CHAPTER 24

Elliptic curves over finite fields

In this final chapter on elliptic curves, we take a brief dip into something much more arithmetic, counting the number (mod p) of solutions in $\mathbb{P}^2(\mathbb{F}_p)$ to the equations for the Hesse and Legendre cubics from the last chapter. These cubics still depend on t, which is taken to be an integer now (rather than a complex number) so that we can reduce modulo p. In a rather bizarre twist, the number of points (over $\mathbb{F}_p$) in each case is given by nearly the same power series as the holomorphic period on the corresponding complex family of elliptic curves from Chapter 23. We summarize one abstract way, due to Y. MANIN, to understand this connection between arithmetic and transcendental algebraic geometry. A brief discussion of the mod p group law and cryptography conclude the chapter.

24.1. Sum formulas

Let p be an odd prime, and $\mathbb{F}_p$ the field with p elements (i.e. $\mathbb{Z}/p\mathbb{Z}$ viewed as a ring). Equality in $\mathbb{F}_p$ will generally be denoted by "$=$", not "$\underset{(p)}{\equiv}$". (We will use the latter for counting points mod p.)

24.1.1. LEMMA. *For $k \in \mathbb{Z}$,*

$$\sum_{x\in\mathbb{F}_p\ (or\ \mathbb{F}_p^*)} x^k = \begin{cases} 0, & p-1 \nmid k \\ -1, & p-1 \mid k \end{cases}$$

in $\mathbb{F}_p$.

PROOF. Given $y \in \mathbb{F}_p^*$, the assignment $x \mapsto yx$ yields an isomorphism of additive groups $\mathbb{F}_p \to \mathbb{F}_p$. Therefore

$$y^k \sum_{x\in\mathbb{F}_p} x^k = \sum_{x\in\mathbb{F}_p} (xy)^k = \sum_{x\in\mathbb{F}_p} x^k. \tag{24.1.2}$$

Now, $\mathbb{F}_p^*$ is a cyclic (multiplicative) group of order $p-1$, and so

$$(\mathbb{F}_p^*)^k = \{1\} \iff p-1 \mid k.$$

Provided $p-1 \nmid k$, then, there exists $y \in \mathbb{F}_p^*$ with $y^k \neq 1$. By (24.1.2), we have

$$0 = (y^k - 1) \sum_{x \in \mathbb{F}_p} x^k$$

which implies (dividing by $y^k - 1$)

$$0 = \sum_{x \in \mathbb{F}_p} x^k.$$

On the other hand, if $p-1 \mid k$, then $x^k = 1$ for all $x \in \mathbb{F}_p^*$ and so

$$\sum_{x \in \mathbb{F}_p} x^k \ = \ \sum_{x \in \mathbb{F}_p^*} 1 \ = \ p-1 \ = \ -1. \qquad \square$$

24.1.3. LEMMA. *For $x \in \mathbb{F}_p$,*

$$\sum_{k=1}^{p-1} x^k = \begin{cases} 0, & x \neq 1 \\ -1, & x = 1 \end{cases}.$$

PROOF. If $x = 1$ then the sum is $\underbrace{1 + \cdots + 1}_{p-1 \text{ times}} = p - 1 = -1$. If $x \neq 1$ then

$$\begin{aligned} \underbrace{(1-x)}_{\neq 0} \sum_{k=1}^{p-1} x^k \ &= \ \sum_{k=1}^{p-1} x^k - \sum_{k=2}^{p} x^k \\ &= \ x - x^p \\ &= \ x(1 - x^{p-1}) \end{aligned}$$

which (since $\mathbb{F}_p^*$ is cyclic of order $p-1$)

$$= \ x(1-1) \ = \ 0. \qquad \square$$

24.1.4. LEMMA. *Let $\xi \in \mathbb{F}_p^*$. Then $\xi^{\frac{p-1}{2}} = \pm 1$, and*

$$\xi \in \mathbb{F}_p^2 \iff \xi^{\frac{p-1}{2}} = 1.$$

PROOF. Since $\mathbb{F}_p^*$ is cyclic of order $p-1$, $(\xi^{\frac{p-1}{2}})^2 = \xi^{p-1} = 1$. Moreover, if a is a generator then we cannot have $a^{\frac{p-1}{2}} = 1$ ($\mathbb{F}_p^*$ would then have order $\frac{p-1}{2}$, a contradiction). Hence $x \mapsto x^{\frac{p-1}{2}}$ yields a surjective homomorphism of multiplicative groups

$$\mathbb{F}_p^* \underset{\theta}{\twoheadrightarrow} \{+1, -1\},$$

whose kernel necessarily has order $\frac{1}{2}|\mathbb{F}_p^*| = \frac{p-1}{2}$. Now if $\xi = \eta^2$ is a square, then $\xi^{\frac{p-1}{2}} = \eta^{p-1} = 1$. As $\frac{p-1}{2}$ elements of $\mathbb{F}_p^*$ are squares (why?), these exhaust the kernel of θ and the non-square elements go to -1. □

24.2. Counting $\mathbb{F}_p$-points on the Legendre elliptic curve

Consider once again the Legendre family of cubics

$$E_t = \{Y^2 Z = X(X-Z)(X-tZ)\},$$

but this time with $t \in \mathbb{Z}$. After reducing mod p we can look at the solutions $E_t(\mathbb{F}_p) \subset E_t(\overline{\mathbb{F}_p})$, i.e. with X, Y, Z in $\mathbb{F}_p$ resp. its algebraic closure; there is a clear analogy to $E_t(\mathbb{Q}) \subset E_t(\bar{\mathbb{Q}})$.

We are going to compute the number of points $|E_t(\mathbb{F}_p)|$ modulo p, i.e. in $\mathbb{F}_p$. (Computing the number in $\mathbb{Z}$ is a much harder problem.) First we claim that

$$(24.2.1) \qquad |E_t(\mathbb{F}_p)| \;=\; 1 + \sum_{x \in \mathbb{F}_p} \left\{ 1 + [x(x-1)(x-t)]^{\frac{p-1}{2}} \right\}.$$

The leading "1" on the RHS counts the point $[0:0:1]$ "at ∞"; the rest of the curve is described by $y^2 = x(x-1)(x-t)$. By Lemma 24.1.4, the quantity in curly brackets yields (mod p) 2 if $x(x-1)(x-t)$ is a square, 1 if $x(x-1)(x-t) = 0$, and 0 if $x(x-1)(x-t)$ is not a square. This exactly counts pairs $(x, y) \in \mathbb{F}_p^2$ solving the affine equation, confirming (24.2.1).

Now $\sum_{x \in \mathbb{F}_p} 1 \underset{(p)}{\equiv} 0$, so the RHS of (24.2.1) is

$$\underset{(p)}{\equiv} \; 1 + \textstyle\sum_{x \in \mathbb{F}_p} x^{\frac{p-1}{2}} (x-1)^{\frac{p-1}{2}} (x-t)^{\frac{p-1}{2}}$$

$$\begin{aligned}
&= 1 + \sum_{x\in\mathbb{F}_p} x^{\frac{p-1}{2}} \left\{ \sum_{\ell=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\ell} x^{\frac{p-1}{2}-\ell}(-t)^{\ell} \right\} \left\{ \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} x^{k}(-1)^{\frac{p-1}{2}-k} \right\} \\
&= 1 + \sum_{x\in\mathbb{F}_p} x^{p-1} \left\{ \sum_{\ell=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\ell} x^{-\ell}(-t)^{\ell} \right\} \left\{ \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} x^{k}(-1)^{\frac{p-1}{2}-k} \right\}.
\end{aligned}$$

The sum here can be rewritten as $\sum_{x\in\mathbb{F}_p} x^{p-1}(\sum_{m=-\frac{p-1}{2}}^{\frac{p-1}{2}} a_m x^m)$, which by Lemma 24.1.1 is just $-a_0$ (mod p). So writing $[\cdot]_0$ for the constant term of a Laurent polynomial, the above

$$\begin{aligned}
&\underset{(p)}{\equiv}\ 1 - \left[\left\{ \sum_{\ell=0}^{\frac{p-1}{2}} \binom{(p-1)/2}{\ell} x^{-\ell}(-t)^{\ell} \right\} \left\{ \sum_{k=0}^{\frac{p-1}{2}} \binom{(p-1)/2}{k} x^{k}(-1)^{\frac{p-1}{2}-k} \right\} \right]_0 \\
&\qquad\qquad = 1 - \sum_{\ell=0}^{\frac{p-1}{2}} (-t)^{\ell}(-1)^{\frac{p-1}{2}-\ell} \binom{(p-1)/2}{\ell}^2 \\
&\qquad\qquad = 1 + (-1)^{\frac{p+1}{2}} \sum_{\ell=0}^{\frac{p-1}{2}} \binom{(p-1)/2}{\ell}^2 t^{\ell} \\
&\qquad\qquad = 1 + (-1)^{\frac{p+1}{2}} \sum_{\ell\geq 0} \binom{-1/2}{\ell}^2 t^{\ell} \\
&\qquad\qquad =: \hat{P}(t).
\end{aligned}$$

For the last step, we use the definition (in $\mathbb{F}_p$)

$$\binom{-1/2}{\ell} := \frac{-1/2 \cdot -3/2 \cdot \cdots \cdot (-1/2 - \ell + 1)}{\ell!},$$

which is evidently 0 when $p > \ell > \frac{p-1}{2}$ (since $\frac{-1}{2} - \frac{p+1}{2} + 1 = \frac{-1-p-1+2}{2} = \frac{p}{2} = 0$), and equals $\binom{\frac{p-1}{2}}{\ell}$ for $0 \leq \ell \leq \frac{p-1}{2}$ (and is *defined* to be 0 for $\ell \geq p$). We conclude:

24.2.2. PROPOSITION. *$\hat{P}(t)$ counts* (mod p) *the $\mathbb{F}_p$-points of E_t.*

Notice that

(24.2.3) $\hat{P}(t)$ is a "mod p" version of the period $P(t)$ from §23.6!

24.3. Counting $\mathbb{F}_p$-points on the Hesse cubic

For this section, take p to be an odd prime with $p \equiv -1 \bmod 3$.

I can't resist doing the same exercise for the other main example from the last chapter, namely

$$E_t = \{XYZ = t(X^3 + Y^3 + Z^3)\}$$

where again we assume $t \in \mathbb{Z}$, but not divisible by p. This has affine form

$$xy = t(x^3 + y^3 + 1)$$

and toric form

$$1 = t\underbrace{(x^2y^{-1} + x^{-1}y^2 + x^{-1}y^{-1})}_{=:\varphi(x,y)},$$

where the Laurent polynomial $\varphi(x,y)$ is defined for $(x,y) \in (\mathbb{F}_p^*)^2$. Using the toric form and Lemma 24.1.3, it is easy to compute the $\mathbb{F}_p^*$-points

$$E_t^*(\mathbb{F}_p) := E_t(\mathbb{F}_p) \cap (\mathbb{F}_p^*)^2.$$

Namely, we have

$$|E_t^*(\mathbb{F}_p)| \underset{(p)}{\equiv} -\sum_{(x,y)\in(\mathbb{F}_p^*)^2} \sum_{k=1}^{p-1} t^k \left(\varphi(x,y)\right)^k,$$

the point being (besides the Lemma) that $t\varphi(x,y)$ is 1 (in $\mathbb{F}_p$) for exactly those (x,y) on E_t. Switching the order of summation this becomes

$$= -\sum_{k=1}^{p-1} t^k \sum_{(x,y)\in(\mathbb{F}_p^*)^2} \varphi(x,y)^k. \tag{24.3.1}$$

Now by Lemma 24.1.1

$$\sum_{(x,y)\in(\mathbb{F}_p^*)^2} x^i y^j = \left(\sum_{x\in\mathbb{F}_p^*} x^i\right)\left(\sum_{y\in\mathbb{F}_p^*} y^j\right) = \left\{\begin{array}{ll} 1, & p-1 \mid i,j \\ 0, & \text{otherwise} \end{array}\right. .$$

For $k \in [1, p-2]$,

$$(\varphi(x,y))^k = [\varphi^k]_0 + \left\{ \begin{array}{c} \text{terms with powers of } x, y \\ \text{not both divisible by } p-1 \end{array} \right\}.$$

Our assumption on p implies that $3 \nmid p-1$, and so

$$(\varphi(x,y))^{p-1} = [\varphi^{p-1}]_0 + x^{2(p-1)}y^{-(p-1)} + x^{-(p-1)}y^{2(p-1)}$$
$$+ x^{-(p-1)}y^{-(p-1)} + \left\{ \begin{array}{c} \text{terms with powers of } x, y \\ \text{not both divisible by } p-1 \end{array} \right\}.$$

(In particular, there are no $x^{-(p-1)}, y^{-(p-1)}, x^{p-1}y^{-(p-1)}, x^{-(p-1)}y^{p-1}$, x^{p-1} or y^{p-1} terms.) So (24.3.1) becomes

$$\underset{(p)}{\equiv} -\sum_{k=1}^{p-1} t^k [\varphi^k]_0 \; - \; t^{p-1} \cdot 3.$$

Recall from §23.2 that $[\varphi^k]_0 = \binom{3m}{m,m,m}$ if $k = 3m$ (and 0 if $3 \nmid k$).

On the other hand, looking along the coordinate axes $X = 0$, $Y = 0$, $Z = 0$ we get (only) the points

$$[1 : -1 : 0], \;\; [0 : 1 : -1], \;\; [-1 : 0 : 1]$$

in $E_t(\mathbb{F}_p)$. For example, along $Z = 0$ (on E_t) we must have $X, Y \neq 0$ and so may assume $Y = 1$; then the equation is $X^3 + 1 = 0$. This has only $X = -1$ as solution: otherwise we would have an element of order 6 in $\mathbb{F}_p^*$, so $6 \mid p-1$, contradicting our assumption on p.

We conclude that[1]

$$|E_t(\mathbb{F}_p)| \underset{(p)}{\equiv} 3(1 - t^{p-1}) - \sum_{m=1}^{\left\lfloor \frac{p-1}{3} \right\rfloor} \binom{3m}{m,m,m} t^{3m} \underset{(p)}{\equiv} -\sum_{m \geq 1} \binom{3m}{m,m,m} t^{3m},$$

again very reminiscent of the $P(t)$ from (23.2.1)!

24.4. Deep reasons for (24.2.3)

With two examples to support it, this amazing relationship between periods and point-counts can't be a coincidence. I am going

[1] again with the convention that the multinomial symbol is zero for $m \geq p$ (and the observation that it *is* zero for $\frac{p-1}{3} < m < p$).

to explain why it happens in the first example, though the second one is quite similar.

The issue is this: in §23.2, why on earth does $|E_t(\mathbb{F}_p)| - 1$ (not counting the point at ∞) appear to solve the Picard-Fuchs equation $\left(t(t-1)D_t^2 + (2t-1)D_t + \frac{1}{4}\right)(\cdot) = 0$? Indeed, $\hat{P}(t) - 1 = \frac{\pm 1}{2\pi} P(t)$, where $P(t)$ is the solution from §23.6!! The two computations were quite elementary, after all, so maybe there's an elementary explanation for their equivalence?

Not so! This is dealt with in [Clemens, "A scrapbook of complex curve theory," pp. 65-69] and I'll just give a hint of the flavor here. It involves an algebro-geometric version of the Lefschetz trace formula (the formula from topology for the number of fixed points of a mapping), the Riemann-Roch theorem, Serre duality, and abstract sheaf theory. However, it isn't hard to summarize.

Consider E_t over $\overline{\mathbb{F}_p}$, $t \in \mathbb{F}_p$. Then writing FP for "number of fixed points", and $frob_p$ for the map $[Z:X:Y] \mapsto [Z^p : X^p : Y^p]$,

$$|E_t(\mathbb{F}_p)| \;=\; \mathrm{FP}\left\{frob_p : E_t(\overline{\mathbb{F}_p}) \to E_t(\overline{\mathbb{F}_p})\right\}.$$

This should make sense to you because as an automorphism of $\overline{\mathbb{F}_p}$, the p^{th}-power (Frobenius) map fixes exactly the elements of $\mathbb{F}_p$. By the Lefschetz-type theorem, it turns out that this

$$\underset{(p)}{\equiv}\; 1 - \mathrm{trace}\left\{ frob_p^*|_{H^1(E_t/\overline{\mathbb{F}_p}, \mathcal{O})} \right\}$$

where the H^1 is sheaf cohomology computed with respect to the Zariski topology, $\mathcal{O}$ is the sheaf of regular functions, and $frob^*$ is the action by pullback (under $frob_p$) on cohomology classes.

This H^1 is a 1-dimensional vector space, with generator represented by a certain rational function h with two simple poles, at $q = [1:0:0]$ and some other point $p \in E_t(\mathbb{F}_p)$. More precisely, $H^1(E_t/\overline{\mathbb{F}_p}, \mathcal{O})$ is isomorphic to the space of rational functions on E_t with poles allowed only at P and Q modulo the subspace of rational functions with poles allowed at *either P or Q* (not both).[2] You should

[2] That this space is 1-dimensional in the more familiar *complex* case is Exercise (2).

also note that pulling back by $frob_p$ stabilizes the vector space we have just described, since (as P, Q are taken to be in $E_t(\mathbb{F}_p)$ rather than $E_t(\overline{\mathbb{F}_p})$) P and Q are fixed under $frob_p$. So the displayed expression at least makes sense.

Next, we expand h in formal power series $h = \frac{1}{y} + \sum_{\ell \geq 0} b_\ell y^\ell$ about q,[3] and also expand a generator $\omega_t \in \Omega^1(E_t/\overline{\mathbb{F}_p})$ (regular differentials) as $[\sum_{k\geq 1} a_k(t) y^{k-1}]dy$, where $a_1(t) = 1$. Recall also from the complex case, that residues of meromorphic functions require, and depend on, a choice of local coordinate; while residues of meromorphic 1-forms are invariant (i.e. require no such choice, as they can already be integrated around a loop without appending a "dz"). So for functions F with a pole at Q, we take residue by computing $Res_q(F\omega)$; if F has no *other* pole, then (as residues sum to zero) the residue has to be zero.

Now, writing τ for the trace of $frob_p^*$ above, we have

$$frob_p^* h \; (= h \circ frob_p) = \tfrac{1}{y^p} + \textstyle\sum_{\ell\geq 0} b_\ell y^{\ell p} = \tau h + f + g.$$

(The last equality, in which f has only a pole at q and g has only a pole at P, is by 1-dimensionality of $H^1(E_t, \mathcal{O})$ and the "explicit description" we gave of it. In that vector space, this reads $frob^*[h] = \tau[h]$.) Moreover, $Res_Q(h\omega_t) = 1$ while

$$\begin{aligned} \tau &= \tau Res_Q(h\omega_t) + Res_Q(f\omega_t) + Res_Q(g\omega_t) \\ &= Res_Q((frob_p^* h) \cdot \omega_t) \\ &= a_p(t), \end{aligned}$$

with the last equality obtained by multiplying out the explicit expressions for $frob_p^* h$ and ω_t. So we end up with

$$|E_t(\mathbb{F}_p)| \underset{(p)}{\equiv} 1 - a_p(t),$$

and (like the periods of ω_t) $a_p(t)$ must satisfy the Picard-Fuchs equation because $[\omega_t]$ does. Again, the "regular" solution of $D_{\mathrm{PF}}(\cdot) = 0$ is unique up to scale, and from there we are essentially done.

[3] Note that y gives a local coordinate about $[1:0:0]$ on E_t; x does not.

In general, a matrix for the transformation $frob_p^* \in \mathrm{End}(H^1(C, \mathcal{O}))$ (for a projective curve $C/\mathbb{F}_p$) is called a *Hasse-Witt matrix*; for C elliptic, this is 1×1 and just the τ above. This generalizes to higher dimension, and its relation to point-counting and periods for Calabi-Yau varieties has been the subject of much recent research. The elliptic curve cases above are also related to modular forms: for fixed t, the a_p's reappear as (the mod p reductions of) the p^{th} coefficients of cusp forms, or (by a beautiful equivalence) as eigenvalues of Hecke operators.

24.5. The group law on $E(\mathbb{F}_p)$

Let $E \subset \mathbb{P}^2$ be defined by

$$F(Z, X, Y) := Y^2 Z - (X^3 + AXZ^2 + BZ^3) = 0,$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \underset{(p)}{\not\equiv} 0$ (p an odd prime). Then E has "good reduction" mod p — that is, it is nonsingular over $\mathbb{F}_p$. If we define the operation "$+$" on $E(\mathbb{F}_p)$ as in §20.1, the proof of associativity in §20.3 (which still made use of the topology of $E(\mathbb{C})$ via the argument from §15.2) is no longer applicable as $\mathbb{F}_p$ is not a subfield of $\mathbb{C}$. This is easy to overcome by using the Cayley-Bacharach Theorem from §15.1, see Exercise (3) below.

24.5.1. REMARK. Given $[a{:}b{:}c] \in E(\mathbb{Q})$, one can scale a, b, c to be relatively prime integers and reduce mod p to get an element of $E(\mathbb{F}_p)$. While this produces a group homomorphism, it is not usually surjective. So we really do need a different explanation of associativity for $E(\mathbb{F}_p)$.

Because one can scale projective coordinates, $\mathbb{Z}$-points and $\mathbb{Q}$-points on a *projective* curve are the same thing. But on the *affine curve* $y^2 = x^3 + Ax + B$, by "$\mathbb{Z}$-points" one usually means that $x, y \in \mathbb{Z}$. If one *defines* $E(\mathbb{Z})$ to mean *affine integral* points together with $\mathcal{O}$, the result is usually not closed under "$+$" (why?) but does contain the torsion subgroup of $E(\mathbb{Q})$ by a theorem of Nagell and Lutz.

By the same arguments as in §20.4, one obtains the formulas

$$(24.5.2)\quad \begin{cases} x_{P+Q} = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q, & y_{P+Q} = -\left(\frac{y_Q - y_P}{x_Q - x_P}\right)(x_{P+Q} - x_P) - y_P \\ x_{2P} = \left(\frac{3x_P^2 + A}{2y_P}\right)^2 - 2x_P, & y_{2P} = -\left(\frac{3x_P^2 + A}{2y_P}\right)(x_{2P} - x_P) - y_P \end{cases}$$

relating affine coordinates of P, Q, and $P+Q$ (in $E(\mathbb{F}_p)$). Exactly as at the beginning of §24.2, we have the point-count formula[4]

$$(24.5.3)\quad |E(\mathbb{F}_p)| = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right) \underset{(p)}{\equiv} 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right).$$

The *Hasse bound* (which we won't prove) gives the related estimate

$$(24.5.4)\qquad \big||E(\mathbb{F}_p)| - p - 1\big| \leq 2\sqrt{p}$$

24.5.5. EXAMPLE. Let E have affine equation $y^2 = x^3 - 2x - 3$ over $\mathbb{F}_7$, and consider $P := (3,2)$. By (24.5.2), $2P = (2,6)$, $3P = 2P + P = (4,2)$, $4P = (0,5)$, $5P = (5,0)$, $6P = (0,2)$, $7P = (4,5)$, $8P = (2,1)$, $9P = (3,5)$, and $10P = (3,2) + (3,5) = \mathcal{O}$. This gives a cyclic subgroup of order 10 in $E(\mathbb{F}_7)$.

There are two ways to check that these are all the points and $E(\mathbb{F}_7) \cong \mathbb{Z}/10\mathbb{Z}$: use (24.5.3) or (24.5.4). For instance, the Hasse bound is $3 \leq |E(\mathbb{F}_7)| \leq 13$, while Lagrange's theorem from group theory gives $10\big||E(\mathbb{F}_7)|$.

24.5.6. EXAMPLE. Consider $y^2 = x^3 - x$ over $\mathbb{F}_{71}$. Since $x^3 - x$ is an odd function, and $(\frac{-a}{71}) = -(\frac{a}{71})$ (as -1 isn't a square mod 71), the sum in (24.5.3) cancels out, and $|E(\mathbb{F}_{71})| = 72 = 8 \cdot 9$. Let $E_2 := \{P \in E(\mathbb{F}_{71}) \mid 8P = \mathcal{O}\}$ and $E_3 := \{Q \in E(\mathbb{F}_{71}) \mid 9Q = \mathcal{O}\}$. Basic structure theory of abelian groups tells us that $E(\mathbb{F}_{71}) = E_2 \times E_3$. As they are abelian, there are three possibilities for E_2 and two for E_3; to determine them see Exercise (4).

[4] Here $(\frac{a}{p})$ is the *Legendre symbol*, which is 1 if a is a nonzero square mod p, 0 if $p \mid a$, and -1 if a is not a square mod p; it is computed by $a^{\frac{p-1}{2}}$ (in $\mathbb{F}_p$) hence satisfies $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

24.6. Elliptic cryptosystems

Given $P, Q \in E(\mathbb{F}_p)$, with $Q \in \langle P \rangle$ (the group generated by P), and $N := |\langle P \rangle|$, there exists a unique solution $n =: \log_P(Q) \in \mathbb{Z}/N\mathbb{Z}$ to $nP = Q$. We may think of this *elliptic discrete logarithm* (EDL) as defining an isomorphism

$$\log_P \colon \langle P \rangle \to \mathbb{Z}/N\mathbb{Z} \tag{24.6.1}$$

of groups. The terminology comes from the analogy between $E(\mathbb{F}_p)$ and the (multiplicative) group $(\mathbb{Z}/p\mathbb{Z})^*$.

While (24.6.1) is (without a quantum computer) very difficult to compute for large p, its inverse is not. To compute nP quickly — in time proportional to $\log_2 p$ — we may use "double-and-add", writing n in binary as as $n_0 + n_1 2 + \cdots + n_r 2^r$ ($n_i = 0$ or 1) and nP as $n_0 P + n_1(2P) + n_2 2(2P) + \cdots + n_r 2(2^{r-1}P)$. The *elliptic El Gamal cryptosystem* gives a simple example of how one can take advantage of this to provide secure communications over a public channel:

- Sender and Receiver agree publically on a prime p, elliptic curve E, and $P \in E(\mathbb{F}_p)$.
- Receiver chooses a *private key* $n \in \mathbb{Z}$, computes and sends the *public key* $Q := nP$ to Sender.
- Sender wants to send a message $M \in E(\mathbb{F}_p)$. To do this, they choose a (private) *ephemeral key* $k \in \mathbb{Z}$, and compute/send the *ciphertext* $(C_1, C_2) := (kP, M + kQ)$ to Receiver.
- Receiver decrypts the ciphertext, by computing $C_2 - nC_1 = M + kQ - nkP = M + knP - nkP = M$.

It turns out that while the difficulty of the ordinary discrete log problem (in $(\mathbb{Z}/p\mathbb{Z})^*$) grows "sub-exponentially" in $\log_2(p)$, that of computing the EDL grows exponentially (like $\sqrt{p}$). Roughly speaking, implementing the above scheme with 50 digit numbers for p, A, and B will give security equivalent to 200 digits in the "ordinary" equivalent, with much greater efficiency.

24.6.2. REMARK. What is a "message in $E(\mathbb{F}_p)$"? One can imagine converting a message into a number in $\mathbb{F}_p$, but this may not be (say) the x-coordinate of a point in $E(\mathbb{F}_p)$. A way around this defect is suggested in Exercise (6).

Exercises

(1) Check that $E_t(\overline{\mathbb{F}_p})$ is closed under $frob_p$, for E_t as in §24.4 and $t \in \mathbb{F}_p$.

(2) Let $E \subset \mathbb{P}^2$ be a smooth cubic over the complex numbers, and $p, q \in E(\mathbb{C})$ two distinct points. Let V be the vector space of meromorphic functions on E with poles only at p and q, with subspaces W_p and W_q (the meromorphic functions with poles only at p and q respectively). Using Abel's theorem, prove that the dimension of $V/(W_p + W_q)$ is one. [Hint: you will also need to use the fact that $\omega \in \Omega^1(E)$ has no zeroes, and that the "residues" of $F \in V$ given by $Res_p(F\omega)$ and $Res_q(F\omega)$ must sum to zero (cf. Prop. 13.1.10(b)).]

(3) Use Cayley-Bacharach to prove associativity for $(E(\mathbb{F}_p), +)$. [Hint: You need to show that P, $Q + R$, and $(P + Q) * R$ are collinear. Take C, D, E in Th. 15.1.2 to be $L_{PQ} \cup L_{Q*R,\mathcal{O}} \cup L_{P*Q,R}$, E, and L_{QR} respectively; this will produce a quadric $\mathcal{Q}$. Then consider the intersection of $L_{P*Q,\mathcal{O}}$ and $\mathcal{Q}$.]

(4) Determine E_2 and E_3 in Example 24.5.6 as follows: (a) for E_2, count the 2-torsion points in $E(\mathbb{F}_{71})$ and the 2-torsion elements in the 3 abelian groups of order 8. (b) For E_3, compute the (affine equation for the) Hessian curve of $y^2 = x^3 - x$, and use this to bound the number of 3-torsion points of $E(\mathbb{F}_{71})$.

(5) With E given by $y^2 = x^3 - x$, find the group structure of $E(\mathbb{F}_5)$ and $E(\mathbb{F}_{11})$.

(6) Modify the encryption-decryption scheme (last 2 steps) in the elliptic El Gamal system of §24.6 as follows: Sender has a message $(m_1, m_2) \in \mathbb{F}_p \times \mathbb{F}_p$ and sends the ciphertext $(R, (c_1, c_2)) := (kP, (x_{kQ}c_1, y_{kQ}c_2))$. As Receiver, use $T = nR = (x_T, y_T)$ to decrypt the message (how?).