ELLIPTIC CURVES OVER $\mathbb{Q}$ AND $\mathbb{Z}_p$

From last time:

DEFINITION: A (real) **elliptic curve** is the solution set E in $\mathbb{R}^2$ to an equation of the form $y^2 = x^3 + ax + b$ for real constants $a, b \in \mathbb{R}$ that satisfy the technical assumption that $4a^3 + 27b^2 \neq 0$. For an elliptic curve E we define $\overline{E} = E \cup \{\infty\}$, where ∞ is a formal symbol.

Intuitively, we think of ∞ as a point infinitely far up or down in the y-direction.

DEFINITION (OPERATION ON AN ELLIPTIC CURVE): For an elliptic curve E, and points $P, Q \in E$ with $P \neq Q$, we set:

$P^\vee :=$ the reflection of P over the x-axis

$P \star Q := R^\vee$, where R is the third point of intersection of the line between P and Q and E

$P \star P := S^\vee$, where S is the other point of intersection of the tangent line to E at P and E.

THEOREM: There is a group structure on $\overline{E}$ with operation $\star$, identity element ∞, and inverse $-^\vee$.

(1) Points of low order[1]. Let $\overline{E} = E \cup \{\infty\}$ be a real elliptic curve the group law above.
   (a) How can you identify the points of order 2 on $\overline{E}$ geometrically? Mark them on each of your placemats. Note: They may not be labelled points.
   (b) How can you identify the points of order 4 on $\overline{E}$ geometrically? Mark them on each of your placemats. Note: They may not be labelled points.
   (c) Points of order 3 on $\overline{E}$ correspond to a special particular case of the group operation $\star$ that we haven't discussed yet: if $3P = \infty$ if and only if P is an inflection point. Discuss whether this rule is "morally consistent" with the rules above or if it is "totally out of left field".
   (d) Mark the points of order 3 on each of your placemats. Note: They may not be labelled points.
   (e) How can you identify the points of order 6 on $\overline{E}$ geometrically? Mark them on each of your placemats. Note: They may not be labelled points.

(a) Points on the x-axis.
(b) Points whose tangent line meets a point in E on the x-axis.
(c) An inflection point corresponds to a triple intersection with the tangent line, so morally, the third point on the line between P and P is P, so $P \star P = P^\vee$, and then $P \star P \star P = P^\vee \star P = \infty$.
(d) OK
(e) Points whose tangent line meets an inflection point in E.

THEOREM: If E is a real elliptic curve given by the equation $y^2 = x^3 + ax + b$ for rational numbers $a, b \in \mathbb{Q}$, then the set of rational points on E (along with the infinity point "∞") form a group with operation $\star$, identity element ∞, and inverse $-^\vee$. We denote this group by $E_{\mathbb{Q}}$.

[1]Recall: The order of an element g in a group G with identity 1 is the smallest integer n such that $g^n = 1$, if such an n exists, and infinite otherwise.

(2) Explain how[2] the theorem about the group structure on $\overline{E}_{\mathbb{Q}}$ above follows from the theorem about the group structure on $\overline{E}$ (real elliptic curves).

> The line between two rational points has a rational slope and rational intersection. Plugging this into the equation for E gives a rational degree three polynomial in x. Two of the roots we already know (from the two points, or a double root in the case of a tangent line) and are rational; then by long division, the third root is rational. Thus the x-coordinate is rational, and the y-coordinate is rational too; still rational after reflecting.

(3) The equation $y^2 = x^3 + 17$ has a rational solution $(-2, 3)$. Use this solution and the group structure on $\overline{E}_{\mathbb{Q}}$ to come up with at least five more rational solutions.

> We have $P^\vee = (-2, -3)$ as well. We also get $2P = (8, -23)$, $2P^\vee = (8, 23)$, etc.

(4) The equation $y^2 = x^3 + 1$ has at least five easy rational solutions: $P = (-1, 0)$, $Q = (0, 1)$, $Q^\vee = (0, -1)$, $R = (2, 3)$, $R^\vee = (2, -3)$. Use the group structure on $\overline{E}_{\mathbb{Q}}$ to try to come up with more rational solutions.

> We find that P$\star P = \infty$, $P \star Q = R^\vee$, $P \star R = Q^\vee$, , $Q \star Q = Q^\vee$ (since Q is an inflection point), $Q \star R = P$, and $R \star R = Q$. Similar things happen with $Q^\vee$ and $R^\vee$. The upshot is that these five points plus ∞ form a finite subgroup of $\overline{E}_{\mathbb{Q}}$ so there are not more solutions that can be generated from these.

DEFINITION: Let $p \geq 5$ be a prime. An **elliptic curve** over $\mathbb{Z}_p$ is the solution set E_p in $\mathbb{Z}_p \times \mathbb{Z}_p$ to an equation of the form $y^2 = x^3 + [a]x + [b]$ for real constants $[a], [b] \in \mathbb{Z}_p$ that satisfy the technical assumption that $[4][a]^3 + [27][b]^2 \neq 0$. For an elliptic curve E_p we define $\overline{E}_p = E_p \cup \{\infty\}$, where ∞ is a formal symbol.

THEOREM: There is a group structure on $\overline{E}_p$ with operation $\star$, identity element ∞, and inverse $-^\vee$ given by the same geometric rules as in the real case.

(5) The elliptic curve $\overline{E}_5 : y^2 = x^3 - x + [1]$.
   (a) Use trial and error to compute all of the points in $\overline{E}_5$.
   (b) For $P = (0, 1)$ and $Q = (1, 1)$, compute $P \star Q$ and $2P$.

---

(6) In this problem, we will prove that the elliptic curve $E : y^2 = x^3 + 7$ has no integer solutions.
   (a) Suppose that (a, b) is an integer solution. Show that a must be odd.
   (b) Show that $b^2 + 1 = (a + 2)((a - 1)^2 + 3)$.
   (c) Show that there exists a prime $q \equiv 3 \pmod 4$ that divides the integer in (b), and obtain a contradiction.

[2] Hint: How do you compute $P \star Q$ algebraically?

(7) Let $a, b \in \mathbb{R}$ be real numbers. Show that every solution point $P = (x, y)$ of the equation $y^2 = x^3 + ax + b$ has a well-defined tangent line (i.e., implicit differentiation yields a well-defined real or infinite "value" of $\frac{dy}{dx}$ at every point) if and only if $4a^3 + 27b^2 \neq 0$.

(8) Use geometric and calculus considerations to give upper bounds on the number of points of
- order 2
- order 3
- order 4

on any real or rational elliptic curve.