NOTES ON ELLIPTIC CURVES

MATH 4150 - SPRING 2018

1. Motivation:

1.1. **Congruent numbers.** In our study of the congruent number problem, we have seen that there are several ways of rephrasing the question of whether a square-free integer n is congruent, and to generate tables of congruent numbers. However, we have also seen that this is numerically infeasible even for small n which are congruent. Worse, if n is not congruent, these procedures do not generate a proof as you don't know how long you have to wait to tell if n is congruent. We have also seen that Fermat-style infinite descent proofs can be given to show that some small numbers, such as $n = 1, 2, 3$, are not congruent.

Ideally, we would like a quick way to test if a number is congruent or not. There is yet another way of rephrasing the problem of congruent numbers which makes this possible. To describe this, we begin with a strange-looking, but yet elementary, lemma. For this, recall that the Diophantine system of equations formulation of n being congruent is to say that there exist $x, y, z \in \mathbb{Q}$ such that

$$X^2 + Y^2 = Z^2, \quad (XY)/2 = n.$$

The lemma is purely a set of algebraic identities, so we omit the proof (as, for the sake of time, we have also omitted the intuitive explanation of where this "strange" lemma comes from).

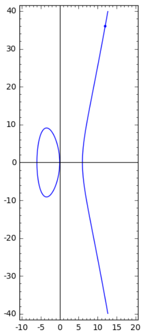
Lemma. *There is a one-to-one correspondence*

$$\left\{(X,Y,Z) \in \mathbb{Q}^3 : X^2 + Y^2 = Z^2, (XY)/2 = n\right\} \leftrightarrow \left\{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 - n^2 x, y \neq 0\right\}$$

given explicitly by $(X,Y,Z) \mapsto (nY/(Z-X), 2n^2/(Z-X))$ *in one direction and* $(x,y) \mapsto ((x^2-n^2)/y, 2nx/y, (x^2+n^2)/y)$ *in the other.*

Note that the equation $y^2 = x^3 - n^2 x$ has 3 "obvious" solutions in the rationals: when $y = 0$, there are the solutions with $x = 0, \pm n$. These, however, are exactly the ones left out of our correspondence! Note also in the correspondence that in one direction we divide by factors of $Z - X$; these are never 0 as the hypotenuse of a right triangle must have length strictly larger than the lengths of the legs.

Here is a numerical example. Our first example of a congruent number is $n = 6$, which is the area of the $3-4-5$ Pythagorean triangle. If we plug this into the explicit formulas in the lemma, we have $(X,Y,Z) = (3,4,5)$, and so $(x,y) = (6 \cdot 4/2, 2 \cdot 6^2/2) = (12, 36)$. Thus, the curve $y^2 = x^3 - 36x$ has the rational point $(12, 36)$ on it:



The curve $y^2 = x^3 - n^2x$ is our first example of an *elliptic curve*. Below, we will discuss the general story of elliptic curves, and we shall find that they have an extra special "structure" on them which has a lot to tell us about Diophantine problems like the congruent number problem.

1.2. **Fermat's Last Theorem.** Another important Diophantine equation, which we've already studied is that which shows up in Fermat's Last Theorem. Recall that this claims that there are no positive integral solutions to the equation

$$x^n + y^n = z^n, \qquad n \geq 3.$$

We have discussed how Fermat-style proofs can be used for some small cases, like $n = 4$, as well as why this problem is extremely difficult (because, unfortunately, the "Fundamental Theorem of Arithmetic" fails for more general number sets than the integers). We now know, thanks to a deep and difficult proof of Wiles, obtained more than 350 years after Fermat first formulated the problem. The key idea behind Wiles' proof relies in an essential way on elliptic curves. Explicitly, an idea proposed by Frey works as follows. Suppose that there were a counter-example to Fermat's Last Theorem, given by a triple (a, b, c). Frey noticed that in such a situation, say when $x^p + y^p = z^p$ (recall that its enough to prove FLT for prime exponents and for $n = 4$ which we know, so we assume here that p is a prime), then we can define a plane curve, called a *Frey curve*, by the equation

$$y^2 = x(x - a^p)(x - b^p).$$

This will turn out, after we've discussed the actual definition, to be an elliptic curve. What was noticed, and later proven by Wiles with help from a result of Serre and Ribet, is that this elliptic curve would have very strange properties. In fact, these properties are so strange, that you suspect such a curve shouldn't exist. Moreover, elliptic curves were also conjectured to be closely related to another mathematical object, called *modular forms*. Serre and Ribet showed that if an elliptic curve is closely related to a modular form, which was shown by Wiles to be true in the cases needed here, then these strange properties cannot occur.

Finally, many other Diophantine equations can be studied via similar elliptic curves and Wiles-style methods. For instance, a relatively recent Annals paper of Bugeaud, Mignotte, and Siksek applied similar methods to show that the only Fibonacci numbers which are perfect powers are $0, 1, 8, 144$, which is a shockingly simple, if not deceptively so, result.

1.3. Cryptography.

We have discussed some important cyrptoschemes, such as RSA. Increasingly important cyrptoschemes, which have many advantages (small key sizes, harder to attack than RSA using methods of attack we saw on the HW, etc.) and are becoming national standards in many arenas, are based on elliptic curves. We shall discuss briefly how this works later in the notes. Just like RSA, there is a mathematical operation which is easy to compute in one direction and hard to invert, which underpins the cyrptography. With RSA, this was multiplication of primes vs. factorization into primes. We have seen another such result in our study of primitive roots: its easy to take a power of an integer mod something, but hard to compute the index (discrete logarithm). Elliptic curves will have a similar "structure" to integers under multiplication mod something (this is the same structure hinted at in the above subsections), this can be used for cyrptography via the same kind of problem of computing discrete logarithms, just with a different group.

For example, if you use Firefox, by playing around in the advanced settings, you can view the information on the elliptic curves it is using to encrypt your data. The chip on your credit card is also able to perform such elliptic curve computations to secure your privacy.

2. Elliptic curves

2.1. Definition and examples.

Ellpitic curves will be, first of all, curves, and specifically curves satisfying an equation of the form:

$$y^2 = x^3 + Ax + B$$

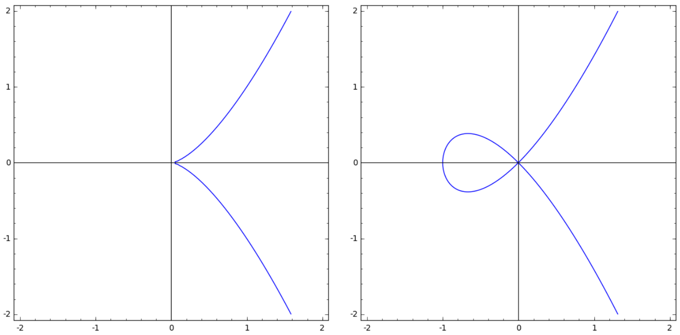
for some numbers A, B. We will have to wait a moment to see "why" equations of precisely this shape are so special. We only want to study curves which don't have any "bad points", or singularities. Just as you saw in Calculus class, some curves have "sharp points", or cusps. For example, the function $y = |x|$ has such a point at the origin, and we don't like this point, as the function is not differentiable there (or, if a particle were to travel along this curve at a constant speed with respect to arc length, it would experience an "infinite" acceleration at that point due to the sudden change of direction, and this never happens in "real life").

In this instance (and, crucially, to unravel the special structure of elliptic curves which makes them so useful), we need to introduce *projective coordinates*. You have possibly heard of the idea of perspective in art or vision, where two parallel lines "look like" they converge very very far away to the same place. For instance, the two rails on a set of train tracks appear to meet off in the distance. There is a related idea in mathematics, where two parallel lines do intersect, just very far away, at "infinity". Roughly speaking, why this is useful here is that if you took two different random lines, which are defined by polynomial equations of degree 1, they almost always intersect exactly once, except for the degenerate case of parallel lines (which has a 0% chance of happening). However, we'd like to count those as intersecting at one point as well, and if we use projective coordinates, curves defined by a polynomial of degree m will always intersect curves defined by polynomials of degree n exactly the nice and predictable number mn times.

We can formally describe this as follows. The (complex) *projective plane* is the set of equivalence relations of triples $(x, y, z) \in \mathbb{C}^3 \setminus \{(0, 0, 0)\}$ under the equivalence relation that $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for each $\lambda \in \mathbb{C}$. If we take a representative of a point in the projective plane, we write it as $(x : y : z)$, and we call this representation a set of *homogenous coordinates*. This is really an extension of an ordinary plane, of ordinary tuples of complex numbers (x, y), as if $z \neq 0$ for some point in the projective plane, then we can WLOG rescale so that $z = 1$ and obtain a representative of the form $(x : y : 1)$, which directly corresponds to the ordered pair (x, y). What we gain by taking the projective plane, is the additional "points at infinity", where $z = 0$. This is called the *line at infinity*.

Note that a curve defined by a polynomial in the projective plane must be homogenous in order to be compatible with the rescaling operation. If we have any ordinary plane curve, we can just "homogenize" the equation by inserting a power of z in each monomial factor until the maximal degree of the original polynomial matches the total degree of each monomial. For instance, for the lines $y = x + 1$ and $y = x - 2$, which are parallel, we rewrite these as the "zero-sets" of $y - x - 1$ and $y - x + 2$, and homogenize to obtain $y - x - z$ and $y - x + 2z$. Incidentally, we can check that these parallel lines now do intersect, as if we subtract the first equation from the second, we obtain $3z = 0$ and so $z = 0$ (so they do only intersect "at infinity"), and plugging back into the original equations we find that $x = y$. Since $(0, 0, 0)$ isn't an allowable point, we have $x, y \neq 0$, and we can thus rescale to find that the lines intersect at infinity at exactly one point, namely $(1 : 1 : 0)$.

What about for a cubic equation $y^2 = x^3 + Ax + b$? Projectivizing this gives the equation $y^2z - x^3 - axz^2 + bz^2 = 0$. What are the points at infinity? Well, if $z = 0$, then we obtain $-x^3 = 0$, and so $x = 0$. Now y isn't also allowed to be 0, so this cubic curve always has precisely one point at infinity, namely the point $(0 : 1 : 0)$. There are two types of bad behavior that can happen for such cubic curves, illustrated in the following picture:



These illustrate (from left to right) the curves $y^2 = x^3$ and $y^2 = x^3 + x^2$. The first has a cusp, and the second also has a problem at the origin, where the curve intersects itself (called a node). What is going on here is that a curve defined by the polynomial equation $f(x_1, x_2, \ldots, x_n) = 0$ has a *singular point* at P on the curve if the partial derivatives at this point **all** vanish at that point. For example, in the case of $y^2 = x^3 + x^2$, we write this as the zero set of the projectivized equation $y^2z - x^3 - x^2z$ which has partial derivatives with respect to x, y, z: $-3x^2 - 2xz$, $2yz$, $y^2 - x^2$, which all vanish at the point $(0 : 0 : 1)$ (corresponding to the origin in the picture above). If a plan curve has no singularities, it is called *smooth*.

Finally, we can say that the equation $E : y^2 = x^3 + Ax + B$ (we can have quadratic and other terms as in the example above, but they can always be converted to an equation of this form by a change of variables) is an *elliptic curve* if it is smooth. For which A, B does this hold? Well, we can write the projectivized version as $f(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$, which has partial derivatives $-3x^2 - Az^2$, $2yz$, and $y^2 - 2Axz - 3Bz^2$. The curve is always smooth at the point at infinity, as if $z = 0$ and these three quantities are all 0, then the first equation implies that $x = 0$, and then the third equation implies that $y = 0$, which isn't allowed. Thus, we can assume that $z = 1$, we solve for the partial derivatives of $f(x, y, 1) = y^2 - x^3 - Ax - B$ being 0:

$$f_x = -3x^2 - A = f_y = 2y = 0.$$

The second implies that $y = 0$, and so the singular points on the curve are where $A = -3x^2$ and $x^3 + Ax + B = 0$ (so that its actually on the curve). Plugging the first into the second gives $x^3 - 3x^3 + B = -2x^3 + B = 0$, or $x^3 = B/2$. Thus, $(B/2)^2 = -(A/3)^3 = x^6$, and so $4A^3 + 27B^2 = 0$. This quantity, $\Delta = 4A^3 + 27B^2$, is called the *discriminant* of the elliptic curve. The answer to our question above, is then that a plane cubic $y^2 = x^3 + Ax + B$ is smooth, and hence an elliptic curve, exactly when $\Delta \neq 0$.

This begs the question, though of what makes elliptic curves special, and why we would make a definition as above. In the next section, we will see that elliptic curves have a very special, and rare, extra structure which gives us a lot of extra information. We have seen that curves described by equations of lower degree, like plane conics, can in many cases have all of their solutions completely parameterized, and that looking for congruence and sign obstructions gives us all instances where there are no rational points. Curves of higher degree certainly show up in interesting Diophantine questions (like Fermat's Last Theorem!), but many things are much harder to determine for high degree curves (even questions like is there a rational solution are not so easy, let alone quantifying how many there are in a given range, even though many problems in number theory can be phrased in terms of such questions). Thus, elliptic curves are an intermediate case, between examples like plane conics which are known fairly explicitly, and higher degree curves where many things are still not known. That is, it is not as though all natural Diophantine equations have to do with elliptic curves, but rather that when we are lucky and they do, we can say a lot more about such problems.

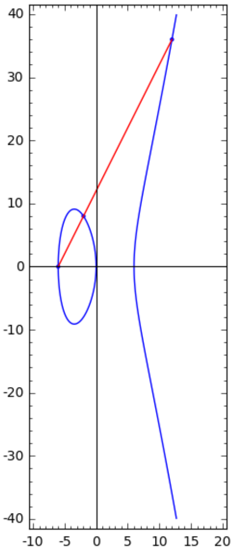
2.2. **Groups.** The special structure on elliptic curves is an instance of what is known as a mathematical *group*. We have seen many examples of groups throughout this class, and in fact we have implicitly used ideas of and general proofs from group theory in theorems sporadically throughout the class. Roughly, a group is just a set, together with the extra structure of an operation, which takes two elements of the set and gives a new element. To be a group, we just need that there is an identity element which when combined with anything leaves it along, everything has an "inverse" which combines to give this identity, and the familiar property of associativity holds.

For instance, the rational numbers, integers, real numbers, and complex numbers are all groups *under* the familiar operation of addition. So are vector spaces under addition, and so are matrices of any size under matrix addition. Groups defined by multiplications are also common: we have the set of real numbers without the number 0 (which has no multiplicative inverse), the set of invertible $n \times n$ matrices under matrix multiplication are examples. We have implicitly been studying the structure of two very important types of groups throughout this class: our properties of modular arithmetic are really saying that the set of congruence classes mod m is a group under addition, and the set of invertible congruence classes mod m (of size $\varphi(m)$) is a group under multiplication. In fact, Euler's theorem is really just an instance of a classical theorem from group theory to this situation, and our study of primitive roots can all be phrased in terms of group theory terms in a nice way (if you've taken abstract algebra, you may want to think about this, if not, if you do take abstract algebra, you can use these examples and proofs from class as a template to think back on when you are learning more abstract versions).

Many other groups come from studying geometry. For example, group theory is famously connected with studying symmetry, and if you want to count numbers of configurations of objects with lots of symmetry (for example, to study Rubik's cubes or benzene rings with chemical attachments), group theory is what you want to study. Elliptic curves give another example of groups defined from geometric pictures. To describe this, we first need a theorem hinted at above.

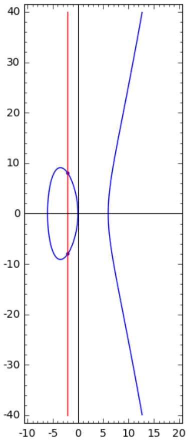
Theorem (Bezout)**.** *Two projective plane curves with no common component (think: e.g. they aren't the same curve, so they don't intersect in infinitely many points, and specifically, if you compute the gcd of their two polynomials, it must be constant), of degrees m, n (=degree of the defining polynomial) intersect exactly mn times (with multiplicity).*

As for what multiplicity means, as an example, if a line intersects a curve, it usually has multiplicity 1 at a point of intersection, but if it is tangent to the curve, then it has multiplicity greater than 1. Now group laws on sets take two elements and combine them to give a third element. Elliptic curves are plane curves of degree 3. Thus, if we have two points on an elliptic curve, and we'd like to "add" them, then there is a unique line between these two points. But a line has degree 1, and by Bezout's Theorem, it intersects an elliptic curve in 3 points, two of which are already accounted for. Here is a picture of this procedure in action. This is for the curve $y^2 = x^3 - 36x$ we saw above in relation to the congruent number problem, together with the two points $(-6, 0)$ and $(12, 36)$ on the curve we saw above, and the line $y = 2(x + 6)$, which intersects the curve at $(-2, 8)$:

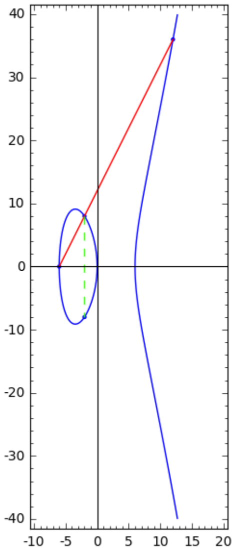


Thus, we have input two points on the curve, and obtained a *third* point on the curve. However, the "sum" of our two points won't be this point, but we are close. To describe the group law, first we must fix a point, any point, on the curve. It is convenient and standard to pick the point at infinity from above as the identity element of our group (playing the role that 0 plays in the group of real numbers under addition), which we then call "0". If we pick another point P on the curve, what should $-P$ be? Well, it should be a point such that when you draw a line through P and $-P$ the third intersection point guaranteed by Bezout's theorem is at infinity. From the pictures of elliptic curves above (they are symmetric around the x-axis as the only dependence on

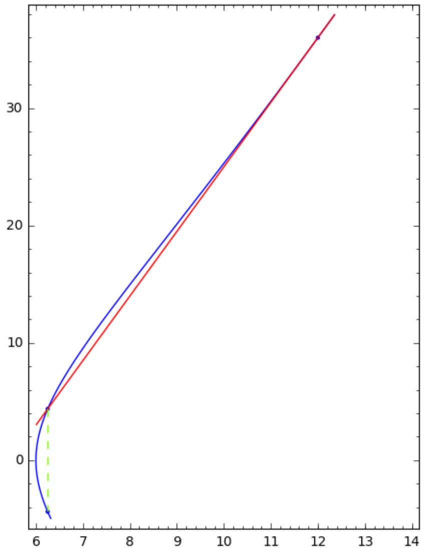
y is invariant under $y \mapsto -y$), we can see that the reflection of P across the x-axis must be $-P$:



Thus, if you add P to 0, the line through $0, P, -P$ is the vertical line through P. If you consider the points you want to add as 0 and P, then the third point of intersection on this line is $-P$, the reflection of P. But we require that $P + 0 = P$, so we have to draw the line connecting P and 0, then intersect with a third point, and *then* reflect across the x-axis to get back to P. In general, to add any two points P and Q, we draw the line and intersect with the curve as above, *then* reflect, so that in the case of $y^2 = x^3 - 36x$, $(-6, 0) + (12, 36) = (-2, -8)$, as pictured:



We have ignored one small issue in this procedure. What if we want to add a point P to itself? Well, then we draw a *tangent* line to the curve at P (which intersects the curve *twice* at that point) and take the third point on the intersection of the line and the curve, and reflect once again. For example, continuing the last example, if $P = (12, 36)$, then we can compute the tangent line to the curve $y^2 = x^3 - 36x$ as follows. We can use implicit differentiation to compute that $2y \cdot y' = 3x^2 - 36$, and so $y' = (3x^2 - 36)/2y$. At P, this gives us that the tangent line has slope $(3 \cdot 144 - 36)/72 = 11/2$, and so we draw a picture with the curve, the base point P, the tangent line (in point-slope form) $y - 36 = 11/2 \cdot (x - 12)$, the third intersection point with the curve $(25/4, 35/8)$, and the reflected point $2P = (25/4, -35/8)$:



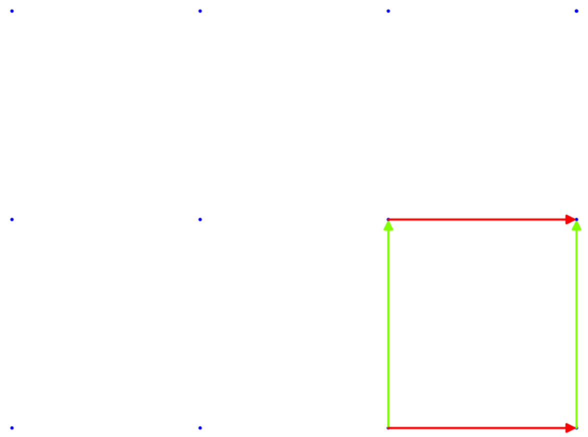
Note that this gives us a procedure for generating many further examples of rational right triangles with area 6. Here, by using the bijection above, we find that this rational point exhibits the rational right triangle with side lengths $(7/10, 120/7, -1201/70))$ and area 6 (note: if you plug in the point $2P$ on the elliptic curve directly into the bijection above, you get three negative numbers; above, we didn't worry about the positivity of solutions required by side lengths of triangles, but this is easy to fix as the degree of each term in $x^2 + y^2 - z^2$ and $xy/2$ is 2). We can generate many more, in fact infinitely many more, such rational triangles by repeating this and continually doubling the points we obtain. This gives the rational points on the curve:

$$\begin{aligned}
4P &= \left(\frac{1442401}{19600}, \frac{1726556399}{2744000}\right), \\
8P &= \left(\frac{4386303618090112563849601}{233710164715943220558400}, \frac{8704369109085580828275935650626254401}{112983858512463619737216684496448000}\right) \\
16P &= \Big(\frac{2113^2 \cdot 33087169^2 \cdot 3033189572179771349774346023748715960 33^2}{2^8 \cdot 5^2 \cdot 7^2 \cdot 31^2 \cdot 1151^2 \cdot 1201^2 \cdot 1249^2 \cdot 10177^2 \cdot 106207^2 \cdot 730753^2 \cdot 205792513^2 \cdot 1727438169601^2}, \\
&\quad (2113 \cdot 16127 \cdot 33087169 \cdot 1807396543 \cdot 1836702719 \cdot 8904449709313 \cdot 12811537941060031 \\
&\quad \times \cdot 188502661525747924577 29 \cdot 127722445692094625215 4497 \\
&\quad \times\ 303318957217977134977434602374871596033/(2^{12} \cdot 5^3 \cdot 7^3 \cdot 31^3 \cdot 1151^3 \cdot 1201^3 \cdot 1249^3 \\
&\quad \times 10177^3 \cdot 106207^3 \cdot 730753^3 \cdot 205792513^3 \cdot 1727438169601^3))\Big)
\end{aligned}$$

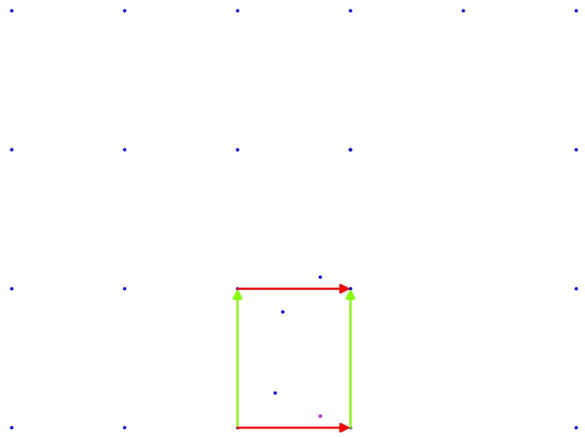
The numerator of the second fraction, in reduced terms has 148 digits! It would certainly be infeasible to find these points, and the corresponding right triangles, by “brute force”. The equations for these fractions get extremely complicated quickly (which is related to why adding points on elliptic curves is handy for cyrtography).

Finally, let’s note that the group operation of “adding” points on an elliptic curve, although is natural from a geometric/graphical perspective, can be defined entirely algebraically. That is, the equation for a line between two points can be written down easily, and finding the third point of intersection can be done by solving the equation for the line for one of the variables and plugging into the other equation which gives a solvable cubic equation (this cubic polynomial already has two known roots, facilitating its factorization). Reflecting a point is also easy algebraically; one just negates the y-variable. Thus, one can write down explicit equations algebraically defining the elliptic curve point addition property. These equations will not look pretty, but they serve an important purpose. Namely, you can study elliptic curves and their group laws in more general contexts. For instance, if the coefficients A, B are rational numbers (and, technically, if there is a rational solution to the equation $y^2 = x^3 + Ax + B$), then we can define a *rational elliptic curve* as the set of rational solutions to the same equation, satisfying the same equations for adding points. These equations preserve rationality and make sense even though you can’t draw an equation for a line or a curve over the rationals (which have loads of gaps at irrational numbers) in the same way that you can draw the pictures over the real numbers.

2.3. **Doughnuts and multi-holed doughnuts.** Now that we know that elliptic curves are special because they have a nice group law on their points, even over smaller sets of numbers like the rational numbers. We can also consider elliptic curves “over” the set of complex numbers. These become very nice geometrically, once we do so. The elliptic “curve” in this case is one-dimensional, as curves are wont to be, but the “dimension” here is counted as a dimension of complex numbers, which in a sense are two-dimensional (indeed, we often picture complex numbers as a plane with real coordinates of any point). Thus, in a certain sense, these "curves" are (real) two-dimensional. What does the picture of the curve look like over $\mathbb{C}$? The answer is that you obtain a very nice mathematical object: a torus. Or, we may think of this as a doughnut. Doughnuts have a very nice group law on them. We can think of a doughnut as the shape we get by starting with a parallelogram, and "gluing" opposite sides together (in the picture, we have drawn a number of points in a simple lattice in the complex plane, a square subtended by four of them, and color-coded the sides to glue together):



Here is how to naturally define a group law structure on this torus. If we have two points in the torus, we can consider them as points in the complex plane, specifically in the colored box. Now to add them, we simply add them as complex numbers. If this sum is also int the box, great, that is the sum. If the sum goes outside the box, we shift the point by adding any of the blue lattice points to it until we end up back in the box. For example, in the following picture, we add the two blue points in the box as complex numbers and obtain the blue point just outside the box, which we shift down to obtain the purple point in the box, and this is the sum of the two blue points on the elliptic curve.



What about smooth plane curves defined by polynomials of other degrees? Well, in the degree 0 case, we have either a point or the empty set, in the degree one case, we have a line, and in the degree 2 case, we are looking at something like a conic section, which we know a lot about (going back to the Greeks). The degree 3 case is the elliptic curve case, which we have seen is very rich. If the degree is $d \geq 1$, then in general we have a curve which, over $\mathbb{C}$ looks like a doughnut, but with $\frac{1}{2}(d-1)(d-2)$ holes in it. While this may have a nice picture over $\mathbb{C}$, there isn't the same kind of natural group law on doughnuts with multiple holes, and higher degree plane curves don't have group laws like elliptic curves do. This makes their study much more difficult.

2.4. **Birch and Swinnerton-Dyer conjecture.** The shape of elliptic curves over $\mathbb{C}$ is fairly simple, as tori are fairly simple. The study of elliptic curves over $\mathbb{R}$ is also fairly simple, as we have calculus, and results like the Intermediate Value Theorem. The study of elliptic curves over $\mathbb{Q}$, is of central interest in number theory, though it is much more difficult. We do know the *Mordell-Weil* theorem, which states that the set of points of an elliptic curve over $\mathbb{Q}$ has a specific shape. While we don't want to define this explicitly, basically, this says that there are finitely many points of finite order on the curve (order here can be defined just like order of an integer modulo m), and that up to these special points, called torsion points, the group of points "looks like" r copies of the integers, namely like the set of r-tuples of integers under vector addition, where r is a mysterious number called the *rank* of the curve. We do not yet know if there is an algorithm to compute these ranks in general, so it is a very difficult number to determine indeed. However, there is a big conjecture of Birch and Swinnterton-Dyer, currently worth $1 million, which claims that there is an analytic object related to elliptic curves which "knows" the rank, and which we can actually compute. For our purposes, what is really important is that this number is positive if and only if there are infinitely many rational points on the curve.

3. The congruent number problem again

The curve $E_n : y^2 = x^3 - n^2x$, related to the congruent number problem, has four natural points on it: the point at infinity, $(0,0)$, and $(0, \pm n)$. These points are all of finite order, namely of order 1 (the identity element has order 1 in all groups), and of order 2 (geometrically, this is the fact that the curve has vertical tangent lines at these points, which is proven by computing the slopes via implicit differentiation). It turns out that these are the *only* torsion points. Thus, all of the above discussions can be combined into one over-arching result.

Theorem. *The number n is congruent if and only if there are infinitely many rational points on the elliptic curve E_n.*

Tunnell, using this and other known results about the "analytic object" hinted at in the last section proved the following beautiful result, which gives a very fast way to test if a number n is congruent.

Theorem (Tunnell)**.** *If n is a square-free integer, consider the four numbers*

$$A_n = \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 32z^2 = n, \ B_n = \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = n$$

$$C_n = \#\{(x,y,z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 64z^2 = n, \ D_n = \#\{(x,y,z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 16z^2 = n.$$

If n is congruent, then $2A_n = B_n$ is n is odd, and $2C_n = D_n$ is n is even. Conversely, if the Birch and Swinnerton-Dyer conjecture holds, then the converse is true.

For example, we saw that the "smallest" triangle representing 157 as a congruent number is absolutely enormous, and you can't find it by brute force computer search. Let's test whether its congruent using Tunnell's criterion. Since n is odd, we should compute A_n and B_n. We can just search for solutions on a computer. Its easy to bound the ranges on x, y, z we have to search through. For example, if $2x^2 + y^2 + 32z^2 = 157$, then $2x^2 \leq 157$ and so $|x| \leq 8$. In this case, we find no solutions to the above quadratic equations, and so $2C_n = C_nD_n = 0$. Thus, assuming the Birch and Swinnerton-Dyer conjecture, we have that 157 is congruent, as we claimed above. We can show unconditionally that 1 isn't congruent via Tunnell's criterion by noting that the only solutions to the equations defining A_n and B_n are $(x,y,z) = (0, \pm 1, 0)$, so that $A_n = B_n = 2$. But $2 \cdot 2 \neq 2$, and so 1 must not be congruent. To search for solutions in these cases, I only needed to test the values of 3 triples for each of A_n and B_n, which is pretty efficient. In general, Bach and Ryan proved that for general n, this criterion can be checked in about time $O(n^{\frac{1}{2}})$.

We conclude with an interesting consequence of all of the above, which is non-obvious.

Corollary 3.1. If n is congruent, then there exist infinitely many rational right triangles with area n.