Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 53–60
Universität Göttingen, 2004

SUPERSINGULAR ELLIPTIC CURVES AND MAXIMAL QUATERNIONIC ORDERS

J.M. Cerviño

Mathematisches Institut der Georg-August Universität Göttingen, Bunsenstr. 3-5, 37073 Göttingen, Germany • *E-mail :* cervino@uni-math.gwdg.de

Abstract. We give an explicit version of the "Deuring correspondence" between supersingular elliptic curves and maximal quaternionic orders, by presenting a deterministic and explicit algorithm to compute it.

1. Introduction

In this note all fields of positive characteristic will be either finite or function fields of curves defined over a finite algebraic extension of $\mathbb{F}_p$. Elliptic curve means often isomorphy class of elliptic curves. All quadratic forms have integral coefficients. For details see [**Cn**].

Let k be a finite field of characteristic p with fixed algebraic closure $\bar{k}$. Let E be an elliptic curve over k and $k(E)$ its function field. Such a curve is called *supersingular* if one, and hence all, of the following equivalences are satisfied:

1. $E(\overline{k})$ has no p torsion;
2. $\mathrm{End}_{\overline{k}}(E)$ is a 4-dimensional $\mathbb{Z}$-lattice;

May 4th, 2004.

3. $k(E)$ has no cyclic (separable and unramified) p-extensions.

Around the 30's Helmut Hasse proved the Riemann hypothesis for zeta functions of elliptic curves. He was also the first to observe, that besides the two well known cases of endomorphism rings of elliptic curves - namely $\mathbb{Z}$ or an order in an imaginary quadratic field extension of $\mathbb{Q}$, the so called *complex multiplication* case -, it was also possible to have an order of a definite quaternion algebra when the base field had positive characteristic. Max Deuring was able to compute the discriminant of this definite algebra. In [**Deu41b**] he proved that the algebra ramifies at p and at ∞. Furthermore in [**Deu41a**] he proved that the endomorphism rings of elliptic curves over a finite field of characteristic p are maximal orders in the quaternion algebra $\mathbb{Q}_{\infty,p}$ (the subindex shows the ramification places of the algebra), and that all maximal orders types of that algebra appear as endomorphism rings of supersingular elliptic curves over $\overline{\mathbb{F}_p}$.

In this note, we recall this correspondence, describe an explicit and deterministic algorithm to compute it and illustrate this algorithm in a concrete example.

2. Deuring correspondence

In the introduction we said that Deuring proved that every maximal order type (isomorphy class) of the quaternion algebra $\mathbb{Q}_{\infty,p}$ appears as an endomorphism ring of a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. But a bijection does not hold in this picture. In order to explain a bijection, we use the property (3) of supersingular elliptic curves.

In [**HW36**] Hasse and Witt study under which conditions a function field of characteristic p possesses cyclic unramified p-extensions. For the case of elliptic function fields they give an invariant A depending on the j invariant of the elliptic function field, such that $A = 0$ if and only if the elliptic function field has no cyclic unramified p-extensions, and therefore by (3), if and only if the elliptic curve is supersingular. This A invariant, called the *Hasse-Witt invariant* of the function field, is actually a polynomial in j, which was first computed in [**Deu41a**, page 201]. With this easily computable polynomial we can find the explicit equations for all the supersingular elliptic curves over $\overline{\mathbb{F}_p}$. Moreover, this Hasse-Witt polynomial factors over $\mathbb{F}_p[j]$ with factors of degree at most 2. Now we state the *Deuring correspondence*:

Theorem 2.1. [**Deu41a**] *Let p be a prime, and let $A(T) \in \mathbb{F}_p[T]$ be the characteristic p Hasse-Witt polynomial. For any $j_0 \in \overline{\mathbb{F}_p}$ denote by $E(j_0)$ any*

elliptic curve in the isomorphy class of those with j-invariant j_0. Then $A(T)$ factors as a product of at most degree 2 polynomials (in $\mathbb{F}_p[T]$) and to these factors correspond bijectively the maximal order types of the quaternion algebra $\mathbb{Q}_{\infty,p}$. The bijection is as follows:
for any irreducible factor A_i of A, choose a root, say $j_0 \in \mathbb{F}_{p^2}$; then:

$$A_i \;\mapsto\; \mathrm{End}_{\overline{\mathbb{F}_p}}(E(j_i)).$$

So, to make this correspondence explicit means to be able to compute the endomorphism ring of any supersingular elliptic curve (up to isomorphy), that means to compute the order type of the endomorphism ring. Let us take a look at the problem in two particular cases.

Example 2.2. *Consider two illustrative cases, $p = 29$ and $p = 37$.*

Case $p = 29$:

Here the Hasse-Witt polynomial is $A_{29}(T) = T(T-2)(T+4)$, and there are only three supersingular elliptic curves over $\overline{\mathbb{F}_{29}}$, namely $E(0)$, $E(2)$ and $E(25)$. In the quaternion algebra over $\mathbb{Q}$ ramified only at ∞ and 29 there are three isomorphy classes of maximal orders. Their $\mathbb{Z}$-bases can be computed explicitly as in **[Piz80]** *(see also the implementations made by F. Rodriguez-Villegas,* `http://www.ma.utexas.edu/users/villegas/cnt/`*). Instead we are going to avoid the computation of such bases until the very end of the algorithm, and we label those maximal order types by $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$.*

Case $p = 37$:

Here $A_{37}(T) = (T-8)(T^2-6T-6)$. This is the first prime where the Hasse-Witt polynomial has a nonlinear factor. The supersingular elliptic curves here are $E(8)$, $E(3+10\sqrt{2})$ and $E(3-10\sqrt{2})$. As explained in (2.1), the last two curves have the same endomorphism ring type, hence there are only two maximal order types in $\mathbb{Q}_{\infty,37}$, say $\mathcal{O}_1$ and $\mathcal{O}_2$.

The problem is to determine which supersingular elliptic curve corresponds to which order type. This will be solved at the end of this paper.

Note that David Kohel in his Berkeley thesis **[Koh96]** (using a different approach) proved a theorem which says that for any given supersingular elliptic curve E *there exists* an algorithm to compute four linearly independent endomorphisms of E, with running time $O(p^{3/2})$ (Theorem 75, loc.cit.). In

the proof he computes the discriminant of the suborder generated by the independent endomorphisms found in his theorem, but cannot control it, and then cannot assure that the result is a $\mathbb{Z}$-basis of the endomorphism ring[(1)].
We propose an algorithm that, for a given prime p, returns a list of pairs $(E_\lambda, \{1, e_1^\lambda, e_2^\lambda, e_3^\lambda\})$, where E_λ runs over all supersingular elliptic curves over $\overline{\mathbb{F}_p}$ and the second coordinate is a $\mathbb{Z}$-basis of the endomorphism ring of E_λ. Since we reduce this problem to a problem of computing on one side representation numbers and on the other graphs of isogenies, by [**Piz80**] (for computing the representation numbers) and [**Mes86**] (for the isogenies graph complexity) we have that the theoretical complexity of our algorithm is $O(p^{5/2})$, much better than the complexity of the already implemented version in PARI, which is more or less $O(p^4)$. Observe that this algorithm gives *all* the bases of endomorphism rings of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ and Kohel's more flexible theoretical algorithm works for one curve at a time, at the expense of loosing certainty, on whether one obtains a base of the maximal order or a base of a finite index sub-order.

2.1. Brandt-Sohn correspondence. We want to explain briefly a connection between maximal order types of the quaternion algebras $\mathbb{Q}_{\infty,p}$ and ternary quadratic forms of discriminant $-p$. In [**Bra43**] Brandt constructs maximal orders of quaternion algebras from ternary lattices *via* Clifford algebras. His idea was then exploited by Friedhelm Sohn in his Dissertation [**Soh57**], where he proves the following:

Theorem 2.3. *There exists an explicit bijection between the classes of ternary quadratic forms of discriminant $-p$ and the maximal order types of the quaternion algebra $\mathbb{Q}_{\infty,p}$.*

Indeed, given any ternary quadratic form

$$f = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3$$

with $a_{ij} \in \mathbb{Z}$ we associate the $\mathbb{Z}$-order with basis $1, e_1, e_2, e_3$ where:

$$\begin{aligned} e_i^2 &= a_{jk}e_i - a_{jj}a_{kk}, \\ e_ie_j &= a_{kk}(a_{ij} - e_k), \\ e_je_i &= a_{1k}e_1 + a_{2k}e_2 + a_{3k}e_3 - a_{ik}a_{jk}, \end{aligned} \tag{1}$$

with (i, j, k) any even permutation of $\{1, 2, 3\}$ (see [**Brz95**]). Therefore once we know a complete set of representatives of the equivalence classes of ternary

(1) See Theorem 84 loc.cit. for conditions when the algorithm gives a base of the endomorphism ring and comment thereafter.

quadratic forms of discriminant $-p$, we can directly compute the $\mathbb{Z}$-bases of all maximal order types of $\mathbb{Q}_{\infty,p}$. Now, since all the quadratic forms of discriminant $-p$ belong to the same genus, we can use an algorithm of Rainer Schulze-Pillot [**SP91**] based on the *ℓ-neighbors* concept introduced by Martin Kneser to compute a representative for each equivalence class, therefore given any prime number p we can compute the bases of representatives for all the maximal order types of $\mathbb{Q}_{\infty,p}$.

3. The algorithm

We now state a key theorem assuring that the algorithm works.

Theorem 3.1. [**Sch97**] *The theta series determine the equivalence classes of definite ternary quadratic forms over $\mathbb{Q}$. This means that any two definite ternary quadratic forms over $\mathbb{Q}$ are integrally equivalent if and only if they have the same representation numbers.*

Recall, that the representation numbers of a definite quadratic form f of dimension d are the:

$$r(f,n) := \#\{x \in \mathbb{Z}^d \mid f(x) = n\};\ n \in \mathbb{Z};$$

and then the theta series for f is:

$$\vartheta(z) := \sum_{n\in\mathbb{Z}} exp(2\pi i r(f,n)z);\ z \in \mathbb{H}.$$

It is a classical result that these theta series are in fact modular forms of weight $d/2$ and level the level of the quadratic form; see [**SP84**] in particular for the case $d = 3$. Since there is only one genus for discriminant $-p$, all the theta series corresponding to quadratic forms of discriminant $-p$ have the same Eisenstein part, and therefore they differ, if at all, in the cuspidal part. C.L. Siegel in his papers on the analytic theory of quadratic forms gives an explicit bound to decide whether a cusp form is zero or not. This bound grows like $p/12$.

Moreover Schiemann gives also a bound $b(p)$, which in our case depends only on the discriminant, such that for any two definite quadratic forms f, g of discriminant $-p$ holds:

$r(f,n) = r(g,n)\ \forall\, n \in \mathbb{Z}$ with $|n| \leqslant b(p) \Rightarrow f$ and g are integrally equivalent.

For computational purposes Siegel's bound is better for us and we use it in the implementation; but asymptotically they are the same.

Now let us go back to our problem. After (3.1), we can distinguish between any two non-equivalent definite ternary quadratic forms and hence by (2.3), between any two maximal order types and finally by Deuring's correspondence (2.1) between two supersingular elliptic curves, and all this by means of looking at the representation numbers up to a fixed bound given by, say Siegel, of a set of representatives of the equivalence classes of ternary quadratic forms of discriminant $-p$ (by reduction theory, there are canonical representatives, which are called *reduced ternary quadratic forms*).

So in order to comlete our algorithm, we must be able to pin-point the supersingular elliptic curves using the data from the representation numbers of the reduced ternary quadratic forms. Let us state this in our concrete examples. We write a ternary quadratic form like in (and from) the table of Brandt-Intrau [**BI58**], namely $f = \begin{pmatrix} a_{11} & a_{22} & a_{33} \\ a_{23} & a_{13} & a_{12} \end{pmatrix}$.

***Example 3.2* (Continued).** *Case $p = 29$:*

We compute the three reduced ternary quadratic forms of discriminant -29: $f_1 = \begin{pmatrix} 1 & 3 & 3 \\ 2 & 0 & 1 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 1 & 0 \end{pmatrix}$ $f_3 = \begin{pmatrix} 1 & 1 & 10 \\ 0 & 1 & 1 \end{pmatrix}$; *which correspond to the maximal orders $\mathcal{O}_1, \mathcal{O}_2$ and $\mathcal{O}_3$.*

Case $p = 37$:

The two reduced ones in this case are: $f_1 = \begin{pmatrix} 2 & 2 & 3 \\ 0 & 2 & 1 \end{pmatrix}$ *and* $f_2 = \begin{pmatrix} 1 & 2 & 5 \\ 1 & 1 & 0 \end{pmatrix}$.

Now our problem is to assign to each supersingular elliptic curve of Example (2.2) *one of these ternary quadratic forms.*

To acomplish this, we must pass the information on the side of quadratic forms and their representation numbers to the side of elliptic curves and isogenies. Before we make this explicit in the following proposition, we introduce some notation.
Let f be any quadratic form and denote by $\mathcal{O}_f$ it's associated order according to (2.3). For any order $\mathcal{O}$ in $\mathbb{Q}_{\infty,p}$ define: $\Gamma_b(\mathcal{O}) := \{(tr(\alpha), nr(\alpha)) \in \mathbb{Z}^2 \mid \alpha \in \mathcal{O} \text{ and } nr(\alpha) \leqslant b\}$, where tr and nr are the reduced trace and reduced norm of the quaternion algebra. Set $\Gamma(\mathcal{O}) = \Gamma_{b_S}(\mathcal{O})$, where b_S is the Siegel bound.

Proposition 3.3. *Let $\{f_1, \ldots, f_t\}$ be a complete set of representatives of reduced ternary quadratic forms of discriminant $-p$. Then the sets $\Gamma(\mathcal{O}_{f_i}) \subset \mathbb{Z}^2$*

for $i = 1, \ldots, t$ are all different, i.e., these subsets characterize univocally the maximal order types in $\mathbb{Q}_{\infty,p}$.

Now we make the simple observation:

Corollary 3.4. *Since the trace and norm on elements of the order correspond to the trace and (separable) degree of the endomorphisms of the elliptic curves, we conclude, that the sets:*

$$\Delta(E) := \{(trace(\varphi), deg(\varphi)) \in \mathbb{Z}^2 \mid \varphi \in \mathrm{End}_{\overline{\mathbb{F}_p}}(E) \text{ and } deg(\varphi) \leqslant b_S\},$$

characterize the supersingular elliptic curves of characteristic p.

Consequently, we must only have to compute the sets $\Gamma(\mathscr{O}_f)$ and $\Delta(E)$ for f running through all the reduced ternary quadratic forms of discriminant $-p$ and E over all the supersingular elliptic curves of characteristic p, and then establish the bijection just by comparing these sets. We make this clear in our:

***Example 3.5* (Continued).** *Case $p = 29$:*

$\Gamma_{[3]}(\mathscr{O}_{f_1}) = \{(-1,3);(1,3);(0,3)\}$;
$\Gamma_{[3]}(\mathscr{O}_{f_2}) = \{(2,3);(-2,3)\}$;
$\Gamma_{[3]}(\mathscr{O}_{f_3}) = \{(-3,3);(3,3);(0;3)\}$; *where the subscript* [3] *denotes simply the subset of norm* 3 *elements of* Γ. *On the elliptic curve side, we simply construct all quotients of the supersingular elliptic curves of degree* 3 *using* [**V7́1**] *and for the trace one can avoid easily the polynomial running time algorithms to do it, since one knows the possible traces, so by testing one gets that:* $\Gamma_{[3]}(\mathscr{O}_{f_1}) = \Delta_{[3]}(E(2))$, $\Gamma_{[3]}(\mathscr{O}_{f_2}) = \Delta_{[3]}(E(25))$ *and* $\Gamma_{[3]}(\mathscr{O}_{f_3}) = \Delta_{[3]}(E(0))$.

Case $p = 37$:

Here the sets $\Gamma_{[3]}(\mathscr{O}_{f_1})$ and $\Gamma_{[3]}(\mathscr{O}_{f_2})$ are also different, but we do it with degree 5 *isogenies and get:* $\Gamma_{[5]}(\mathscr{O}_{f_1}) = \{(0,5)\}$ *and* $\Gamma_{[5]}(\mathscr{O}_{f_2}) = \{(-1,5);(1,5)\}$. *By comparing with the Δ's of the elliptic curves we get:* $\Gamma_{[5]}(\mathscr{O}_{f_1}) = \Delta_{[5]}(E(3 \pm 10\sqrt{2}))$ *and* $\Gamma_{[5]}(\mathscr{O}_{f_2}) = \Delta_{[5]}(E(8))$.

Thus we are able to establish the correspondence between supersingular elliptic curves and reduced ternary quadratic forms, and therefore by using formula (1) we compute directly the bases of the endomorphism rings and finish our algorithm.

References

[BI58] H. Brandt & O. Intrau – Tabellen reduzierten positiver ternärer quadratischer Formen, *Abh. Sächs. Akad. Wiss. Math.-nat. Kl.* **45** (1958), no. 4.

[Bra43] H. Brandt – Zur Zahlentheorie der Quaternionen, *Jber. Deutsch. Math.-Verein.* **53** (1943), p. 23–57.

[Brz95] J. Brzezinski – Definite quaternion orders of class number one, *J. Théér. Nombres Bordeaux* **7** (1995), no. 1, p. 93–96.

[Cn] J. M. Cerviño – Supersingular elliptic curves and maximal quaternionic orders, `http://arxiv.org/pdf/math.NT/0404538`.

[Deu41a] M. Deuring – Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* (1941), p. 197–272.

[Deu41b] ———, Theorie der Korrespondenzen algebraischer Funktionenkörper II, *J. reine angew. Math.* **183** (1941), p. 25–36.

[HW36] H. Hasse & E. Witt – Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p, *Mh. Math. Phys.* **43** (1936), p. 477–492.

[Koh96] D. Kohel – Endomorphism rings of elliptic curves over finite fields, Ph.D. Thesis, University of California at Berkeley, 1996, p. 96.

[Mes86] J.-F. Mestre – Sur la methóde des graphes, exemples et applications, Proceedings of the international conference on class numbers and fundamental units, Nagoya University, 1986, p. 217–242.

[Piz80] A. Pizer – An algorithm for computing modular forms on $\Gamma_0(N)$, *J. Algebra* **64** (1980), no. 2, p. 340–390.

[Sch97] A. Schiemann – Ternary positive definite quadratic forms are determined by their Theta series, *Math. Ann.* **308** (1997), no. 3, p. 507–517.

[Soh57] F. Sohn – Beiträge zur Zahlentheorie der ternären quadratischen Formen und der Quaternionenalgebren, Ph.D. Thesis, Westfälische Wilhelms-Universität zu Münster, 1957, p. 87.

[SP84] R. Schulze-Pillot – Thetareihen positiv definiter quadratischer Formen, *Invent. Math.* **75** (1984), no. 2, p. 283–299.

[SP91] R. Schulze-Pillot – An algorithm for computing genera of ternary quadratic and quaternary quadratic forms, Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Bonn, 1991, p. 134–143.

[Vé71] J. Vélu – Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), p. 238–241.