MATH 6370, LECTURE 11
ELLIPTIC CURVES
APRIL 10

GORDAN SAVIN

Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. Then the quotient $E = \mathbb{C}/L$ is a compact Riemann surface.

$$\mathfrak{p}(z) = \frac{1}{z^2} + \sum_{\omega \in L\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Then $\mathfrak{p}(z)$ is L-periodic meromorphic function, and $z \mapsto (\mathfrak{p}(z), \mathfrak{p}'(z))$ is a bijection from $\mathbb{C}/L$ and the cubic curve

$$y^2 = 4x^3 - g_2(L)x - g_3(L)$$

where

$$g_n(L) = \sum_{\omega \in L\setminus\{0\}} \left(\frac{1}{\omega^{2n}} \right).$$

Since $\mathfrak{p}$ and $\mathfrak{p}'$ have poles at $z = 0$, $0 \in \mathbb{C}/L$ maps to a point O at "infinity" obtained by compactifying the cubic curve in the projective plane. If $L' = c \cdot L$, for some $c \in \mathbb{C}^\times$, then $\mathbb{C}/L \cong \mathbb{C}/L'$. Observe that $g_n(L) = c^{2n} g_n(L')$. We shall be interested in the case where L is a multiple of $\mathbb{Z}[i]$. Then $i \cdot L = L$, hence

$$g_3(L) = g_3(i\dot{L}) = i^6 g_3(L) = -g_3(L)$$

which implies that $g_3(L) = 0$. Moreover, one can pick L so that $g_2(L) = 1$. Hence the Riemann surface $\mathbb{C}/\mathbb{Z}[i]$ is isomorphic to the cubic curve $y^2 = 4x^3 - x$. For practical reasons we shall rewrite this equation slightly. Multiply it by 2 and redefine $x := 2x$. This gives the curve

$$2y^2 = x^3 - x.$$

Observe that $E = \mathbb{C}/L$ is an abelian group. Let $E(m)$ be the m-torsion, that is the set of elements $z \in E$ such that $mz = 0$. This is a subgroup of E, clearly,

$$E(m) = \frac{1}{m}L/L \cong L/mL \cong (\mathbb{Z}/m\mathbb{Z})^2$$

where the middle isomorphism is given by multiplication by m, while the last depends on a choice of a basis of L. Fix a prime p. Then we have an inverse system

$$L/pL \leftarrow L/p^2L \leftarrow \ldots.$$

whose inverse limit

$$\lim_{\leftarrow} L/p^nL \cong \mathbb{Z}_p^2$$

is called the Tate module attached to E. Let $\mathrm{End}(E)$ be the set of endomorphisms of E, that is, the set of group homomorphisms $T : E \to E$. The set of endomorphism forms a ring, since endomorphisms can be added and composed. FIx a prime p. For every n, T induces a homomorphism $T_n : E(p^n) \to E(p^n)$. After identifying $E(p^n) \cong (\mathbb{Z}/p^n\mathbb{Z})^2$, the homomorphism T_n is represented by a 2×2 matrix with coefficients in the ring $\mathbb{Z}/p^n\mathbb{Z}$. These T_n are compatible with the maps $E(p^n) \to E(p^{n-1})$ and patch together to give a 2×2 matrix with coeffcients in $\mathbb{Z}_p$ giving the action of T on the Tate module. Thus for every p we have a ring homomorphism

$$\varphi : \mathrm{End}(E) \to M_2(\mathbb{Z}_p)$$

where $M_2(\mathbb{Z}_p)$ is the ring of 2×2 matrices with coefficients in $\mathbb{Z}_p$. Let's look at $E = \mathbb{C}/\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, every element $\gamma = a + bi \in \mathbb{Z}[i]$ defines a map on $\mathbb{C}$ by $z \mapsto \gamma \cdot z$, for all $z \in \mathbb{C}$, that preserves $\mathbb{Z}[i]$, hence γ defines a map on E. Thus $\mathbb{Z}[i] \subset \mathrm{End}(E)$. It is easy to check

$$\varphi(\gamma) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

if we use 1 and i as the basis of $\mathbb{Z}[i]$.

Let's see how these structures look on the corresponding cubic curve $2y^2 = x^3 - x$. In the projective $\mathbb{P}^2$ space this curve is given by a homogeneous equation $2y^2z = x^3 - xz^2$. Observe that $O = (0 : 1 : 0)$ is the unique point on the curve with $z = 0$, i.e. not on the (x, y)-affine plane. Recall that $0 \in \mathbb{C}/L$ maps to the point O. The group addition $+$ on the curve exploits the fact that a line intersects a cubic projective curve in three points, P, Q and R, counted with multiplicities. These three points add to 0: $P + Q + R = O$. The inverse of a point $P = (x, y)$ is $-P = (x, -y)$. Observe that 2-torsion consists of points such that $P = -P$. This implies that $y = 0$ and we get three points

$$(0, 1),\ (1, 0)\,(-1, 0)$$

and the identity O. The addition is performed as follows. Assume that $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two points on the curve. Let $y = Ax + B$ be the equation of the line through these two points. Substitute this expression for y into $2y^2 = x^3 - x$. This gives a cubic equation in x

$$0 = x^3 - 2A^2x^2 + \ldots = (x - x_1)(x - x_2)(x - x_3)$$

whose two roots are x_1 and x_2, while the third root x_3 is a coordinate of the third intersection point P_3 of the line and the curve. The root x_3 is easy to figure out from the equation

$$2A^2 = x_1 + x_2 + x_3.$$

Finally $y_3 = Ax_3 + B$ gives the other coordinate of the point P_3. The multiplication by i is the automorphism of the curve

$$i \cdot (x, y) = (-x, iy).$$

Exercise: Find the formula for the multiplication by $(1 + i)$, i.e. add (x, y) and $i \cdot (x, y)$, where (x, y) is a point on the curve $2y^2 = x^3 - x$.