JP Journal of Algebra, Number Theory and Applications
Volume 17, Number 1, 2010, Pages 21-25
Published Online: June 1, 2010
This paper is available online at http://pphmj.com/journals/jpanta.htm

A CONCISE FORMULA ON ELLIPTIC CURVES OVER FINITE FIELDS

LINGYUN LI and SHAOHUA ZHANG

School of Computer Science
Liaocheng University
Liaocheng, 252059, P. R. China
e-mail: lilingyun@mail.sdu.edu.cn

School of Mathematics
Shandong University
Jinan, Shandong, 250100, P. R. China
e-mail: shaohuazhang@mail.sdu.edu.cn

Abstract

In this note, using the property of the twist, we obtain a concise formula about the sum of the number of elements of group of rational points on some kinds of elliptic curves over the finite field. This formula can be generalized to the generic case. Moreover, we give some interesting remarks.

1. Introduction

Let F_q be a finite field and let E be an elliptic curve over F_q. $H(E)$ is defined to be the number of elements of group of rational points on the elliptic curve E over the finite field F_q. As we know, like the irregularity of Euler function $\varphi(n)$ for

2010 Mathematics Subject Classification: 11Y50, 11G20, 11G30, 14H52.

Keywords and phrases: elliptic curve, point counting problem, finite fields, the twist of a curve, RSA.

This work was partially supported by the Natural Science Foundation of Shandong Province (No. Y2008G23) and the National Science Foundation (No. 60874075).

Received December 12, 2009

distinct positive integers n, the occurrence of $H(E)$ are irregular for distinct elliptic curves E over F_q. However, like $\sum_{d|n}\varphi(d) = n$, we find similarly that for some kinds of elliptic curves $\mathcal{E}$, $\sum_{E\in\mathcal{E}} H(E)$ have a concise formula. For details, see the following Theorem 1. Furthermore, based on Schoof's work on the point counting problem, we conjecture similarly that there will be a deterministic polynomial time algorithm for counting Euler function. Thus, the RSA modulus can be expected to factor completely in a polynomial time. For more details, see Section 3.

Theorem 1. *Denote the number of elements of group of rational points on the elliptic curves of the form* $y^2 = x^3 + ax + b$ *over a finite field* F_q *by* $H(E_{a,b})$. *Then* $\sum_{(a,b)\in F_q\times F_q} H(E_{a,b}) = (q+1)q(q-1)$ *for* $Char\,(F_q) \neq 2$.

2. The Proof of Theorem 1

In order to prove Theorem 1, firstly, we introduce the concept and property of twist. For details, see [1]. Let F_q be a finite field and let $E_{a,b}$ given in short Weierstrass form $Y^2 = X^3 + aX + b$ be an elliptic curve over F_q. A twist of the curve $E_{a,b}$ is given by $E_{c,d}$, where $c = av^2$ and $d = bv^3$ for some quadratic non-residue $v \in F_q$. A useful property of twist is $H(E_{a,b}) + H(E_{c,d}) = 2q + 2$.

The proof of Theorem 1. Let $v \in F_q$ be a quadratic non-residue. Clearly, the mapping $f : F_q \times F_q \to F_q \times F_q$ with $f(a, b) = (av^2, bv^3)$ is one-to-one. Hence, we have

$$2\sum_{(a,b)\in F_q\times F_q} H(E_{a,b}) = \sum_{(a,b)\in F_q\times F_q} H(E_{a,b}) + \sum_{(av^2,bv^3)\in F_q\times F_q} H(E_{av^2,bv^3}).$$

Using the property of the twist which states that $H(E_{a,b}) + H(E_{av^2,bv^3}) = 2q + 2$, we have $2\sum_{(a,b)\in F_q\times F_q} H(E_{a,b}) = (2q+2)N$, where N is the number of the elliptic curves of the form $y^2 = x^3 + ax + b$ over the finite field F_q. Note that $N = q(q-1)$. Namely, there are exactly $q(q-1)$ pairs (a, b) such that the discriminant

$\Delta = -16(4a^3 + 27b^2) \neq 0$. Therefore, $\sum_{(a,b)\in F_q\times F_q} H(E_{a,b}) = (q+1)q(q-1)$. It finishes the proof of Theorem 1.

3. Some Remarks

Remark 1. In Theorem 1, we do not consider the isomorphism between two distinct elliptic curves. Namely, $y^2 = x^3 + ax + b$ and $y^2 = x^3 + cx + d$ are distinct if $(a, b) \neq (c, d)$. However, they perhaps are isomorphic and $H(E_{a,b}) = H(E_{c,d})$.

Remark 2. Theorem 1 could be generalized. Denote the number of all elliptic curves of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ over any finite field F_q by N, where $a_i \in F_q$. Then the sum of the number of elements of group of rational points on all elliptic curves of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ over F_q is $(q+1)N$. Particularly, the sum of the number of elements of group of rational points on all elliptic curves of the form $y^2 = x^3 + a_2x^2 + a_6$ over F_{3^n} is $(q-1)^2(q+1)$, where $q = 3^n$.

Remark 3. As we know, for large positive integer n, there is not an efficient algorithm for factoring n. Thus, it is hard to compute $\varphi(n)$ if n is composite and its factorization is not known. However, some elementary estimations have been obtained. Sierpiński [6] proved that $\varphi(n) \leq n - \sqrt{n}$ if n is composite. Kendall and Osborn [4] showed that $\varphi(n) > n^{\frac{2}{3}}$ for $n > 30$. Hatalová and Šalát [3] refined it to $\varphi(n) > \frac{\log 2}{2}\frac{n}{\log n}$ for $n \geq 3$. As a special case, let us consider RSA modulus $n = qp$, where p and q are distinct odd primes with $p < q < 2p$. Clearly, in this case, we have $(\sqrt{n}-2)^2 < \varphi(n) < (\sqrt{n}-1)^2$. This implies that $|n - [3\sqrt{n}] + 1 - \varphi(n)| < \sqrt{n}$. Similarly, we have a classical inequation on $H(E)$. In 1930's, Hasse [2] proved that Artin's conjecture which states that $|H(E) - q - 1| \leq 2\sqrt{q}$. In 1985, Schoof [5] published the first deterministic polynomial time algorithm with

$O(\log^9 q)$ operations for computing $H(E)$ for arbitrary elliptic curve E over a large finite field F_q. This is a theoretical breakthrough for the point counting problem. By two aforementioned similar inequations, we believe that there will also be a deterministic polynomial time algorithm for computing Euler function $\varphi(n)$. Thus, the RSA modulus can be expected to factor completely in a polynomial time. Let us try the item to wait.

Remark 4. Many modern factorization algorithms such as the Elliptic Curve Factoring Algorithm and the Number Field Sieve have been showed that there is a sub-exponential time algorithm for factoring a large integer n. People conjecture that there is a deterministic polynomial time algorithm for factoring n. Thus, there is a deterministic polynomial time algorithm for counting Euler function $\varphi(n)$. On the other hand, if we do not know the factorization of n, but we know $\varphi(n)$, can we factor n? These two questions maybe are equivalent (especially, when $n = pq$). Unfortunately, for generic cases, so far it has not been proved or disproved. So, in this note, we would like to stress this problem and hope that people are interested in it.

Remark 5. Based on Remark 4, we try to ask another question: for given large integer n, how to compute $\varphi(n)$? Do we need factor n? If we do not factor n, what shall we do? By Schoof's algorithm, we could get similarly a method as follows: for any given small prime p (for example, $p \sim \log n$), count $\varphi(n) \pmod p$. But is there a deterministic polynomial time algorithm for counting $\varphi(n) \pmod p$? Surely, $\varphi(n) \equiv 0 \pmod 2$. However, how to solve the cases that p is odd? We will further consider these questions.

References

[1] I. F. Blake, G. Seroussi and N. P. Smart, Elliptic curves in cryptography, Reprint of the 1999 original, London Mathematical Society Lecture Note Series, 265, Cambridge University Press, Cambridge, 2000.

[2] H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität 10 (1934), 325-348.

[3] H. Hatalová and T. Šalát, Remarks on two results in the elementary theory of numbers, Acta Fac. Rerum Natur. Univ. Comenian. Math. 20 (1970), 113-117.

[4] D. G. Kendall and R. Osborn, Two simple lower bounds for Euler's function, Texas J. Sci. 17(3) (1965), #3.

[5] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44(170) (1985), 483-494.

[6] W. Sierpiński, Elementary Theory of Numbers, Warszawa, 1964.