Math 4527 (Number Theory 2)

Lecture #17 of 38 $\sim$ March 1, 2021

Elliptic Curve Cryptography (Part 3) + Torsion Points

- Elliptic-Curve Diffie-Hellman
- Elliptic-Curve Digital Signatures
- Torsion Points on Elliptic Curves

This material represents §7.2.3-7.3.1 from the course notes.

Topics Course in Fall 2021

I have just gotten approval to offer a graduate-level course in number theory in Fall 2021. If you will be taking classes at Northeastern then, I would be happy to have any of you take the course with me. I am seeking your interest in the following courses:

1. Elliptic curves and modular forms. This will be a more advanced approach to the study of elliptic curves, which will extend the material we've been doing in this chapter and add quite a bit more to it.
2. Number theory in function fields. Alternate title: "From Fermat's Last Theorem to the Riemann Hypothesis". On the first day of this course I will prove Fermat's Last Theorem, and on the last day I will prove the Riemann hypothesis... but for function fields rather than $\mathbb{Z}$.
3. Algebraic number theory. This is a course that extends and generalizes the material from the next chapter of the course.

This course would serve as reasonable background for any of these

Elliptic Curve Diffie-Hellman, I

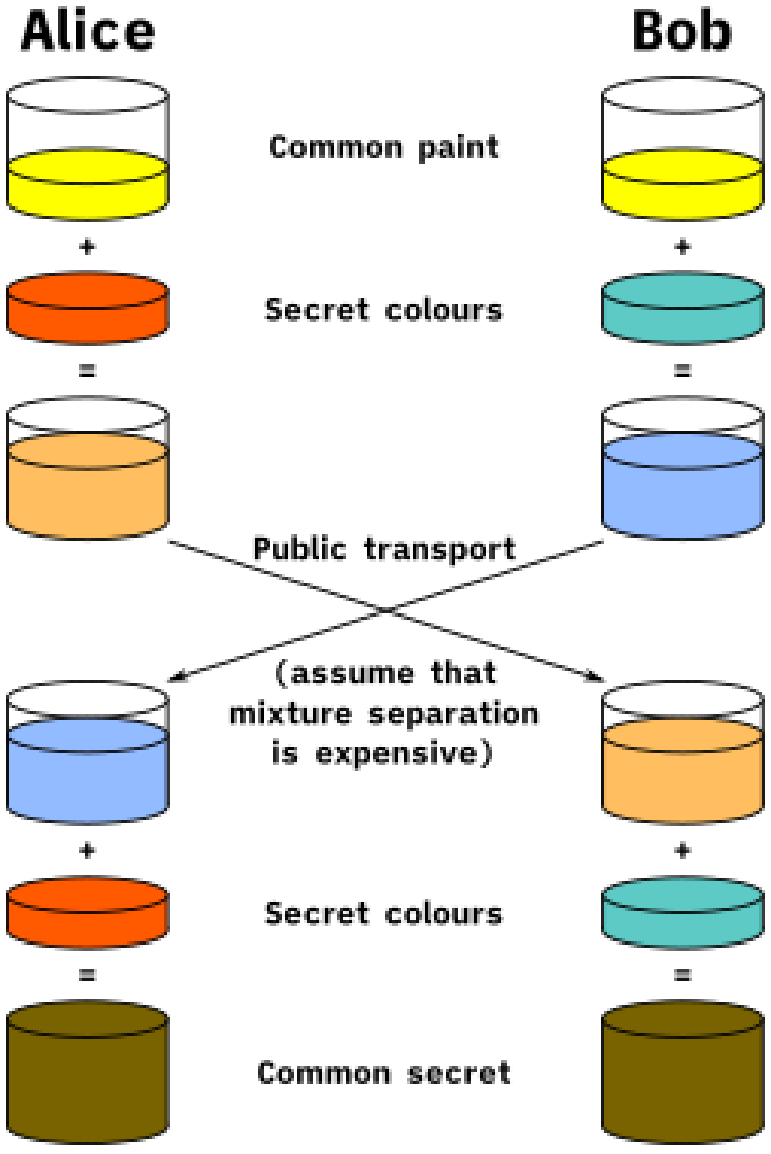
Public-key protocols are fast for small messages, but if Alice needs to send Bob megabytes (or gigabytes or terabytes) of encrypted data, even a very fast implementation of public-key encryption will take an unreasonably long time to encode and decode.

- Symmetric cryptosystems generally do not require nearly as much computation and can be done comparatively efficiently even for large amounts of data.
- Thus, in practice, most efficient cryptographic protocols will require some sort of "key exchange", wherein Alice and Bob must somehow decide what encryption key to use for their symmetric cryptosystem.
- One way to do this is to use an asymmetric cryptosystem to send the key: Alice chooses a key, encrypt it using Bob's public key, and send it to Bob: then Bob can decrypt the message and obtain the key.

Elliptic Curve Diffie-Hellman, II

We will now describe a different procedure for key exchange that is an elliptic-curve version of the Diffie-Hellman key exchange procedure.

The idea of Diffie-Hellman is quite simple, and is contained in this image from wikipedia:



Elliptic Curve Diffie-Hellman, III

The standard implementation of Diffie-Hellman using $\mathbb{Z}/m\mathbb{Z}$ works as follows:

- First, Alice and Bob jointly choose a large prime number p where it is hard to compute discrete logarithms, along with a primitive root g modulo p.
- Alice chooses a secret integer a, and sends Bob $g^a \pmod{p}$.
- Bob chooses a secret integer b, and sends Alice $g^b \pmod{p}$.
- Then the secret key s is given by $g^{ab} \pmod{p}$, which both of them can compute.
- Alice knows a, and has the value of g^b from Bob, so she needs only raise g^b to the ath power.
- Similarly, Bob knows b and has the value of g^a from Alice, so he needs only raise g^a to the bth power.

Elliptic Curve Diffie-Hellman, IV

If Eve is eavesdropping on the conversation, she will have the values of p, along with g, g^a, and g^b modulo p, and she wants to compute the secret key $g^{ab} \pmod{p}$.

- In order to do this, Eve would essentially need to compute one of the exponents a and b; since g is a primitive root, this is equivalent to calculating the discrete logarithm $\log_g(g^a)$ or $\log_g(g^b)$ modulo $p - 1$.
- This discrete logarithm calculation is believed to be hard in general, though both integer factorization and discrete logarithm calculations can be performed in polynomial time using Shor's algorithm on a quantum computer.

Elliptic Curve Diffie-Hellman, V

It is not hard to construct an elliptic-curve version of Diffie-Hellman key exchange for elliptic curves using the same ideas.

- First, Alice and Bob jointly choose a large prime p, an elliptic curve E_p modulo p, and a point P on E having large order.
- Alice chooses a secret integer $a < \mathrm{ord}(P)$, and sends Bob $Q_a = aP$.
- Bob chooses a secret integer $b < \mathrm{ord}(P)$, and sends Alice $Q_b = bP$.
- Then the secret key s is given by $Q_{ab} = (ab)P$, which both of them can compute: Alice evaluates $a(bP)$ while Bob evaluates $b(aP)$.

Elliptic Curve Diffie-Hellman, VI

Example: Use elliptic-curve Diffie-Hellman to construct a secret shared key using $E : y^2 = x^3 + 7x + 1$, $p = 44927$, and $P = (27844, 29401)$, where Alice's secret number is $a = 40006$ and Bob's secret number is $b = 18846$.

- Alice computes $Q_a = aP = (3454, 34367)$ and sends it to Bob. Bob computes $Q_b = bP = (22472, 6971)$ and sends it to Alice.
- Alice then recovers $Q_{ab} = aP_b = (2147, 22480)$ and Bob recovers $Q_{ab} = bQ_a = (2147, 22480)$.
- Bob and Alice now have a secret shared key $Q_{ab} = (2147, 22480)$ that they can use for further communications (e.g., with a symmetric-key cryptosystem).

Elliptic Curve Diffie-Hellman, VII

If Eve is eavesdropping on the conversation, she will know E_p along with P, Q_a, and Q_b , and she wants to compute Q_{ab}.

- In order to do this, Eve would essentially need to compute one of the multipliers a and b. Since P is assumed to have large order, the only reasonable way to do this is for her to evaluate a discrete logarithm on E_p.
- Again, as we have already discussed, computation of discrete logarithms on elliptic curves appears to be very difficult.
- It is of course possible that there is some way to combine the information in P, Q_a, Q_b to find Q_{ab}, but this seems unlikely since the operations of scaling a point by a and scaling a point by b are essentially independent.

Elliptic Curve Diffie-Hellman, VIII

Both the modular and elliptic-curve Diffie-Hellman protocols we have described have no authentication, and are susceptible to a "man-in-the-middle" attack.

- In this attack, Mallory impersonates Alice to Bob and simultaneously impersonates Bob to Alice, and performs a simultaneous key exchange with both of them.
- Then, Mallory will be able to decode messages sent from Alice, and then re-encrypt them to send to Bob.
- As far as Alice and Bob can tell, they are communicating with each other, since their messages are received correctly, at least as long as Mallory is in the middle decoding and re-encoding the messages.

Elliptic Curve Diffie-Hellman, VIII

The problem is that the basic Diffie-Hellman protocol does not authenticate Alice and Bob to one another before creating the key.

- One way to include an authentication step would be for both of Alice and Bob to put a digital signature on their communications during the key creation process, so that the other person feels confident that Mallory is not impersonating either of them.
- We can also use elliptic curves to create digital signatures, which we now describe.

Elliptic Curve Digital Signatures, I

A digital signature must be created in such a way that binds it both to its creator (so that Bob knows Alice and not Eve was the signer and the sender) and to its associated message in a way that cannot easily be altered (so that Bob knows Eve didn't change the message).

- The goal when designing a digital signature algorithm is not to keep the message from being deciphered, but rather to prevent the signature from being easily decoupled from Alice's identity or from Alice's original message.
- Ultimately, however, these ideas are similar enough that we can adapt public-key cryptosystems to create digital signature algorithms.

Elliptic Curve Digital Signatures, II

Here is a digital signature algorithm based off of the ElGamal cryptosystem.

- Alice first creates an ElGamal public key (p, a, b), where p is a large prime for which it is hard to compute discrete logarithms, a is a primitive root mod p, and $b \equiv a^d \pmod{p}$ for her secret choice d with $0 < d < p - 1$.
- If Alice now wants to sign a message m, she first chooses a random integer k relatively prime to $p - 1$.
- She then computes $r \equiv a^k \pmod{p}$ and $s \equiv k^{-1}(m - dr) \pmod{p - 1}$, and her signature is the triple (m, r, s).
- If Bob wants to verify that Alice really signed the message m, he checks whether $b^r r^s$ is congruent to $a^m \pmod{p}$. If so, then he accepts the signature as valid, and if not he rejects it.
- This works $b^r r^s \equiv (a^d)^r a^{ks} \equiv a^{dr} a^{m-dr} \equiv a^m \pmod{p}$.

Elliptic Curve Digital Signatures, III

Suppose now that Eve has intercepted a message pair (m, r, s) that Alice has signed and wants to forge Alice's signature on a new message w.

- Obviously, Eve cannot simply use the signature pair (w, r, s), since Bob will compute $b^r r^s \equiv a^m \not\equiv a^w \pmod{N}$ and reject the signature as invalid.
- In order to find a valid signature z for her message w, she needs to find (r, s) that are solutions to the congruence $b^r r^s \equiv a^w \pmod{N}$.
- If Eve picks a particular r and searches for s, she is attempting to solve $r^s \equiv a^w b^{-r} \pmod{N}$, which is equivalent to computing the discrete logarithm $\log_r(a^w b^{-r})$.

Elliptic Curve Digital Signatures, IV

Another possibility is for Eve to try to choose the value of s first, but this requires solving an even more unusual congruence $b^r r^s \equiv a^w \pmod{N}$, which is a combination of a discrete-log and root-extraction problem.

- It may be possible to choose r and s together in some more efficient manner, but it is not obvious how such a procedure would work.
- Ultimately, if we believe it is difficult to compute discrete logarithms modulo p, then it should also be difficult to forge Alice's ElGamal signature.

Elliptic Curve Digital Signatures, V

We will now describe how to adapt the ElGamal signature algorithm to the elliptic curve setting.

- Some details of the algorithm differ slightly from the modular case since we are dealing with points rather than individual numbers.
- Alice first creates an elliptic-curve ElGamal public key (p, E, Q_a, Q_b) where p is a large prime, E is an elliptic curve modulo p on which it is hard to compute discrete logarithms, Q_a is a point on E whose order has only large prime factors, and $Q_b = dQ_a$ for Alice's secret number d.
- Alice also calculates the number of points N on E_p.

Elliptic Curve Digital Signatures, VI

So, Alice has an elliptic-curve ElGamal public key (p, E, Q_a, Q_b) where Q_a is a point on E whose order has only large prime factors, and $Q_b = dQ_a$ for Alice's secret number d, and E has N points.

- To sign a message m (an integer modulo N), Alice first chooses a random positive integer k relatively prime to N.
- She then computes $Q_r = kQ_a = (x, y)$ and $s = k^{-1}(m - dx) \pmod{N}$, and sends Bob her signed message (m, Q_r, s).
- Bob verifies that Alice's signature is correct by computing $xQ_b + sQ_r$ and comparing it to mQ_a. If the results are equal, he accepts the signature, and otherwise he rejects it.
- The verification works because $xQ_b + sQ_r = x(dQ_a) + s(kQ_a) = (m - dx)Q_a = xdQ_a + mQ_a - dxQ_a = mQ_a$, where we are using the fact that $sk \equiv m - dx \pmod{N}$ to deduce that $ksQ_a = (m - dx)Q_a$ since the order of Q_a necessarily divides N.

Elliptic Curve Digital Signatures, VII

As with the elliptic-curve ElGamal encryption scheme, the security of this procedure ultimately relies on the difficulty of computing a discrete logarithm and the fact that k is randomly chosen.

- It does not depend on the difficulty of computing the number of points on the curve N, which could even be published as part of the public key if desired.

Elliptic Curve Digital Signatures, VIII

Example: Alice publishes her elliptic-curve ElGamal signature key with $E : y^2 = x^3 + 7x + 1$, $p = 44927$, $Q_a = (3174, 1067)$, and $Q_b = dQ_a = (38921, 25436)$ with her secret $d = 25661$. Bob then sends her the message $m = 17781$. Generate a signature for this message with $k = 33050$ and verify that it is correct.

- Alice computes the number of points on the curve, $N = 44651$, which happens to be prime.
- She then computes $Q_r = kQ_a = (11123, 34794) = (x, y)$ and $s = k^{-1}(m - dx) \equiv 42665 \pmod{N}$.
- She then sends the pair (Q_r, s) to Bob, who then evaluates $xQ_b + sQ_r = (29063, 26534) + (36219, 42811) = (35670, 7590)$ and compares it to $mQ_a = (35670, 7590)$.
- The results are equal, so Bob accepts the signature.

Torsion Points, I

We now move from cryptography back into number theory, to discuss the classical problems of finding rational and integral points on a given elliptic curve E.

- Such questions arise quite naturally in the context of solving Diophantine equations, and we will discuss some applications of these results to Diophantine equations later this week.

Torsion Points, II

We first discuss the problem of finding rational points of small order on a given elliptic curve E in Weierstrass form: $y^2 = x^3 + Ax + B$: in other words, we are seeking the m-torsion points P with $mP = \infty$.

- Before making any calculations, we observe that the m-torsion points form a subgroup of all points on E, since $m\infty = \infty$ and if $mP = \infty = mQ$ then $m(P - Q) = \infty$ as well.
- This m-torsion subgroup of E is often denoted $E[m]$. When we want to emphasize the field K over which we are considering E, we will write this subgroup as $E_K[m]$.

Torsion Points, III

Now we can make some observations about $E[m]$ for some small m.

- Trivially, ∞ is the only point of order 1 on E.
- For a point P of order 2, we have $P + P = \infty$. Geometrically, this means that if we consider the tangent line to the graph of E at P, then the third intersection point of P with E is the point at infinity.
- It is not hard to see that this is equivalent to saying that the tangent line at P is vertical. From the explicit formula $2yy' = 3x^2 + A$ we see that this is, in turn, equivalent to saying that $y = 0$.
- Therefore, the points (x, y) of order 2 are those having $y = 0$. Since this requires $x^3 + Ax + B = 0$, we see that there are at most 3 such points.

Torsion Points, IV

If we are searching for points over $\mathbb{C}$ (or another algebraically closed field), then there will be exactly 3 points of order 2, since by assumption the elliptic curve is nonsingular so $x^3 + Ax + B$ has no repeated roots.

- Over arbitrary fields K, we may have a smaller number of roots of the cubic $x^3 + Ax + B$: it is possible that this cubic could have 0, 1, or 3 roots in K (2 roots is not possible because if the cubic has two linear factors then it is a product of 3 linear factors).
- This tells us that the 2-torsion subgroup $E_K[2]$ has order 1, 2, or 4. Since all of the elements have order 1 or 2, this means the group is either the trivial group, $\mathbb{Z}/2\mathbb{Z}$, or the Klein 4-group $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Torsion Points, V

Example: Find the points of order 2 on the elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{Q}$ and over $\mathbb{C}$, and identify the group structure of the 2-torsion group $E[2]$ over each field.

Torsion Points, V

Example: Find the points of order 2 on the elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{Q}$ and over $\mathbb{C}$, and identify the group structure of the 2-torsion group $E[2]$ over each field.

- From the discussion above, the 2-torsion points are the points with $y = 0$, which requires $x^3 + x = 0$ so that $x = 0, \pm i$.
- Over $\mathbb{Q}$, there is therefore one 2-torsion point $\boxed{(0,0)}$. Then the 2-torsion group $E_{\mathbb{Q}}[2]$ is $\{\infty, (0,0)\}$ and its group structure is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Torsion Points, V

Example: Find the points of order 2 on the elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{Q}$ and over $\mathbb{C}$, and identify the group structure of the 2-torsion group $E[2]$ over each field.

- From the discussion above, the 2-torsion points are the points with $y = 0$, which requires $x^3 + x = 0$ so that $x = 0, \pm i$.
- Over $\mathbb{Q}$, there is therefore one 2-torsion point $\boxed{(0,0)}$. Then the 2-torsion group $E_{\mathbb{Q}}[2]$ is $\{\infty, (0,0)\}$ and its group structure is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
- Over $\mathbb{C}$ we have three 2-torsion points: $\boxed{(0,0),\ (i,0),\ (-i,0)}$.
- Then the 2-torsion group $E_{\mathbb{Q}}[2]$ is $\{\infty, (0,0), (i,0), (-i,0)\}$. Since all of the nontrivial elements in this group have order 2, the group structure is isomorphic to the Klein 4-group $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Torsion Points, VI

Example: Find the points of order 2 on the elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{Q}$ and over $\mathbb{C}$, and identify the group structure of the 2-torsion group $E[2]$ over each field.

- We can write out the addition table for $E_{\mathbb{C}}[2]$ explicitly:

$+$	∞	$(0,0)$	$(i,0)$	$(-i,0)$
∞	∞	$(0,0)$	$(i,0)$	$(-i,0)$
$(0,0)$	$(0,0)$	∞	$(-i,0)$	$(i,0)$
$(i,0)$	$(i,0)$	$(-i,0)$	∞	$(0,0)$
$(-i,0)$	$(-i,0)$	$(i,0)$	$(0,0)$	∞

Torsion Points, VII

For points of order 3, we see that such points P satisfy $P + P + P = \infty$ so that $P + P = -P$, so the third intersection point of the tangent line to E at P also goes through P. Equivalently, P is an inflection point of the curve.

- Algebraically, using the doubling formula, we require $2(x, y) = (x, -y)$, so since $2(x, y)$ has x-coordinate $m^2 - 2x$, this requires $m^2 = 3x$ where $m = \frac{3x^2+A}{2y}$.
- Clearing denominators gives $12x(x^3 + Ax + B) = (3x^2 + A)^2$, which is an equation of degree 4 in x. Each x-coordinate corresponds to two possible y-coordinates (since $y = 0$ only occurs for 2-torsion points), so in general we obtain 8 points of order 3 over $\mathbb{C}$.
- In general, the 3-torsion subgroup $E_K[3]$ over an arbitrary K has order at most 9, so since all elements have order 1 or 3, it is either the trivial group, $\mathbb{Z}/3\mathbb{Z}$, or $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.

Torsion Points, VIII

For points of higher order, it is even more difficult to give nice geometric or algebraic descriptions of $E[m]$.

- One may try to compute explicitly the coordinate relations for these points; however, the resulting multiplication-by-m formulas end up being extremely complicated and unpleasant.
- It is a rather long and convoluted (though not conceptually difficult) calculation to show that if $P = (x, y)$, then $mP = (x_m, y_m)$ where x_m^2 is a rational function of degree $m^2 - 1$ in x (one may in fact eliminate y from all of these relations for the x-coordinates) and y_m is a rational function of degree m^2 in x and y.

Torsion Points, IX

Then $mP = \infty$ precisely when the square of the denominator polynomial in the x-coordinate is equal to zero.

- Since this squared denominator polynomial in x has degree $m^2 - 1$, this means there are at most m^2 m-torsion points (note that ∞ must be added to the total).
- One can also show that the denominator polynomial is separable over any field whose characteristic does not divide m, so it has distinct roots.
- In particular, over the complex numbers $\mathbb{C}$, the m-torsion points form a group of order m^2, and thus over subfields of $\mathbb{C}$ (e.g., $\mathbb{Q}$) the m-torsion points will be a subgroup of the m-torsion group over $\mathbb{C}$.

Torsion Points, X

We can use the fact that there are m^2 complex m-torsion points to classify the isomorphism type of the group of complex m-torsion points:

Proposition (Structure of Complex m-Torsion Subgroup)

For any positive integer m and any elliptic curve E over $\mathbb{C}$, the m-torsion subgroup $E_{\mathbb{C}}[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

The result in fact holds over any algebraically closed field (by essentially the same argument) of characteristic not dividing m.

- As a consequence, over any subfield K of $\mathbb{C}$, the m-torsion subgroup $E_K[m]$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.
- Another way to say this is that the group of m-torsion points of E, over any field, always has at most 2 generators.

Torsion Points, XI

Proof:

- Apply the structure theorem for finite abelian groups to write $E[m]$ as a direct product of cyclic groups of prime-power order.
- If there were 3+ cyclic factors of order p^k for some prime p, then the set of elements of order p in $E[m]$ would have 3+ components isomorphic to $\mathbb{Z}/p\mathbb{Z}$: but this would mean $E[p]$ would have order greater than p^2, which is impossible.
- Thus, there are at most 2 cyclic factors of p-power order for any prime p. By the Chinese remainder theorem, this means $E[m]$ has at most 2 generators.
- But since these two generators of $E[m]$ each have order at most m, and $E[m]$ has order m^2, the group must be a direct product $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, as claimed.

Torsion Points, XII

We can say a bit more about the $\mathbb{R}$-points on the elliptic curve E using some basic facts about Lie groups.

- The addition of real points on the elliptic curve is clearly continuous, from our geometric description of the group law, so it is a one-dimensional Lie group. Since the group of real points is also compact (including ∞ is the one-point compactification of the set of points (x, y) on E), we are looking at compact one-dimensional Lie groups.
- If $E(\mathbb{R})$ is connected (i.e., has a single component), then the only such Lie group is the circle group S^1, in which case the set of m-torsion points corresponds to the mth roots of unity on the unit circle and is isomorphic to $\mathbb{Z}/m\mathbb{Z}$.
- If there are two connected components, then the Lie group is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times S^1$, in which case the m-torsion points look like $\mathbb{Z}/m\mathbb{Z}$ for m odd and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ for m even.

Torsion Points, XIII

We can say a bit more about the $\mathbb{C}$-points on the elliptic curve E using a bit of complex analysis and topology.

- The idea is to consider the Riemann surface associated to the nonsingular elliptic curve $y^2 = x^3 + Ax + B$.
- One may prove that this Riemann surface is homeomorphic to a torus $S^1 \times S^1 \cong (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$, which is in turn homeomorphic to $\mathbb{C}$ modulo a discrete lattice $\Lambda \cong \mathbb{Z}^2$.
- The way this works is quite nice, and the result is quite helpful in understanding what the torsion elements look like, so let me explain it a bit more.

Torsion Points, XIII

So: how could we try to write down an analytic map from E to $\mathbb{C}$?

- The idea is to integrate something: specifically, we want to integrate the holomorphic differential
$$d\omega = \frac{dx}{y} = \frac{dx}{\sqrt{(x - r_1)(x - r_2)(x - r_3)}}.$$
- We could then try to get a map from E to $\mathbb{C}$ by sending a point P to the integral $\int_0^P \omega$.
- The problem is that this integral is not well-defined since this function needs branch cuts. So, if we include the point at ∞ (i.e., work with the Riemann sphere instead of $\mathbb{C}$), we can make one branch cut from r_1 to r_2 and another from r_3 to ∞.
- Topologically, this turns the Riemann sphere into a torus.

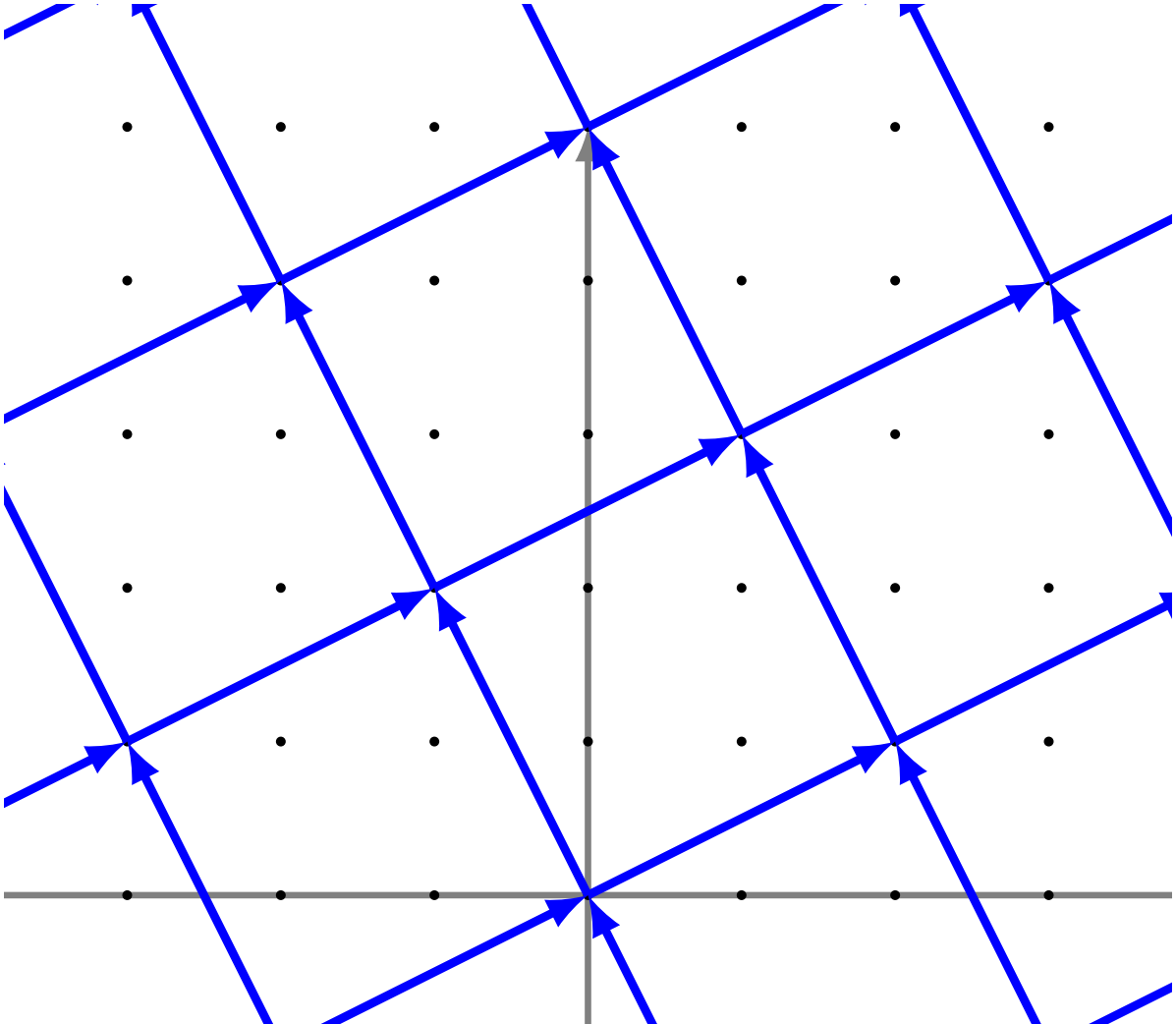
Torsion Points, XIV

Let α be a path looping around the r_1-r_2 branch cut once, and let β be a path looping around the r_3-∞ branch cut once.

- Since α and β generate the fundamental group of the torus, the difference between any two paths between 0 and P on our branch-cut Riemann sphere is homotopic to a $\mathbb{Z}$-linear combination of α and β.
- So the integral $\int_0^P d\omega$ is well-defined up to adding a $\mathbb{Z}$-linear combination of $\omega_1 = \int_\alpha \omega$ and $\omega_2 = \int_\beta \omega$.
- What this all means is that when we integrate along paths, we get a map not from E to $\mathbb{C}$ that is defined only up to adding arbitrary integer multiples of ω_1 and ω_2.
- This is equivalent to saying we get a map from E to the quotient group $\mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{a\omega_1 + b\omega_2 \,:\, a, b \in \mathbb{Z}\}$.

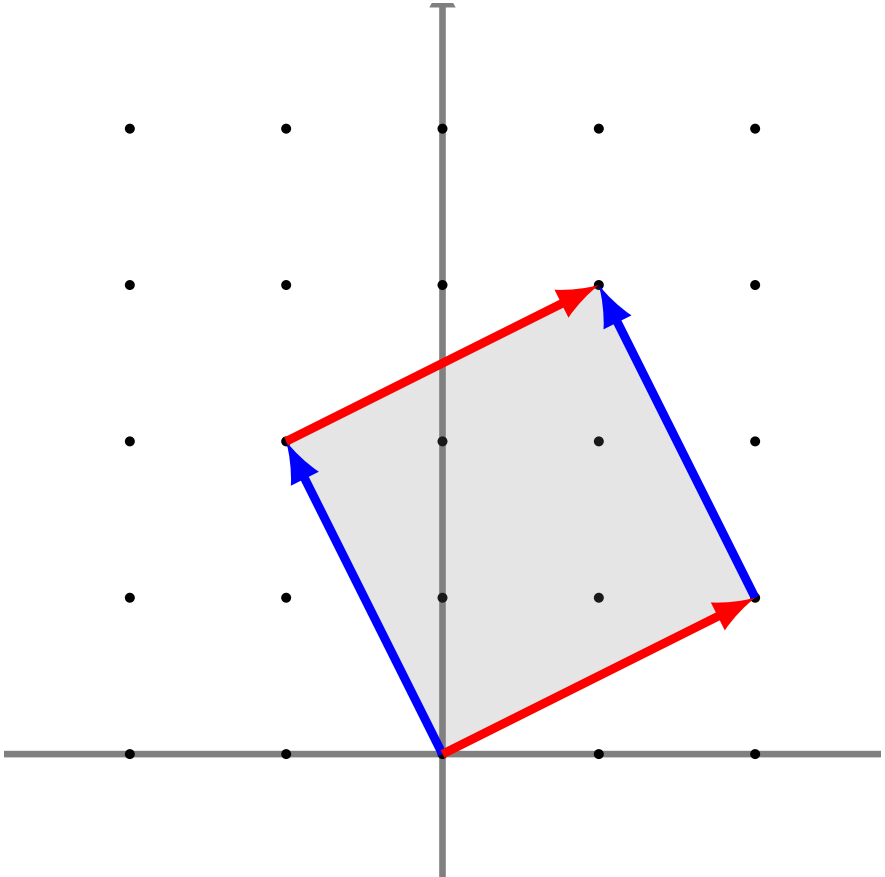
Torsion Points, XV

For example, suppose that $\omega_1 = 2 + i$ and $\omega_2 = -1 + 2i$, so that our lattice is as below:



Torsion Points, XVI

In the quotient group $\mathbb{C}/\Lambda$, we then identify any two points that differ by an element of Λ. Geometrically, we can picture this as being a "fundamental region", with the left and edges identified, and the top and bottom edges also identified (which is a torus):



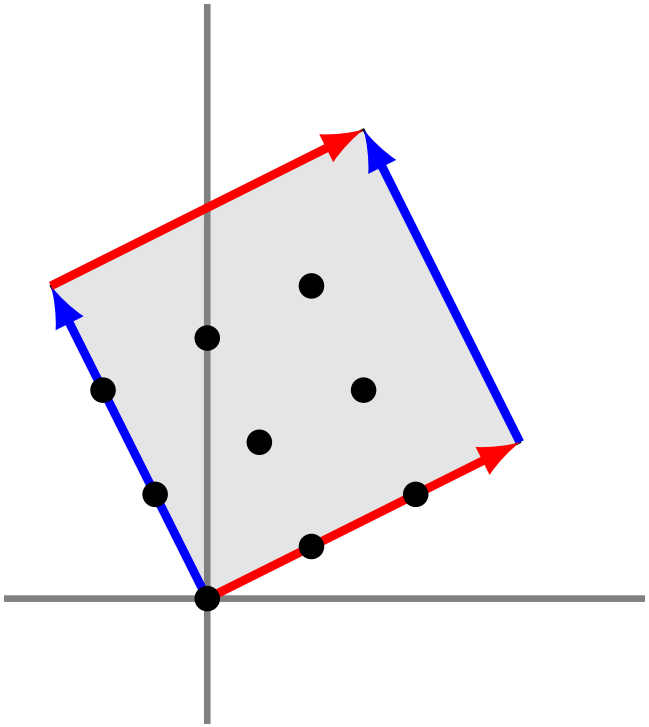
Torsion Points, XVII

The first magical fact is that the map from E to $\mathbb{C}/\Lambda$ is actually diffeomorphic, and the second magical fact is that the map is an isomorphism of groups.

- The group operation inside $\mathbb{C}/\Lambda$ is just the usual one, namely, addition of complex numbers.
- The identity element of the group is of course 0.
- We can then easily identify the m-torsion elements: they simply form the $m \times m$ grid of "m-division points" in the lattice.
- Equivalently, we are looking for points such that $mP \in \Lambda$, which is simply the lattice $\frac{1}{m}\Lambda$.

Torsion Points, XVIII

Here, for example, are the 3-division points of the lattice from earlier:



Torsion Points, XIX

Conversely, one can construct a map from lattices $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ inside $\mathbb{C}$ back to elliptic curves by considering "elliptic functions": functions defined on $\mathbb{C}/\Lambda$.

- Equivalently, we are looking for meromorphic functions on $\mathbb{C}$ such that are "periodic relative to Λ": namely, with $f(z+\omega) = f(z)$ for all $\omega \in \Lambda$ and $z \in \mathbb{C}$.
- These are, equivalently, "doubly-periodic" functions, with $f(z+\omega_1) = f(z+\omega_w) = f(z)$ for all z.
- Functions like $\sin x$ only have one period in $\mathbb{C}$: we want functions with two different periods.

Torsion Points, XX

Here is the standard example of an elliptic function, called the Weierstrass $\wp$-function: it is defined as

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right].$$

- One can check that the series converges uniformly on compact subsets of $\mathbb{C}$, and that it has double poles at each point of Λ but nowhere else in the plane.
- Another example of an elliptic function is the derivative $\wp'_\Lambda(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}$.
- The sum used to define $\wp'$ converges absolutely, and is much easier to see that it is invariant under translation by elements of Λ.

Torsion Points, XXI

So now here is the magic: by comparing Laurent expansions, we can use the $\wp$-function to map from lattices back to elliptic curves.

- To see this, first one computes the Laurent series for $\wp$ around $z = 0$, which is $\wp(z) = z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$, where $G_{2k}(\Lambda) = \sum_{\omega \in \Lambda *} \omega^{-2k}$ is the Eisenstein series of weight $2k$.
- By comparing Laurent expansions, for $g_2 = 60G_4$ and $g_3 = 140G_6$ one has $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.
- The point is that the Laurent series for the difference between the two sides has no negative-degree terms. This means the difference is actually holomorphic on all of $\mathbb{C}$, and it is bounded because it is doubly-periodic. Thus, by Liouville's theorem, it is constant (and the constant is in fact zero).
- Thus, the map $\mathbb{C}/\Lambda \to E$ sending $z \to (\wp(z), \wp'(z))$, where E is the elliptic curve $y^2 = 4x^3 - g_2x - g_3$, is a complex-analytic isomorphism of complex Lie groups.

Torsion Points, XXII

As a final comment, I will remark that the terminology of "complex multiplication" for elliptic curves also arises from this correspondence between elliptic curves over $\mathbb{C}$ and quotients $\mathbb{C}/\Lambda$.

- Specifically, if we happen to have a complex number ζ such that $\zeta\Lambda \subseteq \Lambda$, then we obtain a corresponding "multiplication-by-ζ" endomorphism of the elliptic curve.
- The obvious "multiplication by m" maps are of this form with $\zeta = m$, and for most Λ these are the only such ζ. But for certain lattices, there are nonreal ζ such that $\zeta\Lambda \subseteq \Lambda$.
- For example, if $\Lambda = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, then $\zeta = i$ has $\zeta\Lambda \subseteq \Lambda$, and so the corresponding elliptic curve has a "multiplication by i" map. One can then compute the values of g_2 and g_3 for this lattice to see that the curve is exactly $y^2 = x^3 + x$, which you analyzed on Homework 6.

Summary

We discussed elliptic-curve Diffie-Hellman key exchange.

We discussed elliptic-curve digital signature algorithms.

We discussed torsion points on elliptic curves.

Next lecture: Rational points on elliptic curves.