International Journal of Pure and Applied Mathematics
Volume 77 No. 1 2012, 11-15
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

ON THE NUMBER OF THE PAIRING-FRIENDLY CURVES

Takanori Yasuda[1], Masaya Yasuda[2] §,
Takeshi Shimoyama[3], Jun Kogure[4]

[1]Faculty of Mathematics
Kyushu University
744 Motoka, Nishi-Ku, Fukuoka, 819-0935, JAPAN

[2,3,4]Fujitsu Laboratories Ltd.
1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki
211-8588, JAPAN

Abstract: In pairing-based cryptography, it is necessary to choose an elliptic curve with a small embedding degree and a large prime-order subgroup, which is called a *pairing-friendly curve*. In this paper, we study the number of the pairing-friendly curves with a given large prime-order subgroup.

1. Introduction

In pairing-based cryptography, the Weil or Tate pairing on elliptic curves has been applied to propose many new and novel protocols, such as identity-based encryption [2, 12], short signature [3], and one-round three-way key exchange [7]. To implement pairing-based systems, it is necessary to choose "pairing-friendly" curves. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with q elements. For a fixed prime divisor r of $\sharp E(\mathbb{F}_q)$, we define the *embedding degree of* E to be the smallest integer k with $r \mid q^k - 1$. According to [6, Definition 2.3], the elliptic curve E is *pairing-friendly* if $\rho(E) \leq 2$ and $k < \log_2(r)/8$, where $\rho(E) = \log q / \log r$.

Received: August 12, 2011

§Correspondence author

There are a number of methods of specific constructions of such curves (see [6] for details). In particular, the method of constructing pairing-friendly ordinary elliptic curves works in the following two steps (see [11]):

Step 1 Choose a prime r, integers $k \geq 2$ and t, and a prime power q such that

$$|t| \leq 2q^{1/2},\ t \neq 0, 1, 2,\ r \mid q + 1 - t \text{ and } r \mid \Phi_k(q), \tag{1}$$

where $\Phi_k(x)$ is the k-th cyclotomic polynomial.

Step 2 Construct an elliptic curve E over $\mathbb{F}_p$ with $\sharp E(\mathbb{F}_q) = q + 1 - t$. Then E has a subgroup of order r and an embedding degree k if $r \nmid k$ (see [6, Proposition 2.4]). In particular, the elliptic curve E is pairing-friendly if $\rho(t, r, q) \leq 2$ and $k < \log_2(r)/8$, where $\rho(t, r, q) = \log q / \log r$.

For positive real numbers x and y, Luca and Shparlinski in [9, 10, 11] studied the number of prime powers $q \leq x$ for which there exist a prime $r \geq y$ and an integer t satisfying the above condition (1) and certain condition on the size of the complex multiplication discriminant of the corresponding elliptic curve. Given an elliptic curve E over the field $\mathbb{Q}$ of rational numbers, Cojocaru and Shpalinski in [5] studied the number of primes $p \leq T$ for which the reduction of E modulo p has a large prime factor and also a small embedding.

Fix a large prime number r. For an integer $2 \leq k < \log_2(r)/8$ and a real number $\rho \leq 2$, we define

$$\Psi(k, \rho, r) = \left\{ (t, q) \;\middle|\; \begin{array}{l} \text{(i) } t, q \in \mathbb{Z} \text{ with a prime } q, \\ \text{(ii) } (t, r, q, k) \text{ satisfies the condition (1)}, \\ \text{(iii) } \rho(t, r, q) \leq \rho. \end{array} \right\},$$

which corresponds to the set of the pairing-friendly ordinary elliptic curves over prime fields with a subgroup of order r and an embedding degree k. In this paper, we study the number of the set $\Psi(k, \rho, r)$.

2. Main Result

We define

$$T(k, \rho, r) = \left\{ t \in \mathbb{Z} \;\middle|\; \Phi_k(t - 1) \equiv 0 \bmod r,\ |t| < 2r^{\rho/2} \text{ with } t \neq 0, 1, 2 \right\}.$$

For an element $t \in T(k, \rho, r)$, we also define

$$Q(t, \rho, r) = \left\{ q : \text{ prime} \;\middle|\; q \leq r^{\rho},\ q \equiv t - 1 \bmod r \right\}.$$

Then we have the following lemma:

Lemma 1.

$$\sharp\Psi(k,\rho,r) \leq \sum_{t\in T(k,\rho,r)} \sharp Q(t,\rho,r).$$

Proof. We have $r \mid \Phi_k(t-1)$ if $r \mid q+1-t$ and $r \mid \Phi_k(q)$. This shows the lemma. □

A prime $q \in Q(t,\rho,r)$ has the form

$$q = (t-1) + ar, \quad \exists a \in \mathbb{Z}.$$

For $t \in T(k,\rho,r)$, we see that $t-1$ and r are coprime since $\Phi_k(t-1) \equiv 0 \bmod r$. By the prime number theorem for arithmetic progressions [4], we have

$$\sharp Q(t,\rho,r) \sim \frac{\pi(r^\rho)}{\phi(r)} \sim \frac{r^\rho}{\phi(r)\log(r^\rho)},$$

where $\pi(x)$ denotes the number of primes less than or equal to x and ϕ is the Euler's function. Therefore it follows from Lemma 1 that we have

$$\sharp\Psi(k,\rho,r) \leq \sum_{t\in T(k,\rho,r)} \frac{r^\rho}{\phi(r)\log(r^\rho)} = \frac{r^\rho}{\phi(r)\log(r^\rho)} \cdot \sharp T(k,\rho,r) \tag{2}$$

as $r \to \infty$.

We next consider the number of the set $T(k,\rho,r)$. The following lemma is needed:

Lemma 2. *Let $0 \leq t_0 < r$ be an integer and let $\Omega(t_0)$ denote the set $\{t_0 - 2r, t_0 - r, t_0, t_0 + r\}$. If $t \in \mathbb{Z}$ satisfies $t \equiv t_0 \bmod r$ and $|t| < 2r^{\rho/2}$, then $t \in \Omega(t_0)$.*

Proof. If $t \notin \Omega(t_0)$, then we have $t^2 \geq 4r^2$. This is a contradiction to the condition $|t| < 2r^{\rho/2} \leq 2r$. □

Let S be the group of the k-th power roots of unity in the group $(\mathbb{Z}/r\mathbb{Z})^*$. For any element $t \in T(k,\rho,r)$, let $0 \leq t_0 < r$ be an integer with $t \equiv t_0 \bmod r$. Since $\Phi_k(t_0 - 1) \equiv \Phi_k(t-1) \equiv 0 \bmod r$, we have $t_0 - 1 \bmod r \in S$. Hence any element $t \in T(k,\rho,r)$ satisfies

$$t \in \Omega(t_0),\ 0 \leq \exists t_0 < r \text{ with } t_0 - 1 \bmod r \in S$$

by Lemma 2. Therefore we have $\sharp T(k,\rho,r) \leq 4k$. By the inequality (2), we have the following:

Theorem 1. *We have*

$$\sharp\Psi(k,\rho,r) \leq \frac{4kr^{\rho}}{\phi(r)\log(r^{\rho})}$$

as $r \to \infty$.

For a pairing-based system to be secure, the size of r is required to be large (for example, $r \approx 2^{160}$). Moreover pairing-friendly curves with $\rho \approx 1$ are preferable (see [6, §1.1]). However, the result of Theorem 1 shows that the pairing-friendly ordinary elliptic curves over prime fields with a large prime-order subgroup are very rare if ρ is close to 1.

References

[1] R. Balasubraminian, N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm, *J. Cryptology*, **11** (1998), 141-145.

[2] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Comput.*, **32** (2003), 586-615.

[3] D. Boneh, B. Lynn, H. Shacham, Short signature from the Weil pairing, *J. Cryptology*, **17** (2004), 297-319.

[4] Z.I. Bolrevich, I.R. Shafarevich, *Number Theory*, New York, Academic Press (1966).

[5] A.C. Cojocaru, I.E. Shparlinski, On the embedding degree of reductions of an elliptic curve, *Infomation Processing Letters*, **109** (2009), 652-654.

[6] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, *J. Cryptology*, **23** (2010), 224-280.

[7] A. Joux, A one round protocol for tripartite Diffie-Hellman, *J. Cryptology*, **17** (2004), 263-276.

[8] F. Luca, D.J. Mireles, I.E. Shparlinski, MOV attack in various subgroups on elliptic curves, *Illinois J. Math.*, **48** (2004), 1041-1052.

[9] F. Luca, I.E. Shparlinski, On the exponent of the group of points on elliptic curves in extension fields, *Intern. Math. Research Notices*, **2005** (2005), 1391-1409.

[10] F. Luca, I.E. Shparlinski, On finite fields for pairing based cryptography, *Advances in Mathematics of Communications*, **1** (2007), 281-286.

[11] F. Luca, I.E. Shparlinski, Elliptic curves with low embedding degree, *J. Cryptology*, **19** (2006), 553-562.

[12] R. Sakai, K. Ohgishi, M. Kasahara, Cryptosystems based on pairings, In: *2000 Symposium on Cryptography and Information Security - SCIS 2000*, Okinawa, Japan (2000).