Int. J. Communications, Network and System Sciences, **2012, 5, 1-6**
http://dx.doi.org/10.4236/ijcns.2012.51001 Published Online January 2012 (http://www.SciRP.org/journal/ijcns)

Computation of Complex Primes Using Elliptic Curves: Application for Cryptosystem Design

Boris S. Verkhovsky
Computer Science Department, New Jersey Institute of Technology, Newark, USA
Email: verb73@gmail.com

Submitted December 01, 2011; accepted January 16, 2012

ABSTRACT

This paper provides several generalizations of Gauss theorem that counts points on special elliptic curves. It is demonstrated how to implement these generalizations for computation of complex primes, which are applicable in several protocols providing security in communication networks. Numerical examples illustrate the ideas discussed in this paper.

Keywords: Communication Security; Gauss Formula; Complex Primes; Points Counting; Modular Elliptic Curve; Applets; Dual Elliptic Curves

1. Introduction and Gauss Formula for Counting Points

Knowledge of how to count the number of points on elliptic curve (EC) provides certain advantage in the design of cryptographic systems for secure communication in various applicational environments (transfer of funds in banking, transmission of sensitive information between inventor and his/her attorney, national security agencies, military applications, diplomatic communications, governmental operations, control of weapons of mass distraction, telemedicine etc.). In general, algorithms for counting points on an EC are in the domain of algebraic [1,2] and algorithmic number theories [3,4]. Only in special cases it is possible to provide a closed-form solution [5]. Although validation of these algorithms requires application of algebraic number theory, which is beyond the scope of this paper, their description is rather easy to understand for cryptographers and application-oriented computer scientists.

In this paper we provide several generalizations of Gauss theorem and then demonstrate how to apply them in selection of complex prime parameters for the design of the cryptographic systems. These generalizations are based on intensive computer experiments (CE). As a result, not all proofs that validate the algorithms are provided. Instead, we formulate various conjectures and propositions that are supported by results of these CE.

1.1. Gauss theorem: Consider the elliptic curve (EC)

$$y^2 = \left(x^3 - x\right)\left(\bmod p\right), \qquad (1.1)$$

where p is a real prime; let E denote the number of ordered integer pairs (x, y) that satisfy Equation (1.1); every such integer pair (x, y) is called a point on the EC. There are two major cases:

1). If $p$mod4=3, then EC (1.1) has p points {excluding the point at infinity O [1]};

2). If $p$mod4=1; $p = C^2 + F^2$, where C is *odd*; (1.2) and

$$(C+F)\text{mod}4=1; \qquad (1.3)$$

then

$$E = p - 2C\,; \qquad (1.4)$$

{excluding the point at infinity O} [4].

If Condition (1.3) holds, then the Gauss Formula (1.4) can be applied to compute a complex prime (C, F). This application is based on the observation that an ordered pair of integers (C, F):=C+iF is a complex prime if and only if its norm $C^2 + F^2$ is a prime [5].

However, not all complex primes have components C and F that satisfy (1.3). For instance, (C, F)=(5,2) is the complex prime; yet (5+2)mod4=3.

Therefore, the algorithm provided below is non-deterministic, since its application is restricted by C. F. Gauss Theorem [5].

1.2. Non-deterministic algorithm for computation of complex primes:

Step1: Select a prime $p$mod4=1;

Step2: Count the number of points E on EC

$$y^2 = \left(x^3 - x\right)\left(\bmod p\right) \quad (1.1);$$

Step3: Compute

$$R := \left|p - E\right|/2\,; \quad S := \sqrt{p - C^2}\,; \qquad (1.5)$$

Step4: If $\left(R+S\right)\bmod 4\neq 1$, then repeat Steps 1-4;
Step5: If R is *odd*, then $(C, F):=(R, S)$
else $(C, F):=(S, R)$. (1.6)

*Remark*1.1: Although this algorithm is *not* deterministic, yet, after s trials it finds a complex prime (C, F) with probability $1-1/2^s$.

Integers 61, 977, 1777, 1913, 1933, 4133 are examples of primes, for which Condition (1.3) does not hold.

The following conjectures and propositions generalize Gauss theorem and, as a byproduct, allow to design a *deterministic* algorithm that computes complex primes for every real non-Blum prime p {$p$mod4=1}. These propositions and conjectures also provide insights that help to understand how various criteria were derived and applied for integer factorization algorithms that were described in papers [6,7] recently-published by the author of this paper.

2. Generalizations of Gauss Theorem

As it is shown below, in certain cases the number of points $E\left(a\right)$ on EC

$$y^2=x^3+ax\bmod p \qquad (2.1)$$

can be represented as

$$E\left(a\right)=p+2C\times G\left(a,\ C,\ F\right); \qquad (2.2)$$

where $G(a, C, F)$ is equal either 1 or -1.

*Remark*2.1: In all following discussions, the point at infinity O is excluded from the counting.

Conjecture2.1: Consider the elliptic curve (1.1), where p is a prime; if Condition (1.2) holds, then

$$E\left(-1\right)=p+2\left[\left(C+F\right)\bmod 4-2\right]C. \qquad (2.3)$$

Conjecture2.2: Consider elliptic curve (EC)

$$y^2=\left(x^3+x\right)\left(\bmod p\right); \qquad (2.4)$$

where p is a prime and let condition (1.2) holds; then for every F

$$E\left(1\right)=p+2\left(C\bmod 4-2\right)C. \qquad (2.5)$$

Conjecture2.3: Consider EC

$$y^2=\left(x^3+ax\right)\bmod p, \qquad (2.6)$$

where $a=\pm 1$; and let (1.2) holds; then

$$E\left(a\right)=p+2\left[\left(C+F\left(1-a\right)/2\right)\bmod 4-2\right]C \qquad (2.7)$$

***Corollary*:** Equation (2.7) implies that if Fmod4=0, then elliptic curves (1.1) and (2.4) have equal number of points {see **Table 2.1**}.

Equation (2.7) can be also presented as

$$E(a)=p\pm 2C \quad \text{if}$$
$$\begin{cases}\left(C+F\right)\bmod 4=2\pm 1 \text{ and } a=-1; \\ \quad \text{or } C\bmod 4=2\pm 1 \text{ and } a=1.\end{cases} \qquad (2.8)$$

Table 2.1. Generalized Gauss formula if EC is $y^2=\left(x^3\pm x\right)$mod p.

a	***p***	**1777**	1913	6101	514229	919393
	C*;*F	39;16	43;8	25;74	377;610	823;492
–1	**#*E*(–1)**	**1855**	1999	6151	514983	921039
1	**#*E*(1)**	1855	1999	6051	513475	921039

The table above provides examples of randomly-selected non-Blum primes that confirm formulas (2.3), (2.5) and (2.7).

*Remark*2.2: Elliptic curve (1.1) considered by C.F. Gauss has a remarkable property: if p=1777, then E(–1)=1855 {C.F. Gauss was born in 1777 and died in 1855}, (see **Table 2.1**). The same property holds for $y^2=\left(x^3+x\right)\left(\bmod 1777\right)$: E(1)=1855.

3. Points on Elliptic Curves

In some applications and applets it is necessary to find at least one solution of modular Diophantine equations

$$y^2=x\left(x^2-a\right)\bmod p \text{ (1.1);}$$

or

$$y^2=x\left(x^2+a\right)\bmod p \text{ (2.4).}$$

Several special cases are listed below, where such solutions can be provided in closed forms.

Case1: If

$$a:=-2^{4k+1}; \qquad (3.1)$$

then for every $k\geq 0$

$$\left(x,y\right)=\left(2^{2k+1},2^{3k+1}\right); \qquad (3.2)$$

is on EC $y^2=x\left(x^2-a\right)\bmod p$.

Case2: If

$$a=2^{2w}; \qquad (3.3)$$

then for every *odd* w

$$\left(x,y\right)=\left(2^w,2^{(3w+1)/2}\right); \qquad (3.4)$$

is the point on EC

$$y^2=x\left(x^2+a\right)\bmod p \qquad (3.5)$$

Case3: Let $x^2-a=xb^2$;

consider $a:=x\left(x-b^2\right)$; (3.6)

then $y^2=x\left(x^2-a\right)=x^2b^2$.
Therefore, $y=bx$, *i.e.*, (x, bx) is on EC

$$y^2=x\left(x^2-a\right)\bmod p. \qquad (3.7)$$

Hence, if a=5, or a=6, or a=–3, then respectively (5,10), (3,3), (3,6) are the points on (3.7).

4. Counting Points on Elliptic Curves with $a = \pm 2^d$

In order to design an efficient algorithm that computes complex primes, it is necessary to know how to count points on EC (2.1), where |*a*| is not equal 1; {see Section 8 for an explanation}.

Consider an EC

$$y^2 = \left(x^3 \pm 2^d x\right) \bmod p, \qquad (4.1)$$

where exponent *d* is a non-negative integer; *p* is a prime, *p*mod4 = 1; $p = C^2 + F^2$; let $E(d)$ denote the number of points on the EC (4.1).

Elliptic curves with coefficients $a = \pm 2^d$ have remarkable cyclic properties.

Proposition4.1: If

$$F\text{mod}8=0; \qquad (4.2)$$

then $E(d)$ is independent of exponent *d*, *i.e.*, is the same for all *d*; and

$$E(d) = p + 2C(C \bmod 4 - 2). \qquad (4.3)$$

Proposition4.2: If

$$F\text{mod}8=4; \qquad (4.4)$$

then

$$E(0) = E(2) = \cdots = E(2k);$$

$$E(1) = E(3) = \cdots = E(2k-1); \qquad (4.5)$$

and

$$E(d) = p + (-1)^d\, 2(C \bmod 4 - 2)C. \qquad (4.6)$$

Proposition4.3: If *F*mod4=2, then the number of points on the EC is equal

$$p \pm 2C \text{ if } d \text{ is } \textit{even} \text{ and } p \pm 2F \text{ if } d \text{ is } \textit{odd}. \qquad (4.7)$$

Proposition4.4: For every non-negative integer *d* the following equation holds

$$E(d) = E(d \bmod 4). \qquad (4.8)$$

Proposition4.5: If *F*mod4=2, and if *d*=2*m*<4, then for *m*=0 and *m*=1 the following equations hold:

$$E(2m) = p + 2(-1)^m (C \bmod 4 - 2)C; \qquad (4.9)$$

if *d*=2*m*+1<4, then

$$E(2m+1) = p + (-1)^m (F \bmod 8 - 4)F. \qquad (4.10)$$

Table 4.1 illustrates all cases considered in Propositions 4.1-4.5.

5. Counting Points on Dual EC

Proposition5.1: Let $G(d)$ be the number of points on the dual EC

$$y^2 = \left(x^3 - 2^d x\right) \bmod p; \qquad (5.1)$$

then for every non-negative integer *d*

$$G(d) = E(d+2). \qquad (5.2)$$

Proof is provided in [7].

Tables 4.1 and **5.1** illustrate Proposition 5.1.

6. Counting Points: Detailed Description

In this section we provide a detailed description on how to count the points on the EC (5.1).

Conjecture6.1: If prime *p*mod4=1; $p = C^2 + F^2$, where *C* is *odd*; and *F*mod4=2, then the number of points $G(d)$ on EC

$$y^2 = \left(x^3 - 2^d x\right) \bmod p \quad \text{is equal}$$

$$G(d) = p + 2C(2 - C \bmod 4)(-1)^{(d \bmod 4)/2}; \qquad (6.1)$$

if ***d* is even**;

however, if ***d* is odd**, then there are two cases:

$$G(d) = p + 2F \text{ or } p - 2F. \qquad (6.2)$$

a). if *d*=4*k*+1; then

$$G(d)=p+F(4–F\text{mod}8); \qquad (6.3)$$

b). if *d*=4*k*+3, then

$$G(d)=p–F(4–F\text{mod}8). \qquad (6.4)$$

The following formula summarizes all cases of Conjecture 6.1 for odd *d*:

$$G(d) = p + F\left(4 - F\text{mod}8\right)(-1)^{(d \bmod 4 - 1)/2} \qquad (6.5)$$

Conjecture6.2: If

$$F\text{mod}8=4, \qquad (6.6)$$

then for every integer *k*

$$G(2k) = \begin{cases} p - 2C \text{ if } C \bmod 4 = 1 \\ p + 2C \text{ if } C \bmod 4 = 3 \end{cases}; \qquad (6.7)$$

and

$$G(2k+1) = \begin{cases} p + 2C \text{ if } C \bmod 4 = 1 \\ p - 2C \text{ if } C \bmod 4 = 3 \end{cases}. \qquad (6.8)$$

Conjecture6.3: If

$$F\text{mod}8=0, \qquad (6.9)$$

then for every *d*

$$G(d) = p - 2C(2 - C \bmod 4). \qquad (6.10)$$

Proposition6.4: For every integer *b*, *d* and non-Blum prime *p* elliptic curves

$$y^2 = \left(x^3 \pm b^d x\right) \bmod p;$$

and

Table 4.1. Number of points on EC y^2=(x^3+$2^d x$)mod*p*.

p	*C*	*F*	*d*=0	*d*=1	*d*=2	*d*=3
53	**7**	**2**	67; *p*+2*C*	49; *p*–2*F*	39; *p*–2*C*	57; *p*+2*F*
73	**3**	**8**	79; *p*+2*C*	79	79	79
97	**9**	**4**	79; *p*–2*C*	115; *p*+2*C*	79	115
257	**1**	**16**	255; *p*–2*C*	255	255	255
317	**11**	**14**	339; *p*+2*C*	345; *p*+2*F*	295; *p*–2*C*	289; *p*–2*F*
977	**31**	**4**	1039; *p*+2*C*	915; *p*–2*C*	1039	915
1933	**13**	**42**	1907; *p*–2*C*	1849; *p*–2*F*	1959; *p*+2*C*	2017; *p*+2*F*
4133	**17**	**62**	4099; *p*–2*C*	4257; *p*+2*F*	4167; *p*+2*C*	4009; *p*–2*F*

Table 5.1. Number of points on EC y^2=(x^3–$2^d x$)mod*p*.

p	*C*	*F*	*d*=0	*d*=1	*d*=2	*d*=3
109	3	10	103; *p*–2*C*	129; *p*+2*F*	115; *p*+2*C*	89; *p*–2*F*
977	31	4	1039; *p*+2*C*	915; *p*–2*C*	1039	915
1933	13	42	1959; *p*+2*C*	2017; *p*+2*F*	1907; *p*–2*C*	1849; *p*–2*F*
4133	17	62	4167; *p*+2*C*	4009; *p*–2*F*	4099; *p*–2*C*	4257; *p*+2*F*

$$y^2 = \left(x^3 \pm b^{d \bmod 4} x\right) \bmod p \qquad (6.11)$$

have the same number of points. Proof is provided in [7].

7. Computation of Complex Primes: Deterministic Algorithm

Since the complex integer (*C*, *F*) is a prime if and only if its norm

$$N := C^2 + F^2 \qquad (7.1)$$

is a prime, in a naïve approach we can first select a non-Blum prime *p*, and then find its representation as a sum of two integer squares (7.1). The complexity of such an algorithm is of order $\mathrm{O}\left(\sqrt{p}\right)$. Instead we can apply the generalization of Gauss Theorem described above; {for further details see **Table A1** in the Appendix}.

Step1: Select a prime *p*mod4=1;

Step2: Count the number of points *E*(*a*) on EC

$$y^2 = x^3 + ax \left(\bmod p\right), \text{ where } a = \pm 1; \qquad (7.2)$$

Step3: Compute $C := \left|p - E\left(a\right)\right| / 2$; and

$$F := \sqrt{p - C^2}; \text{then } p = C^2 + F^2 \Rightarrow \left(C, F\right). \qquad (7.3)$$

*Example*7.1: Let *p*=433494437; $a = -1$; then *E*(–1)=433459015; and (*C*, *F*)=(17711,10946).

8. Complexity Analysis

Schoof-Elkies-Atkin (SEA) algorithm counts points on elliptic curves $y^2 = x^3 + ax \bmod p$ with expected running time $T = \mathrm{O}\left(\log^4 p\right)$ if $|a| \neq 1$ [1]; {the SEA is not applicable if $|a|$ =1}. Therefore, if $p = \mathrm{O}\left(2^{1000}\right)$, then $T = \mathrm{O}\left[\left(\log 2^{1000}\right)^4\right] = \mathrm{O}\left(10^{12}\right)$.

9. Conclusions and Unsolved Problem

In this paper we considered families of modular equations (called the EC) and corresponding algorithms that counts the number of integer points on each of these ECs. For all these cases we provided closed-form solutions with one exception {see Section A3 in Appendix, where we provided that case as a Challenge to the readers of this paper}.

Finally, we provided a deterministic algorithm with polynomial time complexity that computes a complex prime (*C*, *F*) for every real prime *p*. In [9] is demonstrated how to implement the complex primes in cryptographic systems based on double moduli reduction, where one modulus is a real prime and another modulus is a complex prime.

10. Acknowledgements

I express my gratitude to K. Engemann, D. Kanevsky and R. Rubino for their comments and to my former students for their assistance in creation of applets that count the number of points on elliptic curves based on my algorithms. Results of computer experiments provided in this paper were performed using these applets.

REFERENCES

[1] R. Lercier, D. Lubicz and F. Vercauteren, "Point Counting on Elliptic and Hyperelliptic Curves," In: H. Cohen and G. Frey, Eds., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman and Hall/CRC, Boca Ra-

ton, 2006, pp. 407-453.

[2] K. Rubin and A. Silverberg, “Ranks of Elliptic Curves,” *Bulletin American Mathematical Society* (*New Series*), Vol. 39, No. 4, 2002, pp. 455-474. doi:10.1090/S0273-0979-02-00952-7

[3] A. Lauder and D. Wan, “Counting Points on Variety over Finite Fields of Small Characteristics,” In: J. P. Buhler and P. Stevenhagen, Eds., *Algorithmic Number Theory*, Cambridge University Press, New York, 2008, pp. 579-612.

[4] R. Schoof, “Counting Points on Elliptic Curves over Finite Fields”, *Journal de Theorie des Nombres de Bordeaux*, Vol. 7, No. 1, 1995, pp. 219-254. doi:10.5802/jtnb.142

[5] C. F. Gauss, “Disquisitiones Arithmeticae,” Verlag, Gottingen, 1863, p. 483.

[6] B. Verkhovsky, “Integer Factorization of Semi-Primes Based on Analysis of a Sequence of Modular Elliptic Equations,” *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 10, 2011, pp. 609-615. doi:10.4236/ijcns.2011.410073

[7] B. Verkhovsky, “Algorithms for Integer Factorization Based on Counting Solutions of Various Modular Equations,” *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 11, 2011, pp. 675-682. doi:10.4236/ijcns.2011.411083

[8] L. Dewaghe, “Remarks on the Schoof-Elkies-Atkin Algorithm,” *Mathematics of Computation*, Vol. 67, No. 223, 1998, pp. 1247-1252. doi:10.1090/S0025-5718-98-00962-4

[9] B. Verkhovsky, “Double-moduli Gaussian Encryption/Decryption with Primary Residues and Secret Controls,” *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 8, 2011, pp. 475-481. doi:10.4236/ijcns.2011.47058

APPENDIX

A1. Computer experiments

Table A1. Generation of Gaussian primes via EC $y^2=x^3+ax(\text{mod}p)$.

EC	*p*	*E*(*a*)	*C*	*F*	(*C*+*F*)mod4	*F*mod4
$a=\pm1$	1000249	1001359	555	832	3 {GGT}	0
$a=1$	1000253	1000947	347	938	1 {GGT}	2
$a=\pm1$	3276509	3278599	1045	1478	3 {GGT}	2
$a=\pm1$	10006001	9999999	3001	1000	1 {GGT}	0
$a=-1$	433,494,437	433,459,015	17,711	10,946	1 {GT}	2

Legend: *GT*=via Gauss Theorem; *GGT*=via Generalized Gauss Theorem.

Table A2. Generation of Gaussian primes using EC $y^2=x^3-2x(\text{mod}p)$.

p	$E(-2)$	*C*	*F*
780,291,637	***p*+2*F***; 780,320,985	23,769	14,674
77,777,677,777	*p*+2*C*; 77,778,071,955	197,089	197,316
59,604,644,783,353,249	*p*+2*C*; 59,604,645,200,773,363	208,710,057	126,667,900
99,194,853,094,755,497	*p*–2*C*; 99,194,852,763,595,215	165,580,141	267,914,296

A2. Generalizations

Consider

$$y^2=x\left(x^2-b^d\right)\left(\text{mod } p\right),\, b>2\,; \qquad \text{(A1)}$$

***Case*A1:** If 2 is a generator or there exists an integer *z* such that

$$2^z=b\left(\text{mod } p\right); \qquad \text{(A2)}$$

then consider

$$y^2=x\left(x^2-2^{dz \bmod 4}\right)\left(\text{mod } p\right)$$

and find *E*(*dz*mod4), {see (5.1) and (5.2)}.

***Example*A1:** Let *p*=73, *b*=37, *d*=2; then $2^{35}=37\left(\text{mod } 73\right)$, *i.e.* *z*=35.

Therefore,

E(*dz*mod4)=*E*(70mod4)=*E*(2); (6.5).

Since $73=3^2+8^2$, then *E*(2)=79.

***Case*A2:** If *b* is a generator or there exists an integer *w* such that

$$b^w=2(\text{mod } p), \qquad \text{(A3)}$$

then

$$b^d=2^{d(p-w-1)}(\text{mod } p).$$

Now consider

$$y^2=x(x^2-2^{d(p-w-1)\bmod 4})(\text{mod } p)\,; \qquad \text{(A4)}$$

and find *E*(*d*(*p*–*w*–1)mod4).

***Case*A3:** Conjectures A1-A3 address the cases where an

Table A3.1. # of points $E(3,0)$ on $y^2=(x^3-3^d x)\bmod p$; if $d=1$, then $E(3,1)=p+2F$.

p	53	89	101	113	137	257	353	449	653
(C, F)	(7,2)	(5,8)	(1,10)	(7,8)	(11,4)	(1,16)	(17,8)	(7,20)	(13,22)
d=0	p–2C	p–2C	p+2C	p+2C	p+2C	p–2C	p–2C	p+2C	p+2C

Table A3.2. # of points $E(3,0)$ on $y^2=(x^3-3^d x)\bmod p$; if $d=1$, then $E(3,1)=p-2F$.

p	5	149	173	197	233	281	317	401	677
(C, F)	(1,2)	(7,10)	(13,2)	(1,14)	(13,8)	(5,16)	(11,14)	(1,20)	(1,26)
d=0	p+2C	p–2C	p+2C	p+2C	p–2C	p–2C	p–2C	p–2C	p+2C

integer solution z of Equation (A2) does not exist.

ConjectureA1: If gcd(CF, b)=1, then there are four distinct counts for d=0,1,2,3:

$$E(3,0)=p+(C\bmod 4-2)(1-F\bmod 4); \qquad \text{(A5)}$$

$$E(3,2)=2p-E(3,0); \qquad \text{(A6)}$$

and

$$E(3,3)=2p-E(3,1); \qquad \text{(A7)}$$

{see **Tables A3.1** and **A3.2**}.

ConjectureA2: If gcd(CF,b)>1, then there are two distinct counts: $p+2C$ and $p-2C$; {see **Table A4**}; namely:

a). $E(b,1)=E(b,3)=2p-E(b,0)$; (A8)

b). if gcd(CF, b) = 1,
then

$$E(b,0)=E(b,2)=p+2C(C\bmod 4-2); \qquad \text{(A9)}$$

c). if Fmod$b$=0 **or** {$b|C$ **and** Fmod4=0},
then

$$E(b,0)=E(b,2)=p-2C(C\bmod 4-2). \qquad \text{(A10)}$$

ConjectureA3: If $b|C$ and Fmod4=2, then for every d

$$E(3,d)=p-2C(C\bmod 4-2); \qquad \text{(A11)}$$

if Fmod4b=0, then for every d

$$E(3,d)=p+2C(C\bmod 4-2). \qquad \text{(A12)}$$

Table A5 illustrates all cases of ConjectureA3.

A3. Unsolved Problem

We leave to the readers to figure out a formula for E(3,1) provided that (A7) holds and E(3,1) is equal either $p+2F$ or $p-2F$, {see above **Tables A3.1** and **A3.2**}.

Table A4. $E(3,0)=E(3,2)$; $E(3,1)=E(3,3)$.

p	C	F	d=0,2	d=1,3
61	**5**	**6**	p+2C	p–2C
97	**9**	**4**	p–2C	p+2C
157	**11**	**6**	p–2C	p+2C
241	**15**	**4**	p+2C	p–2C
613	**17**	**18**	p+2C	p–2C
853	**23**	**18**	p–2C	p+2C
1933	**13**	**42**	p+2C	p–2C

Table A5. $E(3,0)=E(3,1)=E(3,2)=E(3,3)$.

p	C	F	d=0,1,2,3
109	**3**	**10**	p–2C
181	**9**	**10**	p+2C
193	**7**	**12**	p+2C
277	**9**	**14**	p+2C
313	**13**	**12**	p–2C
421	**15**	**14**	p–2C