On the Number of the Pairing-friendly Curves

Yasuda, Takanori
Faculty of Mathematics, Kyushu University

Yasuda, Masaya
Fujitsu Laboratories Ltd. | Fujitsu Laboratories Ltd.

Shimoyama, Takeshi
Fujitsu Laboratories Ltd.

Kogure, Jun
Fujitsu Laboratories Ltd.

出版情報：MI Preprint Series. 2010-29, 2010-09-08. Faculty of Mathematics, Kyushu University
バージョン：
権利関係：

MI Preprint Series

Kyushu University
The Global COE Program
Math-for-Industry Education & Research Hub

On the Number of the Pairing-friendly Curves

Takanori Yasuda Masaya Yasuda, Takeshi Shimoyama and Jun Kogure

MI 2010-29

(Received September 8, 2010)

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

ON THE NUMBER OF THE PAIRING-FRIENDLY CURVES

TAKANORI YASUDA, MASAYA YASUDA, TAKESHI SHIMOYAMA, AND JUN KOGURE

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 $\rho(E) = \log q / \log r$.

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

Key words and phrases. pairing-friendly curves, elliptic curves, embedding degree.

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 and N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm", J. Cryptology, **11** (1998), pp. 141-145.

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

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

[4] Z. I. Bolrevich and I. R. Shafarevich, Number Theory, New York, Academic Press, 1966.
[5] A. C. Cojocaru and I. E. Shparlinski, "On the embedding degree of reductions of an elliptic curve", Infomation Processing Letters, **109** (2009), pp. 652- 654.
[6] D. Freeman, M. Scott and E. Teske, "A taxonomy of pairing-friendly elliptic curves", J. Cryptology, **23** (2010), pp. 224-280.
[7] A. Joux, "A one round protocol for tripartite Diffie-Hellman", J. Cryptology, **17** (2004), pp. 263-276.
[8] F. Luca and D. J. Mireles and I. E. Shparlinski, "MOV attack in various subgroups on elliptic curves", Illinois J. Math., **48** (2004), pp. 1041-1052.
[9] F. Luca and I. E. Shparlinski, "On the exponent of the group of points on elliptic curves in extension fields", Intern. Math. Research Notices, **2005** (2005), pp. 1391-1409.
[10] F. Luca and I. E. Shparlinski, "On finite fields for pairing based cryptography", Advances in Mathematics of Communications, **1** (2007), pp. 281-286.
[11] F. Luca and I. E. Shparlinski, "Elliptic curves with low embedding degree", J. Cryptology, **19** (2006), pp. 553-562.
[12] R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems based on pairings", 2000 Symposium on Cryptography and Information Security - SCIS 2000 (2000), Okinawa, Japan.

Takanori Yasuda
Faculty of Mathematics, Kyushu University
744 Motooka, Nishi-ku, Fukuoka 819-0935 Japan
E-mail address: tyasuda@math.kyushu-u.ac.jp

Masaya Yasuda
FUJITSU LABORATORIES LTD.
1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki, 211-8588 Japan
E-mail address: myasuda@labs.fujitsu.com

Takeshi Shimoyama
FUJITSU LABORATORIES LTD.
1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki, 211-8588 Japan
E-mail address: shimo@labs.fujitsu.com

Jun Kogure
FUJITSU LABORATORIES LTD.
1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki, 211-8588 Japan
E-mail address: kogure@jp.fujitsu.com

List of MI Preprint Series, Kyushu University

The Global COE Program
Math-for-Industry Education & Research Hub

MI

MI2008-1 Takahiro ITO, Shuichi INOKUCHI & Yoshihiro MIZOGUCHI
Abstract collision systems simulated by cellular automata

MI2008-2 Eiji ONODERA
The intial value problem for a third-order dispersive flow into compact almost Hermitian manifolds

MI2008-3 Hiroaki KIDO
On isosceles sets in the 4-dimensional Euclidean space

MI2008-4 Hirofumi NOTSU
Numerical computations of cavity flow problems by a pressure stabilized characteristic-curve finite element scheme

MI2008-5 Yoshiyasu OZEKI
Torsion points of abelian varieties with values in nfinite extensions over a p-adic field

MI2008-6 Yoshiyuki TOMIYAMA
Lifting Galois representations over arbitrary number fields

MI2008-7 Takehiro HIROTSU & Setsuo TANIGUCHI
The random walk model revisited

MI2008-8 Silvia GANDY, Masaaki KANNO, Hirokazu ANAI & Kazuhiro YOKOYAMA
Optimizing a particular real root of a polynomial by a special cylindrical algebraic decomposition

MI2008-9 Kazufumi KIMOTO, Sho MATSUMOTO & Masato WAKAYAMA
Alpha-determinant cyclic modules and Jacobi polynomials

MI2008-10 Sangyeol LEE & Hiroki MASUDA
Jarque-Bera Normality Test for the Driving Lévy Process of a Discretely Observed Univariate SDE

MI2008-11 Hiroyuki CHIHARA & Eiji ONODERA
A third order dispersive flow for closed curves into almost Hermitian manifolds

MI2008-12 Takehiko KINOSHITA, Kouji HASHIMOTO and Mitsuhiro T. NAKAO
On the L^2 a priori error estimates to the finite element solution of elliptic problems with singular adjoint operator

MI2008-13 Jacques FARAUT and Masato WAKAYAMA
Hermitian symmetric spaces of tube type and multivariate Meixner-Pollaczek polynomials

MI2008-14 Takashi NAKAMURA
Riemann zeta-values, Euler polynomials and the best constant of Sobolev inequality

MI2008-15 Takashi NAKAMURA
Some topics related to Hurwitz-Lerch zeta functions

MI2009-1 Yasuhide FUKUMOTO
Global time evolution of viscous vortex rings

MI2009-2 Hidetoshi MATSUI & Sadanori KONISHI
Regularized functional regression modeling for functional response and predictors

MI2009-3 Hidetoshi MATSUI & Sadanori KONISHI
Variable selection for functional regression model via the L_1 regularization

MI2009-4 Shuichi KAWANO & Sadanori KONISHI
Nonlinear logistic discrimination via regularized Gaussian basis expansions

MI2009-5 Toshiro HIRANOUCHI & Yuichiro TAGUCHII
Flat modules and Groebner bases over truncated discrete valuation rings

MI2009-6 Kenji KAJIWARA & Yasuhiro OHTA
Bilinearization and Casorati determinant solutions to non-autonomous 1+1 dimensional discrete soliton equations

MI2009-7 Yoshiyuki KAGEI
Asymptotic behavior of solutions of the compressible Navier-Stokes equation around the plane Couette flow

MI2009-8 Shohei TATEISHI, Hidetoshi MATSUI & Sadanori KONISHI
Nonlinear regression modeling via the lasso-type regularization

MI2009-9 Takeshi TAKAISHI & Masato KIMURA
Phase field model for mode III crack growth in two dimensional elasticity

MI2009-10 Shingo SAITO
Generalisation of Mack's formula for claims reserving with arbitrary exponents for the variance assumption

MI2009-11 Kenji KAJIWARA, Masanobu KANEKO, Atsushi NOBE & Teruhisa TSUDA
Ultradiscretization of a solvable two-dimensional chaotic map associated with the Hesse cubic curve

MI2009-12 Tetsu MASUDA
Hypergeometric τ-functions of the q-Painlevé system of type $E_8^{(1)}$

MI2009-13 Hidenao IWANE, Hitoshi YANAMI, Hirokazu ANAI & Kazuhiro YOKOYAMA
A Practical Implementation of a Symbolic-Numeric Cylindrical Algebraic Decomposition for Quantifier Elimination

MI2009-14 Yasunori MAEKAWA
On Gaussian decay estimates of solutions to some linear elliptic equations and its applications

MI2009-15 Yuya ISHIHARA & Yoshiyuki KAGEI
Large time behavior of the semigroup on L^p spaces associated with the linearized compressible Navier-Stokes equation in a cylindrical domain

MI2009-16 Chikashi ARITA, Atsuo KUNIBA, Kazumitsu SAKAI & Tsuyoshi SAWABE
Spectrum in multi-species asymmetric simple exclusion process on a ring

MI2009-17 Masato WAKAYAMA & Keitaro YAMAMOTO
Non-linear algebraic differential equations satisfied by certain family of elliptic functions

MI2009-18 Me Me NAING & Yasuhide FUKUMOTO
Local Instability of an Elliptical Flow Subjected to a Coriolis Force

MI2009-19 Mitsunori KAYANO & Sadanori KONISHI
Sparse functional principal component analysis via regularized basis expansions and its application

MI2009-20 Shuichi KAWANO & Sadanori KONISHI
Semi-supervised logistic discrimination via regularized Gaussian basis expansions

MI2009-21 Hiroshi YOSHIDA, Yoshihiro MIWA & Masanobu KANEKO
Elliptic curves and Fibonacci numbers arising from Lindenmayer system with symbolic computations

MI2009-22 Eiji ONODERA
A remark on the global existence of a third order dispersive flow into locally Hermitian symmetric spaces

MI2009-23 Stjepan LUGOMER & Yasuhide FUKUMOTO
Generation of ribbons, helicoids and complex scherk surface in laser-matter Interactions

MI2009-24 Yu KAWAKAMI
Recent progress in value distribution of the hyperbolic Gauss map

MI2009-25 Takehiko KINOSHITA & Mitsuhiro T. NAKAO
On very accurate enclosure of the optimal constant in the a priori error estimates for H_0^2-projection

MI2009-26 Manabu YOSHIDA
Ramification of local fields and Fontaine's property (Pm)

MI2009-27 Yu KAWAKAMI
Value distribution of the hyperbolic Gauss maps for flat fronts in hyperbolic three-space

MI2009-28 Masahisa TABATA
Numerical simulation of fluid movement in an hourglass by an energy-stable finite element scheme

MI2009-29 Yoshiyuki KAGEI & Yasunori MAEKAWA
Asymptotic behaviors of solutions to evolution equations in the presence of translation and scaling invariance

MI2009-30 Yoshiyuki KAGEI & Yasunori MAEKAWA
On asymptotic behaviors of solutions to parabolic systems modelling chemotaxis

MI2009-31 Masato WAKAYAMA & Yoshinori YAMASAKI
Hecke's zeros and higher depth determinants

MI2009-32 Olivier PIRONNEAU & Masahisa TABATA
Stability and convergence of a Galerkin-characteristics finite element scheme of lumped mass type

MI2009-33 Chikashi ARITA
Queueing process with excluded-volume effect

MI2009-34 Kenji KAJIWARA, Nobutaka NAKAZONO & Teruhisa TSUDA
Projective reduction of the discrete Painlevé system of type$(A_2 + A_1)^{(1)}$

MI2009-35 Yosuke MIZUYAMA, Takamasa SHINDE, Masahisa TABATA & Daisuke TAGAMI
Finite element computation for scattering problems of micro-hologram using DtN map

MI2009-36 Reiichiro KAWAI & Hiroki MASUDA
Exact simulation of finite variation tempered stable Ornstein-Uhlenbeck processes

MI2009-37 Hiroki MASUDA
On statistical aspects in calibrating a geometric skewed stable asset price model

MI2010-1 Hiroki MASUDA
Approximate self-weighted LAD estimation of discretely observed ergodic Ornstein-Uhlenbeck processes

MI2010-2 Reiichiro KAWAI & Hiroki MASUDA
Infinite variation tempered stable Ornstein-Uhlenbeck processes with discrete observations

MI2010-3 Kei HIROSE, Shuichi KAWANO, Daisuke MIIKE & Sadanori KONISHI
Hyper-parameter selection in Bayesian structural equation models

MI2010-4 Nobuyuki IKEDA & Setsuo TANIGUCHI
The Itô-Nisio theorem, quadratic Wiener functionals, and 1-solitons

MI2010-5 Shohei TATEISHI & Sadanori KONISHI
Nonlinear regression modeling and detecting change point via the relevance vector machine

MI2010-6 Shuichi KAWANO, Toshihiro MISUMI & Sadanori KONISHI
Semi-supervised logistic discrimination via graph-based regularization

MI2010-7 Teruhisa TSUDA
UC hierarchy and monodromy preserving deformation

MI2010-8 Takahiro ITO
Abstract collision systems on groups

MI2010-9 Hiroshi YOSHIDA, Kinji KIMURA, Naoki YOSHIDA, Junko TANAKA & Yoshihiro MIWA
An algebraic approach to underdetermined experiments

MI2010-10 Kei HIROSE & Sadanori KONISHI
Variable selection via the grouped weighted lasso for factor analysis models

MI2010-11 Katsusuke NABESHIMA & Hiroshi YOSHIDA
Derivation of specific conditions with Comprehensive Groebner Systems

MI2010-12 Yoshiyuki KAGEI, Yu NAGAFUCHI & Takeshi SUDOU
Decay estimates on solutions of the linearized compressible Navier-Stokes equation around a Poiseuille type flow

MI2010-13 Reiichiro KAWAI & Hiroki MASUDA
On simulation of tempered stable random variates

MI2010-14 Yoshiyasu OZEKI
Non-existence of certain Galois representations with a uniform tame inertia weight

MI2010-15 Me Me NAING & Yasuhide FUKUMOTO
Local Instability of a Rotating Flow Driven by Precession of Arbitrary Frequency

MI2010-16 Yu KAWAKAMI & Daisuke NAKAJO
The value distribution of the Gauss map of improper affine spheres

MI2010-17 Kazunori YASUTAKE
On the classification of rank 2 almost Fano bundles on projective space

MI2010-18 Toshimitsu TAKAESU
Scaling limits for the system of semi-relativistic particles coupled to a scalar bose field

MI2010-19 Reiichiro KAWAI & Hiroki MASUDA
Local asymptotic normality for normal inverse Gaussian Lévy processes with high-frequency sampling

MI2010-20 Yasuhide FUKUMOTO, Makoto HIROTA & Youichi MIE
Lagrangian approach to weakly nonlinear stability of an elliptical flow

MI2010-21 Hiroki MASUDA
Approximate quadratic estimating function for discretely observed Lévy driven SDEs with application to a noise normality test

MI2010-22 Toshimitsu TAKAESU
A Generalized Scaling Limit and its Application to the Semi-Relativistic Particles System Coupled to a Bose Field with Removing Ultraviolet Cutoffs

MI2010-23 Takahiro ITO, Mitsuhiko FUJIO, Shuichi INOKUCHI & Yoshihiro MIZOGUCHI
Composition, union and division of cellular automata on groups

MI2010-24 Toshimitsu TAKAESU
A Hardy's Uncertainty Principle Lemma in Weak Commutation Relations of Heisenberg-Lie Algebra

MI2010-25 Toshimitsu TAKAESU
On the Essential Self-Adjointness of Anti-Commutative Operators

MI2010-26 Reiichiro KAWAI & Hiroki MASUDA
On the local asymptotic behavior of the likelihood function for Meixner Lévy processes under high-frequency sampling

MI2010-27 Chikashi ARITA & Daichi YANAGISAWA
Exclusive Queueing Process with Discrete Time

MI2010-28 Jun-ichi INOGUCHI, Kenji KAJIWARA, Nozomu MATSUURA & Yasuhiro OHTA
Motion and Bäcklund transformations of discrete plane curves

MI2010-29 Takanori YASUDA, Masaya YASUDA, Takeshi SHIMOYAMA & Jun KOGURE
On the Number of the Pairing-friendly Curves