Math 412. Adventure sheet on elliptic curves

DEFINITION: A (real, affine) **elliptic curve** is the solution set 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 $4a^3 + 27b^2 \neq 0$.

NOTATION: We write E to refer to the elliptic curve that corresponds to the solution set in $\mathbb{R}^2$ of $f_E(x, y) = y^2 - (x^3 + ax + b) = 0$.

Elliptic curves have an interesting operation on them. Given a point $P \in E$, set P' to be the reflection of P over the x-axis. Given two points $P \neq Q \in E$, define $P \star Q$ as follows: take the line through P and Q, and let R be the other point of intersection of E with that line. Set $P \star Q = R'$.

A. PLAYING WITH ELLIPTIC CURVES.

(1) Pick a couple of points P and Q on one of your elliptic curves, and compute P' and $P \star Q$.
(2) Explain why $\star$ is commutative.
(3) Take the solution set of $y = x^2$, and try to do the rule $(-)'$ as defined above. Does this work?
(4) Take the solution set of $x = y^2$, and try to do the rule $(-)'$ as defined above. Does this work?
(5) Take the solution set of $x = y^2$, and try to do the rule $\star$ as defined above. Does this work?
(6) In the diagram, compute $A \star B$, $B \star C$, $A \star (B \star C)$ and $(A \star B) \star C$. What do you observe? What do you suspect about the operation $\star$?
(7) Explain why $P \star P$ doesn't make any sense using the definition above.
(8) Fix a point $P \in E$. What happens if you try to compute $P \star Q$ for points Q getting closer and closer to P? Come up with a reasonable rule for $P \star P$.

Solution.

(1) OK!
(2) It answer only depends on the line going through P and Q, which is quite the same as the line going through Q and P.
(3) No way! This rule takes you off of the curve.
(4) Yeah, this one is OK.
(5) No way! A line intersects a parabola in only two points.
(6) Wow! It looks associative.
(7) There's only one point, and there are infinitely many lines through a point.
(8) They approach a tangent line. A reasonable rule for $P \star P$ is to let R be the third point on the tangent line to P, and set $P \star P = R'$.

B. MAKING A GROUP FROM AN ELLIPTIC CURVE: Let E be an elliptic curve, and $E^* = E \cup \{\infty\}$, where ∞ is an extra element.[1] We will say that "the line through P and ∞" for any point $P \in E$ is the vertical line through P.

(1) Show that, if we try to use the definition of the rule $\star$ as given in the intro, then $P \star \infty = \infty \star P = P$ for all $P \in E$.
(2) Set $\infty' = \infty$. Given $P \in E$, can you find an element $Q \in E$ such that $P \star Q = Q \star P = \infty$?
(3) If we want to make E^* into a group, what would the identity be? What would the inverses be?

[1] Intuitively, we can think of ∞ as a point that is infinitely high up in the y-direction, so that it lies on every vertical line.

(4) If we want to make E^* into a group, what would the elements of order 2 be?

> **Solution.**
> (1) If the line through P and ∞ is the vertical line through P, then it meets the curve at P'. We get that $P \star \infty = P$, and $\infty \star P = P$ too since it is commutative.
> (2) $Q = P'$ works. The line through P and P' is vertical, so it passes through ∞. We get $P \star P' = P' \star P = \infty' = \infty$.
> (3) Based on (1), ∞ would be the right choice for the identity. Based on (2), P' would be a good choice for the inverse of P.
> (4) This would imply $P = P'$, so P must be on the x-axis.

We have noticed already that being able to define the rules $(-)'$ and $(-) \star (-)$ is something very special: if you try to do this with most curves, neither rule will make sense.[2] We will use algebra to see that these rules are well-defined.

C. VERTICAL LINES INTERSECTING ELLIPTIC CURVES.

(1) Show that if $(x, y) \in E$, then $(x, -y) \in E$.
(2) Let $L = \{(x, y) \mid x = c\}$ be a vertical line. Show that $L \cap E$ has at most two points.[3]
(3) Find, using the pictured examples, examples of vertical lines L such that $|L \cap E| = 0$, $|L \cap E| = 1$, and $|L \cap E| = 2$.

> **Solution.**
> (1) We need to use the equation. Replacing y with $-y$ leaves y^2 the same, so this holds. This justifies P'.
> (2) The vertical line is $x = c$. The intersection of the line and the curve consists of points with $x = c$ and $y^2 = c^3 + ac + b$. This gives at most two points.
> (3) OK!

D. NONVERTICAL LINES INTERSECTING ELLIPTIC CURVES: Let $L = \{(x, y) \mid y = mx + d\}$ be a line that is *not* vertical.

(1) Show that the x-coordinates of points in $L \cap E$ are solutions to $f_E(x, mx + d)$.
(2) With the notation of (1), show that $f_E(x, mx + d)$ is a polynomial in x of degree (exactly) 3. Conclude that $|L \cap E| \leqslant 3$.
(3) Show that if L is a line that is not vertical, and $|L \cap E| \geqslant 2$, then $f_E(x, mx + d)$ either has three distinct roots, or has two roots, one of which has multiplicity two.

> **Solution.**
> (1) This just follows from substitution.
> (2) $f_E(x, mx + d) = (mx + d)^2 - x^3 - ax - b = -x^3 + m^2x^2 + (2md - a)x + (d^2 - b)$. This has degree three, so there are at most three different x-values for solutions. Since all of the

[2] The fact that $\star$ is associative is even more amazing!

[3] Hint: Plug in $x = c$ into f_E.

solutions live on a nonvertical line, there can be at most one solution for any x-coordinate. Thus, the intersection contains at most three points.

(3) Suppose that a and b are the x-coordinates of two points in the intersection. We know that $(x-a)(x-b)$ divides $f_E(x, mx+d)$ of degree three, and the quotient has degree one, so there is a third linear factor. Either this gives a third solution, or a repetition of a or b as a root.

FACT: If $L = \{(x,y) \mid y = mx+d\}$, then the polynomial $g_{L,E}(x) = f_E(x, mx+d)$ has x_0 as a double root if and only if L is tangent to E at (x_0, mx_0+d).

If $L' = \{(x,y) \mid x = c\}$, then the polynomial $g_{L',E}(y) = f_E(c,y)$ has y_0 as a double root if and only if L' is tangent to E at (c, y_0).

E. THE GROUP RULE ON E^*.

(1) Let P and Q be distinct points in E with $P \neq P'$, and let L be the line through P and Q. Show that one of the following happens:
   (a) L intersects E in a third point (and no more).
   (b) L is tangent to P and does not intersect E in any other point.
   (c) L is tangent to Q and does not intersect E in any other point.

(2) Let $P \in E$. Show that the tangent line to E through P meets E^* in exactly one other point.[4]

In Case (1a) above, we define $P \star Q$ to be R', where R' is the third point. In Case (1b), we define $P \star Q = P'$. In Case (1c), we define $P \star Q = Q'$. In Case (2), we define $P \star P$ to be R', where R is the other point on the line. Finally, $P \star P' = \infty$, and ∞ acts as the identity.

Solution.

(1) This is just D(2) and D(3) translated with the Fact above.

(2) First, assume that L is not vertical. If $g_{L,E}(x)$ has x_0 as a double root, then $(x-x_0)^2$ divides it. The quotient is another linear factor. By our cheating assumption, it gives another root besides x_0.

Now, if L is vertical, the only way $g_{L,E}(y)$ has a double root is if there is exactly one root, in which case L meets E^* only at the point and at ∞.

THEOREM: This operation $\star$ makes E^* into a group; in particular, it is associative.

F. ELLIPTIC CURVES OVER FINITE FIELDS. Observe that we have interpreted the group operation on E^* purely algebraically: we can compute intersections of lines with E with algebra, and the condition that a line is tangent to E has an interpretation in terms of roots of polynomials. Consequently, we can define elliptic curves over finite fields, and get finite groups from them![5]

[4] We will cheat a little here. We need to rule out the possibility of $g_{E,L}(x)$ having a triple root; just assume it here.

[5] It is worthwhile to think about why the crucial step D3 holds over an arbitrary field.

(1) Let $\mathbb{F} = \mathbb{Z}_{11}$. Consider the *elliptic curve over* $\mathbb{F}$

$$E = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + 2x + 1\}.$$

Check that $P = (0, 10)$ and $Q = (3, 1)$ satisfy $P, Q \in E$.

(2) Compute $P \star Q$.

(3) Compute $P \star P$.

Solution.

(1) We just compute $10^2 = 0^3 + 2 * 0 + 1$ and $1^2 = 3^3 + 2 * 3 + 1$.

(2) First we find the line passing through P and Q. Its slope is $3/(-9) = -3$, and its intercept is 10, so L is given by $y = -3x - 1$. We now find solutions to $g_{E,L}(x) = (-3x - 1)^2 - x^3 - 2x - 1 = -x^3 - 2x^2 + 4x$. We already know $x = 0$ and $x = 3$ are roots. We can divide out those linear factors to get $x - 6$ as another linear factor, so $x = 6$. We plug in to the linear equation to get $y = -3 * 6 - 1 = 3$. The third intersection point is $(6, 3)$. Now we flip over the x-axis (negate the y-coordinate) to get the point $(6, 8)$.

(3) We need to find the line through P that is tangent to it. Unless the line is vertical, it has the from $y = mx + 10 = mx - 1$ for some m. The corresponding $g_{E,L}(x)$ function is $(mx - 1)^2 - x^3 - 2x - 1 = -x^3 + m^2x^2 - (2m + 2)x$. For $x = 0$ to be a double root, we must have $2m + 2 = 0$, so $m = 10$. Now with $m = 10 = -1$, we need the third root of this polynomial. $g_{E,L}(x) = -x^3 + x^2$ in this case, so $x = 1$ is the other root. Using $y = -x - 1$, we get $y = -2$, so the other point in the line is $(1, -2)$. Reflecting over the axis, we get $P \star P = (1, 2)$.