MATH 395 ELEMENTARY NUMBER THEORY

RATIONAL POINTS ON CURVES

Contents

Date: November 30, 2021(Last updated).

1. Pythagoras Draws a Triangle

Recall the Pythagorean theorem $a^2 + b^2 = c^2$. We call a Pythagorean triple three positive integers (a, b, c) that satisfy the equation

$$a^2 + b^2 = c^2.$$

It's a much more complicated problem when we ask for all a, b, c to be integers! For example $(3, 4, 5), (5, 12, 13), (8, 15, 17), (28, 45, 53)$ are such.

As a warm up, try to show that there are infinitely many Pythagorean triples.

So we call a *primitive Pythagorean triple* a Pythagorean triple (a, b, c) such that a, b, and c have no common factors. Let's prove the following theorem.

Theorem 1.1. *Any primitive Pythagorean triple where a is odd and b is even must be given by*

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2}$$

where $s > t > 0$ are any odd integers with no common factors.

We will prove this in a series of steps. The following exercise explains the conditions of the theorem.

Exercise 1. First argue that if a and b are both even, then (a, b, c) is not primitive. Second, show that it is not possible for a and b to be both odd. (Argue that if a, b are odd then c has to be even, then write $a = 2x + 1, b = 2y + 1, c = 2z$ and show why they cannot satisfy $a^2 + b^2 = c^2$.)

Now let's move on to the proof. Starting with a Pythagorean triple (a, b, c) we can write

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

Exercise 2. Show that $c - b$ and $c + b$ have no common factor. Suppose that d is a common factor, then we have to show that $d = 1$. Argue that d must divide $(c + b) + (c - b)$ and $(c + b) - (c - b)$, and also $(c - b)(c + b)$ to conclude that d must indeed be 1.

Remark 1.2. The previous exercise requires proof of the following fact: A nonzero integer d is said to divide an integer m if $m = dk$ for some integer k. Show that if d divides both m and n, then d also divides $m - n$ and $m + n$.

Exercise 3. Show using the previous exercise that $c - b$ and $c + b$ must both be squares. In other words, we can write

$$c + b = s^2, \quad c - b = t^2$$

where $s > t > 0$ are any odd integers with no common factors. Then solve to get

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2}.$$

Exercise 4. Do a quick algebra check to show that (a, b, c) above indeed give a Pythagorean triple. To show that it is in fact primitive, Assume that there is a common prime factor and use the fact (we shall see later) that if a prime divides a product, then it divides one of the factors.

Nice work! You just proved your first number theory theorem!

2. Pythagoras Draws a Circle

So we've found all solutions to $a^2 + b^2 = c^2$. If we divide by c^2, we get

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

In other words, the pair $\left(\frac{a}{c}, \frac{b}{c}\right)$ is a solution to the equation of the circle $x^2 + y^2 = 1$. We call it a *rational point* on the circle, because it is a solution in the rational numbers. Let's find *all* the rational points on the circle.

Suppose m is a rational point, so we can write it as a reduced fraction $m = \frac{p}{q}$. Let L be the line passing through the point $(-1, 0)$ on the circle with slope m.

Exercise 5. Show that the line is given by $y = m(x+1)$. It intersects the circle at two points, one of them being $(-1, 0)$. Show that the second point of intersection has coordinates

$$\left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right).$$

Exercise 6. Argue that if (x_1, y_1) is a rational solution to $x^2 + y^2 = 1$, then the line formed by (x_1, y_1) and $(-1, 0)$ will have a slope that is a rational number.

Together, we have:

Theorem 2.1. *Every rational point on the circle is given by*

$$(x, y) = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right),$$

where m runs over all rational numbers.

We can relate this to Pythagorean triples by substituting $m = p/q$ to get

$$(x, y) = \left(\frac{q^2-p^2}{q^2+p^2}, \frac{2pq}{q^2+p^2}\right),$$

and clearing denominators gives us the triple $(q^2 - p^2, 2pq, q^2 + p^2)$, though not necessarily primitive!

Exercise 7. Let's show that the triple $(q^2 - p^2, 2pq, q^2 + p^2)$ is primitive if and only if $p < q$, p, q have no common factor, and one of p, q is even and the other is odd. Hint: For the backwards implication, assume that $q^2 - p^2, 2pq, q^2 + p^2$ have a common factor d that divides all three terms. Then d divides also divides the terms

$$(q^2 - p^2) + (q^2 + p^2), \quad \text{and} \quad (q^2 - p^2) - (q^2 + p^2)$$

and conclude that d must be 1.

So we found all rational points on $x^2 + y^2 = 1$. Now let's show that $x^2 + y^2 = 3$ has *no* rational points! Note that

$$\left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2 = 3 \Leftrightarrow (ad)^2 + (bc)^2 = 3(bd)^2$$

So it is enough to consider the equation $a^2 + b^2 = 3c^2$. Assume there is an integer solution (a, b, c), and that a, b, c have no common divisor. We say $a \equiv b \pmod{m}$, "a is congruent to b modulo m," if $a - b$ is divisible by m.

Exercise 8. Show that if c is even, then a and b must be both odd or both even. In either case, show that this leads to a contradiction.

Exercise 9. Show that if c is odd, then $3c^2 \equiv 3 \pmod{4}$ and $a^2 + b^2 \equiv 1 \pmod{4}$, which gives a contradiction.

Either way, we get a contradiction. Thus we have proven:

Theorem 2.2. *The circle $x^2 + y^2 = 3$ has no rational points.*

Let's conclude this section with a general criterion proved by Legendre.

Theorem 2.3. *Let $a, b, c \in \mathbb{Z}$. Then $ax^2 + by^2 + c = 0$ has a rational point if and only if*

(1) *Not all a, b, c have the same sign,*

(2) *abc is squarefree,*

(3) *$-ab$ is a square* mod *c, $-ac$ is a square* mod *b, and $-bc$ is a square* mod *a.*

In the case that we have just studied, we have $a = 1, b = 1, c = -3$. Also, $abc = -3$ is clearly squarefree. Then it you can check that $-ab = -1 \equiv 2$ is not a square mod 3, so it fails the criterion. In general, you see that for the circle of radius $\sqrt{c}$, we have to know something about squares modulo some integer. We'll now take a trip through quadratic residues to pick up a few more tools.

3. Prime time with Euclid

Let's take a diversion into some classical elementary number theory. We'll start with the Euclidean algorithm: Let a, b be positive integers. Then we divide recursively:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Exercise 10. Prove that $r_n = \gcd(a, b)$, and explain why this process always terminates in a finite number of steps. Then use this to prove Bézout's identity: Given any two integers a and b, there are integers x and y such that

$$ax + by = \gcd(a, b).$$

Use the last result to prove the next, called Euclid's Lemma (which we assumed for our classification of primitive Pythagorean triples).

Exercise 11. Let a, b positive integers and p a prime. Prove that if $p|ab$, then $p|a$ or $p|b$ (or both).

And now for the fundamental theorem of arithmetic, the unique prime factorization of integers.

Exercise 12. Prove that every integer $n > 1$ can be represented as a product of prime factors in only one way, up to rearranging the factors. (Hint: First, show by induction that any positive integer is a prime or a product of primes. Second, assume by that n has two prime factorizations. Use the previous facts to show that these two factiorizations must be the same up to rearrangement.)

Euclid famously showed that there are infinitely many primes. The proof was by contradiction, therefore not constructive. Let's show something a little stronger.

Theorem 3.1. *There are infinitely many primes p such that $p \equiv 3 \pmod 4$.*

Let's suppose we have a finite list of such primes $3, p_1, \ldots, p_r$ to begin with. Note that $p_1 > 3$. Then we define a new number

$$N = 4p_1 \cdots p_r + 3.$$

Exercise 13. Argue that there is at least one prime q in the prime factorization of N such that $q \equiv 3 \pmod 4$. Then show that q is not in the list of primes $p_1, \ldots, p_r$. So you've produced a new prime congruent to 3 mod 4!

This proof is actually *constructive*: it gives an infinite list of actual primes. But it's not everything! But this process doesn't work for 1 mod 4. Here's a general theorem for the record.

Theorem 3.2 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Let a, m be integers with $\gcd(a, m) = 1$. Then there are infinitely many primes p such that $p \equiv a \pmod m$.*

4. Pythagoras meets Fermat

Now let's prove the $n = 4$ case of the Fermat theorem:

Theorem 4.1. *The equation $x^4 + y^4 = z^4$ has no solution in the positive integers.*

Actually, we'll show that $x^4 + y^4 = z^2$ has no solution, which is stronger (do you see why?). The proof willabe by the method of descent. We will assume to the contrary that there exists a solution, and use that solution to construct a smaller solution. This process can then be repeated to give a contradiction, because you can't keep getting smaller and smaller positive integer solutions.

So assume that (x, y, z) is a solution. If they have a common divisor, we can cancel it like in the case of the Pythagoras theorem, so we can assume they have no common divisor. So we have in fact a primitive Pythagorean triple

$$(x^2, y^2, z) = \left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}\right)$$

where s, t are odd and relatively prime.

Exercise 14. (Easy) Show that $s \equiv t \pmod 4$.

Exercise 15. Consider the equation $2y^2 = s^2 - t^2 = (s - t)(s + t)$. Show that there must be relatively prime integers u and $2v$ such that

$$s + t = 2u^2 \text{ and } s - t = 4v^2.$$

Then solve to get

$$x^2 + 4v^4 = u^4.$$

Explain why $(x, 2v^2, u^2)$ is a primitive Pythagorean triple.

Once again, let's write

$$(x, 2v^2, u^2) = \left(ST, \frac{S^2 - T^2}{2}, \frac{S^2 + T^2}{2}\right)$$

where S, T are odd and relatively prime.

Exercise 16. Show that $S + T = 2X^2$ and $S - T = 2Y^2$ for some $X, Y \in \mathbb{Z}$. Substitute this into u^2 to get $u^2 = X^4 + Y^4$, so we have obtained a new solution to the equation $x^4 + y^4 = z^2$! Finally, argue that $u < z$ so in fact the new set of solutions is smaller than the first. This proves the theorem.

The first step in Fermat's Last Theorem goes like this: Assume to the contrary that $a^n + b^n = c^n$ has a solution for some $n > 2$. Then one considers the equation $y^2 = x(x - a^n)(x - b^n)$. This is a special *elliptic curve* known as the *Frey curve*. Mathematician Kenneth Ribet proved that this curve does not satisfy a certain property called modularity. But then it was later shown by Andrew Wiles et al. that every elliptic curve is modular. So the Frey curve cannot exist, and therefore the Fermat equation has no solutions!

5. Let's get Elliptic

An elliptic curve is an equation of the form $y^2 = x^3 + ax^2 + bx + c$. The reason that we study elliptic curves is that any general cubic

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

can be transformed into an elliptic curve by a change of variables, which we call the Weierstrass normal form.

Let's start simple cases.

Theorem 5.1. *The elliptic curve $y^2 = x^3 + x$ has only one rational point $(0, 0)$.*

We'll assume that we have a rational solution $(x, y) = (\frac{a}{b}, \frac{c}{d})$ written in reduced fractions, and show that it must be $(0, 0)$. Substituting and clearing denominators, we have

$$b^3c^2 = a^3d^2 + ab^2d^2. \tag{1}$$

Any integer solution to this equation will be a rational point.

Exercise 17. By rearranging the equation in different ways, show that argue that $d^2|b^3$ and $b|d$.

Since $b|d$, let's write $d = bv$ for some $v \in \mathbb{Z}$. In fact, let's prove that that $b = v^2$ and $d = v^3$.

Exercise 18. First argue that $b = v^2z$ for some $z \in \mathbb{Z}$. Then substitute $b = v^2z$ and $d = v^3z$ into Equation (1), and use that to conclude that $z = 1$.

So now we have $c^2 = a^3 + av^4 = a(a^2 + v^4)$.

Exercise 19. Argue that a and $a^2 + v^4$ are relatively prime, and in fact they must be squares.

So we can write $a = u^2$ and $a^2 + v^4 = w^2$. Substituting the first into the second, we get $u^4 + v^4 = w^2$.

Exercise 20. Now put this all together! Use the preceding results and what you know about the Fermat equation $x^4 + y^4 = z^4$ to conclude the theorem.

Now let's try the elliptic curve $y^2 = x^3 - 3x + 7$. You can check that $P = (2, 3)$ is an (integral) point on the curve. This time, we'll use some calculus to find new rational points on the curve.

Exercise 21. Use implicit differentiation to find an equation for the tangent line to the curve at the point $P = (2, 3)$. Intersect the line with the curve, and solve to find a second rational point Q. Reflect the point Q across the x-axis, and call it R. Intersect the curve with the line through P and R to get a third rational point.

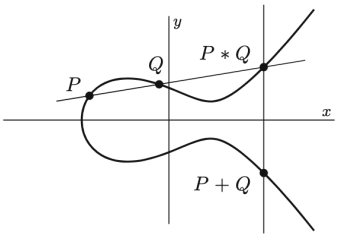
Now that we're warmed up, let's dive a little deeper into the wild world of elliptic curves!

6. Elliptic Arithmetic

Start with E an elliptic curve $y^2 = x^3+ax^2+bx+c$. Change variables $(x, y) \mapsto (\frac{X}{Z}, \frac{Y}{Z})$ to get

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

When $Z = 0$, we get $X^3 = 0$ and call that the point at infinity, labelled O. It is a triple root, this means that the cubic meets the line at infinity in three points, but the points are all the same.



We are going to learn how to do arithmetic with rational points on E. Using the scheme above, we can see that the 'negative' of a point $P = (x, y)$ on E is the reflection along the x-axis $-P = (x, -y)$, where by negative, we mean that $P + (-P) = O$. Now set

$$P = (x_1, y_1), \quad Q = (x_2, y_2), \quad P * Q = (x_3, y_3), \quad P + Q = (x_3, -y_3).$$

Exercise 22. Assume that P and Q are given as above, and let's compute $P + Q$. First show that the line joining P and Q is given by

$$y = mx + d, \qquad m = \frac{y_2 - y_1}{x_2 - x_1}, \qquad d = y_1 - mx_1 = y_2 - mx_2.$$

Substitute $y = mx + c$ into $y^2 = x^3 + ax^2 + bx + c$ and rearrange to get

$$0 = x^3 + (a - m^2)x^2 + (b - 2md)x + (c - d^2).$$

This is a cubic equation in x. We know that x_1, x_2 are roots, so let x_3 be the third one. Therefore

$$x^3 + (a - m^2)x^2 + (b - 2md)x + (c - d^2) = (x - x_1)(x - x_2)(x - x_3).$$

Expand and compare the coefficient of x^2 on both sides to get $a - m^2 = -x_1 - x_2 - x_3$, so that

$$x_3 = m^2 - a - x_1 - x_2, y_3 = mx_3 + d.$$

Exercise 23. Work out the above with the concrete example of $y^2 = x^3+17$ with points $P = (-1, 4)$ and $Q = (2, 5)$ to show that $P + Q = (-\frac{8}{9}, -\frac{109}{27})$.

Exercise 24. What happens if we let $Q \to P$? Let's show that $P + P = 2P$. In this case we can't use the slope formula above since it's $\frac{0}{0}$. Find the tangent line at P by differentiating implicitly to show that

$$\left.\frac{dy}{dx}\right|_P = \frac{f'(x_1)}{2y_1}.$$

Use this to show that on $y^2 = x^3 + 17$ the point $P = (-1, 4)$ doubles to $2P = (\frac{137}{64}, \frac{2651}{512})$.

These operations suggest that the rational points on a (nice) elliptic curve, $E(\mathbb{Q})$ form a *group*.[1]

[1] A group is a set that has an identity element and is closed under multiplication and addition operations.

Definition 6.1. We say an element P of a group has finite order m if $mP = P + \cdots + P = O$ and $nP \neq O$ for all $1 \leq n < m$. If such an m exists we say P has finite order, and if not then it has infinite order.

Let E be an elliptic curve

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Exercise 25. Show that there are 4 points of order 2 on E. First argue that for any point P on E such that $2P = O$, its y coordinate is 0. Then use this to obtain 3 points that are different from O.

Now let's look for points of order 3.

Exercise 26. Let P be a point of order 3. Write the relation as $2P = -P$. Use this to argue that P is a point of order 3 if and only if the x-coordinate of $2P$ is equal to the x-coordinate of P. Use Exercise 24 to show that the x-coordinate of $2P$ is equal to

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Set that equal to x and to get

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0.$$

Conclude that P is a point of order 3 if and only if its x-coordinate is a solution to the equation above.

Remark 6.2. There is also a geometric way to describe the points of order 3: as inflection points on E, that is, the points where the tangent line to the cubic has a triple order contact. We can see this geometrically. The condition $2P = -P$ means when we draw the tangent at the point P, then take the third intersection point and connect it with O, we get $-P$. That is the case only if the third intersection of the tangent at P is the same point P. So $2P = -P$ if and only if P is an inflection point. Analytically, you can prove this by using the second derivative

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)}$$

to deduce that P is a point of order 3 if and only if it is a point of inflection.

More generally, we have the following theorem of Mordell:

Theorem 6.3. *The group $E(\mathbb{Q})$ is equal to the sum of $r \geq 1$ copies of $\mathbb{Z}$ generated by points of infinite order, and $E(\mathbb{Q})_{\text{tors}}$, the group of finite-order points. Hence*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

where $E(\mathbb{Q})_{tors}$ is called the torsion subgroup. The integer r is called the rank of E.

7. Doing more with less

When we consider the integers modulo a prime p, we call the resulting number system a finite field. It is written as $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$. Given a polynomial equation, we can look at its coefficients mod p and look for solutions in $\mathbb{F}_p$. If it does have a solution, we again call that solution a rational point over $\mathbb{F}_p$. We write it as

$$E : y^2 = f(x) \pmod{p}.$$

It turns out that the addition law on elliptic curves work well when $p \neq 2$ and the discriminant

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \not\equiv 0 \mod p,$$

(recall that the discriminant of a quadratic equation is $b^2 - 4ac$; this one is for cubics). We write $E(\mathbb{F}_p)$ for the set of rational points of E over $\mathbb{F}_p$. In other words,

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 - x^3 - ax^2 - bx - c \equiv 0 \bmod p\}$$

Actually, as before, we include again another point $\bar{O}$ that lies 'at infinity.'

Exercise 27. Consider the curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. Besides the point at infinity, show that there are exactly 8 other points in $E(\mathbb{F}_p)$ by putting in all the possibilities of x mod 5 into x^3+x+1 and checking to see if it is a square mod 5.

So we showed that $|E(\mathbb{F}_p)| = 9$. As a group, $E(\mathbb{F}_p)$ can either be equal to $\mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/3\oplus\mathbb{Z}/3\mathbb{Z}$.

Exercise 28. Prove that $E(\mathbb{F}_p) = \mathbb{Z}/9\mathbb{Z}$ by showing it has an element of order greater than 3. In particular, let $P = (0, 1) \in E(\mathbb{F}_5)$. Show that $3P \neq O$.

Now if we start with $E(\mathbb{Z})$, the group of integral points over $\mathbb{Z}$, we have a map

$$E(\mathbb{Z}) \to E(\mathbb{F}_p), \qquad P \mapsto \bar{P}$$

induced from the map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ sending $x \mapsto \bar{x} = x \pmod{p}$ and sending O to $\bar{O}$. Earlier, we wrote $E(\mathbb{Q})_{\text{tors}}$ as the group of elements of finite order (including O). It is a consequence of the Nagell-Lutz theorem that all these elements have *integral* coordinates. In other words,

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/p_1\mathbb{Z} \oplus \mathbb{Z}/p_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k\mathbb{Z}$$

for some finite set of primes $p_1, \ldots, p_k$. We'll show that this torsion subgroup can be identified with a subgroup of $E(\mathbb{F}_p)$.

Theorem 7.1. *Let E be an elliptic curve and p a prime not dividing $2D$. Then the reduction mod p map is an isomorphism from $E(\mathbb{Q})_{\text{tors}}$ to a subgroup of $E(\mathbb{F}_p)$.*[2]

Exercise 29. First, argue that negatives go to negatives, i.e., $\overline{-P} = -\overline{P}$. Then show that

$$P_1 + P_2 + P_3 = O \Rightarrow \bar{P}_1 + \bar{P}_2 + \bar{P}_3 = \bar{O}.$$

Argue that if any of P_1, P_2, P_3 is equal to O, then this follows from the first identity.

[2] A homomorphism between groups is a map that respects the group structure. An isomorphism is a bijective homomorphism.

Exercise 30. Continuing from the previous exercise, now assume that none of P_1, P_2, P_3 are equal to O. Write

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3).$$

Argue that $P_1 + P_2 + P_3 = O$ implies that P_1, P_2, P_3 lie on a straight line. Do this by substituting the equation of the line into the cubic as in Exercise 22 and reduce mod p, and also reducing the equations

$$y_i = mx_i + d \qquad i = 1, 2, 3$$

mod p. Finally, argue that the map is bijective by showing that only $P \mapsto \bar{O}$ if and only if $P = O$. In other words, the only element that maps to O is $\bar{O}$.

Now let's see how this is useful. Pick one of the following examples to work out.

Exercise 31. Let $E : y^2 = x^3 + 3$. Check that $D = -3^5$, so the theorem holds for all $p \geq 5$. Check that $|E(\mathbb{F}_5)| = 6$ and $|E(\mathbb{F}_7)| = 13$. This means that $|E(\mathbb{Q})_{\text{tors}}|$ must divide 6 and 13, so it must be trivial.

Exercise 32. Let $E : y^2 = x^3 - 43x + 166$. Check that $D = -2^{15} \cdot 13$. Then verify that $P = (3, 8)$ is an integral point on E and has order 7, by computing $2P, 4P$, and $8P$. Now check that $|E(\mathbb{F}_3)| = 7$, and use this to conclude that $|E(\mathbb{Q})_{\text{tors}}|$ must divide 7, and in fact it is equal to 7.

8. Triangles, again

Let's go back to triangles. We'll call any triangle primitive if the length of its sides are all relatively prime integers. We first prove the following non-existence statement.

Theorem 8.1. *There exists no pair of a primitive right triangle and primitive isosceles triangle which have the same perimeter and area.*

Exercise 33. By contradiction, assume there exists such a pair. First, note that since every rational isosceles triangle with a rational area has a rational height, it is a union of the two copies of a rational right triangle. Argue then that we can assume that the given triangles have sides of lengths

(1) $(x^2+y^2, x^2-y^2, 2xy)$ and $(u^2+v^2, u^2+v^2, 4uv)$, or

(2) $(x^2+y^2, x^2-y^2, 2xy)$ and $(u^2+v^2, u^2+v^2, 2(u^2-v^2)$,

for positive integers x, y, u, v such that $\gcd(x,y) = \gcd(u,v) = 1$, and exactly one of x and y (resp. u and v) are even.

Exercise 34. In case (1), show that

$$2x^2 + 2xy = 2u^2 + 4uv + 2v^2$$
$$xy(x^2-y^2) = 2uv(u^2-v^2)$$

Then use the fact that $x, x+y, u+v > 0$, to argue that this is equivalent to

$$x(x+y) = (u+v)^2$$
$$y(x-y) = 2uv(u-v)/(u+v).$$

Finally, show that this implies $(u-v)/(u+v)$ is a positive integer, and that this is a contradiction.

Exercise 35. (Optional) Prove case (2) in the same way.

Now we'll discuss the proof of the following theorem of Hirakawa and Matsumura (2018).

Theorem 8.2. *Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area. This unique pair is the right triangle with sides of lengths* $(377, 135, 352)$ *and the isosceles triangle with sides of lengths* $(366, 366, 132)$.

We'll first go over the parts that we can work out by hand.

Exercise 36. As in Exercise 33, argue that by rescaling, we may assume that such a pair exists, and the given rational triangles have sides of lengths

(1) $(k(1+x^2), k(1-x^2), 2kx)$ and $(1+u^2, 1+u^2, 4u)$, or

(2) $(k(1+x^2), k(1-x^2), 2kx)$ and $(1+u^2, 1+u^2, 2(1-u^2))$

respectively with positive rational numbers x, u, k.

Let's work out Case 2 first.

Exercise 37. First show that Case 2 implies

$$k + kx = 2$$
$$k^2x(1 - x^2) = 2u(1 - u^2),$$

and that this is equivalent to

$$k(1 + x) = 2$$
$$(2 - k)(2k - 2) = ku(1 - u^2)$$

Argue that the former equation has a unique solution (x, u, k) for every solution (u, k) with $0 < k < 2$ of the latter, this simultaneous equation is equivalent to the single latter equation under the condition $0 < k < 2$. In fact, argue that it is equivalent to

$$2k^2 - (u^3 - u + 6)k + 4 = 0.$$

Exercise 38. Argue that in the last equation, the discriminant of the left hand side as a polynomial in k must be a square integer since k is rational. Call it s^2. Conclude that

$$s^2 = (u^3 - u + 6)^2 - 32.$$

It is possible to verify that this curve has rational points

$$(u, s) = (0, \pm 2), (1, \pm 2), (-1, \pm 2), (5/6, \pm 217/216).$$

(Also, there are 2 points at infinity). Argue that the points $(u, s) = (5/6, \pm 217/216)$ imply that

$$(k, x, u) = (27/16, 5/27, 5/6), (32/27, 11/16, 5/6)$$

respectively, both of which give the unique pair in the statement up to similitude. The first 3 pairs $(0, \pm 2), (1, \pm 2), (-1, \pm 2)$ do not give triangles. Check this for at least one pair.

This last equation gives a hyperelliptic curve. For us, without saying what a genus is, a hyperelliptic curve $y^2 = f(x)$ is a curve of genus $g > 1$ where $f(x)$ is a polynomial of degree $n = 2g + 1 > 4$ or $n = 2g + 2 > 4$ with n distinct roots. In the case above, we have $g = 2, n = 6$.

Now back to Case 1.

Exercise 39 (Optional)**.** First show that Case 1 implies

$$k + kx = 1 + 2u + u^2$$
$$k^2x(1 - x^2) = 2u(1 - u^2)$$

and that this is equivalent to

$$k(1 + x) = w^2$$
$$(w^2 - k)w(2k - w^2) = 2k(w - 1)(w - 2),$$

where $w = u + 1$. Argue that the former equation has a unique solution (x, w, k) for every solution (w, k) with $w > 1, k > 0$ of the latter, this simultaneous equation is equivalent to the single latter equation under the condition $w > 1, k > 0$. In fact, argue that it is equivalent to

$$-w^5 + 3kw^3 - 2k^2w = 2kw^2 - 6kw + 4k,$$

and rearrange to get

$$2wk^2 + (-3w^3 + 2w^2 - 6w + 4)k + w^5 = 0.$$

Exercise 40. Argue that in the last equation, the discriminant of the left hand side as a polynomial in k must be a square integer since k is rational. Call it s^2. Conclude that

$$r^2 = (-3w^3 + 2w^2 - 6w + 4)^2 - 8w^6.$$

Again this gives a hyperelliptic curve. One can check that it has the following rational points

$$(w, r) = (0, \pm 4), (1, \pm 1), (2, \pm 8), (12, \pm 868),$$

and also two points at infinity. Show that none of these points give triangles.

So how far are we from proving the theorem? Well, we produced the unique triangle that we're looking for, and in both cases we found 10 explicit rational points on each of the two curves, C_1, C_2. That is, $C_i(\mathbb{Q}) \geq 10$ for $i = 1, 2$. If we can show that $C_i(\mathbb{Q}) \leq 10$, then this implies that $C_i(\mathbb{Q}) = 10$ in each case, and we've found all possible rational points, end of story.

It turns out that this is true, but you have to use a big result due to Chabauty and Coleman. It roughly says that

$$C(\mathbb{Q}) \leq C(\mathbb{F}_p) + (2g - 2)$$

for curves C with $g \geq 2$ and satisfying certain conditions, including $p > 2g$.[3]

[3]The important condition is on what is called the Jacobian variety associated to C, but that's way beyond our scope.

9. Interlude: The theory

Now for an interlude. Let's talk about the theoretical underpinnings of what you've been looking at all semester. Mostly, we're going to go over a bunch of definitions.

9.1. **Irreducible nonsingular curves.** We write $\mathbb{Q}[x, y]$ for the set of polynomials in two variables x, y with coefficients in $\mathbb{Q}$. We call a polynomial $p(x, y) \in \mathbb{Q}[x, y]$ *irreducible* if it cannot be factored into a product of lower-degree polynomials in $\mathbb{Q}[x, y]$. If $p(x, y)$ is irreducible, the level set

$$\{(x, y) \in \mathbb{R}^2 : p(x, y) = 0\},$$

or just $p(x, y) = 0$ for short, defines a curve in the plane. (More variables adds more dimensions; e.g., $p(x, y, z) = 0$ would be a surface). If $f(x, y) = 0$ defines the set of solutions S in $\mathbb{R}$, and $g(x, y) = 0$ the set T, then it can be shown that the product

$$f(x, y)g(x, y) = 0$$

has solution set equal to $S \cup T$. In other words, it is enough to study irreducible polynomials.

If $p(x, y)$ has a solution in say, $(x_0, y_0) \in \mathbb{Z}^2$, then we say that the curve defined by $p(x, y)$ is defined over $\mathbb{Z}$, and we call (x_0, y_0) an *integral point* on the curve, and analogously for rational points. Conversely, if a curve has no rational points (resp. integral), then we say it is not defined over $\mathbb{Q}$ (resp. $\mathbb{Z}$).

We call the curve $p(x, y) = 0$ smooth/nonsingular at (x_0, y_0) if $p(x_0, y_0) = 0$ and at least one of the partial derivatives $p_x(x_0, y_0)$ or $p_y(x_0, y_0)$ is defined and nonzero. If it is smooth at all its points in $\mathbb{C}^2$, we say it is smooth/nonsingular in $\mathbb{C}^2$. If $p(x, y) = 0$ is not smooth at a given point, we call that point a singularity and say the curve is singular at that point. Implicitly, all the curves we have been working with this semester have been nonsingular.

9.2. **The point at infinity.** The degree of a polynomial $p(x, y)$ is the largest sum of the exponents of its individual terms, e.g., $x^3y^2 - y^4 + 1$ has degree 5. Now if $p(x, y)$ is of degree n, we can *homogenize* it by multiplying each of its terms with some power of another variable (say z) to make every term have degree n. For example,

$$x^3y^2 - y^4 + x^2 + 1 \mapsto x^3y^2 - y^4z + x^2z^3 + z^5,$$

which can also be viewed as the change of variables

$$(x, y) \mapsto \left(\frac{x}{z}, \frac{y}{z}\right)$$

and then multiplying by z^5. The resulting polynomial $p(x, y, z)$ is called a *homogeneous* polynomial of degree n, and we say it is the homogenisation of $p(x, y)$. Setting $z = 0$ then shows us the behaviour of the point at infinity! Notice that we can easily dehomogenise it by setting $z = 1$. (If you dehomogenise at a different variable, the point at infinity gets mapped to the origin, and you can see better what is happening there.)

9.3. **Group theory.** A *group* $(G, +)$ is a set G with a binary operation $+ : G \times G \to G$ satisfying

(1) Associatively: $(a + b) + c = a + (b + c)$ for all $a, b, c \in G$.

(2) Identity: There is a unique element 0 in G such that $a + 0 = 0 + a = a$ for all $a \in G$.

(3) Inverse: For all $a \in G$ there is a unique element $-a$ such that $a + (-a) = (-a) + a = 0$.

Moreover, we say G is commutative, or abelian, if $a+b=b+a$ for all $a,b\in G$. If the cardinality $|G|$ is finite (resp. infinite), then we say G is a finite group (resp. infinite). A *subgroup* of G is a subset H of G that is closed under $+$, meaning that for any $h,h'\in H$, $h+h'$ is also in H. We say G is *finitely generated* if there is a finite subset $\{a_1,\dots,a_n\}$ such that any element of G can be written as a linear combination of $a_1,\dots,a_n$. You should think of this as like basis for a vector space. Any finitely generated abelian group can be written as the direct sum

$$G\simeq \mathbb{Z}a_1\oplus\cdots\oplus\mathbb{Z}a_n=\mathbb{Z}^r\oplus\mathbb{Z}/p_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_k\mathbb{Z}.$$

The lefthand side is just the spanning basis. The righhand side divides these into the generators of infinite and finite order. The number r of infinite order generators is called the rank of G.

By the addition law on the elliptic curve, one can check that $(E(\mathbb{Q}),+)$ forms a finitely generated abelian group. The points of finite order $E(\mathbb{Q})_{\text{tors}}$ forms a subgroup. More generally, given given an algebraic curve C, its rational points $C(\mathbb{Q})$ also forms a group, and $C(\mathbb{Q})_{\text{tors}})$ is a subgroup.

9.4. **Genus.** A compact, closed, orientable surface in $\mathbb{R}^3$ is a surface that has is contained in a bounded subset of $\mathbb{R}^3$, has no boundary, and whose normal vector $\vec{n}$ at every point is such that $\vec{n}\neq-\vec{n}$. (The Mobius strip, for example, is not closed and not orientable.) It is a fact that every such surface is equivalent to a donut with finitely many holes. The number of holes g is called the *genus* of the surface. If we identify $\mathbb{R}^2$ with $\mathbb{C}$, then we can view the compactification of $\mathbb{R}^2$ as the complex sphere, sometimes written as $\mathbb{P}^1(\mathbb{C})$, and we can view our surfaces as subsets of $\mathbb{P}^1(\mathbb{C})$. (So that we get the point at infinity.)

If $p(x,y)$ is an irreducible polynomial of degree n and defines a nonsingular curve, then as a surface in $\mathbb{P}^1(\mathbb{C})$ it has genus

$$g=\frac{(n-1)(n-2)}{2}$$

If we take it for granted, then the complex points of the elliptic curve $E(\mathbb{C})$ is a bounded, closed, orientable surface of genus 1, since $n=3$ in this case. If $g=0$, the curve is either a line or a conic, which we understand well. If $g=1$, this is the elliptic curve. (Any nonsingular cubic is 'birationally equivalent' to a cubic in Weierstrass normal form $y^2=x^3+ax^2+bx+c$, so studying cubics reduces to studying elliptic curves.)

A major theorem of Faltings says that any nonsingular rational algebraic curve C of genus $g\geq 2$ has only finitely many rational points. That is, $|C(\mathbb{Q})|<\infty$. If $n>3$, then $g>1$, then Faltings' theorem holds.

10. A Rhombus Among Us

Recall that a rhombus is a quadrilateral with sides of equal length. So up to scaling, is uniquely determined by the interior angles, θ and $\pi - \theta$. Call such a rhombus a θ-integral (resp. rational) rhombus if it has integer (resp. rational) sides, and $\sin\theta, \cos\theta \in \mathbb{Q}$.

In 1995, R. K. Guy introduced a problem of Bill Sands, that asked for examples of an integral right triangle and an integral rectangle with a common area and a common perimeter. Guy showed that there are infinitely many such integral isosceles triangle and rectangle pairs. In 2006, A. Bremner and Guy proved that there are infinitely many such Heron triangle and rectangle pairs. Since then many other variations have appeared, and we have seen one so far. Here is one by Peng and Zhang from 2018.

Theorem 10.1. *There does not exist any integral isosceles triangle and θ-integral rhombus pairs with a common area and a common perimeter.*

As usual, we proceed by contradiction. Assume such a pair exists.

Exercise 41. Let p be the side length of the rhombus and θ its smallest interior angle. Show that the perimeter is $4p$ and the area is $p^2 \sin\theta$ where $\theta = 2t/(t^2+1)$ for some $t \geq 1$.

Exercise 42. As for the isosceles triangle, let's just work with the case where it has lengths $(u^2+v^2, 2uv, 2(u^2-v^2))$. Then deduce the formulas

$$2uv(u^2-v^2) = p^2 \sin\theta$$
$$4u^2 = 4p.$$

Use this and the previous exercise to show that

$$\frac{2u(v(u-v)(u+v)t^2 - u^3t + v(u-v)(u+v))}{t^2+1} = 0.$$

Exercise 43. From the last equation, using the fact that the denominator is quadratic in t to deduce the formula for the discriminant

$$u^6 - 4u^4v^2 + 8u^2v^4 - 4v^6 = w^2.$$

Make the substitution $U = \frac{u}{v}$ and $W = \frac{w}{v^3}$ to get

$$W^2 = U^6 - 4U^4 + 8U^2 - 4.$$

This is a hyperelliptic sextic curve of genus 2, and the rank of its Jacobian is 1. A computer search shows that its only (finite) rational points are $(U, W) = (\pm 1, \pm 1)$. Use this to argue that the simultaneous equations in Exercise 42 have no nonzero rational solutions, hence a contradiction.

We call a Heron triangle a triangle that has side lengths and area that are all integers. Just like Pythagorean triples, we have another characterisation:

Theorem 10.2. *All Heron triangles are of the form*

$$((v+w)(u^2-vw), v(u^2+w^2), w(u^2+v^2)),$$

for positive integers u, v, w, where $u^2 > vw$.

There's many proofs of this, here is one.

Exercise 44. Suppose our triangle has integral lengths a, b, c and angles α, β, γ opposite to each side. Use the law of cosines

$$\cos\gamma = \frac{a^2+b^2-c^2}{2ab}$$

and $\sin\gamma = \sqrt{1-\cos\gamma}$ to compute the area $A = \frac{1}{2}ab\sin\gamma$. In particular, show that its area is $\sqrt{s(s-a)(s-b)(s-c)}$ where $s = (a+b+c)/2$.

Exercise 45. Use the previous result to conclude that all Heron triangles are as described above.

Let's prove the second result of Peng and Zhang, but assuming a few facts that we will take for granted.

Theorem 10.3. *There are infinitely many Heron triangle and θ-integral rhombus pairs with a common area and a common perimeter.*

Suppose that the Heron triangle has sides (a, b, c), and the rhombus has side p and smallest interior angle θ.

Exercise 46. Argue that by scaling, we can assume $w = 1$. Then show that

$$uv(v+1)(u^2-v) = p^2\sin^2\theta,$$
$$2u^2(v+1) = 4p.$$

Exercise 47. Continuing, argue that since $\sin\theta$ and $\cos\theta$ are rational, we can write

$$\sin\theta = \frac{2t}{t^2+1}, \qquad \cos\theta = \frac{t^2-1}{t^2+1}$$

for some rational $t \geq 1$. (The case $t = 1$ was proved by Guy. So we will take this as given.) Show that the simultaneous equations imply

$$\frac{u(v+1)(2t^2u^2v - tu^3v - 2t^2v^2 - tu^3 + 2u^2v - 2v^2)}{2(t^2+1)} = 0.$$

Argue that this implies that

$$2t^2u^2v - tu^3v - 2t^2v^2 - tu^3 + 2u^2v - 2v^2 = 0, \tag{2}$$

and solve for v to get

$$v = \frac{(2t^2u - tu^2 + 2u \pm \sqrt{g(t)})u}{4(t^2+1)}$$

where

$$4u^2t^4 - 4u(u^2+2)t^3 + u^2(u^2+8)t^2 - 4u(u^2+2)t + 4u^2.$$

(Gross!). Finally note that since v is a positive rational number, $g(t)$ should be a rational perfect square.

Thus we are once again led to the rational points on the discriminant curve $s^2 = g(t)$.

Exercise 48. Show that the quartic curve has a rational point $P_0 = (0, 2u)$. Using Fermat's method of descent, we shall construct another rational point $P_1 = (t_1, s_1)$. To do so, set

$$s = rt^2 + qt + 2u,$$

where r, q are unknown variables. Check that

$$s^2 - g(t) = \sum_{i=1}^{4} a_i t^i$$

where

$$\begin{aligned} a_1 &= 4u^3 + 4qu + 8u, \\ a_2 &= -4u^2 + 4ru + q^2 - 8u^2, \\ a_3 &= 4u^3 + 2rq + 8u, \\ a_4 &= r^2 - 4u^2. \end{aligned}$$

Exercise 49. From the above, argue that $a_3 = a_4 = 0$ implies that $r = -2u$ and $q = u^2 + 2$. Then show that this implies that the equation $s^2 - g(t) = 0$ has rational roots

$$t = 0, \frac{2u(u^2+2)}{3u^2-1}.$$

Then show that

$$t_1 = \frac{2u(u^2+2)}{3u^2-1}, \qquad s_1 = -\frac{2u(u^6 - 4u^4 + 14u^2 + 3)}{(3u^2-1)^2}.$$

Put t_1 in Equation (2) to get

$$v = \frac{u^2(u^2+2)}{4u^4+1}.$$

Exercise 50. Finally, put this all together to conclude for the triangle

$$(a, b, c) = \left(\frac{u^2(3u^2-1)(u^4+6u^2+1)}{(4u^2+1)^2}, \frac{u^2(u^2+2)(u^2+1)}{4u^2+1}, \frac{u^2(u^6+20u^4+12u^2+1)}{(4u^2+1)^2} \right)$$

and for the rhombus

$$p = \frac{(u^4+6u^2+1)u^2}{2(4u^2+1)}$$

and

$$\sin\theta = \frac{4u(u^2+2)(3u^2-1)}{(4u^2+1)(u^4+6u^2+1)}.$$

Argue that since u, v, p are positive rational numbers, $0 < \sin\theta < 1$, $u^2 > v$ and $t_1 > 1$, we have $u > \frac{\sqrt{3}}{3} = \frac{1}{\sqrt{3}}$, so this gives infinitely many Heron triangles and θ-integral rhombus pairs.

Appendix A. Legendre makes some squares

Definition A.1. Let p be a prime number. A nonzero number that is congruent to a square mod p is a called a quadratic residue mod p. Otherwise, we call it it a quadratic nonresidue mod p. A number that is congruent to 0 mod p is neither.

Let's build some intuition about quadratic (non)residues. We'll first learn a multiplication rule for quadratic (non)residues for odd primes p. First, we need some auxiliary facts:

Exercise 51. Show that $(p-b)^2 \equiv b^2 \pmod{p}$. Use this fact to explain why, in order to list all quadratic residues mod p, we only have to compute half of them. Namely, when p is odd, we only need to compute

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \pmod{p}.$$

(When p is even, we just need to know if our nonzero number is even or odd, of course.) Hint: Think about the squares of the remaining numbers $(p+1)/2, \ldots, (p-1)$.

Exercise 52. Let p be an odd prime. First show that the first half of the list of residues are distinct. In other words, if a, b are integers between 1 and $(p-1)/2$ such that $a^2 \equiv b^2 \pmod{p}$, then it must be that $a = b$. Use the fact that $a^2 \equiv b^2 \pmod{p}$ implies that

$$p \mid a^2 - b^2 = (a-b)(a+b)$$

to conclude that $a = b$. Use this to conclude that there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues mod p.

Now let's multiply!

Exercise 53.
(1) Show that if a and b are quadratic residues mod p, then so is ab.
(2) Show that if a is a quadratic residue and b is a quadratic nonresidue mod p, then ab is a nonresidue. Proceed by contradiction.

Exercise 54. (3) Show that if a and b are quadratic nonresidues mod p, then ab is a quadratic residue. To do this, first prove that the sequence $a, 2a, \ldots, (p-1)a \pmod{p}$ is a rearrangement of the sequence $1, 2, \ldots, (p-1)$. (Hint: Notice that if $\gcd(a, p) = 1$, then none of $a, 2a, \ldots, (p-1)a$ is divsible by p. Then argue that if two numbers in this list, say ja and ka are congruent mod p, so $p|(j-k)a$ and we must have that $j = k$.)

Finally, use the Exercise 14 to figure out which of the $(p-1)$ numbers are quadratic (non)residues, and use this to conclude.

We can rephrase the above as follows. Define the Legendre Symbol of a mod p to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue mod } p \\ -1, & \text{if } a \text{ is a quadratic nonresidue mod } p \end{cases}$$

Then we have

Theorem A.2. *For odd primes p, the Legendre Symbol satisfies* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Appendix B. Congruent number problem

One nice problem that we did not discuss is the congruent number problem. A natural number is a *congruent number* if it is the area of a right triangle with rational lengths.

The original congruent number problem asks: given $N \in \mathbb{N}$, does there exist a square a^2 such that $a^2 - N$ and $a^2 + N$ are also squares? We can reformulate this in terms of triangles: does there exist a rational right triangle with area N?

Exercise 55. Let N be the area of a rational triangle with sides (a, b, c). Show that

$$\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - N, \qquad \left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + N.$$

So there exists a square $(c/2)^2$ such that $(c/2)^2 \pm N$ are squares. Moreover, if (a, b, c) is a primitive Pythagorean triple $(2uv, u^2 - v^2, u^2 + v^2)$, then $N = uv(u^2 - v^2)$.

Now if N is a congruent number, then we may form the elliptic curve

$$y^2 = x^3 - Nx.$$

Exercise 56. Show that

$$(x, y) = \left(\frac{c^2}{4}, \frac{(b^2 - a^2)c}{8}\right)$$

is a rational point on the curve.

In fact, there is a 1-1 correspondence between congruent numbers and some rational points on this elliptic curve. The bijection is given by

$$(a, b, c) \mapsto \left(\frac{Nb}{c-a}, \frac{2N^2}{c-a}\right), \qquad (x, y) \mapsto \left(\frac{x^2 - N}{y}, \frac{2Nx}{y}, \frac{x^2 + N}{y}\right)$$

Exercise 57. Try this with $N = 5$. Show that $(\frac{3}{2}, \frac{20}{3}, \frac{49}{12})$ is the associated triple. The torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ consists of the points

$$\{O, (0, 0), (\pm 5, 0)\}.$$

Verify that the points (± 5.0) have order 2 and $(0, 0) + (5, 0) + (-5, 0) = O$.