Korean J. Math. **16** (2008), No. 4, pp. 451–455

ON THE POINTS OF ELLIPTIC CURVES

Jangheon Oh

Abstract. In this paper we give some results on the points of elliptic curves which have application to elliptic curve cryptography.

1. Introduction

In this paper, we prove two theorems(Theorems 2.1 and 2.3) about points on elliptic curves. First, we prove that given an elliptic curve E_p over a finite field $\mathbb{F}_p$ and two points on the curve there exist an infinite family of elliptic curves E with positive rank defined over $\mathbb{Q}$ and two points on the curve such that the reduction mod p of E and points give rise to the prescribed elliptic curve E_p and the points on it. If one of the lifted curve has rank 1, we can solve the ECDLP(elliptic curve discrete logarithm problem). Secondly, we give a formula on the number of points of elliptic curves defined over the ring $\mathbb{Z}/n$, where n is a positive integer.

2. Main results

Let us consider the ECDLP problem $Q^{\sim} = mP^{\sim}$ where $P^{\sim}, Q^{\sim}$ are points in an elliptic curve $E(\mathbb{F}_p)$. Suppose a lifting $E/\mathbb{Q}$ of $E^{\sim}/\mathbb{F}_P$ is of rank 1 and contains points P, Q which are reduced to $P^{\sim}, Q^{\sim}$. Moreover, if P, Q are not torsion points, then we have a dependence equation $aP + bQ = O$. Hence we have a good chance to solve the ECDLP problem. Let $(\frac{\cdot}{p})$ denote the Legendre symbol.

Theorem 2.1. *Let $E_p : y^2 = x^3 + ax + b$ be an elliptic curve defined over a finite field $\mathbb{F}_p$ and $P^{\sim} = (x_0, y_0), Q^{\sim} := mP^{\sim}$ be points on the*

Received June 26, 2008. Revised October 1, 2008.
2000 Mathematics Subject Classification: 14H52, 94A60.
Key words and phrases: elliptic curves, ECDLP, liftings of points on elliptic curves.

elliptic curve E_p with $(\frac{y_0}{p}) = 1$. Then there exists an integer D such that the elliptic curve $E^D : Dy^2 = x^3 + ax + b$ defined over $\mathbb{Q}$ has a positive rank and the reduction of E^D is E_p. Moreover, the curve E^D contains points P, Q which are reduced to $P^{\sim}, Q^{\sim}$.

Proof. Since $(\frac{y_0}{p}) = 1$, we can find an integer r such that $\frac{1}{r^2} \equiv y_0 \mod p$. Let $s = rx_0$. Then, for an integer $D := (s^3 + asr^2 + br^3)r$, the point $P = (\frac{s}{r}, \frac{1}{r^2})$ is a rational point of the elliptic curve E^D. Note that $D \equiv 1 mod p$. Hence the reduction of E^D mod p is the elliptic curve E_p. Moreover, by the Nagell-Lutz theorem, the point P is of infinite order. Obviously, the point $Q = mP$ is on the curve E^D and it is reduced to a point $Q^{\sim}$. This completes the proof □

The following theorem gives a useful information to find elliptic curves over $\mathbb{Q}$ the ranks of the quadratic twists of which are uniformly bounded.

For the polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ having three distinct roots, define

$$F(u, v) = v(u^3 + au^2v + buv^2 + cv^3) = v^4 f(\frac{u}{v}),$$

and

$$\Psi = \{(u, v) \in \mathbb{Z}^2 : gcd(u, v) = 1 \ \text{ and } \ F(u, v) \neq 0\}.$$

If $n \in \mathbb{Q}^*$, let $s(n)$ denote the squarefree part of n, i.e., $s(n)$ is the unique squarefree integer such that $n = s(n)m^2$ with $m \in \mathbb{Q}$. Note that $s(f(\frac{u}{v})) = s(F(u, v))$ for all $u, v \in \mathbb{Z}$ such that $F(u, v) \neq 0$. If α is a nonzero rational number, and $\alpha = \frac{u}{v}$ with u, v relatively prime integers, define $h(\alpha) = max\{1, log|u|, log|v|\}$. For nonnegative real numbers j and k define the infinite sums

$$S_E(j, k) = \sum_{(u,v)\in\Psi} \frac{1}{|s(F(u, v))|^k h(\frac{u}{v})^j},$$

$$R_E(j, k) = \sum_{t=1}^{\infty} \sum_{(u,v)\in\Psi, t^2|F(u,v)} \frac{t^{2k}}{|F(u, v)^k| h(\frac{u}{v})^j}.$$

If d is a positive integer, let

$$\Omega_d = \{\alpha \in \mathbb{Z}/d^2\mathbb{Z} : f(\alpha) \equiv 0 (mod \ \ d^2)\}.$$

If d, d' are positive integers and $\alpha \in \Omega_d$, let $\omega_{\alpha,d,d'}$ be a shortest nonzero vector in the lattice

$$L_{\alpha,d,d'} = \{(u, v) \in \mathbb{Z}^2 : u \equiv \alpha v (mod \ \ d^2) \ \text{ and } \ v \equiv 0 (mod \ \ d'^2)\}.$$

Define

$$Q_E(j,k) = \sum_{d,d'=1, gcd(d,d')=1}^{\infty} \frac{(dd')^{2k}}{max(1, log(dd'))^j} \sum_{\alpha\in\Omega_d, \omega_{\alpha,d,d'}\in\Psi} ||\omega_{\alpha,d,d'}||^{-4k}.$$

THEOREM 2.2. [3] *If j is a positive real number, then the following conditions are equivalent:*
(a) $rank_{\mathbb{Z}} E^D(\mathbb{Q}) < 2j$ for every $D \in \mathbb{Z} - \{0\}$.
(b) $S_E(j,k)$ converges for some $k \geq 1$.
(c) $S_E(j,k)$ converges for every $k \geq 1$.
(d) $R_E(j,k)$ converges for some $k \geq 1$.
(e) $R_E(j,k)$ converges for every $k \geq 1$.
(f) $Q_E(j,k)$ converges for some $k \geq 1$.
(g) $Q_E(j,k)$ converges for every $k \geq 1$.

Let n be an integer whose factors are greater than 3 and E be " an elliptic curve defined over $\mathbb{Z}/n$", by which we mean that E is a curve satisfying the equation $y^2 = x^3 + ax + b$ with

$$gcd(4a^3 + 27b^2, n) = 1 \tag{1}$$

for $a, b \in \mathbb{Z}/n$. In this paper we compute the number of points E_n of the set $E(\mathbb{Z}/n)$, where

$$E(\mathbb{Z}/n) = \{(x,y)|y^2 \equiv x^3 + ax + b(modn), x, y \in \mathbb{Z}/n\}.$$

Hence, if we denote $N_{E,p}$ the number of points of the group $E(\mathbb{F}_p)$, $E_p = N_{E,p} - 1$ for a prime p since we do not include the point at infinity in counting E_n. If E is an elliptic curve defined over $\mathbb{Z}/n$, then by abuse of notation we denote the elliptic curve reducing the coefficients of E by modulo p by E. The explicit formula for E_n is as follows.

THEOREM 2.3. *Suppose that the prime power factorization of n is $n = \prod_{i=1}^{k} p_i^{a_i}$. Then*

$$E_n = \prod_{i=1}^{k} {p_i}^{a_i - 1}(N_{E,p_i} - 1).$$

As a corollary, we prove

Corollary 2.4. *Let* $n = \prod_{i=1}^{k} p_i^{a_i}$ *be an integer such that* $p_i \equiv 2(mod 3)$ *for all* $i = 1, \cdots, k$. *Then* $E_n^b = n$ *for any* $0 < b < n, gcd(b, n) = 1$, *where* E^b *is an elliptic curve* $y^2 = x^3 + b$.

Theorem 2.3 directly comes from Lemma 2.5 and the Chinese Remainder Theorem. If the condition (1) is not satisfied, then Theorem 2.3 may not hold. For example, $E_{13} = 14, E_{13^2} = 13^2$ for the curve $E : y^2 = x^3 + x + 3$.

The proof of Corollary 2.4 directly comes from Theorem 2.3 and Lemma 2.6.

Lemma 2.5. *Let* $E := y^2 = x^3 + ax + b$ *be an elliptic curve defined over* $\mathbb{Z}/p^{m+1}$ *for a prime* p *and an integer* $m \geq 1$. *Then*

$$E_{p^{m+1}} = pE_{p^m}.$$

Proof. Suppose that $(\alpha, \beta) \in E(\mathbb{Z}/p^m)$. Then α, β satisfy $\beta^2 - \alpha^3 - a\alpha - b = dp^m$ for some integer d. We will lift the point (α, β) to a point in $E(\mathbb{Z}/p^{m+1})$. Write $\alpha_1 = \alpha + a_1p^m, \beta_1 = \beta + b_1p^m$ for some integers $0 \leq a_1, b_1 \leq (p-1)$. Then

$$\begin{aligned} & {\beta_1}^2 - {\alpha_1}^3 - a\alpha_1 - b \\ \equiv\ & \beta^2 + 2b_1\beta p^m - \alpha^3 - 3\alpha^2 a_1 p^m - a\alpha - aa_1p^m - b \\ \equiv\ & p^m(d + 2b_1\beta - (3\alpha^2 + a)a_1) \qquad (mod p^{m+1}). \end{aligned}$$

Both $3\alpha^2 + a$ and β cannot be zero modulo p by the assumption of (1), so we may assume one of them, say $3\alpha^2 + a$, is not zero modulo p. If we take $a_1 \equiv (3\alpha^2 + a)^{-1}(d + 2b_1\beta)(mod p)$, then $(\alpha_1, \beta_1) \in E(\mathbb{Z}/p^{m+1})$ for any integer $0 \leq b_1 \leq (p-1)$. Hence every point in $E(\mathbb{Z}/p^m)$ can be lifted to p different points in $E(\mathbb{Z}/p^{m+1})$. Conversely every point in $E(\mathbb{Z}/p^{m+1})$ can be reduced to a point in $E(\mathbb{Z}/p^m)$, which completes the proof. □

Okamoto and Uciyama [2] proposed a digital signature scheme based on the difficulty of factoring $n = p^2q$. Suppose that we have a factorization of an integer $n = p^2q$. Then we can compute E_n using Schoof's algorithm and the formula $E_n = p(N_{E,p} - 1)(N_{E,q} - 1)$ in Theorem 2.3. Conversely, suppose that we have an algorithm for counting E_n. Then we see by Theorem 2.3 that $\frac{n}{gcd(n,E_n)} = 1, p, q, pq$. So we can find a factor of n with probability $\frac{1}{2}$.

Note that $gcd(n, E_n) = n$ only for those elliptic curves with $p \equiv q \equiv 2(mod 3), a = 0$ by following lemma.

LEMMA 2.6. *Let $p \neq 3$ be an odd prime. Then $p \equiv 2(mod 3)$ if and only if for $0 < b < p$, $E^b : y^2 = x^3 + b$ is a cyclic group of order $p + 1$.*

Proof. ($\Rightarrow$) See the proof of Lemma 1 in [1]
($\Leftarrow$) Assume that $p \equiv 1(mod 3)$. Then there exist a third root of unity $\omega \in \mathbb{F}_p$. Let t be the number of $(x^3 + b)'s$ such that $x^3 + b$ is a nonzero square for nonzero x. When b is not a cubic, then $E_p^b = 6t$ or $6t + 2$ depending on whether b is a square or not. If b is a cubic, then $E_p^b = 6t+3$ or $6t+5$ depending on whether b is a square or not. Therefore E_p^b cannot be p since p is congruent $1(mod 3)$. □

References

[1] K.Koyama, U.Maurer, T.Okamoto, and S.A.Vanstone, *New public key Schemes based on Elliptic Curves over the ring $\mathbb{Z}_n$* , Advanecs in Cryptology-Crypto 91(1992), LNCS no.576, Springer-Verlag, 252-266.

[2] T. Okamoto, S. Uchiyama,*A New Public-key Cryptosystem as Secure as Factoring*, Advances in Cryptology - EUROCRYPT '98(1998) Proceedings, Springer Verlag, 308-318.

[3] K.Rubin and A.Silverberg, *Ranks of elliptic curves in families of quadratic twists*, Experimental Math., 9(2000), 583-590.

Department of Applied Mathematics
Sejong University
Seoul 143-747, Korea
E-mail: oh@sejong.ac.kr