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:

$$P^\vee := \text{the reflection of } P \text{ over the } x\text{-axis}$$
$$P \star Q := R^\vee, \text{ where } R \text{ is the third point of intersection of the line between } P \text{ and } Q \text{ and } E$$
$$P \star P := S^\vee, \text{ where } S \text{ is the other point of intersection of the tangent line to } E \text{ at } P \text{ and } E.$$

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.

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 $\overline{E}_{\mathbb{Q}}$.

(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).

(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.

(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.

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

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.

(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.