Pendulums and Elliptic curve over $\mathbb{F}_q$

Sachin Kumar
University of Waterloo, Faculty of Mathematics

January 6, 2024

Abstract

The idea of elliptic curves over a finite field, $\mathbb{F}_q$ is not just useful in theoretical aspects of mathematics, but also in applied sense (mainly in cryptography and algebraic coding theory, which is the study of error-correcting codes and information theory). In this essay, I will also talk about solving equation of a moving pendulum, which is fascinating in number theoretic aspects, trust me there is no physics! Just a little though :)

Elliptic curve over $\mathbb{F}_q$

Let k be a fixed finite field, of cardinality $q = p^f$. If E/k is an elliptic curve, then $\#E(k) = 1+q-a$, where $a = a(E)$ is an integer which tells you a lot about E (note that $a^2 \leq 4q$, and equality really can occur). For example, if $l \neq p$ is a prime then the l-adic Tate module of E has an action of Frobenius with characteristic polynomial $X^2 - aX + q$. Because of this, and the Tate conjecture or whatever, which is certainly a theorem in this setting, two elliptic curves E and F over k are isogenous if and only if $a(E) = a(F)$.

The number a tells you the number of k-points of E. It also tells you the number of k'-points for k' any finite extension of k, for the following reason: If k' any finite extension of k of degree n then Frobenius on the l-adic Tate module of E/k' is just the n^{th} power of Frobenius on the Tate module of E/k. Hence, if α and β are the roots of $X^2 - aX + q$ then,

$$\#E(k') = 1 + q^n - \alpha^n - \beta^n$$

An elliptic curve is supersingular if it has no point of order p over $\bar{k}$, that is, if $\#E(k')$ is prime to p for all finite extensions k' of k. One checks easily that this is true if and only if a is prime to p.

Given $a \in \mathbb{Z}$ with $a^2 \leq 4q$, is there an elliptic curve over k with $a = a(E)$? I don't think so! In fact I guess I can prove that this isn't the case. It's true if $p \nmid a$ or if $a^2 = 4q$, and probably in some other cases too. But I think that in the general case there is trouble. Here's why.

Let a be an arbitrary integer with $a^2 \leq 4q$. Let π be a root of $X^2 - aX + q$. Then either π is a quadratic irrational with norm $\sqrt{q}$, or $q = p^f = p^{2g} = r^2$ is the square of an integer and $a = \pm 2r$ and $\pi = \pm r = \pm p^g$. In either case, Theorem 5.1(c) of Milne's Corvalis article (where he explains Honda-Tate theory) applies, and we deduce the existence of a simple abelian variety $A = A_\pi$ with some property or other. What's the dimension of this variety? One has to do two calculations, which I'll try to sketch here.

Easy Case: $a^2 = 4q$. Then $f = 2g$ is even, $q = p^{2g} = r^2$ with $r = p^g$, and $a = \pm 2r$, so $\pi = \pm r$. By Milne Theorem 5.1(a), we have $\mathbb{Q}(\pi) = \mathbb{Q}$ and $e = \text{lcm}(2, 2) = 2$. Hence the dimension of A is 1, and A is a super singular elliptic curve over k with either as few points as possible, or as many as possible, depending on the sign of a. Note that one of these forms will be a quadratic twist of the other, at least if $p > 2$. Note also that the endomorphism ring of A over k, A/K is already an order in the quaternion algebra over $\mathbb{Q}$ of discriminant p.

Messier Case: $|a| < 2\sqrt{q}$. Then π is a quadratic irrational, so $\mathbb{Q}(\pi)$ is an imaginary quadratic field $\mathbb{Q}(\sqrt{a^2-4q})$.

The subcase we're interested in is when a is prime to p. Then $\pi\bar{\pi} = q$ and $\pi + \bar{\pi} = a$, so π and $\bar{\pi}$ are coprime. Because, $\mathbb{Q}(\pi)$ is imaginary quadratic and $|\pi| > 1$, π can't be an unit. An easy check now shows that p must split in $\mathbb{Q}(\pi)$, and π is coprime to one of the primes above p, but $\pi = v^f$ for the other one. Milne's result about invariants of division algebras shows that the invariants of the division algebra $\mathrm{End}(A)$ are all integers, so $E = \mathbb{Q}$, so $e = 1$ (in Milne's notation) and A is 1-dimensional and hence an elliptic curve, and the endomorphism ring is an order in an imaginary quadratic field.

Perhaps, one can do something when $q|a^2$ in some cases (I think p has to not split in this case if one wants an elliptic curve?). Bu there is an example to show that there can be problems in general: consider $q = p^{10}$ and $a = p^2$. Then π is a root of $X^2 + pX + p^{10}$ so the slopes of π are 2 and 8, so p splits, and the ords of π wrt the two primes above p are 2 and 8, and the ord of q is 10, so the invariants of the division algebra are $1/5$ and $4/5$ and it has dimension 25. So A is 5-dimensional.

Note that if $q|a^2$ then one could get examples of supersingular elliptic curves where the endomorphism ring gets bigger if one extends the ground field. For example if $a = 0$ and q is an odd power of p, then $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$ and in this case I guess we have a supersingular elliptic curve whose endomorphism ring over the ground field is just an order in an imaginary quadratic field.

Pendulums and Elliptic Curves

Recently, I read a paper on how to solve the equation of a moving pendulum! I didn't know that one could solve this equation! Probably it has been known since Newton or something. I tried to work out, how analogous calculation went when gravity was imaginary!

Consider a swinging pendulum. Let θ be the angle from the vertical to the pendulum. Gravity exerts a force of mg downwards. The pendulum shaft swallows up some of this force ($mg\cos(\theta)$) and what is left contributes to acceleration, and we deduce

$$\ell\ddot{\theta} = -g\sin(\theta)$$

Apparently, in the case where $g = \ell = 1$ (this is not actually in the paper, it said that one could replace t by λt and then every dot introduces a new factor of λ, so we can rescale) but let us not do this because it confuses me a bit (no intuition), let's set $K = -g/\ell$ and solve the equation,

$$\ddot{\theta} = K\sin\theta$$

We should remember that K is supposed to be a negative real number at this point. Multiply by $\dot{\theta}$ and integrate, getting

$$\frac{1}{2}\dot{\theta}^2 = -K\cos(\theta) + E$$

(which is just conservation of energy; E is something like energy divided by ml). In this real case, we'll also let $E \in \mathbb{R}$. Note that the left-hand side is always non-negative so we had better have $E \geq K$ (recall that $K < 0$) because otherwise the left hand side will always be negative whatever

the value of θ. Note also that the degenerate case $E = K$ has only the solution $\theta = \dot{\theta} = 0$, so we may as well assume $E > K$.

The trick now is to set $z = e^{i\theta}$. Then $\dot{z} = i\dot{\theta}z$ so the conservation of energy equation becomes

$$\frac{1}{2}\left(\frac{\dot{z}}{iz}\right)^2 = -K\left(\frac{z+z^{-1}}{2}\right) + E$$

and clearing denominators gives

$$\dot{z}^2 = Kz^3 + Kz - 2Ez^2$$

which shows that the pair $(z, \dot{z})$ lives on an elliptic curve over the reals. This hasn't solve the equation yet though, because the statement "$(z, \dot{z})$ lives on an elliptic curve" is simply the statement that energy is conserved. We'll come back to this equation in a minute when I've worked out what the Weierstrass $\mathcal{P}$-function is.

Weierstrass $\mathcal{P}$

Let Λ be a lattice in the complex numbers. Define

$$\mathcal{P}_\Lambda(z) = z^{(-2)} + \sum_{0\neq\lambda\in\Lambda}\left(\frac{1}{(z-\Lambda)^2} - \frac{1}{\lambda^2}\right)$$

Recall that $\mathcal{P}$ is periodic wrt Λ, is even, has a double pole at a point in Λ, and its derivative $\mathcal{P}'_\Lambda(z) = -2\sum_{\lambda\in\Lambda}(z-\lambda)^{-3}$ vanishes at points of $\frac{1}{2}\Lambda$ that aren't in Λ. $\mathcal{P}$ scales like this: $\mathcal{P}_{\alpha\Lambda}(\alpha z) = \alpha^{-2}\mathcal{P}_\Lambda(z)$.

For $k \geq 4$ even set $G_k(\Lambda) = \sum_{0\neq\lambda\in\Lambda}\lambda^{-k}$. The key equation is that if $Y = \mathcal{P}'_\Lambda(z)$ and $X = \mathcal{P}_\Lambda(z)$ then

$$Y^2 = 4X^3 - 60G_4(\Lambda)X - 140G_6(\Lambda)$$

Solving pendulums with Weierstrass $\mathcal{P}$

We know

$$\dot{z}^2 = Kz^3 + Kz - 2Ez^2$$

Let's first kill the coefficient of z^2 by replacing z by $Z = z - 2E/3K$ and we get

$$\dot{Z}^2 = KZ^3 + 0Z^2 + \cdots$$

Next we need to scale. Set $X = (K/4)Z$, so $\dot{X} = (K/4)\dot{Z}$ and substitute in and multiply by a constant. We get

$$\dot{X}^2 = 4X^3 + (K^4/4 - E^2/3)X + (EK^2/24 - E^3/27)$$

and of course the point is that this now looks awfully like the equation involving the $\mathcal{P}$-function.

The discriminant of the cubic had better be non-zero, because otherwise it has repeated roots and isn't an elliptic curve at all. Bashing it out, it turns out that we want to avoid the case $E^2 = K^2$. Because $E > K$ is assumed, it turns out that for the cubic to have distinct roots, we should hence assume $E \neq -K$. The physical reason this case is tricky is that if $E = -K$, then $\theta = \pi$ and $\dot{\theta} = 0$ is a solution to the equation, which corresponds to the pendulum sitting in the unstable equilibrium position, a case which we choose to avoid. Presumably, if we start else where then the pendulum slowly swings upto the unstable equilibrium point, corresponding to the solution to the equations going off to a cusp.

In fact one can now see the dichotomy. Recall $K < 0$ and $E > K$. If $E > -K$, then there is too much energy the system and it goes around and around,and this corresponds to the cubic having three distinct roots. If however $K < E < -K$, then $E^2 < K^2$ and $K + E < 0$, we'll never make it to the top,and the cubic has only one real root. I don't know quite what the significance of the number of real roots of the cubic is, but it clearly has some kind of physical meaning.

In any case, if we choose a lattice Λ with $-60G_4(\Lambda)$ and $-140G_6(\Lambda)$ being those real numbers in the coefficients of the cubic then we have a solution $X = \mathcal{P}_\Lambda(t + z_0)$ and $\dot{X} = \mathcal{P}'_\Lambda(t + z_0)$ for any $z_0 \in \mathbb{C}$. For this to have real physical meaning we would like $|z| = 1$ and this forces $|X + E/6| = |K|/4$ which will be true for some $X = \mathcal{P}_\Lambda(z_0) \in \mathbb{C}$ and these will be the meaningful initial conditions.

Now, finally we would like a mathematical explanation for the physically obvious fact that in every case apart from $E = -K$, the motion of the pendulumis periodic. This is because $G_4(\Lambda)$ and $G_6(\Lambda)$ are real, so the j-invariant of Λ is real, so Λ is homothetic to one of the form $\Lambda_\tau := \mathbb{Z} \oplus \mathbb{Z}\tau$ with τ in the upper-half plane and with real part either 0 or 1/2. In fact is it the case that the lattice is rectangular if and only if the real points of the curve are disconnected if and only if the cubic has three real roots if and only if there's enough energy in the system to get the pendulum to the top? This sounds like it might be right!

The complex case

The reason I let K stay, and indeed be < 0, was that I want to set $K = i$, but I think that all the formal algebra I did remains valid, and it's only comments about $E > K$ and the number of real roots that have to be changed/ignored. Note that if E is real then it seems to me that the curve is still defined over the reals and so again we'll get periodic motion.

If however E is complex, then the j-invariant of the curve could well be complex. The question now is that we are given explicit values for $G_4(\Lambda) = 1/120 + E^2/180$ and $G_6(\Lambda) = E/3360 + E^3/3780$ and we are wondering whether Λ contains any non-zero real numbers-this would correspond to periodicity or contains any numbers which are close to being real.