Constructing Supersingular Elliptic Curves Depending on the Coefficients of Weierstrass Equation

Samaa Fuad Ibraheem
University of Technology
School of Applied Science

Abstract:

In the use of elliptic curves in its applications (especially in cryptography), one often needs to construct elliptic curves with a known type (number of points) over a given finite field F_p, where some types are more secure than others. So we introduce a simple way to construct a supersingular elliptic curve by computing the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ where $f(x)= x^3+ax+b$. And we give an algorithm that compute that coefficient and construct the required curve.

Keywords: Weierstrass equation, supersingular elliptic curve, cryptography, algorithm.

1. Introduction

Let F_q be a finite field with $q=p^r$ elements where p is a prime number and r is a positive integer. Efficiently, constructing supersingular elliptic curves of prescribed order has its impact outside the area of arithmetic geometry.

In other application as cryptography, a supersingular curve of prime order $N=\#E(F_q)$ has the property that, its embedding degree with respect to N is very small and this makes supersingular curves suitable for pairing based cryptographic systems [2].

In 2008 Broker [1] gives an algorithm that construct a supersingular elliptic curve over the finite field F_q with trace of Frobenous t depending on the result due to Waterhouse [7], where the inputs are a prime power q and an integer t. Later, L.R. Finotti [3] gives a formula for the supersingular polynomial in characteristic $p\geq 5$ depending on the Hass invariant of E that defined on finite prime field F_p.

In this research, we'll follow a similar approach to introduce a formula for supersingular elliptic curve derived from the Hass invariant too, but we obtained another different result. We give an algorithm for computing this formula to construct a supersingular elliptic curve over the finite field F_p. This algorithm depends on the field elements a and b that define the equation of the elliptic curve $E(F_p)$ of characteristic greater than 3.

Section (2) contains elliptic curves and group structure and some important definitions.

Section (3) contains the computation of Hass invariant and the formula that derived to constructing supersingular elliptic curves. For the facility of our computation there is an algorithm that constructs a supersingular elliptic curve using the formula which introduced in our research.

2. Elliptic Curve and Group Structure [8]

Let K be a field. An elliptic curve over K is a pair $(E,\mathcal{O})$ where E is a non singular curve of genus one over K with a point $\mathcal{O} \in E$ called the point at infinity. The set of points $(x, y) \in K\times K$ verifying the (non-singular) weierstrass equation:

$$E(K): y^2+a_1xy+a_3y= x^3+a_2x^2+a_4x+a_6 \quad (a_i\in K) \quad \ldots(1)$$

together with the point $\mathcal{O}$.

The set of points (x,y) that satisfied equation (1) and $\mathcal{O}$ form an abelian group where $\mathcal{O}$ is the additive identity element. This group is denoted by E(K) and the group operation is denoted by (+).

When the characteristic of the field K is greater than 3, the weierstrass equation of an elliptic curve equation(1) can be simplified to

$$E(K): y^2 =x^3+ax+b \qquad a, b \in K \quad \ldots (2)$$

Definition (2-1)[6]

The discriminant (Δ) of the polynomial $f(x) = x^3+ax+b$ is $-4a^3-27b^2$.

The curve given by weierstrass equation (1) can be non singular if and only if $\Delta\neq 0$ [6]. So, to construct an elliptic curve defined over $K=F_p$ (prime field of characteristic $p > 3$), we must make sure that the parameters a and b satisfy the quantity

$$4a^3+27b^2\neq 0 \bmod p \qquad \ldots(3)$$

Definition (2-2)[4,5]

The order of an elliptic curve is defined as the number of points on the curve, and it is denoted by #E.

2.1 Supersingular Elliptic Curves

Let $E(F_q)$ be an elliptic curve with trace t and q is a power of p. E is said to be supersingular if p divides t, where $\#E(F_q)=q+1-t$. In other words we can say that E is supersingular, if and only if $t^2 = 0, q, 2q, 3q$ or $4q$. Particularly when $q = p$, the curve E over prime field of characteristic $p>3$ is supersingular if and only if t is congruent to 0 modulo p, i.e. E has exactly $(p + 1)$ points [5].

3. Determining the Supersingular elliptic Curves

Consider the Elliptic Curve E defined over the prime field F_p. The type of E can be determined from the coefficient of x^{p-1} in the cubic equation $(x^3+ax+b)^{(p-1)/2}$ which has roots in $\overline{K}$ (an algebraic closure of K) as the following theorem states.

Theorem (3.1) [6, p. 140]:

Let K be a finite field of characteristic p > 2. Let E be an elliptic curve defined over K with Weierstrass equation E: $y^2 = f(x)$, where $f(x) \in K[x]$ is a cubic polynomial with distinct roots (in $\overline{K}$). Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.

Note: The Hasse invariant of E defined in equation (1) is the coefficient of x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$ [3].

3.1 The Formula for Supersingular Elliptic Curve

Let E be an elliptic curve defined over the field F_p of characteristic p greater than 3 with Weiersrass equation $E: y^2=x^3+ax+b$. By putting s=p-1 we'll compute the coefficient of x^s in $(x^3+ax+b)^{s/2}$ which is equal to the coefficient of x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$ as follows:

Since

$$(x^3+(ax+b))^n = \sum_{r=0}^{n} \binom{n}{r} x^{3(n-r)} (ax+b)^r$$

then

$$(x^3+(ax+b))^{\frac{s}{2}} = \sum_{r=0}^{s/2} \binom{s}{2}{r} x^{3(\frac{s}{2}-r)} (ax+b)^r$$

$$= \sum_{r=0}^{s/2} \sum_{m=0}^{r} \binom{s}{2}{r} \binom{r}{m} a^{r-m} b^m x^{3(\frac{s}{2}-r)+r-m} \cdots(4)$$

Now, the terms in x^s are obtained when $x^s = x^{3(\frac{s}{2}-r)+r-m}$, i.e. $s = 3(\frac{s}{2}) - 2r - m$.

Substituting in (4) gives:

$$\sum_{r=0}^{s/4} \sum_{m=0}^{r} \binom{\frac{s}{2}}{\frac{s}{4}-\frac{m}{2}} \binom{\frac{s}{4}-\frac{m}{2}}{m} a^{\frac{s}{4}-\frac{3m}{2}} b^m x^s \cdots(5)$$

It's clearly that m, r must be integers and $m \geq 0$,.also that $\frac{s}{4} - \frac{3}{2}m \geq 0 \Rightarrow \frac{s}{4} \geq \frac{3}{2}m \Rightarrow \frac{s}{6} \geq m,$ then equation (5) becomes

$$\sum_{m=0}^{[s/6]} \binom{\frac{s}{2}}{\frac{s}{4}-\frac{m}{2}} \binom{\frac{s}{4}-\frac{m}{2}}{m} a^{\frac{s}{4}-\frac{3m}{2}} b^m x^s \cdots(6)$$

Where $\left[\frac{s}{6}\right]$ is the greatest integer function.

If we let $Z_1 = \frac{s}{2}$ and $Z = \frac{1}{2}\left(\frac{s}{2} - m\right)$ then,

$\frac{1}{2}(Z_1 - m) = Z, (Z_1 - m) = 2Z$. Therefore ($Z_1$-m) is even quantity, which yields that (Z_1-m) becomes even only when Z_1, m are both even or both odd, so we have two cases:

Case1:

If Z_1, m are both even then $Z_1 \equiv 0 \bmod 2$, $m \equiv 0 \bmod 2$ and $s \equiv 0 \bmod 4$ i.e $p \equiv 1 \bmod 4$. In other words, when $p \equiv 1 \bmod 4$; m must be even less than or equal to (s/6).

Case2:

If Z_1, m are both odd then $Z_1 \equiv 1 \bmod 2$, $m \equiv 1 \bmod 2$ and $s \equiv 2 \bmod 4$, i.e. $p \equiv 3 \bmod 4$. In other words, when $p \equiv 3 \bmod 4$; m must be odd less than or equal to (s/6).

For example take an elliptic curve E: $y^2=x^3+ax+b$ defined on F_{13}. E is supersingular iff the coefficient $\sum_{m=0}^{\left[\frac{s}{6}\right]} \binom{\frac{s}{2}}{\frac{s}{4}-\frac{m}{2}} \binom{\frac{s}{4}-\frac{m}{2}}{m} a^{\frac{s}{4}-\frac{3m}{2}} b^m$ equal to zero.

Since $p=1 \bmod 4$ then m is even less than or equal to 2, i.e. m=0, 2 and the coefficient is $20a^3+15b^2$.

Therefore if we want to find all supersingular elliptic curves that defined on F_{13}, we must find the parameters a and b that satisfy:

$$20a^3+15b^2=0 \bmod 13 \quad \ldots(7)$$

The values of a and b that satisfy equation(7) is:

a	1	1	3	3	4	4	9	9	10	10	12	12
b	4	9	4	9	6	7	4	9	6	7	6	7

which can be found using the following algorithm after giving the value of p as an input.

(Note: The above results are obtained by using a program written in Matlab language)

3.2 An Algorithm for Finding the Supersingular Curves

Input: prime number p

Outputs: a,b which makes the elliptic curve $y^2=x^3+ax+b$ a supersingular

1. set s=p-1
2. if $p=1 \bmod 4$,m1=0, otherwise m1=1

3. for a from 0 to s do the following:
   3.1 for b from 0 to s do the following:
      3.1.1 if $4a^3+27b^2 \neq 0 \bmod p$
         % computing Hass invariant
         1. for m from m1 to [s/6] step 2 do the following:
            3.1.1.1.1 w1=factorial(s/2)/(factorial(s/4-m/2)*factorial((s/2)-(s/4-m/2)))
            3.1.1.1.2 w2=factorial(s/4-m/2)/(factorial(s/4-m/2-m)*factorial(m))
            3.1.1.1.3 w=w+w1*w2*a^(s/4-3*m/2)*b^m
      3.1.2 if w =0 mod p, return a,b

4. Conclusion

From this research, the supersingular elliptic curves that defined on F_p can be found without computing #E, by computing the coefficient of x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$ which is $\sum_{m=0}^{[s/6]} \binom{\frac{s}{2}}{\frac{s}{4}-\frac{m}{2}} \binom{\frac{s}{4}-\frac{m}{2}}{m} a^{\frac{s}{4}-\frac{3m}{2}} b^m$ and finding the values of a, b that makes the above coefficient equal to zero, thus makes $E(F_p)$ a supersingular elliptic curve. In this research we reduce the calculation by putting the available values of m in two cases, even or odd values. For computations we introduce an algorithm for computing the coefficient as well as finding the values of a and b which makes the elliptic curve that defined on F_p as a supersingular elliptic curve.

References:

1. R. Broker, **Constructing Supersingular Elliptic Curves,** 2008, available at: http://www.math.brown.edu/~reinier/supersingular.pdf.
2. H. Cohen, G. Frey, **Handbook of elliptic and hyperelliptic curve cryptography**, Discrete mathematics and its applications, Chapman and Hall-CRC, 2006.
3. L. R. A. Finotti, **A Formula For The supersingular polynomial**, 2008, available at: http://www.math.utk.edu/~finotti.
4. N. Koblitz, **A Course in Number Theory and Cryptography**, Springer-Verlag, New York, 1987.
5. A. Menezes, **Elliptic Curve Public Key Cryptosystems**, Kluwer Academic Publisher, Boston, 1993.
6. H. Silverman, **The Arithmetic of Elliptic Curves**, Graduate Text in Mathematics 106, Springer-Verlag, 1985.
7. W.W. Waterhouse, **Abelian Varieties Over Finite Fields**, Ann.Scient. Ec. Norm. Sup., vol.4, pp. 521-560, 1969.
8. S.Y. Yan, **Number Theory for Computing**, Springer-Verlag, 2000.

إنشاء منحنيات مفردة مفرطة بالاعتماد على معاملات معادلة ويرسترس

الخلاصة:

ان معرفة نوع المنحني الاهليليجي (elliptic curve) المعرّف على الحقل المنته F_p له اهمية عند استخدام تلك المنحنيات الاهليليجية في التطبيقات وخاصة في انظمة التشفير. حيث ان بعض الانواع تكون اكثر أمنية من غيرها. ولذلك قدمنا طريقة بسيطة لانشاء منحني اهليلجي مفرد مفرط (supersingular) عن طريق حساب معامل x^{p-1} في $f(x)^{(p-1)/2}$ حيث $f(x)=x^3+ax+b$. مع خوارزمية لحساب ذلك المعامل لانشاء المنحني المطلوب.