Arch. Math. 86 (2006) 121–128
0003–889X/06/020121–08
DOI 10.1007/s00013-005-1442-7

Archiv der Mathematik

A simple criterion for the m-cyclicity of the group of rational points on an elliptic curve defined over a finite field

By

HUGUES VERDURE

Abstract. We give a simple criterion for the cyclicity of the m-torsion subgroup of the group of rational points on an elliptic curve defined over a finite field of characteristic larger than 3 for $m = 2, 3, 4, 6, 12$.

1. Introduction and notation. The aim of this paper is to give a very simple criterion for the cyclicity of the m-torsion of the group of rational points of an elliptic curve defined over a finite field, in the case where m is a divisor of 12.

In this paper, $p \geqq 5$ is a prime number and q is a power of p. We denote by F_q the field with q elements, and by $\overline{\mathrm{F}_q}$ its algebraic closure. F_q^n is the product of n copies of F_q, while $\mathrm{F}_q^{(n)}$ is the subset of n-th powers.

We refer to [4] for the theory of elliptic curves, and we will use its notation. If

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

is an elliptic curve defined over F_q, and $D \in \mathrm{F}_q \backslash \mathrm{F}_q^{(2)}$, then we define the D-twist $\widetilde{E}^D$ of E to be the elliptic curve defined over F_q by

$$\widetilde{E}^D : y^2 = x^3 + Da_2x^2 + D^2a_4x + D^3a_6.$$

We have the following property:

$$\#\widetilde{E}^D(\mathrm{F}_q) + \#E(\mathrm{F}_q) = 2q + 2.$$

Moreover, if $d \in \mathrm{F}_{q^2}$ is a square root of D, then

$$\varphi_d : E(\mathrm{F}_{q^2}) \longrightarrow \widetilde{E}^D(\mathrm{F}_{q^2})$$

Mathematics Subject Classification (2000): 14H52.

defined by $\varphi_d(x, y) = (Dx, d^3y)$ is an isomorphism of abelian groups that preserves the rationality of 2-torsion points.

When studying torsion on elliptic curves, it is natural to look at division polynomials ψ_n. They have the property that a point $P = (x, y) \in E(\overline{\mathrm{F}_q})$ is n-torsion if and only if $\psi_n(x, y) = 0$. The interested reader can look at [1]. We will just need two of them, namely the third and the fourth, and they are defined as follows:

$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$$

and

$$\frac{\psi_4}{2y} = 2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2.$$

2. Cyclicity of $E(\mathrm{F}_q)[m]$ for $m = 2, 3, 4, 6, 12$. As shown in [2], there exists a necessary but not sufficient condition such that $E(\mathrm{F}_q)[m] \approx (\mathrm{Z}/m\mathrm{Z})^2$, namely $m^2 \mid \#E(\mathrm{F}_q)$ and $m \mid q - 1$. We shall provide a partial converse when m is a divisor of 12. The results we are now presenting are known for $m = 2$ and $m = 3$ (see [3]), but we haven't found any proofs in the literature. To the best of our knowledge, the results are unknown for other m. We give here a simple proof of the following result:

Theorem 2.1. *Let E be an elliptic curve defined over F_q by a Weierstrass equation*

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

of discriminant Δ. Let $m = 2, 3, 4, 6, 12$. Assume that $m^2 \mid \#E(\mathrm{F}_q)$ and $m \mid q - 1$. Then we have

$$E(\mathrm{F}_q)[m] \approx (\mathrm{Z}/m\mathrm{Z})^2 \Leftrightarrow \Delta \in \mathrm{F}_q^{(m)}.$$

Before proceeding with the proof, we make some remarks.

Remark 2.2. The previous result is the best possible, in the sense that it can not be extended to any other positive integer m, since the discriminant is defined up to the 12-th power of a multiplicative constant.

Remark 2.3. Under changes of variables $x = x' - x_0$, the discriminant and the form of the Weierstrass equation are unchanged. We will therefore make such changes of variables freely.

Remark 2.4. In the proof, we shall define quantities with indices. Except for P_i, x_i, and y_i, these indices are the actual weights of the quantities.

We shall now prove Theorem 2.1 in several steps.

2.1. 2-cyclicity. In this section, we shall prove the main theorem when $m = 2$.

Proof of Theorem 2.1 when $m = 2$. We have

$$E[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}$$

where the x_i's are the 3 distinct roots of $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Since $2 \mid \#E(\mathrm{F}_q)$, one of them is in F_q. Then f either splits or has an irreducible factor of degree 2. We then have

$$\begin{aligned} E(\mathrm{F}_q)[2] \approx (\mathrm{Z}/2\mathrm{Z})^2 &\Leftrightarrow f \text{ splits} \\ &\Leftrightarrow \mathcal{D} \in \mathrm{F}_q^{(2)} \end{aligned}$$

where $\mathcal{D}$ is the discriminant of $f(x)$. But

$$\mathcal{D} = -4a_6a_2^3 + a_4^2a_2^2 + 18a_6a_4a_2 - 4a_4^3 - 27a_6^2 = \frac{\Delta}{16},$$

and the theorem is proved in the case $m = 2$.

Remark 2.5. We didn't use the fact that $4 \mid \#E(\mathrm{F}_q)$ but just $2 \mid \#E(\mathrm{F}_q)$.

Corollary 2.6. *Let E be an elliptic curve defined over F_q. Assume that the j-invariant j is such that $j \neq 1728$ and that E has a non-zero rational 2-torsion point. Then we have*

$$E(\mathrm{F}_q)[2] \textit{ is cyclic } \Leftrightarrow (j - 1728) \textit{ is not a square}.$$

Proof This follows immediately from

$$j - 1728 = \frac{c_6^2}{\Delta}. \quad \square$$

2.2. 3-cyclicity.

Lemma 2.7. *Let E be an elliptic curve defined over F_q by a Weierstrass equation*

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Assume that $q \equiv 1$ [3] and $\#E(\mathrm{F}_q) \equiv 0$ [9]. Then we have

$$x_0 \in \mathrm{F}_q \textit{ is a root of } \psi_3 \Leftrightarrow \exists P = (x_0, y_0) \in E(\mathrm{F}_q)[3].$$

Proof. By definition, we have: $x_0 \in \overline{\mathrm{F}_q}$ is a root of ψ_3 if and only if there exists a point $P = (x_0, y_0) \in E[3]$, and therefore, one way is straightforward. Assume now that $x_0 \in \mathrm{F}_q$ is a root of ψ_3. Thus there exists a point $P = (x_0, y_0) \in E[3]$. Assume that $y_0 \notin \mathrm{F}_q$. Since

$$y_0^2 = x_0^3 + a_2x_0^2 + a_4x_0 + a_6,$$

we can deduce that $D = y_0^2 \in \mathrm{F}_q \backslash \mathrm{F}_q^{(2)}$. We then consider the D-twist $\widetilde{E}^D$ of E. We know that $\varphi_{y_0}(x_0, y_0) \in \widetilde{E}^D(\mathrm{F}_{q^2})$, and it is easy to see that this point is in fact in $\widetilde{E}^D(\mathrm{F}_q)$. Since this is a point of 3-torsion, we thus get

$$2(q+1) = \#E(\mathrm{F}_q) + \#\widetilde{E}^D(\mathrm{F}_q) \equiv 0\ [3]$$

which contradicts the assumption $q \equiv 1\ [3]$. □

Proof of Theorem 2.1 when $m = 3$. By hypothesis, there exists a point $P = (x_0, y_0)$ rational and of order exactly 3, and we can assume that $x_0 = 0$ by a suitable change of variable. We thus have

$$E(\mathrm{F}_q)[3] \approx (\mathrm{Z}/3\mathrm{Z})^2 \Leftrightarrow \exists x \in \mathrm{F}_q^*,\ \psi_3(x) = 0.$$

By Lemma 2.7, the x-coordinates of rational points of exact order 3 are given by the roots of ψ_3 in F_q, and in our case, $\psi_3(x) = 3x\varphi_3(x)$, where

$$\varphi_3(x) = x^3 + \frac{b_2}{3}x^2 + b_4 x + b_6$$

($b_8 = 0$ since $x_0 = 0$). This polynomial is either irreducible (no other rational points of order 3), or splits (all the 3-torsion points are rational). By a suitable change of variable, put φ_3 in the form

$$\theta_3(x) = x^3 + \alpha_4 x + \alpha_6$$

with

$$\alpha_4 = b_4 - \frac{b_2^2}{27} = 2a_4 - \frac{16a_2^2}{27},$$

and

$$\alpha_6 = b_6 - \frac{b_2 b_4}{3} + \frac{2b_2^3}{729} = \frac{1}{729}\,(128a_2^3 - 648a_2a_4 + 2916a_6).$$

Note that the two polynomials are of the same type. We have to consider two cases. If $\alpha_4 = 0$, then $a_4 = \frac{8}{27}a_2^2$, and since $b_8 = 0$,

$$a_2\left(a_6 - \frac{16}{729}a_2^3\right) = 0.$$

Now, $\Delta \neq 0$ implies that $a_2 = a_4 = 0$ and we find that

$$\Delta = (-3)^3(4a_6)^2 = (-3)^3\alpha_6^2.$$

We finally get that

$$\Delta \in \mathrm{F}_q^{(3)} \Leftrightarrow \alpha_6 \in \mathrm{F}_q^{(3)} \Leftrightarrow \theta_3 \text{ splits.}$$

If $\alpha_4 \neq 0$, note that $b_8 = 0$ and $\Delta \neq 0$ imply $a_2 a_4 \neq 0$. We consider the resolvent polynomial

$$g(x) = x^2 + \frac{3\alpha_6}{\alpha_4}x - \frac{\alpha_4}{3},$$

whose discriminant is

$$\delta = \frac{36(-12a_2^2a_4^2 + 54a_4^3 + 64a_2^3a_6 - 324a_2a_4a_6 + 729a_6^2)}{(8a_2^2 - 27a_4^2)^2} = \frac{9a_4^2}{4a_2^2}.$$

Since this is a non-zero square in F_q, the polynomial $g(x)$ has two distinct rational roots $\alpha, \beta \in \mathrm{F}_q$. Note that none of them is zero since their product is equal to $-\frac{\alpha_4}{3}$. Let r be a root of θ_3 in $\overline{\mathrm{F}_q}$. Since

$$\beta^3 + \alpha_4\beta + \alpha_6 = -\frac{\beta}{3\alpha_4^2} \cdot \mathrm{discriminant}(\theta_3) \neq 0,$$

$r \neq \beta$. Consider then $z = \frac{r-\alpha}{r-\beta}$. It is obvious that $z \in \mathrm{F}_q$ if and only if $r \in \mathrm{F}_q$, and therefore, φ_3 splits if and only if $z \in \mathrm{F}_q$. We now look at $A = z^3$. Since we know that $r^3 + \alpha_4 r + \alpha_6 = 0$, $\alpha\beta = -\frac{\alpha_4}{3}$ and $\alpha + \beta = -\frac{3\alpha_6}{\alpha_4}$, we easily find that

$$(r-\alpha)^3 = -\alpha(3r^2 - 3(\alpha+\beta)r + \alpha^2 + \alpha\beta + \beta^2)$$

and similarly for $(r-\beta)^3$. Then we have

$$A = \frac{\alpha}{\beta} \in \mathrm{F}_q$$

which means that φ_3 splits if and only if $A = \frac{\alpha}{\beta}$ is a cubic residue in F_q. Finally, remembering that $b_8 = 0$, we get that

$$A = \frac{\alpha}{\beta} = \left(\frac{128a_2^4 - 864a_2^2a_4 + 729a_4^2 + 2916a_2a_6}{128a_2^4 - 432a_2^2a_4 - 729a_4^2 + 2916a_2a_6}\right)^{\pm 1} = \left(\frac{\Delta}{8a_4^3}\right)^{\pm 1},$$

and thus A is a cubic residue in F_q if and only if Δ is.

Corollary 2.8. *Let E be an elliptic curve defined over F_q. Assume that the j-invariant j is such that $j \neq 0$. Then we have*

$$E(\mathrm{F}_q)[3] \approx (\mathrm{Z}/3\mathrm{Z})^2 \Leftrightarrow j \in \mathrm{F}_q^{(3)},\ q \equiv 1\ [3] \text{ and } 9 \mid \#E(\mathrm{F}_q).$$

P r o o f We have

$$j = \frac{c_4^3}{\Delta}. \quad \square$$

2.3. 4-cyclicity.

Lemma 2.9. *Let E be an elliptic curve defined over F_q by a Weierstrass equation*

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Assume that $q \equiv 1$ [4] and $\#E(\mathrm{F}_q) \equiv 0$ [16]. Suppose also that

$$E(\mathrm{F}_q)[2] \approx (\mathrm{Z}/2\mathrm{Z})^2.$$

Then we have

$$x_0 \in \mathrm{F}_q \text{ is a root of } \psi_4/2y \Leftrightarrow \exists P = (x_0, y_0) \in E(\mathrm{F}_q)[4] \backslash E(\mathrm{F}_q)[2].$$

Proof. As in the proof of Lemma 2.7, one way is straightforward. Assume now that $x_0 \in \mathrm{F}_q$ is a root of $\psi_4/2y$. Thus there exists a point $P = (x_0, y_0) \in E[4]$. Assume that $y_0 \notin \mathrm{F}_q$. As in Lemma 2.7, using twists, we can find a point of order exactly 4 on any D-twist. We also have that every 2-torsion point on E, as well as on $\widetilde{E}^D$ is rational. That means that the number of rational points on $\widetilde{E}^D$ is divisible by 8. Thus we have

$$2(q+1) = \#E(\mathrm{F}_q) + \#\widetilde{E}^D(\mathrm{F}_q) \equiv 0 \ [8]$$

which is absurd since $q \equiv 1$ [4]. □

Proof of Theorem 2.1 when $m = 4$. We first note that since the theorem is true for $m = 2$, we have $E(\mathrm{F}_q)[2] \approx (\mathrm{Z}/2\mathrm{Z})^2$, and the previous lemma applies. Moreover, the assumption $\#E(\mathrm{F}_q) \equiv 0$ [16] says that there exists a rational point $P_0 = (x_0, y_0)$ of order exactly 4 on E. Let

$$P_1 = 2P_0 = (x_1, y_1).$$

By a suitable change of variable, we may assume that $x_1 = 0$, which implies that $a_6 = 0$. Moreover, since

$$0 = x_1 = \frac{x_0^4 - b_4x_0^2 - 2b_6x_0 - b_8}{4x_0^3 + b_2x_0^2 + 2b_4x_0 + b_6},$$

we get that $x_0^2 = a_4$. Finally, since $E(\mathrm{F}_q)[2] \approx (\mathrm{Z}/2\mathrm{Z})^2$, the polynomial

$$f(x) = x^3 + a_2x^2 + a_4x = x(x^2 + a_2x + a_4)$$

splits, which is equivalent to

$$a_2^2 - 4a_4 \in \mathrm{F}_q^{(2)}.$$

We denote by δ_2 one of its square roots. Since $(x_0, y_0) \in E(\mathrm{F}_q)$,

$$y_0^2 = x_0^3 + a_2x_0^2 + a_4x_0 = a_4(a_2 + 2x_0).$$

Knowing that $a_4 \in \mathrm{F}_q^{(2)}$, we find that $a_2 + 2x_0 \in \mathrm{F}_q^{(2)}$. Now, since

$$(a_2 - 2x_0)(a_2 + 2x_0) = \delta_2^2,$$

$a_2 - 2x_0 \in \mathrm{F}_q^{(2)}$ as well. We denote by t_+, t_- square roots of $a_2 \pm 2x_0$ in F_q, with the additional property that $t_+ t_- = \delta_2$.

We now consider

$$\begin{aligned}\frac{\psi_4}{2y}(x) &= 2x^6 + 4a_2x^5 + 10a_4x^4 - 10a_4^2x^2 - 4a_2a_4^2x - 2a_4^3 \\ &= 2(x - x_0)(x + x_0)(x^2 + (a_2 - \delta_2)x + a_4)(x^2 + (a_2 + \delta_2)x + a_4).\end{aligned}$$

The discriminant $\mathcal{D}$ of the fourth factor of this polynomial is

$$\begin{aligned}\mathcal{D} &= (a_2 + \delta_2)^2 - 4a_4 \\ &= 2\delta_2(a_2 + \delta_2) \\ &= \delta_2(t_+^2 + t_-^2 + 2\delta_2) \\ &= \delta_2[(t_+ + t_-)^2 + 2(\delta_2 - t_+t_-)] \\ &= \delta_2(t_+ + t_-)^2.\end{aligned}$$

We then see that

$$\mathcal{D} \in \mathrm{F}_q^{(2)} \Leftrightarrow \delta_2 \in \mathrm{F}_q^{(2)},$$

and similarly for the third factor. Since $q \equiv 1$ [4] and $\Delta = 16a_4^2\delta_2^2 = (2x_0)^4\,\delta_2^2$,

$$\delta_2 \in \mathrm{F}_q^{(2)} \Leftrightarrow \Delta \in \mathrm{F}_q^{(4)}.$$

Putting all the pieces together, we get that

$$\Delta \in \mathrm{F}_q^{(4)} \Leftrightarrow E(\mathrm{F}_q)[4] \approx (\mathrm{Z}/4\mathrm{Z})^2.$$

2.4. 6- and 12-cyclicity.

Proof of Theorem 2.1 when $m = 6, 12$. The theorem is a direct consequence of our theorem when $m = 2, 3, 4$.

References

[1] I. BLAKE, G. SEROUSSI and N. SMART, Elliptic curves in cryptography. London Math. Soc. Lecture Note Ser. **265**, Cambridge 2000.

[2] R. SCHOOF, Nonsingular plane cubic curves over finite fields. J. Combin. Theory Ser. A, **46**, 183–211 (1987).

[3] J. P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972).
[4] J. H. SILVERMAN, The arithmetic of elliptic curves. Graduate Texts in Math. **106**, 1986.

Received: 25 January 2005

Hugues Verdure
Institutt for Matematikk og Statistikk
Universitetet i Tromsø
N-9037 Tromsø
Norway
hugues.verdure@matnat.uit.no