LECTURE 8, WEDNESDAY 03.03.04

FRANZ LEMMERMEYER

1. Group Laws on Elliptic Curves

Let $P * Q$ denote the third point of intersection of the line PQ with the elliptic curve E.

Proposition 1. *For points $O, P, Q, R \in E(K)$ we have*

(1) $P * Q = Q * P$;
(2) $P * (P * Q) = Q$;
(3) $((P * Q) * O) * R = ((Q * R) * O) * P$.

The first two properties are trivial, the third one is deep. Note that $*$ is not associative: for $R = P * P$, associativity would imply $R * Q = (P * P) * Q = P * (P * Q) = Q$ for any Q, that is, $P * P = R = (R * Q) * Q = Q * Q$ for any pair of points P, Q on E.

A different formulation of the last property is the following:

(4) $(A * B) * (C * D) = (A * C) * (B * D)$ for A, B, C, D on E.

In fact, assume this identity holds; putting $A = O$, $B = P * Q$, $C = Q * R$ and $D = Q$ we get $((P*Q)*O)*R = ((Q*R)*O)*P$. Conversely, if $((P*Q)*O)*R = ((Q * R) * O) * P$, then put $O = A$, $P = B * D$, $Q = D$, and $R = C * D$.

Proposition 2. *Fix any point $\mathcal{O}$ on the elliptic curve. Then $P + Q = (P * Q) * \mathcal{O}$ and $-P = P * (\mathcal{O} * \mathcal{O})$ define an abelian group law on E with neutral element $\mathcal{O}$.*

Proof. We have

$$\begin{aligned}
P + Q &= (P * Q) * \mathcal{O} = (Q * P) * \mathcal{O} = Q + P,\\
P + \mathcal{O} &= (P * \mathcal{O}) * \mathcal{O} = P,\\
P + (-P) &= (P * (-P)) * \mathcal{O} = (P * (P * (\mathcal{O} * \mathcal{O}))) * \mathcal{O} = (\mathcal{O} * \mathcal{O}) * \mathcal{O} = \mathcal{O},\\
(P + Q) + R &= (((P * Q) * \mathcal{O}) * R) * \mathcal{O} = (((Q * R) * \mathcal{O}) * P) * \mathcal{O}\\
&= (Q + R) + P = P + (Q + R).
\end{aligned}$$

This proves our claims. □

The group law simplifies a little bit if we take a flex as $\mathcal{O}$ (this is a point for which $\mathcal{O} * \mathcal{O} = \mathcal{O}$, i.e., where the tangent intersects the curve with multiplicity 3), because then $-P = P * \mathcal{O}$, which implies that $P + Q + R = \mathcal{O}$ if and only if P, Q, R are collinear. In fact:

- Assume that P, Q, R are collinear; then $P * Q = R$, hence $-R = R * \mathcal{O} = (P * Q) * \mathcal{O} = P + Q$.
- Assume that $P + Q + R = 0$; then $-R = P + Q$, hence $R * \mathcal{O} = (P * Q) * \mathcal{O}$ and thus $R = P * Q$.

2. Conics over Finite Fields

Consider the affine hyperbola $\mathcal{H} : xy = 1$ over the finite field $\mathbb{F}_q$ with $q = p^f$ elements. Clearly for every nonzero $x \in \mathbb{F}_p^\times$ there is a unique y such that $(x, y) \in \mathcal{H}(\mathbb{F}_p)$, hence $\#\mathcal{H}(\mathbb{F}_q) = q - 1$. What is the group structure of $\mathcal{H}(\mathbb{F}_q)$? From the homework we know that $\mathcal{H}(\mathbb{F}_q) \simeq \mathbb{F}_q^\times$, and since the multiplicative group of a finite field is cyclic, we get

Proposition 3. *Consider $\mathcal{H} : xy = 1$ over the finite field $\mathbb{F}_q$. Then*

$$\mathcal{H}(\mathbb{F}_q) \simeq \mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}.$$

Next consider the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 1$ (with *Delta* an integer) over finite fields $\mathbb{F}_q$ of odd characteristic p.

If $\Delta = \delta^2$ is a square in $\mathbb{F}_q$, then the Pell conic can be written as $(X - \delta Y)(X + \delta Y) = 1$, and the coordinate transformation $\xi = X - \delta Y$, $\eta = X + \delta Y$ turns this into the standard hyperbola $\xi\eta = 1$. Since the neutral element $N = (1, 0)$ on $\mathcal{C}$ transforms into the neutral element $(\xi, \eta) = (1, 0)$ on the hyperbola, the transformation is a group homomorphisms, and we have $\mathcal{C}(\mathbb{F}_q) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ if Δ is a square in $\mathbb{F}_q$, in particular whenever $q = p^f$ with f even.

If Δ is not a square in $\mathbb{F}_q$ (this implies that $q = p^f$ for some odd f), then $K = \mathbb{F}_q(\sqrt{\Delta})$ is a quadratic extension of $\mathbb{F}_q$. We now imitate the isomorphism $\phi : \mathcal{C}(\mathbb{Z}) \longrightarrow \mathcal{O}_K^\times$ from the last lecture and define

$$\phi : \mathcal{C}(\mathbb{F}_q) \longrightarrow K^\times : (x, y) \longmapsto x + y\sqrt{\Delta}.$$

This is easily seen to be an injective group homomorphism. An element of im ϕ has the property $N(x + y\sqrt{\Delta}) = x^2 - \Delta y^2 = 1$, so if we denote the kernel of the norm map $N : K \longrightarrow \mathbb{F}_q$ by $K[N]$, then clearly im $\phi = K[N]$. But since $K[N]$ is a subgroup of the cyclic group $K^\times$, we conclude that $K[N]$ and therefore $\mathcal{C}(\mathbb{F}_q)$ is cyclic, too.

Let us now count the number of elements in $K[N]$. We claim that the norm map on finite fields is surjective. To prove this we observe that $(x + y\sqrt{\Delta})^q = x - y\sqrt{q}$: in fact, the Frobenius automorphism $x \longmapsto x^q$ fixes every element in the base field $\mathbb{F}_q$; moreover,

$$\sqrt{\Delta}^{q-1} = \Delta^{\frac{p-1}{2}\cdot(1+p+\ldots+p^{f-1})} = (-1)^{(1+p+\ldots+p^{f-1})} = -1$$

by Euler's criterion since Δ is a nonsquare in $\mathbb{F}_p$ and f is odd. This shows that the norm of $\alpha = x + y\sqrt{\Delta}$ can be written as $N\alpha = \alpha^{1+q}$. The kernel of the norm $N : K^\times \longrightarrow \mathbb{F}_q^\times$ is the group of all $\alpha \in K^\times$ with $\alpha^{1+q} = 1$, that is, the set of roots of the polynomial $X^{1+q} - 1$. Over fields, a polynomial of degree $1 + q$ can have at most $1 + q$ roots, hence $\#\ker N \le 1 + q$. On the other hand, the image has at most as many elements as $\mathbb{F}_q^\times$, namely $q - 1$. Finally, we have $\mathbb{F}_q^\times / \ker N \simeq \text{im } N$; the left hand side has at least $\frac{q^2-1}{q+1} = q - 1$ elements, the right hand side at most that many. Thus we have equality, and the same proof works for general extensions of finite fields:

Proposition 4. *Let E/F be an extension of finite fields. Then the norm map $N : E^\times \longrightarrow F^\times$ (in the sense of Galois theory: the norm is the product of all conjugates) is surjective.*

In particular we have shown

Proposition 5. *Consider a Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 1$ over a finite field $\mathbb{F}_q$ in which Δ is not a square. Then*

$$\mathcal{C}(\mathbb{F}_q) \simeq \mathbb{Z}/(q+1)\mathbb{Z};$$

in fact, $\mathcal{C}(\mathbb{F}_q)$ is isomorphic to the subgroup of elements of norm 1 in the quadratic extension $K = \mathbb{F}_q(\sqrt{\Delta}\,)$.

3. Conics over $\mathbb{Z}/m\mathbb{Z}$

Now that we know the structure of the groups $\mathcal{C}(\mathbb{F}_q)$ (at least for $p \nmid \Delta$), what about $\mathcal{C}(\mathbb{Z}/m\mathbb{Z})$? Here we have the following general result:

Proposition 6. *If $\mathcal{C} : X^2 - \Delta Y^2 = 1$ is a conic defined over rings R and S with neutral elements $(1,0)$, and if $f : R \longrightarrow S$ is a ring homomorphism, then $f_*(x,y) = (f(x), f(y))$ induces a group homomorphism $f_* : \mathcal{C}(R) \longrightarrow \mathcal{C}(S)$. If f is injective (bijective), then so is f_*.*

Proof. The proof that f_* is a ring homomorphism is a formal exercise. Now assume that f is injective, i.e. $\ker f = \{0\}$. This implies that $f : R^\times \longrightarrow S^\times$ is injective. If $(x,y) \in \ker f_*$, then $f(x) = 0$ and $f(y) = 1$, hence $x = 0$ and $y = 1$ since f is injective.

Now assume that f is bijective and let $g : S \longrightarrow R$ be its inverse map. Then f_* and g_* are inverse maps of each other, hence f_* is bijective, too. □

Observe that surjective ring homomorphisms $f : R \longrightarrow S$ do not necessarily induce surjective group homomorphisms $f_* : \mathcal{C}(R) \longrightarrow \mathcal{C}(S)$, as the example $f : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ shows.

In particular, the Chinese Remainder Theorem applies to conics in the sense that

$$\mathcal{C}(\mathbb{Z}/m\mathbb{Z}) \simeq \prod_i \mathcal{C}(\mathbb{Z}/p^{a_i}\mathbb{Z})$$

whenever $m = \prod_i p^{a_i}$, that is, if

$$\mathbb{Z}/m\mathbb{Z} \simeq \prod_i \mathbb{Z}/p^{a_i}\mathbb{Z}.$$

We have proved

Proposition 7. *Let $\mathcal{C} : X^2 - \Delta Y^2 = 1$ be a Pell conic, and let $R = \mathbb{Z}/m\mathbb{Z}$ for some odd integer $m = \prod_i p^{a_i}$ coprime to Δ. Then $\mathcal{C}(R) \simeq \prod \mathcal{C}(p_i^{a_i})$.*

This takes care of $\mathcal{C}(\mathbb{Z}/m\mathbb{Z})$ for squarefree m coprime to 2Δ. We will deal with the general case when we get to p-adic numbers; now, let us discuss a few applications of these results.

4. Factorization Algorithms

In this section we will see that there are more things you can do with a good supply of finite groups than with a drunken sailor. Let us start with factorization methods.

Pollard's p-1 Method. The following method was dreamed up by Pollard in 1974. Suppose we are given a number N we want to factor; assume for now that we already know a prime factor p of N. By Fermat's Little Theorem, we have $a^{p-1} \equiv 1 \bmod p$ for any a coprime to p. Thus we could recover p from $\gcd(N, a^{p-1}-1)$ except when the other factors of N also happen to divide $a^{p-1}-1$, which is not very likely. The problem is, of course, that we do not know the exponent $p-1$; the good news is that we only need some multiple of $p-1$: whenever $n \equiv 0 \bmod p-1$, we have $p \mid \gcd(N, a^n - 1)$.

Suppose our p has the property that $p-1$ only has small prime factors, say $< B$ for some bound B (in practice, B can be 10^5 or, if you have lots of fast computers, even higher). Then compute

$$n = \prod q^{a(q)+1}, \quad \text{where} q^a(q) < B \le q^{a(q)+1},$$

and the product is over all primes.

For example, if $B = 5$, we take

$$n = 2^3 \cdot 3^2 \cdot 5.$$

In order that n have a good chance of being a multiple of $p-1$, it be divisible by all small primes, and the smaller primes should appear with a larger exponent. The choice $n = B!$ would also be ok (the best possible choice is the one that minimizes the expected runnning time; this requires a careful complexity analysis and lots of experiments).

As an example, consider the integer $N = 377$; pick $a = 2$ (why not?) and compute $\gcd(N, 2^n - 1)$. Note that it is sufficient to compute $2^n \bmod N$ (otherwise this method would be horribly slow). Now $2^n = 2^{360} \equiv 339 \bmod 377$, and $\gcd(377, 338) = 13$. Note that $13 - 1 = 2^2 \cdot 3 \mid n$, whereas the other factor 29 satisfies $29 - 1 = 2^2 \cdot 7$.

In practice, you can test $\gcd(N, a^k - 1)$ for $k = 2^{a(2)}$, $k = 2^{a(2)} \cdot 3^{a(3)}$, $k = 2^{a(2)} \cdot 3^{a(3)} \cdot 5^{a(5)}$ etc. If $a^n \equiv 1 \bmod N$, the gcd calculation will yield the trivial factor N, and you should replace the bound B by some smaller integer.