ELLIPTIC CURVES WITH MANY POINTS OVER A SMALL FINITE FIELD

M. A. Soomro*, A.H. Sheikh** and S. H. Sandilo*

ABSTRACT

This note contains examples of elliptic curvs with maximal possible number of rational points over a finite field F_q. More precisely this is done for every $q = p^n$ with $p \leq 19$ a prime number and $1 < n \leq 5$ and also for all $q = p \leq 97$ a prime number. The examples were computed using the computer algebra package Maple and the free mathematics software system Sage.

Keywords: *Elliptic Curves, Finite fields*

1. INTRODUCTION

We denote by $N_q(1)$ the maximal number of rational points that an elliptic curve E over a finite field F_q of cardinality q can have. A result of Deuring and Waterhouse (see [4, Thm. 4.1]); for an exposition see also [1, p. 15-16]) states that

$$N_q(1) = \begin{cases} q+m \text{ if } q = p^e \,\&\, e \geq 5 \text{is odd} \,\&\, p \mid m; \\ q+m+1 \qquad\qquad otherwise. \end{cases}$$

Here p is the characteristic of F_q and m is the largest integer less than or equal to $2\sqrt{q}$.

In this research, we present, for many small q, an elliptic curve over F_q attaining this bound.

2. THE PRIME FIELDS

Over F_2 the equation $y^2 + y = x^3 + x$ defines an elliptic curve with $N_2(1) = 5$ rational points. For odd prime numbers p, we search over equations $y^2 = x^3 + ax + b$ satisfying $4a^3 + 27b^2 \neq 0$ in order to find an example with $N_p(1) = p + 1 + \lfloor 2\sqrt{p} \rfloor$ rational points. Using Maple, this is very simple for small p. The result is given in the Table (1).

3. FIELDS OF CARDINALITY p^2

To find examples of elliptic curves over F_{p^2} having $N_{p^2}(1) = p^2 + 1 + 2p$ rational points, we use the following lemma.

Lenmma 3.1 Suppose E / F_q is an elliptic curve. Then

$$\#E(F_{q^2}) = q^2 + 1 + 2q \Leftrightarrow \#E(F_q) = q + 1.$$

Proof

By Chap.V, Sec. 2 in [3] and Chap. IV, Sec. 3 in [5].

Let $\#E(F_q) = q + 1 - a$. Write $X^2 - aX + q = (X - \alpha)(X - \beta)$ with $\alpha, \beta \in \mathbb{C}$. Then

$$\#E(F)_{q^n} = q^n + 1 - \alpha^n - \beta^n$$

for all $n \geq 1$.

So in particular one has $\#E(F_{q^2}) = q^2 + 1 - \alpha^2 - \beta^2$. This implies

$$\begin{aligned} \#E(F_{q^2}) = q^2 + 1 + 2q \\ \Leftrightarrow \ \alpha^2 + \beta^2 = -2q, \\ \Leftrightarrow \alpha^2 + \beta^2 + 2\alpha\beta = 0, \\ \Leftrightarrow (\alpha + \beta)^2 = 0 \\ \Leftrightarrow \alpha + \beta = 0 \\ \Leftrightarrow \#E(F_q) = q + 1, \end{aligned}$$

which proves the lemma.

q	$N_q(1)$	Elliptic Curve
2	5	$y^2 + y = x^3 + x$
3	7	$y^2 = x^3 + 2x + 1$
5	10	$y^2 = x^3 + 3$
7	13	$y^2 = x^3 + 3$
11	18	$y^2 = x^3 + x + 3$
13	21	$y^2 = x^3 + 4$
17	26	$y^2 = x^3 + 3x$
19	28	$y^2 = x^3 + 8$
23	33	$y^2 = x^3 + x + 11$
29	40	$y^2 = x^3 + 4x$
31	43	$y^2 = x^3 + 3$
37	50	$y^2 = x^3 + 2x$
41	54	$y^2 = x^3 + 2x + 4$
43	57	$y^2 = x^3 + 9$
47	61	$y^2 = x^3 + x + 38$
53	68	$y^2 = x^3 + x$
59	75	$y^2 = x^3 + 2x + 22$
61	77	$y^2 = x^3 + 6x + 29$
67	84	$y^2 = x^3 + 1$
71	88	$y^2 = x^3 + x + 9$
73	91	$y^2 = x^3 + 5$
79	97	$y^2 = x^3 + 3$
83	102	$y^2 = x^3 + 2x + 19$
89	108	$y^2 = x^3 + x + 8$
97	117	$y^2 = x^3 + 2$

Table 1: List of Curves over prime fields

More generally, any elliptic curve over F_q, having precisely $q + 1$ rational points, will have $N_{q^{2s}}(1) = q^{2s} + 1 + 2q^s$ rational points over the field $F_{q^{2s}}$, with s any odd integer.

For $q = p$ prime the existence of such an elliptic curve (i.e. having precisely $p + 1$ rational points) over F_p follows, as before, from the results of Deuring and of Waterhouse (see [4, Thm. 4.1]).

To have explicit examples, first note that for $p = 2$, the equation $y^2 + y = x^3$ defines an elliptic curve with exactly $3 = p + 1$ rational points over F_2. Next, for every prime number $p \equiv 5 \bmod (6)$ the equation $y^2 = x^3 + 1$defines an elliptic curve with precisely $p + 1$ rational points over F_p. (This is well-known; compare, e.g., Exer. IV-4.10 in [3].)

Similarly (see Exer. IV-4.8 in [3]) for every prime number $p \equiv 3 \bmod (4)$ the equation $y^2 = x^3 + x$ defines an elliptic curve whose number of rational points over $F_p$equals $p + 1$. With these remarks, we have examples for every prime $p \leq 19$ except $p = 13$.

One has $\#E(F_{13}) = 14$ for the elliptic curve E: $y^2 = x^3 + x + 4$.

This discussion is summarized in the Table 2.

p	$N_{p^2}(1)$	Elliptic Curve
2	9	$y^2 + y = x^3$
3	16	$y^2 = x^3 + x$
5	36	$y^2 = x^3 + 1$
7	64	$y^2 = x^3 + x$
11	144	$y^2 = x^3 + x$
13	196	$y^2 = x^3 + x + 4$
17	324	$y^2 = x^3 + 1$
19	400	$y^2 = x^3 + x$

Table 2

4. FIELDS OF CARDINALITY p^3

Most of the curves given in the following Table 3 are found by a simple trick given in Section 7 and other by using the free mathematics software system Sage.

Write $F_{p^3} = F_p[z]$ in which z satisfies $g(z) = 0$ for a monic irreducible $g \in F_p[X]$ of degree 3.

Note that if E is defined over F_{p^3}, then the p-power Frobenius map defines an isomorphism $E(F_{p^3}) \simeq E^{(p)}(F_{p^3})$. Here $E^{(p)}$ denotes the elliptic curve obtained from E by raising the coefficients of its equation to the power p. In particular, in an equation involving z the number of points does not depend on

which zero of g in $F_p[z]$ is taken.

p	$N_{p^3}(1)$	Elliptic Curve	Minimal Polynomial of z
2	14	$y^2 + xy + y = x^3 + 1$	
3	38	$y^2 = x^3 + 2x^2 + 2x$	
5	148	$y^2 = x^3 + x + 2$	
7	381	$y^2 = x^3 + z^2$	$X^3 + 6X^2 + 4$
11	1404	$y^2 = x^3 + x + 4$	
13	2291	$y^2 = x^3 + z^2x + z^{75}$	$X^3 + 2X + 11$
17	5054	$y^2 = x^3 + x + 4$	
19	7025	$y^2 = x^3 + z^2x + z^9$	$X^3 + 4X + 17$

Table 3

5. FIELDS OF CARDINALITY p^4

If an elliptic curve E over a finite field F_q satisfies $\#E(F_q) = q + 1$, then as in Lemma 3.1, $\#E(F_{q^4}) = q^4 + 1 - 2q^2$. This implies that a quadratic twist E^{tw} of E over F_{q^4} satisfies $\#E^{tw}(F_{q^4}) = q^4 + 1 + 2q^2 = N_{q^4}(1)$, by the following two lemmas.

Lemma 5.1 Suppose q is odd, and let C/F_q be the hyperelliptic curve corresponding to an equation $y^2 = f(x)$ with $f \in F_q[X]$ square free. Suppose $\alpha \in F_q^*$ is not a square and define the hyper-elliptic curve C^{tw}/F_q corresponding to the equation $\alpha\, y^2 = f(x)$. Then

$$\#C(F_q) + \#C^{tw}(F_q) = 2q + 2.$$

Proof For $x_0 \in F_q$. If $f(x_0) = 0$, then this contributes one point to both curves. If $f(x_0) \in F_q^{*2}$, then this contributes 2 points to C and 0 points to C^{tw}. If $f(x_0) \in F_q^* \backslash F_q^{*2}$, then this contributes 0 points to C and 2 points to C^{tw}. Finally, consider points at infinity.If f has odd degree, then both C and C^{tw} have one rational point at infinity. If f has even degree and leading coefficient in F_q^{*2}, then C has 2 points at infinity while C^{tw} has no point at infinity. In the remaining case C^{tw} has 2 points and C has none. Therefore $\#C(F_q) + C^{tw}(F_q) = 2q + 2$.

Now if $E: y^2 = x^3 + Ax + B$ is an elliptic curve over odd finite field $F_q$and satisfies $\#E(F_q) = q + 1$, then $\#E(F_{q^4}) = q^4 + 1 - 2q^2$. Take an $\alpha \in F_{q^4}^*$, not a square, we make another curve

$$E^{tw}: \alpha\, y^2 = x^3 + Ax + B$$

equivalently $E^{tw}: y^2 = x^3 + \alpha^2 Ax + \alpha^3 B$ (see Exer. 2.23 and 4.10 in [5]). Then

$$\#E(F_{q^4}) + \#E^{tw}(F_{q^4}) = 2q^4 + 2,$$

Therefore,

$$\#E^{tw}(F_{q^4}) = q^4 + 1 + 2q^2,$$

hence E^{tw} is the required maximal elliptic curve over F_{q^4}.

Lemma 5.2 Suppose $q = 2^n$. Then a generalized Weierstrass equation for an elliptic curve over F_q is

$$E: y^2 + (a_1x + a_3)y = f(x) \tag{1}$$

with $f(x)$ monic of degree 3. The quadratic twist isomorphic to (1) over $F_{q^2} = F_q(\beta)$, where β satisfies an irreducible polynomial $X^2 + X + a = 0$ for some $a \in F_q$, is

$$E^{tw}: \eta^2 + (a_1x + a_3)\eta = f(x) + a(a_1x + a_3)^2. \tag{2}$$

It satisfies

$$\#E(F_q) + \#E^{tw}(F_q) = 2q + 2.$$

Proof Take $x_0 \in F_q$. Let $a_1x_0 + a_3 = \xi$ and $f(x_0) = \delta$. First suppose $\delta = 0$. If $\xi = 0$ we obtain one point on both E and E^{tw}. If $\xi \neq 0$ then the equations (1) and (2) at x_0 give

$$y^2 + \xi y = 0, \tag{3}$$

$$\eta^2 + \xi\eta = a\xi^2. \tag{4}$$

Clearly (3) has precisely 2 solutions, namely $y = 0$ and $y = \xi$. The equation (4) has no solution $\eta \in F_q$, since if $\eta \in F_q$ would be a solution then $\frac{\eta}{\xi} \in F_q$ would be a zero of $X^2 + X + a = 0$, which is assumed to be irreducible.

Now suppose $\delta \neq 0$. If $\xi = 0$ we obtain one point on both E and E^{tw}. If $\xi \neq 0$ then the Equations (1) and (2) at x_0 give

$$y^2 + \xi y = \delta, \tag{5}$$

$$\eta^2 + \xi\eta = \delta + a\xi^2. \tag{6}$$

If both Equations (5) and (6) would have a solution $y$and $\eta \in F_q$ respectively, then $\frac{y+\eta}{\xi} \in F_q$ would be a zero of $X^2 + X + a = 0$ which is not possible.

Now Suppose the Equation (5) has no solution in F_q. Then it has 2 solutions in $F_{q^2} = F_q(\beta)$. Let $y_0 = y_1 + y_2\beta$, where $y_1, y_2 \in F_q$ and $y_2 \neq 0$, be one of the solutions of the Equation (5) in F_{q^2}. Hence

$$(y_1 + y_2\beta)^2 + \xi(y_1 + y_2\beta) = \delta,$$

which can be written as

$$y_1^2 + y_2^2\beta + y_2^2 a + y_1\xi + y_2\beta\xi = \delta, \tag{7}$$

comparing coefficients of β shows

$$y_2^2 + \xi y_2 = 0$$

so $y_2 = \xi$. So the equation (7) gives

$$y_1^2 + \xi y_1 = a\xi^2,$$

hence y_1 is a solution of the Equation (4).

Finally, both the curves have one point at infinity. Therefore $\#E(F_q) + \#E^{tw}(F_q) = 2q + 2$.

For instance, for $q = p$ odd we have the curves over F_p, with precisely $p + 1$ rational points, in the table of Section 3. Take a curve $E: y\text{^}2 = x^3 + x$ having $\#E(F_3) = 4$ and $\alpha = z \in F_{3^4}\}$ satisfying $z^4 + 2z^3 + 2 = 0$. Then z is not square in F_{3^4}, since $X^8 + 2X^6 + 2 \in F_3[X]$ is irreducible. Hence $E^{tw}: zy^2 = x^3 + x$ equivalently $E^{tw}: y^2 = x^3 + z^2 x$ is the required elliptic curve over F_{3^4} with $\#E(F_{3^4}) = N_{3\text{^}4}(1) = 100$. For $q = 2$, the curve $E: y^2 + y = x^3$ has $\#E(F_2) = 3$. Write $F_{2^4} = F_2[z]$ in which z satisfies $z^4 + z + 1 = 0$. Then quadratic twist of this curve $L = F_{2^4}(\beta)$, where β satisfies irreducible polynomial $X^2 + X + z^3$, will be

$$E^{tw}: y^2 + y = x^3 + z^3.$$

and it has the maximum possible number of point over $K = F_{2^4}$. This discussion is summarized in the Table 4.

p	$N_{p^4}(1)$	Elliptic Curve	Minimal Polynomial of z
2	25	$y^2 + y = x^3 + z^3$	$X^4 + X + 1$
3	100	$y^2 = x^3 + z^2x$	$X^4 + 2X^3 + 2$
5	676	$y^2 = x^3 + z^3$	$X^4 + 4X^2 + 4X + 2$
7	2500	$y^2 = x^3 + z^2x$	$X^4 + 5X^2 + 4X + 3$
11	14884	$y^2 = x^3 + z^2x$	$X^4 + 8X^2 + 10X + 2$
13	28900	$y^2 = x^3 + z^2x + 4z^3$	$X^4 + 3X^2 + 12X + 2$
17	84100	$y^2 = x^3 + z^3$	$X^4 + 7X^2 + 10X + 3$
19	131044	$y\text{^}2 = x\text{^}3 + z\text{^}\{2\}x$	$X^4 + 2X^2 + 11X + 2$

Table 4

6. FIELDS OF CARDINALITY p^5

From the elliptic curves over the field with cardinality p^5 in the following Table 5 some are found by using the trick given in Section 7 and some by using free mathematics software system Sage.

p	$N_{p^5}(1)$	Elliptic Curve	Minimal Polynomial of z
2	44	$y^2 + xy + y = x^3 + x^2 + x$	
3	275	$y^2 = x^3 + 2x^2 + x + 1$	
5	3237	$y^2 = x^3 + z^{97}x + 1$	$X^5 + 4X + 3$
7	17066	$y^2 = x^3 + x + z^{601}$	$X^5 + X + 4$
11	161854	$y^2 = x^3 + x + 1$	
13	372512	$x^3 + zx + z^{333760}$	$X^5 + 4X + 11$
17	1422241	$y^2 = x^3 + \frac{3}{4}x^2 + z^{1351944}x + z^{198311}$	$X^5 + X + 14$
19	2479247	$y^2 = x^3 + \frac{1}{4}x^2 + z^{508237}x + z^{1608725}$	$X^5 + 5X + 17$

Table 5

7. A TRICK

By Chap. 4, Sec. 3 in [5], if we have a curve E / F_q with $\#E(F_q) = N$, then we can find the number of point of the same curve over F_{q^n}. Namely write $N = q + 1 - a$ and $\alpha, \beta \in C$ be the zero's of $X^2 - aX + q$. Then $\#E(F_{q^n}) = q^n + 1 - \alpha^n - \beta^n$.

Example 7.1 The curve $E: y^2 = x^3 + 2x^2 + 2$ has $\#E(F_3) = 2$, then we can write $\#E(F_3) = 3 + 1 - 2$, therefore $a = 2$, then by [Chap. 4, Sec. 3 in [5], we have $\alpha = 1 + i\sqrt{(2)}, \beta = 1 - i\sqrt{2}$. Then

$$\#E(F_{3^3}) = 3^3 + 1 - (1+i\sqrt{2})^3 - (1-i\sqrt{2})^3 = 38 = N_{3^3}(1).$$

By this trick we can find some maximal curves over F_{p^3} and F_{p^5} with coefficients from F_p.

p	$\#E / F_p$	$N_p^3(1)$	equation
2	2	14	$y^2 + xy = x^3 + x^2 + x$
3	2	38	$y^2 = x^3 + 2x^2 + 2$
5	4	148	$y^2 = x^3 + x + 2$
11	9	1404	$y^2 = x^3 + x + 4$
17	14	5054	$y^2 = x^3 + x + 3,$

Table 6

Also

p	$\#E / F_p$	$N_{p^5}(1)$	equation
2	4	44	$y^2 + xy + y = x^3 + x^2 + x$
3	5	275	$y^2 = x^3 + 2x^2 + 1$
11	14	161854	$y^2 = x^3 + x + 1.$

Table 7

REFERENCES

[1] J. P. Serre, Rational points on curves over finite fields. Unpublished Notes by F.Q. Gouvea of lectures at Harvard University, 1985.

[2] J.H. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics 106, Springer Verlag, New York, 1986.

[3] J.H. Silverman and J. Tate, Rational points on elliptic curves. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[4] W.C. Waterhouse, Abelian varieties over finite fields, Ann. sci. de

[5] Lawrence C. Washington, Elliptic Curves Number Theryoy and Cryptography, by Taylor & Francis Group, LLC, University of Maryland College Park, Maryland, U.S.A, second edition (2008).