Elliptic curves over finite fields with many points

Antonella Perucca

Abstract

Following Waterhouse we determine the maximal number of rational points for elliptic curves defined over a finite field. Along the way we determine the isogeny classes of elliptic curves defined over a finite field by describing the possible values of the trace of the geometric Frobenius.

Let $\mathbb{F}_q$ be a finite field, where $q = p^a$. Let E be an elliptic curve defined over $\mathbb{F}_q$. The Hasse bound implies that $\#E(\mathbb{F}_q) \leq q + 1 + \lfloor 2\sqrt{q} \rfloor$. Then the maximum of $\#E(\mathbb{F}_q)$ where E is an elliptic curve over $\mathbb{F}_q$ is a number N_q which is at most $q + 1 + \lfloor 2\sqrt{q} \rfloor$.

Theorem 1. *The number N_q is either $q + 1 + \lfloor 2\sqrt{q} \rfloor$ or $q + \lfloor 2\sqrt{q} \rfloor$. It is $q + 1 + \lfloor 2\sqrt{q} \rfloor$ if and only if at least one of the following occurs: p does not divide $\lfloor 2\sqrt{q} \rfloor$; q is a square; $q = p$.*

Proof. The number of rational point of an elliptic curve E defined over $\mathbb{F}_q$ equals $q+1-\beta$ where β is the trace of the geometric Frobenius of E. Then to prove the theorem it suffices to show the following two things: 1) there exists an elliptic curve E defined over $\mathbb{F}_q$ such that the trace β of the Frobenius equals $-\lfloor 2\sqrt{q} \rfloor$ if and only if either p does not divide $\lfloor 2\sqrt{q} \rfloor$ *or* q is a square *or* $q = p$; 2) if p divides $\lfloor 2\sqrt{q} \rfloor$ then there exists an elliptic curve E defined over $\mathbb{F}_q$ such that the trace β of the Frobenius equals $-(\lfloor 2\sqrt{q} \rfloor - 1)$. Remark that if p divides $\lfloor 2\sqrt{q} \rfloor$ then p does not divide $\lfloor 2\sqrt{q} \rfloor - 1$. Also remark that if p divides $\lfloor 2\sqrt{q} \rfloor$ then $q = p$ is equivalent to requiring $p = 2, 3$ and $\lfloor 2\sqrt{q} \rfloor = p^{\frac{a+1}{2}}$. Then the theorem is a consequence of the following result. □

Theorem 2. *Let β be an integer such that $|\beta| \leq \lfloor 2\sqrt{q} \rfloor$ ($q = p^a$, as above). Then there exists an elliptic curve E defined over $\mathbb{F}_q$ such that the trace of the Frobenius equals β if and only if one of the following cases occur:*

- *p does not divide β*
- *q is a square (i.e. a is even) and*
  $\beta = \pm 2\sqrt{q}$
  or $\beta = \pm\sqrt{q}$ *and* $p \not\equiv 1 (\mathrm{mod} 3)$
  or $\beta = 0$ *and* $p \not\equiv 1 (\mathrm{mod} 4)$
- *q is not a square (i.e. a is odd) and*
  $\beta = 0$
  or $\beta = \pm p^{\frac{a+1}{2}}$ *and* $p = 2, 3$.

Let A be a simple abelian variety of dimension g defined over the finite field $\mathbb{F}_q$ (where $q = p^a$). Call $P(X)$ the mimimal polynomial of the geometric Frobenius. Call $h(X)$ the characteristic polynomial of the geometric Frobenius. We know that $P(X)$ and $h(X)$ have coefficients in $\mathbb{Z}$ and that $h(X)$ is a power of $P(X)$. The constant term of h is q^g. In particular for an elliptic curve we have $h(X) = X^2 - \beta X + q$ for some integer β.

The geometric Frobenius π is a Weil-q-number i.e. an algebraic integer π such that $|\psi(\pi)| = q$ for every embedding $\psi : \mathbb{Q}(\pi) \to \bar{\mathbb{Q}}$. For an elliptic curve the roots of $h(X)$ are π and $\frac{q}{\pi}$ and so $\beta = \pi + \frac{q}{\pi}$. In particular $|\beta| \leq 2\sqrt{q}$.

The endomorphisms of A defined over $\mathbb{F}_q$ are a free $\mathbb{Z}$-module $\mathrm{End}\, A$ of finite rank. The $\mathbb{Q}$-algebra $\mathrm{End}_0\, A = \mathrm{End}\, A \times_{\mathbb{Z}} \mathbb{Q}$ is a central simple algebra over $\mathbb{Q}(\pi)$. Thus the center of $D := \mathrm{End}_0\, A$ is $L := \mathbb{Q}(\pi)$.

By the Brauer theory the L-algebra D is determined (up to isomorphism) by its invariants at the places of L. The invariants are rational numbers in $[0, 1)$, seen as representatives of residue classes in $\mathbb{Q}/\mathbb{Z}$. The invariants at the complex places are always 0. The sum of all the invariants is an integer. The l.c.m. of the invariants equals $\sqrt{[D : L]}$.

The following theorem by Tate implies that the algebraic integer π determines D (remark that it determines also the dimension of the variety).

Theorem 3 (Tate)**.** *The central simple algebra D/L does not split at every real place of L (i.e. the invariant at every real place is $\frac{1}{2}$). It does split at every finite place not above p (i.e. the corresponding invariant is 0). For a finite place w over p the corresponding invariant is:*

$$inv_w(D/L) = \frac{w(\pi)}{w(q)}[L_w : \mathbb{Q}_p] \pmod{\mathbb{Z}}$$

where L_w is the completion of L at w. The dimension g of the variety is given by the formula

$$2g = [L : \mathbb{Q}]\sqrt{[D : L]}.$$

Proof. First case: the minimal polynomial of the Frobenius has degree 1.
We deduce that $h(X) = (X - \alpha)^2$ where $\alpha^2 = q$ and $2\alpha = \beta \in \mathbb{Z}$. Then $\alpha \in \mathbb{Z}$ and $\alpha = \pm\sqrt{q}$. *In this case q is a square and $\beta = \pm 2\sqrt{q}$.* Now we prove that there exists an elliptic curve defined over $\mathbb{F}_q$ having such a minimal polynomial. The root of $P(X)$ is a Weil-q-number by construction. Then by the Honda-Tate theory there exists a simple abelian variety A defined over $\mathbb{F}_q$ having minimal polynomial P (the isogeny class of A is uniquely determined by that condition). So we have to prove that the dimension of A is 1. We calculate the invariants of the central simple algebra $D := \mathrm{End}_0(A)$ over $L := \mathbb{Q}(\pi)$. Now $L = \mathbb{Q}$ so there is only one infinite prime, real. Then invariants are: $inv_\infty = \frac{1}{2}$; $inv_\ell = 0$ for every prime $\ell \neq p$. Since the sum of the invariants is an integer we must have $inv_p = \frac{1}{2}$. The l.c.m. of the denominators is 2 so by the Tate's theorem we deduce that the dimension of A is 1.

Second case: the minimal polynomial of the Frobenius has degree 2.
In this case $P(X) = h(X) = X^2 - \beta X + q$. Remark that *in this case* $|\beta| < 2\sqrt{q}$: in fact $|\beta| \leq 2\sqrt{q}$ and that π is a Weil-q-number so if $|\beta| = 2\sqrt{q}$ then $\pi = q/\pi = \pm\sqrt{q}$ and we are in the preceeding case.Hence π is a totally imaginary Weil-q-number. The roots of $P(X)$ are Weil-q-numbers by construction. Then by the Honda-Tate theory there exists a simple abelian variety A defined over $\mathbb{F}_q$ having minimal polynomial P (the isogeny class of A is uniquely determined by that condition). We study the invariants of the central simple algebra $D := \mathrm{End}_0(A)$ over $L := \mathbb{Q}(\pi)$. We have $L = \mathbb{Q}(\sqrt{\beta^2 - 4q})$ where $\beta^2 < 4q$. Since L is an extension of $\mathbb{Q}$ of degree 2, by the Tate's theorem we deduce that A is an elliptic curve if and only if the l.c.m. of its invariants (which is $\sqrt{[D : L]}$) is equal to 1.

Since π is totally imaginary there are no real embeddings of L into $\mathbb{Q}$. Then the invariants of D corresponding to the infinite primes are zero. The invariants for the primes of L over the rational primes different from p are zero. If there is only one prime over (p) we deduce (because the sum of the invariants is an integer) that D has every invariant zero. *If (p) ramifies or stays prime in $\mathbb{Q}(\sqrt{\beta^2 - 4q})$ then there exists an elliptic curve corresponding to the considered mimimal polynomial.*

We conclude the study of this case by proving the following. *If (p) splits completely in $\mathbb{Q}(\sqrt{\beta^2-4q})$ then there exists an elliptic curve corresponding to the considered mimimal polynomial if and only if p does not divide β.* So suppose that (p) splits completely in L, which means that $(p) = \mathcal{P}_1\mathcal{P}_2$. Let $i = 1, 2$. Since the inertia degree and ramification index of $\mathcal{P}_i$ over $\mathbb{Q}$ are both 1 then the completion $L_{\mathcal{P}_i}$ has degree 1 over $\mathbb{Q}_p$. Then by the Tate's theorem the invariant at $\mathcal{P}_i$ has denominator 1 if and only if $v_{\mathcal{P}_i}(q)$ divides $v_{\mathcal{P}_i}(\pi)$. Since $q = p^a$ we have $(q) = \mathcal{P}_1^a\mathcal{P}_2^a$. Since π is an algebraic integer of L of norm q and the primes over (p) are only $\mathcal{P}_1$ and $\mathcal{P}_2$ we have $(\pi) = \mathcal{P}_1^{t_1}\mathcal{P}_1^{t_2}$ where $t_1 + t_2 = a$. Then $v_{\mathcal{P}_i}(q) = a$ and $v_{\mathcal{P}_i}(\pi) = t_i$. Since $t_1 + t_2 = a$ it follows that $v_{\mathcal{P}_i}(q)$ divides $v_{\mathcal{P}_i}(\pi)$ if and only if either t_1 or t_2 is zero. Remark that $(\frac{q}{\pi}) = \mathcal{P}_1^{t_2}\mathcal{P}_1^{t_1}$. Then either t_1 or t_2 is zero if and only if β (which is $\pi + \frac{q}{\pi}$) does not belong neither to $\mathcal{P}_1$ nor to $\mathcal{P}_2$. Since β is an integer it belongs to $\mathcal{P}_1$ if and only if it belongs to $\mathcal{P}_2$. Because we are working in a Dedekind ring and the ideals $\mathcal{P}_1$ and $\mathcal{P}_2$ are coprime, the condition is then equivalent to requiring that β does not belong to $\mathcal{P}_1\mathcal{P}_2$. This exactly means that β is not a multiple of p.

Conclusions. We have an elliptic curve defined over $\mathbb{F}_q$ such that the trace of the geometric Frobenius is β in the following cases: if q is a square and $\beta = \pm\sqrt{q}$ (from the first case); if $\beta^2 < 4q$ and (p) does not split completely in $\mathbb{Q}(\sqrt{\beta^2-4q})$ (from the second case); if $\beta^2 < 4q$, (p) splits completely in $\mathbb{Q}(\sqrt{\beta^2-4q})$ and $p \nmid \beta$ (from the second case). We conclude thanks to the following lemma.

Remark that in the cases described by the lemma we are in the second case since $\beta^2 < 4q$. Also remark that $p \nmid \beta$ implies that we are in the second case and we have an elliptic curve both whether p splits or not. $\square$

Lemma 4. *Let $q = p^a$ and let β be an integer such that $\beta^2 < 4q$. The prime p of $\mathbb{Z}$ does not split completely in $\mathbb{Q}(\sqrt{\beta^2-4q})$ if and only if one of the following cases occur:*

- *q is a square and*
  $\beta = 0$, $p \not\equiv 1 (\mathrm{mod} 4)$
  or $\beta = \pm\sqrt{q}$, $p \not\equiv 1(\mathrm{mod} 3)$
- *q is not a square and*
  $\beta = 0$
  or $\beta = \pm p^{\frac{a+1}{2}}$, $p = 2, 3$.

Proof. Write $\beta = p^b\lambda$ where λ is either zero or coprime to p. If $\lambda = 0$ or equivalently $\beta = 0$ then $\mathbb{Q}(\sqrt{\beta^2-4q}) = \mathbb{Q}(\sqrt{-p})$ if a is odd and $\mathbb{Q}(\sqrt{\beta^2-4q}) = \mathbb{Q}(\sqrt{i})$ if a is even. If a is odd p clearly ramifies. If a is even then 2 ramifies and $p \neq 2$ stays prime in the Gaussian integers if and only if $p \equiv 3(\bmod 4)$. *So if $\beta = 0$ then p does not split completely in $\mathbb{Q}(\sqrt{\beta^2-4q})$ if q is not a square or if $p \not\equiv 1(\mathrm{mod}4)$.*

If $\lambda \neq 0$ and $2b < a$ then p splits completely. We have $\mathbb{Q}(\sqrt{\beta^2-4q}) = \mathbb{Q}(\sqrt{\lambda^2-4p^{a-2b}})$. The prime p does not divide the discriminant of this extension of $\mathbb{Q}$ so p does not ramify. We have to exclude the case where p stays prime which means that (p) is a maximal ideal. This is an elementary computation. Let m^2 be the maximal square dividing $\lambda^2 - 4p^{a-2b}$, let $\gamma = \lambda^2 - 4p^{a-2b}/m^2$ and call $\lambda' = \lambda/m$. Remark that $(m, p) = 1$. Let $\mathbb{Z}[\alpha]$ be the ring of integers of $\mathbb{Q}(\sqrt{\beta^2-4q})$: according to whether γ is congruent to 1 or to 3 modulo 4 one can take $\alpha = \frac{1-\sqrt{\gamma}}{2}$ or $\alpha = \sqrt{\gamma}$. The mimimal polynomial f of α is $x^2 + 2x + \frac{1-\gamma}{4}$ or respectively $x^2 - \gamma$. It suffices to show that the class of f in $\mathbb{F}_p[x]$ is not an irreducible polynomial. The class of f in $\mathbb{F}_p[x]$ is respectively $(x + \frac{1+\lambda'}{2})(x + \frac{1-\lambda'}{2})$ or $(x + \lambda')(x - \lambda')$.

If $\lambda \neq 0$ and $2b = a$ (a is even!) then because $\beta^2 < 4q$ we deduce that $|\lambda| < 2$ hence $\lambda = \pm 1$. Hence $\beta = \pm\sqrt{q}$. In this case $\mathbb{Q}(\sqrt{\beta^2-4q}) = \mathbb{Q}(\sqrt{-3})$ and one easily has the following: 3

ramifies, $p \equiv 2(\text{mod}3)$ stays prime, $p \equiv 1(\text{mod}3)$ splits completely. *So if $\beta = \pm\sqrt{q}$ then p does not split completely in $\mathbb{Q}(\sqrt{\beta^2 - 4q})$ if $p \not\equiv 1(\text{mod}3)$.*

If $\lambda \neq 0$ and $2b \geq a$ then because $\beta^2 < 4q$ we deduce that $|\lambda| < 2$ hence $\lambda = \pm 1$. Also $2b < a + 1$ because $\beta^2 < 4q$. So we have $2b = a + 1$ (a is odd!) and therefore (because $\beta^2 < 4q$) p is 2 or 3. If $p = 2$ we have $\mathbb{Q}(\sqrt{\beta^2 - 4q}) = \mathbb{Q}(\sqrt{i})$ and 2 ramifies. If $p = 3$ we have $\mathbb{Q}(\sqrt{\beta^2 - 4q}) = \mathbb{Q}(\sqrt{-3})$ and 3 ramifies. *So if $\beta = \pm p^{\frac{a+1}{2}}$ and $p = 2, 3$ then p does not split completely in $\mathbb{Q}(\sqrt{\beta^2 - 4q})$.* $\square$

By Honda-Tate theory the isogeny classes of elliptic curves defined over $\mathbb{F}_q$ are determined by the mimimal polinomial of the Frobenius and hence by its trace (it being monic and with constant term q). Since we know that this trace β is an integer such that $|\beta| \leq 2\sqrt{q}$, Theorem 2 determines the isogeny classes of elliptic curves defined over $\mathbb{F}_q$.

An elliptic curve is supersingular iff there exists a power of π which is a power of p. Then from the proof of Theorem 2 we have: the elliptic curves arising from the first case are supersingular; the elliptic curves arising from the second case are ordinary if (p) splits (one can see this from the factorization of the ideals generated by p and π); the elliptic curves arising from the second case are supersingular if (p) does not split (one can calculate π in each sub-case and check the criterion for supersingularity).

References

[1] D. Husemöller, Elliptic Curves, Springer Verlag, Graduate Text in Mathematics (111), 2004.

[2] D. Mumford, Abelian Varieties, Oxford University Press, 1970.

[3] F. Oort, Abelian varieties over finite fields, `http://www.math.uu.nl/people/oort/A-AVffGoe07-2-oort.ps`

[4] J. H. Silverman, The arithmetic of elliptic curves, Springer Verlag, Graduate Text in Mathematics (106), 1986.

[5] I. Reiner, Maximal Orders, Academic Press, 1975.

[6] W. C. Waterhouse, Abelian varieties over finite fields, Ann. scient. Éc. Norm. Sup., Série 4 vol. 2 (1969), pp.521–560.