CONSTRUCTING SUPERSINGULAR ELLIPTIC CURVES

Reinier Bröker

Abstract. We give an algorithm that constructs, on input of a prime power q and an integer t, a supersingular elliptic curve over $\mathbf{F}_q$ with trace of Frobenius t in case such a curve exists. If GRH holds true, the expected run time of our algorithm is $\widetilde{O}((\log q)^3)$. We illustrate the algorithm by showing how to construct supersingular curves of prime order.

1. Introduction

Let $\mathbf{F}_q$ be the finite field of $q = p^f$ elements with p prime. It is a classical problem to construct an elliptic curve over $\mathbf{F}_q$ with prescribed order. In case the requested curve is ordinary, there is no algorithm known that solves this problem in time polynomial in $\log q$. In this paper we investigate the *supersingular* case.

A classical result due to Waterhouse [10, Theorem 4.1] states that there exists a supersingular elliptic curve over $\mathbf{F}_q$ with trace of Frobenius t if and only if t lies in the small set S_q consisting of those traces for which one of the following holds:

(a) if $[\mathbf{F}_q : \mathbf{F}_p]$ is *even* and one of the following is true
- (i) $t = \pm 2\sqrt{q}$
- (ii) $t = \pm\sqrt{q}$ and $p \not\equiv 1 \bmod 3$
- (iii) $t = 0$ and $p \not\equiv 1 \bmod 4$;

(b) if $[\mathbf{F}_q : \mathbf{F}_p]$ is *odd* and one of the following is true
- (i) $t = 0$
- (ii) $t = \pm\sqrt{2q}$ and $p = 2$.
- (iii) $t = \pm\sqrt{3q}$ and $p = 3$.

In this artice we give an algorithm to efficiently construct a supersingular elliptic curve over $\mathbf{F}_q$ with prescribed trace of Frobenius. We prove the following Theorem.

Theorem 1.1. *The algorithm presented in this paper computes, on input of a prime power q and an integer $t \in S_q$, a supersingular elliptic curve over $\mathbf{F}_q$ with trace of Frobenius t. If GRH holds true, the expected run time of the algorithm is $\widetilde{O}((\log q)^3)$.*

2000 *Mathematics Subject Classification*. Primary 14H52, Secondary 11G15.

Here, the $\widetilde{O}$-notation indicates that terms that are of logarithmic size in the main term have been disregarded. In Section 2 we give the algorithm for prime fields, and illustrate it with an example. The non-prime case is explained in Section 3. We illustrate how Theorem 1.1 can be applied to efficiently construct elliptic curves of prime order of prescribed size.

2. The prime case

The main ingredient in the Algorithm is to construct a supersingular curve over the prime field $\mathbf{F}_p$, i.e., a curve with trace of Frobenius 0. We will construct such a curve as reduction of a curve in characteristic 0 using a result due to Deuring.

Theorem 2.1. *Let E be an elliptic curve defined over number field L whose endomorphism ring is the maximal order $\mathcal{O}_K$ in an imaginary quadratic field K, and let $\mathfrak{p}|p$ be a prime of L where E has good reduction. Then $E \bmod \mathfrak{p}$ is supersingular if and only if p does not split in K.*

Proof. See [9, Theorem 13.12]. □

Let E be a curve as in Theorem 2.1, and let H be the Hilbert class field of K, i.e., the largest totally unramified abelian extension of K. By CM-theory [9, Theorem 10.1], the j-invariant $j(E)$ generates H over K. We have

$$H = K[X]/(P_K),$$

where P_K is the minimal polynomial over $\mathbf{Q}$ of the j-invariant $j(E)$. The polynomial P_K is called the Hilbert class polynomial. Its degree equals the class number h_K of K, and it has *integer* coefficients. There are a few algorithms [2, 4, 6, 3] to explicity compute P_K.

If we now take K such that p remains inert in $\mathcal{O}_K$, then the roots of $P_K \in \overline{\mathbf{F}}_p[X]$ are j-invariants of supersingular curves by Theorem 2.1. Since the j-invariant of a supersingular curve is contained in $\mathbf{F}_{p^2}$ by [9, Theorem 13.6], the polynomial P_K splits in this case already over $\mathbf{F}_{p^2}$. An other way of seeing this last fact is using class field theory: the Artin map gives an isomorphism

$$\mathrm{Gal}(H/K) \xrightarrow{\sim} \mathrm{Cl}(\mathcal{O}_K)$$

and as $(p) \in \mathcal{O}_K$ is a principal prime, it splits completely in H/K. Hence, the inertia degree of $p \in \mathbf{Z}$ is 2.

The following Lemma gives a sufficient condition for $P_K \in \mathbf{F}_p[X]$ to have a root in $\mathbf{F}_p$.

Lemma 2.3. *Let K be an imaginary quadratic field with class number h_K. Then:*

$$h_K \text{ is odd} \iff K = \mathbf{Q}(i) \text{ or } K = \mathbf{Q}(\sqrt{-2}) \text{ or } K = \mathbf{Q}(\sqrt{-q}) \text{ with } q \text{ prime and congruent to } 3 \bmod 4.$$

Proof. Let D be the discriminant of K, and let $p_1, \ldots, p_n$ be the odd prime factors of D. The *genus field*

$$G = K(\sqrt{p_1^*}, \ldots, \sqrt{p_n^*})$$

with $p_i^* = (-1)^{(p_i-1)/2} p_i$ is the largest unramified abelian extension of K that is abelian over $\mathbf{Q}$, and the Galois group $\mathrm{Gal}(G/K)$ is isomorphic to the 2-Sylow group of $\mathrm{Cl}(\mathcal{O}_K)$, cf. [5, Section 6]. We see that h_K is odd if and only if we have an equality $L = K$. This yields the lemma. $\square$

These observations lead to the following algorithm to construct a supersingular elliptic curve over $\mathbf{F}_p$.

Algorithm 2.4. Input: a prime p. Output: a supersingular curve over $\mathbf{F}_p$.
1. If $p = 2$, return $Y^2 + Y = X^3$.
2. If $p \equiv 3 \bmod 4$, return $Y^2 = X^3 - X$.
3. Let q be the smallest prime congruent to 3 mod 4 with $\left(\frac{-q}{p}\right) = -1$.
4. Compute $P_K \in \mathbf{Z}[X]$ for $K = \mathbf{Q}(\sqrt{-q})$.
5. Compute a root $j \in \mathbf{F}_p$ of $P_K \in \mathbf{F}_p[X]$.
6. If $q = 3$, return $Y^2 = X^3 - 1$. Else, put $a \leftarrow 27j/(4(1728 - j)) \in \mathbf{F}_p$ and return $Y^2 = X^3 + aX - a$.

Lemma 2.5. *Algorithm 2.4 returns a supersingular curve over $\mathbf{F}_p$. If GRH holds true, the expected run time is $\widetilde{O}((\log p)^3)$.*

Proof. The correctness of the Algorithm is clear from the discussion preceding it. The main point in the run time analysis is Step 3. As p is congruent to 1 mod 4, we have $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$ by quadratic reciprocity. We therefore want q to be inert in both $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(i)$. Hence, we are looking for a prime q with prescribed Frobenius symbol in the $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$-extension $L = \mathbf{Q}(\sqrt{p}, i)$ of $\mathbf{Q}$. Under GRH, there exists [8] an effectively computable constant c such that there such a prime q with

$$q \leq c\,(\log d_L)^2,$$

where $d_L = 2^4 p^2$ is the discriminant of $L/\mathbf{Q}$.

Under GRH, computing P_K in Step 4 takes time $\widetilde{O}((\log p)^2)$ by [2, Theorem 1.1]. By construction, this polynomial has a root modulo p. The degree of P_K equals the class number h_K which is of size $\widetilde{O}(\log p)$ by Brauer-Siegel. Finding a root j of $P_K \in \mathbf{F}_p[X]$ therefore takes probabilistic time $\widetilde{O}(\deg(P_K)(\log p)^2) = \widetilde{O}((\log p)^3)$ by [7, Section 14.5]. $\square$

Example. The smallest prime $p > 10^{100}$ with $p \equiv 1 \bmod 12$ is $p = 10^{100} + 1293$. In this case, the prime $q = 11$ is inert in both $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(i)$. An elliptic curve with j-invariant $-32768 \in \mathbf{F}_p$ is supersingular.

3. The Algorithm

Let $q = p^f$ be a prime power and let $t \in S_q$ be the trace of Frobenius of the elliptic curve we want to construct. Using Algorithm 2.4, we construct a supersingular curve $E/\mathbf{F}_p$. Let $E'/\mathbf{F}_q$ be the base change of this curve to $\mathbf{F}_q$. Let t' be trace of Frobenius of E'.

Lemma 3.1. *We have $t' = 0$ if $f = [\mathbf{F}_q : \mathbf{F}_p]$ is odd, $t' = 2\sqrt{q}$ if f is divisible by 4 and $t' = -2\sqrt{q}$ otherwise.*

Proof. The Frobenius φ_E of E satisfied $\varphi^2 + p = 0$. We derive $\mathrm{Tr}(\varphi_{E'}) = \mathrm{Tr}(\varphi_E^f) = \mathrm{Tr}((-p)^{f/2})$, which yields the lemma. □

We contend that there exists a twist of E' that has trace of Frobenius t. Indeed, if f is odd, we only need to consider the cases $p = 2, 3$. For these two small primes, there is only one supersingular j-invariant in characteristic p so the requested curve with trace of Frobenius t has j-invariant $j(E')$.

Suppose that f is even. For $p \not\equiv 1 \bmod 4$, we twist the can twist the curve E' by a primitive fourth root of unity $i \in \mathbf{F}_q$ to get curves with trace of Frobenius $\pm 2\sqrt{q}$ and 0. Similarly, for $p \not\equiv 1 \bmod 3$, we can twist by a primitive sixth root of unity $\zeta_6 \in \mathbf{F}_q$ to obtain curves with trace of Frobenius $\pm 2\sqrt{q}$ and $\pm\sqrt{q}$. For $p \equiv 1 \bmod 12$, we twist by -1.

Algorithmically, twisting E' to get a curve with trace of Frobenius t is easy. Indeed, suppose that we want to twist by a power of ζ_6. We compute an element $\alpha \in \mathbf{F}_q^*$ generating $\mathbf{F}_q^*/\mathbf{F}_q^{*6}$. The twists of $E' : Y^2 = X^3 + b$ are then given by

$$Y^2 = X^3 + \alpha^k b$$

for $k = 0, \ldots, 5$, and an easy computation shows that the traces of Frobenius for these curves are $t', t'/2, -t'/2, -t', -t'/2, t'/2$ respectively. Twisting by i and -1 proceeds similarly. Finally, also for $p = 2, 3$ all $\overline{\mathbf{F}}_q$-isomorphisms are explicitly known [9, Appendix 1].

Proof of Theorem 1.1. We compute a supersingular elliptic curve $E/\mathbf{F}_p$ using Algorithm 2.4 and base change this to a curve E' over $\mathbf{F}_q$. This takes time $\widetilde{O}((\log p)^3)$. We compute the right twist of E' in time $\widetilde{O}((\log q)^2)$. □

Example. Suppose we want to construct an elliptic curve with prime order of k decimal digits. We look for a prime p such that $p^2 + p + 1$ is a prime of k digits. We cannot prove that such a p exists, but heuristically there are many. Indeed, by the *Bateman-Horn* conjecture [1] we expect that we have

$$\pi(x, A) \sim 1.52 \int_2^x \frac{1}{(\log t)^2} \mathrm{d}t,$$

where $\pi(x, A)$ denotes the number of primes p up to x such that $p^2 + p + 1$ is prime.

Having found such a prime p, we construct a supersingular elliptic curve $E/\mathbf{F}_p$ and base change it to $E'/\mathbf{F}_{p^2}$. The curve E' has p^2+2p+1 points by Lemma 3.1. If we twist E' by ζ_6 we get a curve of prime order p^2+p+1.

References

1. P. T. Bateman, R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. of Comp. 16, 1962, pp. 363–367.
2. R. Bröker, *A p-adic algorithm to compute the Hilbert class polynomial*, Preprint, 2006, available at `http://www.math.ucalgary.ca/~reinier/padidj.pdf`.
3. R. Bröker, A. Enge, K. Lauter, F. Morain, *Computing the Hilbert class polynomial*, In preparation.
4. J.-M. Couveignes, T. Henocq, *Action of modular correspondences around CM-points*, Algorithmic Number Theory Symposium V, Springer Lecture Notes in Computer Science, vol. 2369, 2002, pp. 234–243.
5. D. A. Cox, *Primes of the form* x^2+ny^2, John Wiley & Sons, 1989.
6. A. Enge, *The complexity of class polynomial computation via floating point approximations*, Preprint, 2006.
7. J. von zur Gathen, J. Gerhard, *Modern computer algebra*, Cambridge University Press, 1999.
8. J. C. Lagarias, A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields, ed. A. Fröhlich, Academic Press, 1977, pp. 409–465.
9. S. Lang, *Elliptic functions*, Springer Graduate Texts in Mathematics, vol. 112, 1987.
10. W. W. Waterhouse, *Abelian varieties over finite fields*, Ann. scient. Éc. Norm. Sup., (4), 1969, pp. 521–560.

University of Calgary, Department of Mathematics and Statistics, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada

E-mail address: `reinier@math.ucalgary.ca`