Math 180A - Notes

Neil Donaldson

Winter 2022

1 Introduction

In this section[1] we motivate the study of number theory via some classic problems, and investigate the familiar Pythagorean triples.

While modern number theory has many applications and invokes a wide array of techniques from across mathematics, at its heart it is concerned with the *integers* and with integer solutions to equations: these are called *Diophantine Equations* in honor of Diophantus of Alexandria, a Greek Mathematician of the 3rd century CE, and one of the fathers of number theory. Here are some classic problems and examples; some at least should be familiar to you.

1. Find all the integer points (x, y) on the line $3x - 2y = 1$. The answer is $(x, y) = (1 + 2n, 1 + 3n)$ where $n \in \mathbb{Z}$. Can you *prove* right now that these are *all* the solutions?
2. If n is an odd integer then $n^2 - 1$ is a multiple of 8.
3. Find all *Pythagorean triples*: positive integers x, y, z such that $x^2 + y^2 = z^2$.
4. Prime numbers: if n is prime, what is the next prime? Is there a formula for the nth prime? Is $n^2 + n + 41$ always prime whenever n is an integer?
5. Which integers can be written as the sums of two squares? Three? Four?
6. Fermat's Last Theorem:[2] if $n \geq 3$ is an integer, then there are no positive integers x, y, z such that $x^n + y^n = z^n$.

1.1 Notation & Divisibility

To orient ourselves, we start by standardizing notation for our sets of interest.

Natural Numbers: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$

Whole Numbers: $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$

Integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Rational Numbers: $\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}\}$

The real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ will not play much role in this class.

[1] Corresponds roughly to § 1–3 in the textbook: *A Friendly Introduction to Number Theory*, Joseph H. Silverman, 4th ed.

[2] Historical note: In 1637 Pierre de Fermat left a note in the margin of a copy of Diophantus' *Arithmetica* famously claiming to have proved his 'theorem.' A complete proof took mathematicians another three and a half centuries…

Divisibility in the integers

After years of calculus, restricting oneself to the integers can feel alien. The fundamental difficulty is that division is often impossible: e.g. $7 \div 4 = \frac{7}{4}$ is not an integer! In algebraic language the integers fail to be closed under division and form merely a *ring*, not a *field* like the rational or real numbers. Our first order of business is to identify those pairs of integers for which division is permitted.

Definition 1.1. Let $m, n \in \mathbb{Z}$. We say that m *divides* n, and write $m \,|\, n$, if

$$\exists k \in \mathbb{Z} \text{ such that } n = km$$

We also say that m is a *divisor* or *factor* of n.

A *common divisor/factor* of two integers x, y is any (positive) integer d such that $d \,|\, x$ and $d \,|\, y$. We say that x, y are *relatively prime* or *coprime*[a] if the only positive common factor is 1.

[a] Colloquially, "x, y have no common factors."

Examples 1.2. 1. By taking $k = 3$ in the definition, we see that $4 \,|\, 12$ (that is $12 = 3 \cdot 4$).

2. By contrast, $7 \nmid 9$ since $\nexists k \in \mathbb{Z}$ such that $9 = 7k$.
3. For *every* $m \in \mathbb{Z}$ we have $m \,|\, 0$, since $0 = 0m$ (i.e. $k = 0$ works in the definition!). This includes the counterintuitive fact that $0 \,|\, 0$.
4. The common divisors of $x = 18$ and $y = 12$ are 1, 2, 3 and 6.
5. -16 and 27 are relatively prime.

A few observations and tips are in order concerning the definition.

- For brevity, the word *positive* is usually omitted when discussing (common) divisors. For instance, in Example 4 above, -2 plainly divides both 18 and 12.
- It would be tempting to say that m divides n if and only if $\frac{n}{m}$ is an integer but this is incorrect:
  - Certainly $\frac{n}{m} \in \mathbb{Z} \implies m \,|\, n$ is true (take $k = \frac{n}{m}$).
  - The converse is *false*; $0 \,|\, 0$ is the sole counter-example.

  More philosophically, since divisibility is solely a property of the integers, it is cleaner not to introduce rational numbers into the discussion.
- Keep the line vertical! $m \,|\, n$ is a *proposition* (a statement which is either true or false), whereas $m/n = \frac{m}{n}$ is (usually) a rational *number.* Some version of the following is a very common mistake:

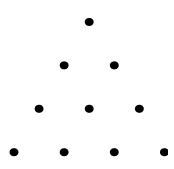
  $$m \,|\, n \nleftrightarrow m/n \nleftrightarrow \frac{m}{n} \in \mathbb{Z}$$

  Not only are we confusing propositions with numbers, but in the context of the previous observation, the resulting fraction is upside-down!

Exercises 1.1 The exercises in this chapter are to be treated informally. Rigorous arguments might require some facts about integers with which you're only somewhat familiar (e.g. prime factorization) but that we'll develop properly in future chapters. The point is to investigate and to *play.*

1. An integer is *triangular* if it is the sum of the first n natural numbers. For example:

   $1 = 1$
   $3 = 1 + 2$
   $6 = 1 + 2 + 3$
   $10 = 1 + 2 + 3 + 4$

   (a) Prove that a number is triangular if and only if it may be written in the form $\frac{1}{2}n(n+1)$ where n is a natural number.

   (b) A number is *square-triangular* if it is both square ($= m^2$) and triangular. Certainly 1 is square-triangular. Find the next square-triangular number.

   (c) Finding all square-triangular numbers m^2 is equivalent to finding all integer solutions (m, n) to the equation

   $$m^2 = \frac{1}{2}n(n+1)$$

   Prove that this is equivalent to finding integers (m, k) such that

   $$m^2 = k(2k+1) \quad \text{or} \quad m^2 = k(2k-1)$$

   (*Hint: n is either even or odd...*)

   (d) Suppose that $d \in \mathbb{N}$ is a divisor/factor of *both* k and $2k+1$. Explain why $d = 1$.

   (e) By part (d), if (m, k) solves $m^2 = k(2k+1)$, then *both* k and $2k+1$ are *perfect squares.* Prove that finding square-triangular numbers is equivalent to finding all integer solutions (x, y) to the equations[a]

   $$x^2 - 2y^2 = \pm 1$$

   (f) Find the first few pairs of solutions (x, y) to these equations and therefore find the first *five* square-triangular numbers.
   (*Hint: This is easier with a spreadsheet or by writing some computer code. Try evaluating $\sqrt{2y^2 \pm 1}$ for $y = 1, 2, 3, 4, \ldots$ and spotting when this is an integer.*)

2. Try summing the first few odd numbers and see if the results satisfy some pattern. Once you find the pattern, express it algebraically. Can you find a *geometric* verification that your formula is correct?
   (*Hint: How can you create a square with $n+1$ dots per side from a square with n dots per side?*)

3. The consecutive odd numbers 3, 5, and 7 are all primes. Are there infinitely many such *prime triplets*? That is, are there infinitely many prime numbers p such that $p+2$ and $p+4$ are also prime?

[a] The equation $x^2 - 2y^2 = 1$ is an example of *Pell's equation,* the solutions of which are related to fun things such as *continued fractions* and rational approximations to $\sqrt{2}$. For example $(99, 70)$ is a solution and $\frac{99}{70} = 1.4142857\ldots \approx \sqrt{2}$.

1.2 Pythagorean Triples

We consider positive integers x, y, z for which $x^2 + y^2 = z^2$. It is easy to find many:

1. Take a known triple, e.g. $(3, 4, 5)$, and multiply by a constant. Thus $(3n)^2 + (4n)^2 = (5n)^2$ for any $n \in \mathbb{N}$. We immediately have infinitely many triples.

2. Use a spreadsheet or computer program: generate pairs (x, y) of integers, take the square-root of $x^2 + y^2$, and test whether this is an integer. The following snippets (loosely C++/Python) do exactly this[3] returning all Pythagorean triples with $x, y \leq 100$.

```
for(int x=1; x<=100; ++x)
    {for(int y=x; y<=100; ++y)
        {real z=sqrt(x^2+y^2);
            if(z-floor(z)==0){write(x,y,z);}
        }
    }
```

```
for x in range (1,101):
    for y in range (x,101):
        z=sqrt(x^2+y^2);
        if z-floor(z)==0:
            print(x,y,z);
```

We need a different approach if we want to describe *all* triples. First we reduce the problem a little.

Definition 1.3. A Pythagorean triple (x, y, z) is *primitive* if no pair of x, y, z has a common factor.

For instance $(3, 4, 5)$ is primitive, while $(6, 8, 10)$ is not. We now state some basic results that help narrow our search:

Lemma 1.4. *Suppose that (x, y, z) is a Pythagorean triple.*

1. *If any pair of x, y, z have a common factor, the third shares this factor.*
2. *All non-primitive triples are a common multiple of a primitive triple.*
3. *If (x, y, z) is primitive, then z is odd.*

Proof. 1. Suppose WLOG that d is a common divisor of x, y. Then $d^2 \,|\, z^2$ and so[4] that $d \,|\, z$.

2. If (x, y, z) is non-primitive, then some pair has a common divisor, which divides all three by part 1. Divide x, y, z by their *greatest common factor* d to obtain the primitive triple $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$.

3. If (x, y, z) is primitive, then at most one of x, y, z can be even. Moreover, they cannot all be odd, since odd + odd $\neq$ odd.

   If $z = 2m$ were even, then $x = 2k + 1$ and $y = 2l + 1$ are both odd. But then

   $$4m^2 = z^2 = x^2 + y^2 = (2k + 1)^2 + (2l + 1)^2 = 4(k^2 + l^2 + k + l) + 2.$$

   The right hand side is not divisible by 4, so we have a contradiction. ∎

[3] This is inefficient but is fine for an initial investigation. If you want to play with it, try entering the C version into the Asymptote Web Application, or the Python into a Sage Cell. A more efficient algorithm might be based on Theorem 1.5.

[4] That $d^2 \,|\, z^2 \implies d \,|\, z$ is not as obvious as it may seem: it requires unique prime factorization (later).

To summarize the Lemma, it is enough for us to find all primitive Pythagorean triples (x, y, z) where x, z are odd and y is even. In such a situation, we start by factorizing:

$$x^2 = z^2 - y^2 = (z + y)(z - y)$$

Suppose that $z + y$ and $z - y$ had a common factor d: plainly d is odd, since both $z \pm y$ are odd. Then $\exists a, b \in \mathbb{Z}$ for which

$$\begin{cases} z + y = ad \\ z - y = bd \end{cases} \implies \begin{cases} 2z = (a + b)d \\ 2y = (a - b)d \end{cases}$$

Since d is odd, it must be a common divisor of both y and z: since (x, y, z) is primitive, $d = 1$.
It now follows[5] that $z + y$ and $z - y$ are both *perfect squares*: write

$$z + y = s^2, \qquad z - y = t^2$$

and solve for y, z and $x = st$. Again, s, t are relatively prime for otherwise y, z would have a common factor. They must also plainly both be odd. Finally, it is worth checking that the expressions we've found really do provide a triple:

$$(st)^2 + \left(\frac{s^2 - t^2}{2}\right)^2 = s^2t^2 + \frac{s^4 + t^4 - 2s^2t^2}{4} = \frac{s^4 + t^4 + 2s^2t^2}{4} = \left(\frac{s^2 + t^2}{2}\right)^2$$

We have therefore proved the main classification result.

Theorem 1.5. *(x, y, z) is a primitive triple with x odd and y even if and only if then there exist odd coprime integers $s > t \geq 1$ such that*

$$x = st, \qquad y = \frac{s^2 - t^2}{2}, \qquad z = \frac{s^2 + t^2}{2}$$

All Pythagorean triples are simply multiples of these or result from switching the order of x, y.

Examples 1.6. 1. Take $s = 9, t = 5$ to obtain the primitive triple $(45, 28, 53)$.

2. The non-primitive triple $(160, 168, 232)$ has common divisor $d = 8$ and is therefore 8 times the primitive triple $(20, 21, 29)$. This has x even and so we compute

   $$s = \sqrt{z + x} = \sqrt{49} = 7, \quad t = \sqrt{z - x} = \sqrt{9} = 3$$

   Putting it together, we obtain the representation

   $$(160, 168, 232) = 8\left(\frac{s^2 - t^2}{2}, st, \frac{s^2 + t^2}{2}\right) = 8\left(\frac{7^2 - 3^2}{2}, 7 \cdot 3, \frac{7^2 + 3^2}{2}\right)$$

Other descriptions of the Pythagorean triples are available: see e.g. Exercise 2.

[5] This again requires unique factorization. If p is a prime factor of x, then $p^2 \mid x^2$. Both factors of p must divide either $z + y$ or $z - y$, since these are coprime. Now repeat with all primes dividing x...

Exercises 1.2 1. (a) We showed that for any primitive Pythagorean triple (x, y, z), either x or y must be even. Use a similar argument to prove that either x or y must be a multiple of 3.

(*Hint: what remainders can squares have after dividing by three?*)

(b) By examining a list of primitive Pythagorean triples, make a guess about when x, y or z is a multiple of 5. Try to show that your guess is correct.

2. Try this alternative approach to finding all primitive Pythagorean triples (x, y, z) where y is even. Let $\hat{y} = \frac{1}{2}y$. Then

$$\hat{y}^2 = \frac{1}{4}y^2 = \frac{1}{4}(z^2 - x^2) = \frac{z-x}{2} \cdot \frac{z+x}{2}$$

The right side is the product of two coprime integers, which must therefore both be perfect squares. Define positive integers u, v by

$$u^2 = \frac{1}{2}(z+x), \qquad v^2 = \frac{1}{2}(z-x)$$

(a) Explain why $\frac{z-x}{2}$ and $\frac{z+x}{2}$ are coprime integers.

(b) Find x, y and z in terms of u and v.

(c) Argue that u and v have no common factor and that precisely one must be even.

(d) Compare with the solution in Theorem 1.5: how do s and t relate to u and v?

3. Let $m \geq 2$ be an integer and write the sum $\frac{1}{m-1} + \frac{1}{m+1}$ as a fraction in lowest terms. For example $\frac{1}{1} + \frac{1}{3} = \frac{4}{3}$, $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$, and $\frac{1}{3} + \frac{1}{5} = \frac{8}{15}$.

(a) Compute the next three examples.

(b) Examine the numerators and denominators of the fractions in (a) and compare them with a table of primitive Pythagorean triples. Formulate a conjecture about such fractions.

(c) Prove that your conjecture is correct.
(*Hint: $m - 1$ and $m + 1$ differ by 2...*)

1.3 Pythagorean Triples and the Unit Circle

The previous discussion of Pythagorean triples was algebraic. Now we introduce a little geometry. If (x, y, z) is a (primitive) Pythagorean triple, observe that

$$x^2 + y^2 = z^2 \implies \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

whence $(\frac{x}{z}, \frac{y}{z})$ is a *rational point* (point with rational co-ordinates) on the unit circle.
Conversely, suppose that α and β are positive rational numbers such that $\alpha^2 + \beta^2 = 1$. Write α, β in lowest terms over the smallest common denominator: i.e.

$$(\alpha, \beta) = \left(\frac{x}{z}, \frac{y}{z}\right)$$

where z is the smallest positive integer for which this is possible. Now observe that

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \implies x^2 + y^2 = z^2$$

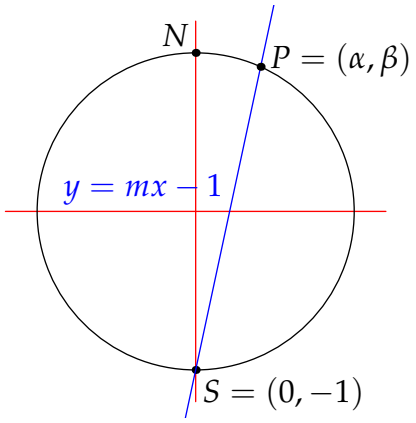
so that (x, y, z) is a Pythagorean triple! More is true, if (x, y, z) were non-primitive, then all three would be divisible by some $d \geq 2$ thus contradicting the minimality of z. To summarize:

Theorem 1.7. 1. *If (x, y, z) is a primitive Pythagorean triple, then $(\frac{x}{z}, \frac{y}{z})$ is a rational point in the first quadrant of the unit circle.*

2. *If (α, β) is a rational point in the first quadrant of the unit circle with α, β in lowest terms, then $\alpha = \frac{x}{z}$ and $\beta = \frac{y}{z}$ where (x, y, z) is a primitive Pythagorean triple.*

We could now use Theorem 1.5, to obtain an expression for the rational points on the circle. Instead, we start with the circle and work geometrically…
Suppose $P = (\alpha, \beta)$ is a point on the unit circle with rational co-ordinates. Provided $\alpha \neq 0$, the line joining P to the south pole $S = (0, -1)$ has *rational gradient*

$$y = mx - 1 \text{ where } m = \frac{\beta + 1}{\alpha} \in \mathbb{Q}$$



By substituting $y = mx - 1$ into the equation for the circle, $x^2 + y^2 = 1$ we obtain a relationship between P and m:

$$\begin{aligned} x^2 + m^2x^2 - 2mx + 1 = 1 &\implies x[(m^2 + 1)x - 2m] = 0 \\ &\implies x = 0, \frac{2m}{m^2 + 1} \end{aligned}$$

Plainly $x = 0$ corresponds to $S = (0, -1)$, while the other solution yields the second intersection P:

$$y = mx - 1 = \frac{2m^2}{m^2 + 1} - 1 \rightsquigarrow P = (\alpha, \beta) = \left(\frac{2m}{m^2 + 1}, \frac{m^2 - 1}{m^2 + 1}\right)$$

The correspondence is in fact tighter: if $m = 0$, we recover $S = (0, -1)$, while[6] $m = \infty$ results in the north pole $N = (0, 1)$. We have therefore proved:

[6] Take limits $\lim_{m \to \infty} (x, y) = (0, 1)$.

Theorem 1.8. *The extended rational numbers $\mathbb{Q} \cup \{\infty\}$ are in bijective correspondence with the rational points (α, β) on the unit circle:*

$$m \mapsto (\alpha, \beta) = \left(\frac{2m}{m^2+1}, \frac{m^2-1}{m^2+1} \right)$$

where m is the gradient of the line joining the south pole $(0,-1)$ with (α, β).

Example 1.9. The above picture shows the line with gradient $m = \frac{14}{3}$, which generates the point $P = \left(\frac{\frac{28}{3}}{\frac{196}{9}+1}, \frac{\frac{196}{9}-1}{\frac{196}{9}+1} \right) = (\frac{84}{205}, \frac{187}{205})$. Note that $(84, 187, 205)$ is a primitive Pythagorean triple.

This method may also be applied to other quadratic curves.

Corollary 1.10. *Suppose $\mathcal{C}$ is a quadratic curve in the plane whose equation has rational coefficients*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \quad \text{where} \quad a, b, c, d, e, f \in \mathbb{Q}$$

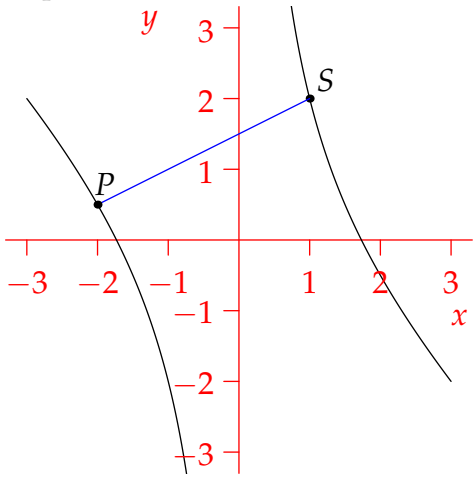
and on which lies a rational point S. Then all rational points on $\mathcal{C}$ may be found by drawing a line through S which is either vertical or has rational gradient and intersecting it with $\mathcal{C}$.

Example 1.11. To find all rational points on the hyperbola $x(y+x) = 3$, we start by choosing the rational point $S = (1, 2)$. The line through S with gradient m has equation

$$y = m(x-1) + 2$$

Substituting into the original curve, we obtain

$$\begin{aligned} &(m+1)x^2 + (2-m)x - 3 = 0 \\ \implies &(x-1)[(m+1)x + 3] = 0 \\ \implies &x = 1, -\frac{3}{m+1} \end{aligned}$$



It follows that all rational points on the hyperbola are given by

$$(x, y) = \left(-\frac{3}{m+1}, \frac{2-2m-m^2}{m+1} \right) : m \in \mathbb{Q} \setminus \{-1\}$$

In this case, $m = -4$ returns the base point S.

The line with gradient $m = -1$ and the vertical line ($m = \infty$) do not yield solutions: this is geometrically clear since they are parallel to the asymptotes of hyperbola. A full discussion of the problem requires an introduction to projective geometry, in which it can be seen that the lines intersect the hyperbola in so-called *ideal points* at infinity. The details are a matter for another course.

Hopefully these introductory discussions convince you of the variety of approaches that may be required in number theory. It is now time to begin a thorough discussion of the integers, of divisibility, and particularly the prime numbers.

Exercises 1.3 1. (a) Use lines through the point $(1,1)$ to describe all points of the circle $x^2+y^2=2$ whose co-ordinates are rational numbers.

(b) (Harder) Repeat part (a) for the conic with equation $x^2-xy-3y^2=-1$ and initial point $(2,1)$.

(*Hint: remember that there's another point with* $x=2\ldots$)

2. Suppose you attempt to apply the same procedure to find all rational points on the circle $x^2+y^2=3$. What goes wrong?

(*Hint: If* x, y *are rational, write both as fractions over the same denominator…*)

3. (a) Consider a general cubic polynomial equation

$$(x-a)(x-b)(x-c)=x^3+p_2x^2+p_1x+p_0=0$$

where a,b,c are the roots. Prove that if the coefficients $p_0,\ldots,p_2$ are rational numbers and that *two* of the roots are rational, then so is the third root.

(b) The curve $y^2=x^3+8$ contains the points $(1,-3)$ and $(-\frac{7}{4},\frac{13}{8})$. The line through these two points intersects the curve in exactly one other point. Use part (a) to help you find it.

The numbers are a little tricky, but persevere: this generalization of the line-intersection method to cubic curves is particularly important with regard to the construction of addition on elliptic curves, a central topic in modern number theory.