Koch and R.F. Tichy, eds.), Walter de Gruyter, Berlin-New York 2000, 153-161.

[3] I.Gaál and N. Schulte, *Computing all power integral bases of cubic fields,* Math. Comp. **53** (1989), 689–696.

[4] I.Gaál, A.Pethő and M.Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms-with an application to index form equations in quartic number fields,* J.Number Theory, **57**, (1996), 90–104.

[5] K.Győry, *Sur les polynomes á coefficients entiers et de discriminant donné, III.*, Publ. Math. (Debrecen), **23**(1976), 141–165.

[6] K.Győry, *Effective finiteness theorems for polynomials with given discriminant and integer elements with given discriminant over finitely generated domains,* J. reine angew. Math. **346** (1984), 54–100.

[7] F. Leprévost, S. Fermigier and C. Fieker, *Sur certaines surfaces elliptiques et courbes elliptiques de Mordell de rang ≥ 1 associées á des discriminants de polynômes cubiques ou quartiques*, J. Number Theory **78** (1999), 149–165.

[8] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publ. Boston/Dordrecht/London, 1997.

[9] L.J.Mordell, Diophantine Equations, Academic Press, New York-London, 1969.

[10] G. Miller, *Riemann's hypothesis and test for primality*, J. Comput and System Sci. **13** (1976), 300–317.

[11] T.Nagell, *Sur les discriminants des nombres algébriques*, Arkiv för Math., **7** (1967), 265–282.

[12] P. Nagy, Nyilvános kulcsú titkosítások, (Public key cryptosystems), Diploma work, University of Debrecen, 2000.

[13] M. Rabin, *Probabilistic algorithms for testing primality,* J. Number Theory **12** (1980), 128–138.

[14] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théorie des Nombres de Bordeaux, **7** (1995), 219–254.

[15] J.H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer Verlag, 1992.

[16] http://emmy.math.uni-sb.de/~simath, homepage of the Simath group.