IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728,p-ISSN: 2319-765X, Volume 8, Issue 1 (Sep. - Oct. 2013), PP 01-04
www.iosrjournals.org

The Effect of Field Extension on the Group Structure of Elliptic Curves

Aliyu Danladi Hina
Dept Of Pre-ND, School Of General Studies, The Federal Polytechnic, Bauchi.Nigeria

Abstract: *An elliptic curve E defined over a finite field K, E(K) is the set of solutions to the general Weierstrass polynomial E:* $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ *where the coefficients* a_1, a_2, a_3, a_4, a_6 *є K. There exist a well defined addition of points on each curve such that the points form an abelian group under the addition operation. This group is either cyclic or isomorphic to the product of two cyclic groups. These set of solutions that form the group lie in the closure of the field K over which the curve is defined. If we allow the set to lie only in a particular extension of K, the addition operation is well defined there too. Therefore we can associate a group to every extension K' of the field K denoted by E(K'). Will the structure of the group defined over the base field K, be affected if the same group is made to lie in the extension K' of K?*

Key words: *Cyclic group, Elliptic Curve, Field Extension, Finite Field, Sylow Theorem*

I. Introduction

The points defined on an elliptic curve has been shown to have formed an abelian group which of course satisfies all the group axioms. With elliptic curves groups, the operation "+" was found to be compatible with its geometry, and hence the group structure. When evaluated to provide evidence for abelian group law, an identity element, inverse elements, abelian properties, and associativity were clarified.

The points on an elliptic curve over an arbitrary field form a group, and by the algebraic formulae the group operations eventually amount to computations in the field where the elliptic curve is defined, one has to choose a field with an efficiently implementable arithmetic. Basically, this requirement narrows down to the finite fields. While the rational numbers and more generally number fields also allow exact computations, they have two drawbacks: First, numbers may become arbitrarily big, which destroys the efficiency of the operations. Andreas Enge [2].

Every point on an elliptic curve is one of two kinds: a point of finite order or a point of infinite order. For P to be a point of finite order means there exist a smallest integer n such that $nP = \vartheta$. If no such n exists then P is of infinite order. In other words, P being of infinite order means you can never get the point at infinity by adding P to itself, no matter how many times you do it.

The torsion points, namely those that have finite order, play an important role in
the study of elliptic curves. all points are torsion points on an elliptic curve over a finite field. Andrija Petronicic [3].

Darel H. et al (2004), showed that in the applications of elliptic curves to cryptography, one often needs to construct elliptic curves with known number of points over a prime field F_q, where n is a prime. An elliptic curve over F_q is defined in terms of the solutions to an equation in F_q. The form of the equation defining an elliptic curve over F_q differs depending on whether the field is a prime finite field or a field of characteristic 2.

II. Group Order

Let E be an elliptic curve defined over F_q. The number of points in $E(F_q)$, denoted $\#E(F_q)$, is called the order of E over F_q.

The Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
has at most two solutions for each $x \in F_q$, and that $\#E(F_q) \in [1, 2q+1]$. Hasse's theorem which provides tighter bounds for $\#E(F_q)$.

Theorem 1: Let E be an elliptic curve defined over F_q. Then
$q+1-2\sqrt{q} \le \#E(F_q) \le q+1+2\sqrt{q}$. The interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ is called the Hasse interval.

If E is defined over F_q, then $\#E(F_q) = q + 1 - t$ where $|t| \le 2\sqrt{q}$; t is called the trace of E over F_q. Since $2\sqrt{q}$ is small relative to q, we have $\#E(F_q) \approx q$. The next result determines the possible values for $\#E(F_q)$ as E ranges over all elliptic curves defined over F_q .

Example 1. (orders of elliptic curves over F_{37}) Let q = 37. Table below lists, for each integer n in the Hasse interval $[37+1-2\sqrt{37}, 37+1+2\sqrt{37}]$, the coefficients (a, b) of an elliptic curve $E : y^2 = x^3 + ax + b$ defined over F_{37} with $\#E(F_{37}) = n$.

n(a, b)	n(a, b)	n(a, b)	n(a, b)	n(a, b)
26(5, 0)	31(2, 8)	36(1, 0)	41(1, 16)	46(1,11)
27(0, 9)	32(3, 6)	37(0, 5)	42(1, 9)	47(3, 15)
28 (0, 6)	33(1, 13)	38(1, 5)	43(2, 9)	48(0, 1)
29 (1, 12)	34(1, 18)	39(0, 3)	44(1, 7)	49(0, 2)
30 (2, 2)	35(1, 8)	40(1, 2)	45(2, 14)	50(2, 0)

The admissible orders n = $\#E(F_{37})$ of elliptic curves E : $y^2 = x^3 + ax + b$ defined over F_{37}. Darrel, H. et al. [7]
If E is an elliptic curve defined over F_q, then E is also defined over any extension F_{q^n} of F_q . The group $E(F_q)$ of F_q -rational points is a subgroup of the group $E(F_{q^n})$ of F_{q^n} -rational points and hence $\#E(F_q)$ divides $\#(F_{q^n})$. If $\#E\left(F_q\right)$ is known, then $\#\,E(F_{q^n})$ can be efficiently determined by the following result. Darrel, H. et al. [7]

Theorem 2: Let E be an elliptic curve defined over F_p, and let $\#E(F_q) = q + 1 - t$. Then $\#E(F_{q^n}) = q^n + 1 - V_n$ for all $n \geq 2$, where $\{V_n\}$ is the sequence defined recursively by $V_0 = 2$, $V_1 = t$, and $V_n = V_1V_{n-1} - qV_{n-2}$ for $n \geq 2$.
However, in some cases where the exact order of the group is required, some other methods would have to be employed, e.g. The Legendre symbol or the Baby-Step Giant- Step method. Below is an illustration of the Legendre symbol method. Collins G. S. [6]
Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$ over F_q. Then
$\left|E(F_{q)}\right| = q + 1 + \sum_{x \in F_q} (\frac{x^3 + ax + b}{q})$ Kenneth H. Rosen [14]
Example 2: Let E be the curve given by $y^2 = x^3 + ax + b$ over F_7. Then

$$\left|E(F_{q)}\right| = 7 + 1 + \sum_{x \in F_q} (\frac{x^3 + 6x + 3}{7})$$

$$= 7 + 1 + (3/7) + (3/7) + (2/7) + (6/7) + (0/7) + (4/7) + (3/7)$$

$$= 7 + 1 - 1 - 1 + 1 - 1 + 0 + 1 - 1$$

$$= 6$$

III. Group Structure

We use Z_n to denote a cyclic group of order n.
Theorem 3: A cyclic group is isomorphic to Z / nZ for some $n \in N$. In particular any infinite cyclic group is isomorphic to $(Z, _+)$ and any finite cyclic group of order n is isomorphic to Z / nZ for some natural number n > 0. ALI W., [1]
The following theorem describes the group structure of $E(F_q)$.
Theorem 4: Let E be an elliptic curve defined over Fq. Then $E(F_q)$ is isomorphic to $Z_{n1} \oplus Z_{n2}$ where n_1 and n_2 are uniquely determined positive integers such that n_2 divides both n_1 and $q - 1$. Darrel, H. et al. [7].
Note that $\#E(F_q) = n_1n_2$. If $n_2 = 1$, then $E(F_q)$ is a cyclic group. If $n_2 > 1$, then $E(F_q)$ is said to have rank 2. If n_2 is a small integer (e.g., n = 2, 3 or 4), we sometimes say that $E(F_q)$ is almost cyclic. Since n_2 divides both n_1 and $q - 1$, one expects that $E(F_q)$ is cyclic or almost cyclic for most elliptic curves E over F_q.
Example 3. The elliptic curve E: $y^2 = x^3 + 4x + 20$ defined over F_{29} has $\#E(F_{29}) = 37$. Since 37 is prime, $E(F_{29})$ is a cyclic group and any point in $E(F_{29})$ except for ϑ is a generator of $E(F_{29})$. The following shows that the multiples of the point P = (1, 5) generate all the points in $E(F_{29})$.

0P = ϑ	8P = (8, 10)	16P = (0, 22)	24P = (16, 2)	32P = (6, 17)
1P = (1, 5)	9P = (14, 23)	17P = (27, 2)	25P = (19, 16)	33P = (15, 2)
2P = (4, 19)	10P = (13, 23)	18P = (2, 23)	26P = (10, 4)	34P = (20, 26)
3P = (20, 3)	11P = (10, 25)	19P = (2, 6)	27P = (13, 6)	35P = (4, 10)
4P = (15, 27)	12P = (19, 13)	20P = (27, 27)	28P = (14, 6)	36P = (1, 24)
5P = (6, 12)	13P = (16, 27)	21P = (0, 7)	29P = (8, 19)	
6P = (17, 19)	14P = (5, 22)	22P = (3, 28)	30P = (24, 7)	
7P = (24, 22)	15P = (3, 1)	23P = (5, 7)	31P = (17, 10)	

Theorem 5: Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n , or is 0 (i.e. char. (K) $\nmid$ n or char.(K) = 0), then $E[n] \simeq Z_n \oplus Z_n$ If the characteristic of K is p > 0 and p|n , write $n = p^r n'$ with $p \nmid n'$ Then $E[n] \simeq Z_{n'} \oplus Z_{n'}$ or $Z_n \oplus Z_{n'}$.
Theorem 6: Let E: $y^2 = x^3 + ax + b$ be an elliptic curve defined over K, and let K' be any field extension of K. Then $E(K') = \{(x, y) \in K'^2 : y^2 = x^3 + ax + b\} \cup \{\vartheta\}$
Is a subgroup of E. infact, E(K') ≤ E(K''), for any extension K'' of K'.
We would give detailed group structure of such curves and try to determine if $E(F_{p^n})$ can be completely determined by $E(F_p)$ given that the curves are supersingular and with $a_p = 1$

Theorem 7: Let E be an elliptic curve defined over a finite field of $q = p^n$ elements. Then $\#E(Fq) = 1 + q - a_q$; where a_q is an integer in the range $-2\sqrt{q} \leq a_q \leq 2\sqrt{q}$. Joseph H. S. [12]

For n =2, $q = p^2$, $\#E(F_{p^2})$ can be computed as a function of p and a_p without the need to know a_{p^2}.

Lemma 1: Let E be an elliptic curve defined over Fp. Then,

$$\#(F_{p^2}) = (1 + p + a_p)(1 + p - a_p). \qquad \text{Joseph H. S. [14]}$$

The group structure of elliptic curves can be classified based on their order.

Theorem 8: Let E be a supersingular curve of order q + 1 − t over Fq where $q = p^n$. Then E lies in one of the following classes of curves:

1. t = 0 and $E(F_q) \cong Z_{q+1}$.
2. t = 0 and $E(F_q) \cong Z_{(q+1)/2} \oplus Z_2$ and $q \equiv 3 \bmod 4$.
3. $t^2 = q$ (and n is even).
4. $t^2 = 4q$ (and n is even)
5. $t^2 = 2q$ (and p = 2 and n is odd).
6. $t^2 = 3q$ (and p = 3 and n is odd). Collins G. S. [6]

The following lemma gives the group structure of class of curves above.

Lemma 2: Let E be an elliptic curve over Fq, where $q = p^n$ and let $|E(F_q)| = q + 1 - a$. Then;

1. If $t^2 = q$, 2q, or 3q, then $E(F_q)$ is cyclic. (Nos 3, 5 and 6 above)
2. If $t^2 = 4q$, then either $E(F_q) \cong Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$ or $(F_q) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$, for $t = 2\sqrt{q}$ or $t = -2\sqrt{q}$ respectively.
3. If t = 0 and $q \not\equiv 3 \bmod 4$, then $E(F_q)$ is cyclic. If t = 0 and $q \equiv 3 \bmod 4$, then either $E(F_q)$ is cyclic, or $E(F_q) \cong Z(q+1)/2 \oplus Z_2$. Collins G. S. [6]

Theorem 9: Let E be a supersingular elliptic curve defined over Fp. Then $E(F_{p^2})$ is uniquely determined by $E(F_p)$.

We would use this theorem to completely determine the group structure of $E(F_{p^2})$ knowing only the order of $E(F_q)$ for all supersingular curves over F_p. We will try and compute $\# E(F_{p^2})$ as a function of p and a_p for any $q = p^n$.

If E is an elliptic curve defined over F_q, then E is also defined over any extension F_{q^n} of F_q . The group $E(F_q)$ of F_q -rational points is a subgroup of the group $E(F_{q^n})$ of F_{q^n} -rational points and hence $\# E(F_q)$ divides $\# E(F_{q^n})$. If $\# E(F_q)$ is known, then $\#E(F_{q^n})$ can be efficiently determined by the following result.

Theorem 10: Let E be an elliptic curve defined over Fq, and let $\# E(F_q) = q + 1 - t$. Then $\# E(F_{q^n}) = q^n + 1 - V_n$ for all $n \geq 2$, where $\{V_n\}$ is the sequence defined recursively by $V_0 = 2$, $V_1 = t$, and $V_n = V_1V_{n-1} - qV_{n-2}$ for $n \geq 2$.

Theorem 11: Let E be an elliptic curve defined over F_p. Then $E(F_{p^2})$ is uniquely determined by $E(F_p)$.

Proof. By Theorem 8, we have five cases to consider. Let $q = p^2$. Suppose that $a_p = 0$ so that our curve is of type (2). Andrija Peronicic, [3] we will find that $a_q = (a_p)^2 - 2p = -2p = -2\sqrt{q}$. Since we are considering $q = p^2$, the power of p is even and the a_q term characterizes our group structure to be $(Z/(P \pm 1))^2$ by lemma 2.

Suppose that our curve is of type (3) in Theorem 8. This means that $a_p = \pm\sqrt{q}$ P and that $p \not\equiv 1 \pmod 3$. Computing as above, $a_q = - p = - \sqrt{q}$ with q an even power of p. we conclude that $E(F_{p^2})$ is cyclic.

Suppose that our curve is of type (4) in Theorem 8. Then $a_p = \mp 2\sqrt{p}$ and as before we compute $a_q = 2\sqrt{q}$ with n even. Again, the group structure of $E(F_{p^2})$ is determined to be $(Z/(p \pm 1))^2$.

Suppose that our curve is of type (5) in Theorem 8. Then we have $a_p = \mp\sqrt{2p}$ and p = 2. Now, $a_q = 0$ and note that $2 \equiv 1$ (mod4) is satisfied. It follows that the group structure of $E(F_{p^2})$ is given $\mathbb{Z}/2 \oplus \mathbb{Z}/$ (q+1)/2 or cyclic if $q \equiv 3 \pmod 4$. Finally, suppose that our curve is of type (6) in Theorem 8. Hence $a_p = \pm\sqrt{3p}$ and $a_q = \sqrt{q}$ with $3 \not\equiv 1 \pmod 3$ and the group structure of $E(F_{p^2})$ is cyclic. Andrija P. [3]

IV. Conclusion

It follows that upon a degree two extension of $E(F_p)$, denoted by $E(F_{p^2})$ both possible group structures defined on the extension field occur; and depends on the group structure defined on the base field F_p. This can be computed by the process described above for both a_p = -1 and a_p = 1. The approach taken in this research can become substantially more difficult for a_p with large absolute value. In particular, we can have more primes ` for which the Sylow-`subgroup of E(Fp2) is not uniquely determined and it becomes more difficult to find the possible group structure for each ℓ.

Referrences

[1] Ali Wesin (2004). Lecture Notes: Basic Algebra. University Kustepe Sisli Istanbul Turkey

[2] Andreas Enge (1999), elliptic Curve and their application to cryptography. Chapman and Hall/CRC, New York.

[3] Andrija Petronicic (2008). The Group Structure of Elliptic Curves Defined over Finite Fields, Project Thesis bard College, Annandale-on-Hudson. New York

[4] Berlekamp E. R. (1970). Factoring Polynomials over Large Finite Fields. Mathematics of Computation Vol. 24, No. 11

[5] Carlos Moreno (1991). Algebraic Curves over Finite Fields. Cambridge University Press.

[6] Collins G. S. (2010). Elliptic Curve, Cryptography and Factorization. Project IV University of Durham.

[7] Darrel H., Alfred M. and Scott V. (2004). Guide To Elliptic Curve Cryptography. springer-Valag, New York Inc.

[8] David S. Dummit and Richard M. Foote (1991). *Abstract Algebra.* Prentice-Hall, Englewood Cliffs, New Jersey.

[9] Felipe Voloch (1988). *A Note on Elliptic Curves Over Finite Fields.* Bull. Soc. Math France Vol. 116

[10] Heer Zhao (2007). *The Extension Group of Elliptic Curve.* M. Sc Thesis, Universiteit Leiden.

[11] Henri Cohen and Gerhard Frey (2006). *Handbook of Elliptic and Hyperbolic Curve Cryptography*. Chapman and Hall/CRC, New York.

[12] Joseph H. Silverman (1986). *The Arithmetic of Elliptic Curves.* Springer-Verlag, USA.

[13] Joseph H. S. and John Tate (1992). *Rational Points on Elliptic Curve.* Springer- Verlag, New York.

[14] Kenneth H. Rosen (2006). *Discrete Mathematics and Its Applications.* Chapman & Hall, USA.

[15] Mathew P. Young (2006). *Basics of Elliptic Curve.* American Institute Of Mathematics.

[16] Mullin R. C., Onyszchuk I. M. and Wilson R. M. (1987). *Discrete Applied Mathematics.* Massachusetts Kluwer Academic Press.

[17] Patrick Morandi (1996). *Field and Galois Theory.* Springer-Verlag, U. S. A.R. Lidl And H. Niederreiter (1996). *Finite Fields.* Cambridge University Press, Cambridge.

[18] R. Schoof (1985). *Elliptic curves over Finite Fields and the computation of square roots mod p*. Math. Comp. 44.

[19] Sarah Miers (2001). *Implementing Elliptic Curve Cryptography using normal and Polynomial Basis.* ECE Journal no.636.