Math 4527 (Number Theory 2)

Lecture #13 of 38 $\sim$ February 18, 2021

Elliptic Curves Modulo p

- The Addition Law
- Elliptic Curves Modulo p
- Orders of Points

This material represents §7.1.2-7.1.3 from the course notes.

Recall, I

Last time we introduced elliptic curves:

Definition

An elliptic curve E over a field K is a curve having an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for appropriate coefficients a_1, a_2, a_3, a_4, a_6 in K. This expression is called the Weierstrass form of E.

We will primarily work in the situation where K does not have characteristic 2 or 3, in which case we can change variables to put E into reduced Weierstrass form $y^2 = x^3 + Ax + B$.

Recall, II

We also discussed the group law, which allows us to construct new points on an elliptic curve from other ones:

Definition (Group Law I)

If P_1 and P_2 are two distinct points on the elliptic curve $E : y^2 = x^3 + Ax + B$, let $Q = (x', y')$ be the third intersection point of E with the line L joining P_1 and P_2. We define the sum $P_1 + P_2$ to be the point $-Q = (x', -y')$.

Definition (Group Law II)

If P is any point on the elliptic curve $E : y^2 = x^3 + Ax + B$, let $Q = (x', y')$ be the third intersection point of E with the tangent line L to E at P. We define the sum $P + P$ to be the point $-Q = (x', -y')$.

Recall also that we have a point ∞ that we consider to lie on every

The Group Law, I

Our main result is that the addition law on an elliptic curve (including the point at ∞) gives the points on E the structure of an abelian group:

Theorem (The Group Law)

If K is any field and E is any elliptic curve defined over K, then for any points P, P_1, P_2, and P_3 on E, the following are true:

1. *The addition law is commutative: $P_1 + P_2 = P_2 + P_1$.*
2. *The addition law is associative:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.
3. *The point at ∞ is a two-sided identity: $P + \infty = P = \infty + P$.*
4. *The point P has a two-sided inverse $-P$:* $P + (-P) = \infty = (-P) + P$.

The Group Law, II

Proof:

- We will give arguments for an elliptic curve of the form $y^2 = x^3 + Ax + B$, but the theorem holds in full generality for any elliptic curve.
- Commutativity: Immediate from the geometric definition we have given, since the line used in computing $P_1 + P_2$ and $P_2 + P_1$ is the same in each case.
- ∞ is an identity: Consider the sum $P + \infty$. The line passing through P and ∞ is the vertical line through P which also intersects E at the point $-P$. Then by the geometric definition, $P + \infty = -(-P) = P$.
- Inverses: Consider the sum $P + (-P)$. The line passing through P and $-P$ is a vertical line, so the other point on it is ∞. The reflection of ∞ is also ∞, so $P + (-P) = \infty$.

The Group Law, III

<u>Proof</u> (continued):

- Associativity: This is the only nontrivial result in this theorem.
- One approach to compute $(P_1 + P_2) + P_3$ and $P_1 + (P_2 + P_3)$ explicitly using the addition law. If $P_i = (x_i, y_i)$ then the x-coordinate of $(P_1 + P_2) + P_3$ is

$$\frac{\left(\frac{(y_2-y_1)\left(\frac{(y_2-y_1)^2}{(x_2-x_1)^2}-2x_1-x_2\right)}{x_2-x_1}+y_1+y_3\right)^2}{\left(-\frac{(y_2-y_1)^2}{(x_2-x_1)^2}+x_1+x_2+x_3\right)^2} - \frac{(y_2-y_1)^2}{(x_2-x_1)^2} + x_1 + x_2 - x_3.$$

The Group Law, IV

Proof (continued):

- The y-coordinate is

$$-\frac{\left(\frac{(y_2-y_1)\left(\frac{(y_2-y_1)^2}{(x_2-x_1)^2}-2x_1-x_2\right)}{x_2-x_1}+y_1+y_3\right)\left(\frac{\left(\frac{(y_2-y_1)\left(\frac{(y_2-y_1)^2}{(x_2-x_1)^2}-2x_1-x_2\right)}{x_2-x_1}+y_1+y_3\right)^2}{\left(-\frac{(y_2-y_1)^2}{(x_2-x_1)^2}+x_1+x_2+x_3\right)^2}-\frac{2(y_2-y_1)^2}{(x_2-x_1)^2}+2x_1+\right.}{-\frac{(y_2-y_1)^2}{(x_2-x_1)^2}+x_1+x_2+x_3}$$

$$+\frac{(y_2-y_1)\left(\frac{(y_2-y_1)^2}{(x_2-x_1)^2}-2x_1-x_2\right)}{x_2-x_1}+y_1$$

  and this doesn't even fit on the slide!

- One can then compute the coordinates of the other sum and compare them, and then reduce all of the expressions using the relations $y_i^2 = x_i^3 + Ax_i + B$. (Calculation omitted.)

The Group Law, V

Proof (continued):

- There are (as you should expect) more highbrow proofs that are motivated by various things from algebraic geometry.
- The nicest approach comes from studying divisors on curves (which have a natural group structure to them) and then constructing a map from divisors to points on the curve and showing that this map agrees with the addition law.
- Another approach is to use Bèzout's theorem: two plane curves of degrees m and n not sharing a common component will intersect in mn points (counting multiplicities) over an algebraically closed fields.
- As a consequence, one may show that if C_1 and C_2 are two plane cubics intersecting in 9 points, then any other cubic D passing through 8 of those points must be a linear combination of them, and thus also pass through the 9th.

The Group Law, VI

Proof (continued):

- Now construct the following lines:

1. L_1 through P_1, P_2, S.
2. M_1 through ∞, S, $-S$.
3. L_2 through $-S$, P_3, T.
4. M_2 through P_2, P_3, U.
5. L_3 through ∞, U, $-U$.
6. M_3 through $-U$, P_1, T'.

- Then $T = (P_1 + P_2) + P_3$ and $T' = P_1 + (P_2 + P_3)$.
- Let C_1 be the cubic $L_1 L_2 L_3$ and C_2 be the cubic $M_1 M_2 M_3$.
- Then C_1 and E both pass through the 9 points P_1, P_2, P_3, S, $-S$, ∞, U, $-U$, and T.
- Since C_2 also passes through the first 8 of these points, it must also pass through the 9th, which is T.
- But since C_2 and E can only intersect in 9 points and they are P_1, P_2, P_3, S, $-S$, ∞, U, $-U$, and T', we must have $T' = T$, as claimed.

The Group Law, VII

For convenience in doing numerical computations, we can write down the general formula for the addition law on any curve:

Proposition (Explicit Group Law)

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on the elliptic curve $E : y^2 = x^3 + Ax + B$. Then $P_1 + P_2 = (x_3, y_3)$ where $x_3 = m^2 - x_1 - x_2$ and $y_3 = -m(x_3 - x_1) - y_1$,

with $m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2 \\ (3x_1^2 + A)/(2y_1) & \text{if } P_1 = P_2 \end{cases}.$

If m is infinite, then $P_1 + P_2 = \infty$.

Note that group law is rational, in the sense that the result is always a rational function of the inputs. In particular, the sum of two points whose coordinates lie in a field K will also lie in K.

The Group Law, VIII

Proof:

- If $P_1 \neq P_2$ then the line joining P_1 and P_2 has equation $y - y_1 = m(x - x_1)$ where $m = (y_2 - y_1)/(x_2 - x_1)$.
- We therefore obtain the equation $(mx - mx_1 + y_1)^2 = x^3 + Ax + B$, which has the form $x^3 - m^2x^2 + Cx + D = 0$ for some C, D.
- The polynomial $x^3 - m^2x^2 + Cx + D$ must factor as $(x - x_1)(x - x_2)(x - x_3)$, so upon multiplying out we see that $x_1 + x_2 + x_3 = m^2$. This yields the stated value of x_3, and then $y_3 = m(x_3 - x_1) + y_1$ (where we have multiplied by -1 to account for the vertical reflection).
- If $P_1 = P_2$ then everything is the same, except instead m is the slope of the tangent line at P_1. By implicit differentiation, we see that $2yy' = 3x^2 + A$ so $m = \dfrac{3x_1^2 + A}{2y_1}$ here, as claimed.

Elliptic Curves Modulo p, I

We have primarily dealt with elliptic curves over the real numbers. Now we will look at elliptic curves modulo p where p is a prime.

- All of our analysis of elliptic curves carries into this setting essentially verbatim: in particular, the properties of the addition law and the algebraic formulas remain the same, though we must rely on algebra rather than geometric intuition.
- One difficulty that arises is that if we want to work over a field of characteristic 2 or 3, we will need to use the general Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ rather than the reduced Weierstrass form $y^2 = x^3 + Ax + B$.
- To keep things simple, we will therefore assume p is a prime with $p \geq 5$.

Elliptic Curves Modulo p, II

As we showed earlier, an elliptic curve $y^2 = x^3 + Ax + B$ is nonsingular modulo p precisely when its discriminant $\Delta = -16(4A^3 + 27B^2)$ is nonzero.

- This observation still holds modulo p.
- In particular, we can see that a curve of this form will always be singular modulo 2.
- More generally, if we have any elliptic curve with integer coefficients, we see that the primes p for which the curve is singular mod p (the primes of "bad reduction") are precisely the primes dividing the discriminant Δ.

We can work out examples of the addition law using the explicit formulas from earlier.

Elliptic Curves Modulo p, III

Example: If $P_1 = (1,3)$ and $P_2 = (0,2)$ on the elliptic curve $y^2 = x^3 + 4x + 4$ modulo 5, find $P_1 + P_2$ and $P_1 + P_1$.

- Recall that adding $Q_1 = (x_1, y_1)$ to $Q_2 = (x_2, y_2)$ produces (x_3, y_3) where $x_3 = m^2 - x_1 - x_2$ and $y_3 = -m(x_3 - x_1) - y_1$, and $m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } Q_1 \neq Q_2 \\ (3x_1^2 + A)/(2y_1) & \text{if } Q_1 = Q_2 \end{cases}$.

Elliptic Curves Modulo p, III

Example: If $P_1 = (1, 3)$ and $P_2 = (0, 2)$ on the elliptic curve $y^2 = x^3 + 4x + 4$ modulo 5, find $P_1 + P_2$ and $P_1 + P_1$.

- Recall that adding $Q_1 = (x_1, y_1)$ to $Q_2 = (x_2, y_2)$ produces (x_3, y_3) where $x_3 = m^2 - x_1 - x_2$ and $y_3 = -m(x_3 - x_1) - y_1$, and $m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } Q_1 \neq Q_2 \\ (3x_1^2 + A)/(2y_1) & \text{if } Q_1 = Q_2 \end{cases}$.
- With $(x_1, y_1) = (1, 3)$ and $(x_2, y_2) = (0, 2)$ we obtain $m = (2 - 3)/(0 - 1) = 1$, so $x_3 = 0$ and $y_3 = -1(0 - 1) - 3 = 3$, so $P_1 + P_2 = (0, 3)$.
- Likewise, with $(x_1, y_1) = (x_2, y_2) = (1, 3)$ we obtain $m = (3 + 4)/(2 \cdot 3) = 2$, so $x_3 = 2$ and $y_3 = -2(2 - 1) - 3 = 0$, so $P_1 + P_1 = (2, 0)$.

Elliptic Curves Modulo p, IV

Since there are only finitely many pairs of numbers modulo p, any elliptic curve E will have only finitely many points modulo p, and so we can in principle write them all down (at least if p is small).

- Usually, the easiest procedure for doing this is to try plugging in each possible value of x and then try to compute the square root of $x^3 + Ax + B$ to find the value of y.
- In our count, we also include the point at ∞ on our list.
- We can then write out the complete addition table for the points on E.

Elliptic Curves Modulo p, V

Example: Find all of the points on the (nonsingular) elliptic curve $y^2 = x^3 + 4x + 4$ modulo 3, construct an addition table for them, and identify the group structure.

Elliptic Curves Modulo p, V

Example: Find all of the points on the (nonsingular) elliptic curve $y^2 = x^3 + 4x + 4$ modulo 3, construct an addition table for them, and identify the group structure.

- First, we find all the points by plugging in each of the possible x and computing the necessary square roots. We obtain

x	0	1	2
$x^3 + 4x + 4$	1	0	2
y	± 1	0	n/a

- Thus, there are 4 points on the curve modulo 3: $(0, 1)$, $(0, 2)$, $(1, 0)$, and ∞.

Elliptic Curves Modulo p, VI

Example: Find all of the points on the (nonsingular) elliptic curve $y^2 = x^3 + 4x + 4$ modulo 3, construct an addition table for them, and identify the group structure.

Elliptic Curves Modulo p, VI

Example: Find all of the points on the (nonsingular) elliptic curve $y^2 = x^3 + 4x + 4$ modulo 3, construct an addition table for them, and identify the group structure.

- We can now compute all of the sums using the algebraic formulas:

$+$	∞	$(0,1)$	$(0,2)$	$(1,0)$
∞	∞	$(0,1)$	$(0,2)$	$(1,0)$
$(0,1)$	$(0,1)$	$(1,0)$	∞	$(0,2)$
$(0,2)$	$(0,2)$	∞	$(1,0)$	$(0,1)$
$(1,0)$	$(1,0)$	$(0,2)$	$(0,1)$	∞

- We can see that $(1,0) = 2(0,1)$, $(0,2) = 3(0,1)$, and $\infty = 4(0,1)$. Thus, the group of points is cyclic (of order 4) and generated by the point $(1,0)$.

Elliptic Curves Modulo p, VII

Example: Verify that the elliptic curve $y^2 = x^3 + 4x + 4$ of discriminant $\Delta = -2^8 \cdot 43$ is nonsingular mod p and then find all the points on the curve mod p, where $p = 5$, 7, 11, and 13.

Elliptic Curves Modulo p, VII

Example: Verify that the elliptic curve $y^2 = x^3 + 4x + 4$ of discriminant $\Delta = -2^8 \cdot 43$ is nonsingular mod p and then find all the points on the curve mod p, where $p = 5$, 7, 11, and 13.

- Since none of 5, 7, 11, 13 divide the discriminant, the curve is nonsingular for each of these moduli.
- To count the points, we plug in each possible value of x mod p and then try to compute the square root of $x^3 + Ax + B$.

Elliptic Curves Modulo p, VIII

Example: Verify that the elliptic curve $y^2 = x^3 + 4x + 4$ of discriminant $\Delta = -2^8 \cdot 43$ is nonsingular mod p and then find all the points on the curve mod p, where $p = 5$, 7, 11, and 13.

Elliptic Curves Modulo p, VIII

<u>Example</u>: Verify that the elliptic curve $y^2 = x^3 + 4x + 4$ of discriminant $\Delta = -2^8 \cdot 43$ is nonsingular mod p and then find all the points on the curve mod p, where $p = 5$, 7, 11, and 13.

- Modulo 5, we obtain

x	0	1	2	3	4
$x^3 + 4x + 4$	4	4	0	3	4
y	± 2	± 2	0	n/a	± 2

  and so there are 8 points modulo 5: $(0,2)$, $(0,3)$, $(1,2)$, $(1,3)$, $(2,0)$, $(4,2)$, $(4,3)$, and ∞.

- Modulo 7, we obtain

x	0	1	2	3	4	5	6
$x^3 + 4x + 4$	4	2	6	1	0	2	6
y	± 2	± 3	n/a	± 1	0	± 3	n/a

  and so there are 10 points modulo 7: $(0,2)$, $(0,5)$, $(1,3)$, $(1,4)$, $(3,1)$, $(3,6)$, $(4,0)$, $(5,3)$, $(5,4)$, and ∞.

Elliptic Curves Modulo p, IX

Example: Verify that the elliptic curve $y^2 = x^3 + 4x + 4$ of discriminant $\Delta = -2^8 \cdot 43$ is nonsingular mod p and then find all the points on the curve mod p, where $p = 5$, 7, 11, and 13.

Elliptic Curves Modulo p, IX

Example: Verify that the elliptic curve $y^2 = x^3 + 4x + 4$ of discriminant $\Delta = -2^8 \cdot 43$ is nonsingular mod p and then find all the points on the curve mod p, where $p = 5$, 7, 11, and 13.

- Modulo 11, we obtain

x	0	1	2	3	4	5	6	7	8	9	10
$x^3 + 4x + 4$	4	9	9	10	7	6	2	1	9	10	10
y	± 2	± 3	± 3	-	-	-	-	± 1	± 3	-	-

and so there are 11 points modulo 11: $(0, \pm 2)$, $(1, \pm 3)$, $(2, \pm 3)$, $(7, \pm 1)$, $(8, \pm 3)$, and ∞.

- Modulo 13, we obtain

x	0	1	2	3	4	5	6	7	8	9	10	12	13
$x^3 + 4x + 4$	4	9	7	4	6	6	10	11	2	2	4	1	12
y	± 2	± 3	-	± 2	-	-	± 6	-	-	-	± 2	± 1	± 5

and so there are 15 points modulo 13: $(0, \pm 2)$, $(1, \pm 3)$, $(3, \pm 2)$, $(6, \pm 6)$, $(10, \pm 2)$, $(12, \pm 1)$, $(13, \pm 5)$, and ∞.

Elliptic Curves Modulo p, X

Notice that the number of points on the elliptic curve E modulo p in the example above was fairly close to p for each value we tested. It turns out that this is no accident:

Theorem (Hasse's Theorem)

Let E be a nonsingular elliptic curve defined over a finite field with q elements. Then the number of points $N_q(E)$ on E whose entries are in K satisfies $|N_q(E) - q - 1| \leq 2\sqrt{q}$.

A better bound holds for singular curves: including the singular point itself, the number of points is always either p, $p+1$, or $p+2$ depending on the type of singularity.

The proof involves heavier-duty stuff than we will really be focusing on, but I can give some of the ideas of the proof very briefly.

Elliptic Curves Modulo p, XI

Proof (outline):

- First, observe that the p-power Frobenius map $\varphi : E \to E$ defined via $(x, y) \mapsto (x^p, y^p)$ is a well-defined homomorphism from the group of points on E to itself (such a map is called an endomorphism of E) and has degree p.
- Then the group $E(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points is the kernel of $1 - \varphi$, so $\deg(1 - \varphi) = \#E(\mathbb{F}_p)$. The map $1 - \varphi$ can also be shown to be separable.
- Now observe that the degree map on the space of separable endomorphisms of E is a positive-definite quadratic form.
- Finally, apply the Cauchy-Schwarz inequality: $|\deg(1 - \varphi) - \deg(\varphi) - \deg(1)| \leq 2\sqrt{\deg(\varphi)\deg(1)}$, which reduces to $|\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$ as claimed.

Elliptic Curves Modulo p, XII

To motivate why result like the Hasse bound should hold, let's compute the expected number of points on E modulo p.

- For each of the p possible values of x, there are either 2, 1, or 0 possible values of y, according to whether x is a nonzero square, zero, or a nonsquare.
- When p is an odd prime, there are $(p-1)/2$ nonzero squares modulo p (namely $0^2, 1^2, \dots, [(p-1)/2]^2$).
- Thus, the expected number of values of y for any particular x is $\dfrac{1}{p}\left[2 \cdot \dfrac{p-1}{2} + 1 \cdot 1 + 0 \cdot \dfrac{p-1}{2}\right] = \dfrac{1}{p}[p-1+1] = 1$.
- Since there are p possible x, the expected number of points (x, y) is $p \cdot 1 = p$. Together with the point at ∞, this gives $p+1$ expected points on the curve E.

Elliptic Curves Modulo p, XIII

Trivially, we can see that $1 \leq N_p(E) \leq 2p + 1$: each value of x contributes at most 2 values of y, and the point at ∞ always counts.

- We can rewrite these bounds as $|N_p(E) - p + 1| \leq p$.
- Compare to Hasse's theorem: $|N_p(E) - p + 1| \leq 2\sqrt{p}$.
- We can see that Hasse's theorem is a substantially stronger bound, since the exponent of p is much lower.

Elliptic Curves Modulo p, XIV

In fact, we can push this a little further.

- If we assume (somewhat unreasonably) that the behavior of the x-coordinates are independent, then we are adding 1 to the sum of p independent, identically-distributed copies of a distribution with mean $\mu = 1$ and standard deviation $\sigma \approx 1$.
- By the central limit theorem, we would expect the resulting distribution to be approximately normal, with mean $1 + p\mu = p + 1$ and standard deviation $\sigma\sqrt{p} \approx \sqrt{p}$.
- We would therefore expect the "probability" of having an elliptic curve E such that $|N_p(E) - p + 1| > C\sqrt{p}$ to be very small whenever C is moderately large.
- The Hasse bound makes this very precise – indeed, it tells us that the distribution is actually a bit tighter around $p + 1$ than the central limit theorem would predict.

Elliptic Curves Modulo p, XV

If one adopts this "central limit theorem" sort of viewpoint, it naturally leads to the question of what the actual distribution of the quantity $\dfrac{N_p(E) - p + 1}{2\sqrt{p}}$ looks like.

- By the Hasse bound, we know that this quantity is always between -1 and $+1$.
- There are various ways one could then try to view this quantity as having a distribution.
- One way: fix p and vary the curve E.
- It is known that all of the possible numbers of points satisfying the Hasse bound are achieved by at least one E. But it is tricky to assign a sensible notion to the distribution here, since there are only finitely many elliptic curves E modulo a fixed p.

Elliptic Curves Modulo p, XVII

The inverse approach (fix E and vary p) has a more precise conjecture:

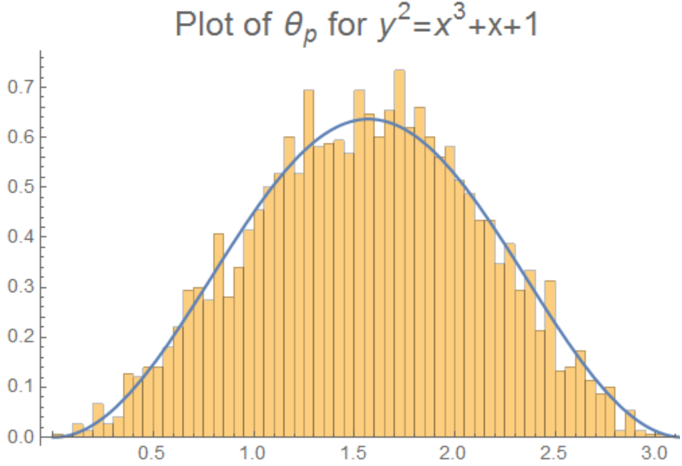
Conjecture (Sato-Tate Conjecture)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. If θ_p is defined to be the real number in $[0, \pi]$ such that $\cos\theta_p = \dfrac{N_p(E) - p + 1}{2\sqrt{p}}$, then for $p \in [1, N]$ as $N \to \infty$, the probability density function of θ_p approaches $\frac{2}{\pi}\sin^2\theta$ on $[0, \pi]$.

This result was proven (for most cases) in 2008 by Clozel, Harris, Shepherd-Barron, and Taylor.

Elliptic Curves Modulo p, XVIII

Here's a plot of the values of θ_p for $y^2 = x^3 + x + 1$ against the density function for the smallest 3000 primes:



Orders of Points on Elliptic Curves, I

Now that we've established some properties of the group law, we can use it to construct analogies between the structure of the points on an elliptic curve modulo p under addition and the units modulo n under multiplication.

- The point, so to speak, is that the points on an elliptic curve modulo p and the invertible residue classes modulo n are both finite abelian groups (E under the addition law, $(\mathbb{Z}/m\mathbb{Z})^{\times}$ under multiplication).

Orders of Points on Elliptic Curves, II

Our first goal is to define the order of a point on an elliptic curve. To do this we will use the addition operation on the curve:

Definition

Suppose E is an elliptic curve defined over a field K, and P is a point on E. For any positive integer k, we define the point kP to be the sum $\underbrace{P + P + \cdots + P}_{k \text{ terms}}$, and we also define $0P = \infty$ and $(-k)P$ as the additive inverse $-(kP)$.
The smallest positive k for which $kP = \infty$ is then called the <u>order</u> of P; if no such k exists, then we say P has infinite order.
A point of finite order is called a <u>torsion point</u> and a point with $mP = \infty$ is called an <u>m-torsion point</u>.

This is the same as the usual definition of the order of an element of a group, and the (m-)torsion elements of an abelian group.

Orders of Points on Elliptic Curves, III

A few remarks:

- Note that kP is well-defined because the addition law is associative: it does not matter the order in which we perform the additions. Likewise, we can see more or less immediately that $(a+b)P = aP + bP$ for any integers a and b.
- Over the real or complex numbers, "most" points on an elliptic curve will have infinite order.
- More precisely, as we will essentially show later, the set of torsion points on an elliptic curve over $\mathbb{C}$ is countably infinite, while the set of all points on the curve is uncountable.
- As we will show in a moment, however, on an elliptic curve modulo p all points have finite order.

Orders of Points on Elliptic Curves, IV

Example: Find the order of the point $P = (1, 3)$ on the elliptic curve $E : y^2 = x^3 + 4x + 4$ modulo 5.

Orders of Points on Elliptic Curves, IV

Example: Find the order of the point $P = (1, 3)$ on the elliptic curve $E : y^2 = x^3 + 4x + 4$ modulo 5.

- We simply compute the multiples of P using the addition law repeatedly.
- We obtain $2P = P + P = (2, 0)$, $3P = 2P + P = (1, 2)$, $4P = 3P + P = \infty$.
- Since $4P$ is the smallest multiple of P that gives the point ∞, the order of P is 4.

Orders of Points on Elliptic Curves, IV

We can compute large multiples of a particular point using successive doubling, in analogy to the procedure of successive squaring:

Algorithm (Successive Doubling Algorithm)

To compute kP, first find the binary expansion of $k = \underline{b_j b_{j-1} \cdots b_0}$. Then compute the multiples $2P$, $4P$, $8P$, ... , $2^j P$ by using the doubling part of the addition law. Finally, compute $kP = \sum_{\substack{0 \le i \le j \\ b_i = 1}} 2^{b_i} P$ using the addition law.

For example, to compute $77P$, we write $77 = 64 + 8 + 4 + 1$ compute $P, 2P, 4P, \ldots, 64P$ via doubling, and then add up $64P + 8P + 4P + P = 77P$.

Orders of Points on Elliptic Curves, V

The successive doubling algorithm is analogous to successive squaring inside $\mathbb{Z}/m\mathbb{Z}$.

- We can speed the successive doubling procedure up a bit by also using subtractions: unlike with modular arithmetic, where it is comparatively expensive to compute inverses, if $P = (x, y)$ then we have the trivial formula $-P = (x, -y)$.
- We will also observe that this procedure works for any elliptic curve, not just an elliptic curve modulo p. The only issue is that large multiples of a typical point will usually grow very complicated over an infinite field.

Orders of Points on Elliptic Curves, VI

Orders of points on an elliptic curve share many of the same properties as orders of units modulo an integer m, and the proofs of these results are also essentially the same.

Proposition (Properties of Order on Elliptic Curves)

Suppose E is an elliptic curve and P is a point on E.

1. *If P has finite order k and $mP = \infty$, then k divides m.*
2. *If $mP = \infty$ but $(m/q)P \neq \infty$ for any prime divisor q of m, then P has order m.*
3. *If E is an elliptic curve modulo a prime p and N is the number of points on E modulo p, then $NP = \infty$. In particular, the order of P divides N.*

We will prove these properties next time.

Summary

We outlined some proofs showing that the addition law makes the points on an elliptic curve into an abelian group.

We discussed elliptic curves modulo p.

We discussed some properties of orders of points on elliptic curves.

Next lecture: More with orders of points, elliptic curve factorization.