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.

We write $f_E(x, y) = y^2 - (x^3 + ax + b)$ for the elliptic curve E as above, so

$$E = \{(x, y) \in \mathbb{R}^2 \mid f_E(x, y) = 0\}.$$

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

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

$$P \star Q := R^\vee, \text{ where } R \text{ is the third}^1 \text{ point of intersection of the line between } P \text{ and } Q \text{ and } E.$$

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

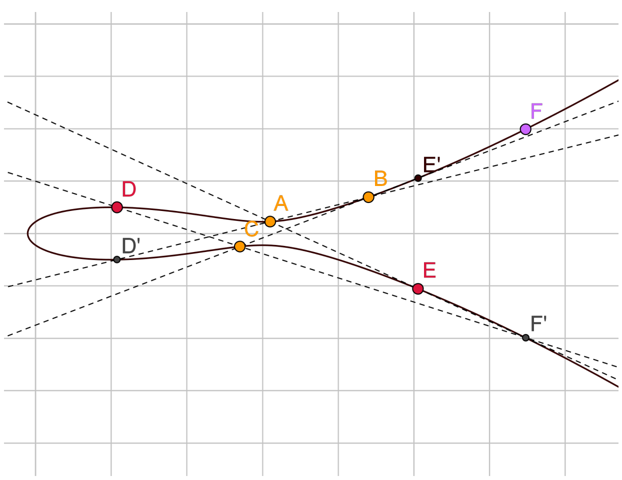
(1) Drawing the operations $\star$ and $-^\vee$:
  (a) For each of the curves given, see if you can find labeled points P, Q, R such that $P \star Q = R$. Can you find all such triples?
  (b) For each of the curves given, mark your own points and see if you can compute the operation $\star$.

Answers vary for different placemats and selected points.

(2) Explain why $P \star Q = Q \star P$.

The line between P and Q is the same as the line between Q and P.

(3) Compute $(A \star B) \star C$ and $A \star (B \star C)$ in the example below. How is this related to the Theorem above?



$A \star B = D$, and $D \star C = F$, while $B \star C = E$ and $A \star E = F$. Thus, $(A \star B) \star C = F = A \star (B \star C)$. This corresponds to the associativity of the operation.

(4) Let E be the elliptic curve given by the equation $y^2 = x^3 + 2x + 4$.
  (a) Verify that $P = (-1, 1)$ and $Q = (0, 2)$ are points in E.
  (b) Compute $R = P \star Q$ and $S = Q \star R$.

For (a), plug in the values to check. For (b), we compute R by taking the line between P and Q, which is $y = x + 2$, and plugging this into the equation to get $(x+2)^2 = x^3 + 2x + 4$. This yields $0 = x^3 - x^2 + 2x = x(x-2)(x+1)$. The roots $x = 0$ and $x = -1$ correspond to P and Q, so the third point corresponds to $x = 2$. Then $(2, 4)$ is the third point on the line. We reflect to get $R = (2, -4)$.

We repeat the process with Q, R, to get $S = (7, 19)$.

(5) The operation $-^\vee$:
- (a) Explain algebraically why $P \in E$ implies $P^\vee \in E$, so $-^\vee$ is a valid operation on E.
- (b) For which points is $P = P^\vee$?
- (c) Explain geometrically why $P = P^\vee$ implies the tangent line to E at P is vertical.

(a) If $P = (x_0, y_0) \in E$, so that $y_0^2 = x_0^3 + ax_0 + b$, then $(-y_0)^2 = x_0^3 + ax_0 + b$, so that $P^\vee = (x_0, -y_0) \in E$.
(b) Points on the x-axis.
(c) Reflection over the x-axis reflects the tangent line as well. If the tangent line had nonzero slope m, then its reflection would have slope $-m \neq m$. The case of a horizontal tangent on the x-axis is also impossible, though it takes a little longer to argue geometrically, and we'll skip it for now.

(6) The doubling operation on an elliptic curve:
- (a) Let E be an elliptic curve and $P, Q \in E$. What happens to the line between P and Q if P stays fixed and Q approaches P?
- (b) Use the previous part to come up with a definition for $2P := P \star P$.
- (c) For each of the curves given, choose some points P and find $2P$ geometrically.
- (d) Let E be the elliptic curve given by the equation $y^2 = x^3 + 2x + 1$ and $P = (0, 1)$. Compute $2P$, $3P$, and $4P$.

(a) The line approaches the tangent line to E at P.
(b) $2P := P \star P$ should be the reflection of the point Q that is on intersection of the tangent line at P and E.
(c) Answers vary.
(d) To compute $2P$ we compute the tangent line to E at P. From calculus, this line is $y = x + 1$. Plugging this into the original equation, we get $(x+1)^2 = x^3 + 2x + 1$, so $0 = x^3 - x^2 = x^2(x-1)$. The double root $x = 0$ corresponds to the point P, so the other point is with $x = 1$, namely $(1, 2)$. Thus $2P = (1, -2)$. Continuing $3P = (8, 23)$, and $4P = \left(\frac{-7}{16}, \frac{13}{64}\right)$.

(7) The group operation and ∞: Let's agree that "the line between P and ∞" is the vertical line through P and that "the reflection of ∞ over the x-axis is ∞."
- (a) With the agreements above, explain why the definition of $\star$ is consistent with $P \star \infty = \infty \star P = P$.
- (b) Given an element P, according to the agreements above, what element Q solves $P \star Q = \infty$?
- (c) Are your answers consistent with the Theorem above?

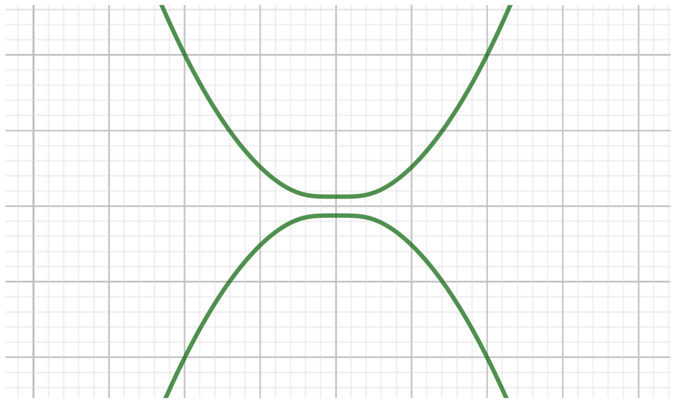
(a) To compute $P \star \infty$, we may be inclined to take the vertical line through P, and take the other intersection point, which is $P^\vee$, then reflect, to get P.
(b) If $P \star Q = \infty$, then Q is the point on the line between P and $\infty^\vee = \infty$, which is $P^\vee$.
(c) Yes.

(8) Well-definedness of $\star$:

(a) Consider the equation $y^2 = -x^2 + 1$. Note that $-^\vee$ makes sense on this curve. Take two points P, Q on this curve, and attempt the operation $\star$. What goes wrong?

(b) Consider the equation $y^2 = \frac{1}{4}(x^4 + 1)$, depicted below. Take various combinations of points P, Q on this curve, and attempt the operation $\star$. What goes wrong?

(c) Draw a random squiggle that is symmetric over the x-axis. Take various combinations of points P, Q on this squiggle, and attempt the operation $\star$. What goes wrong?



(9) Well-definedness of $\star$ continued:

(a) Let E be an elliptic curve, and $L = \{(x, y) \mid y = mx + b\}$ be a nonvertical line. Show that the x-coordinates of points in $L \cap E$ are exactly the zeros of $g_{E,L}(x) := f_E(x, mx + b)$.

(b) Show that $L \cap E$ has at most three points. Thus, for $P \neq Q \in E$, there is at most one other point on E and on the line between P and Q.

(c) Show that if $|L \cap E| \geq 2$, then either $g_{E,L}$ has three distinct roots, or else it has two roots, one of which has multiplicity two.

LEMMA: The condition $4a^3 + 27b^2 \neq 0$ guarantees that every point on E has a tangent line; i.e., implicit differentiation specifies a well-defined value (or infinity) for $\frac{dy}{dx}$ at each point.

LEMMA: If $P = (x_0, y_0) \in E$ and L a (nonvertical) line through P, then $g_{E,L}(x)$ has a double root at x_0 if and only if L is the tangent line to E at P.

(d) Use the Lemmas above to show that if $P \neq Q$ and L is the lime between P and Q, exactly one of the following happens:

- L intersects E in a third point (and no more).
- L is the tangent line to E at P and does not intersect E anywhere else.
- L is the tangent line to E at Q and does not intersect E anywhere else.

What should the value of $P \star Q$ be in each case?

(e) Prove the Lemmas above.