Table of Contents

Chapter 1

What Is Number Theory?

Exercises

1.1. The first two numbers that are both squares and triangles are 1 and 36. Find the next one and, if possible, the one after that. Can you figure out an efficient way to find triangular–square numbers? Do you think that there are infinitely many?

Solution to Exercise 1.1.
The first three triangular–square numbers are 36, 1225, and 41616. Triangular–square numbers are given by pairs (m, n) satisfying $m(m+1)/2 = n^2$. The first few pairs are $(8, 6)$, $(49, 35)$, $(288, 204)$, $(1681, 1189)$, and $(9800, 6930)$. The pattern for generating these pairs is quite subtle. We will give a complete description of all triangular–square numbers in Chapter 28, but for now it would be impressive to merely notice empirically that if (m, n) gives a triangular–square number, then so does $(3m+4n+1, 2m+3n+1)$. Starting with $(1, 1)$ and applying this rule repeatedly will actually give all triangular–square numbers.

1.2. Try adding up the first few odd numbers and see if the numbers you get satisfy some sort of pattern. Once you find the pattern, express it as a formula. Give a geometric verification that your formula is correct.

Solution to Exercise 1.2.
The sum of the first n odd numbers is always a square. The formula is

$$1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2.$$

The following pictures illustrate the first few cases, and they make it clear how the general case works.

$$\begin{array}{cc} 3 & 3 \\ 1 & 3 \end{array} \qquad \begin{array}{ccc} 5 & 5 & 5 \\ 3 & 3 & 5 \\ 1 & 3 & 5 \end{array} \qquad \begin{array}{cccc} 7 & 7 & 7 & 7 \\ 5 & 5 & 5 & 7 \\ 3 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{array}$$

$$1+3=4 \qquad 1+3+5=9 \qquad 1+3+5+7=16$$

1.3. 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 primes?

Solution to Exercise 1.3.
The only prime triplet is 3, 5, 7. The reason is that for any three odd numbers, at least one of them must be divisible by 3. So in order for them all to be prime, one of them must equal 3. It is conjectured that there are infinitely many primes p such that $p+2$ and $p+6$ are prime, but this has not been proved. Similarly, it is conjectured that there are infinitely many primes p such that $p+4$ and $p+6$ are prime, but again no one has a proof.

1.4. It is generally believed that infinitely many primes have the form N^2+1, although no one knows for sure.

(a) Do you think that there are infinitely many primes of the form N^2-1?

(b) Do you think that there are infinitely many primes of the form N^2-2?

(c) How about of the form N^2-3? How about N^2-4?

(d) Which values of a do you think give infinitely many primes of the form N^2-a?

Solution to Exercise 1.4.
First we accumulate some data, which we list in a table. Looking at the table, we see that N^2-1 and N^2-4 are almost never equal to primes, while N^2-2 and N^2-3 seem to be primes reasonably often.

N	N^2-1	N^2-2	N^2-3	N^2-4
2	3	2	1	0
3	$8=2^3$	7	$6=2\cdot 3$	5
4	$15=3\cdot 5$	$14=2\cdot 7$	13	$12=2^2\cdot 3$
5	$24=2^3\cdot 3$	23	$22=2\cdot 11$	$21=3\cdot 7$
6	$35=5\cdot 7$	$34=2\cdot 17$	$33=3\cdot 11$	$32=2^5$
7	$48=2^4\cdot 3$	47	$46=2\cdot 23$	$45=3^2\cdot 5$
8	$63=3^2\cdot 7$	$62=2\cdot 31$	61	$60=2^2\cdot 3\cdot 5$
9	$80=2^4\cdot 5$	79	$78=2\cdot 3\cdot 13$	$77=7\cdot 11$
10	$99=3^2\cdot 11$	$98=2\cdot 7^2$	97	$96=2^5\cdot 3$
11	$120=2^3\cdot 3\cdot 5$	$119=7\cdot 17$	$118=2\cdot 59$	$117=3^2\cdot 13$
12	$143=11\cdot 13$	$142=2\cdot 71$	$141=3\cdot 47$	$140=2^2\cdot 5\cdot 7$
13	$168=2^3\cdot 3\cdot 7$	167	$166=2\cdot 83$	$165=3\cdot 5\cdot 11$
14	$195=3\cdot 5\cdot 13$	$194=2\cdot 97$	193	$192=2^6\cdot 3$
15	$224=2^5\cdot 7$	223	$222=2\cdot 3\cdot 37$	$221=13\cdot 17$

Looking at the even values of N in the N^2-1 column, we might notice that 2^2-1 is a multiple of 3, that 4^2-1 is a multiple of 5, that 6^2-1 is a multiple of 7, and so on.

Having observed this, we see that the same pattern holds for the odd N's. Thus $3^2 - 1$ is a multiple of 4 and $5^2 - 1$ is a multiple of 6 and so on. So we might guess that $N^2 - 1$ is always a multiple of $N + 1$. This is indeed true, and it can be proved true by the well known algebraic formula

$$N^2 - 1 = (N - 1)(N + 1).$$

So $N^2 - 1$ will never be prime if $N \geq 2$.

The $N^2 - 4$ column is similarly explained by the formula

$$N^2 - 4 = (N - 2)(N + 2).$$

More generally, if a is a perfect square, say $a = b^2$, then there will not be infinitely many primes of the form $N^2 - a$, since

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

On the other hand, it is believed that there are infinitely many primes of the form $N^2 - 2$ and infinitely many primes of the form $N^2 - 3$. Generally, if a is not a perfect square, it is believed that there are infinitely many primes of the form $N^2 - a$. But no one has yet proved any of these conjectures.

1.5. The following two lines indicate another way to derive the formula for the sum of the first n integers by rearranging the terms in the sum. Fill in the details.

$$\begin{aligned} 1 + 2 + 3 + \cdots + n &= (1 + n) + (2 + (n - 1)) + (3 + (n - 2)) + \cdots \\ &= (1 + n) + (1 + n) + (1 + n) + \cdots . \end{aligned}$$

How many copies of $n + 1$ are in there in the second line? You may need to consider the cases of odd n and even n separately. If that's not clear, first try writing it out explicitly for $n = 6$ and $n = 7$.

Solution to Exercise 1.5.
Suppose first that n is even. Then we get $n/2$ copies of $1 + n$, so the total is

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

Next suppose that n is odd. Then we get $\frac{n-1}{2}$ copies of $1 + n$ and also the middle term $\frac{n+1}{2}$ which hasn't yet been counted. To illustrate with $n = 9$, we group the terms as

$$1 + 2 + \cdots + 9 = (1 + 9) + (2 + 8) + (3 + 7) + (4 + 6) + 5,$$

so there are 4 copies of 10, plus the extra 5 that's left over. For general n, we get

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

Another similar way to do this problem that doesn't involve splitting into cases is to simply take two copies of each term. Thus

$$\begin{aligned} 2(1+2+\cdots+n) &= (1+2+\cdots+n)+(1+2+\cdots+n) \\ &= (1+2+\cdots+n)+(n+\cdots+2+1) \\ &= (1+n)+(2+n-1)+(3+n-2)+\cdots+(n+1) \\ &= \underbrace{(1+n)+(1+n)+\cdots+(1+n)}_{n \text{ copies of } n+1} \\ &= n(1+n) = n^2+n \end{aligned}$$

Thus the twice the sum $1+2+\cdots+n$ equal n^2+n, and now divide by 2 to get the answer.

1.6. For each of the following statements, fill in the blank with an easy-to-check criterion:

(a) M is a triangular number if and only if _____ is an odd square.

(b) N is an odd square if and only if _____ is a triangular number.

(c) Prove that your criteria in (a) and (b) are correct.

Solution to Exercise 1.6.

(a) M is a triangular number if and only if $1+8M$ is an odd square.

(b) N is an odd square if and only if $(N-1)/8$ is a triangular number. (Note that if N is an odd square, then N^2-1 is divisible by 8, since $(2k+1)^2 = 4k(k+1)+1$, and $4k(k+1)$ is a multiple of 8.)

(c) If M is triangular, then $M = m(m+1)/2$, so $1+8M = 1+4m+4m^2 = (1+2m)^2$. Conversely, if $1+8M$ is an odd square, say $1+8M = (1+2k)^2$, then solving for M gives $M = (k+k^2)/2$, so M is triangular.

Next suppose N is an odd square, say $N = (2k+1)^2$. Then as noted above, $(N-1)/8 = k(k+1)/2$, so $(N-1)/8$ is triangular. Conversely, if $(N-1)/8$ is trianglular, then $(N-1)/8 = (m^2+m)/2$ for some m, so solving for N we find that $N = 1+4m+4m^2 = (1+2m)^2$, so N is a square.

Chapter 2

Pythagorean Triples

Exercises

2.1. **(a)** We showed that in any primitive Pythagorean triple (a, b, c), either a or b is even. Use the same sort of argument to show that either a or b must be a multiple of 3.

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

Solution to Exercise 2.1.
(a) If a is not a multiple of 3, it must equal either $3x + 1$ or $3x + 2$. Similarly, if b is not a multiple of 3, it must equal $3y + 1$ or $3y + 2$. There are four possibilities for $a^2 + b^2$, namely

$$\begin{aligned}
a^2 + b^2 &= (3x + 1)^2 + (3y + 1)^2 = 9x^2 + 6x + 1 + 9y^2 + 6y + 1 \\
&= 3(3x^2 + 2x + 3y^2 + 2y) + 2, \\
a^2 + b^2 &= (3x + 1)^2 + (3y + 2)^2 = 9x^2 + 6x + 1 + 9y^2 + 12y + 4 \\
&= 3(3x^2 + 2x + 3y^2 + 4y + 1) + 2, \\
a^2 + b^2 &= (3x + 2)^2 + (3y + 1)^2 = 9x^2 + 12x + 4 + 9y^2 + 6y + 1 \\
&= 3(3x^2 + 4x + 3y^2 + 2y + 1) + 2, \\
a^2 + b^2 &= (3x + 2)^2 + (3y + 2)^2 = 9x^2 + 12x + 4 + 9y^2 + 12y + 4 \\
&= 3(3x^2 + 4x + 3y^2 + 4y + 2) + 2.
\end{aligned}$$

So if a and b are not multiples of 3, then $c^2 = a^2 + b^2$ looks like 2 more than a multiple of 3. But regardless of whether c is $3z$ or $3z+1$ or $3z+2$, the numbers c^2 cannot be 2 more than a multiple of 3. This is true because

$$\begin{aligned}
(3z)^2 &= 3 \cdot 3z, \\
(3z + 1)^2 &= 3(3z^2 + 2z) + 1, \\
(3z + 2)^2 &= 3(3z^2 + 4z + 1) + 1.
\end{aligned}$$

(b) The table suggests that in every primitive Pythagorean triple, exactly one of a, b, or c is a multiple of 5. To verify this, we use the Pythagorean Triples Theorem to write a and b as $a = st$ and $b = \frac{1}{2}(s^2 - t^2)$. If either s or t is a multiple of 5, then a is a multiple of 5 and we're done. Otherwise s looks like $s = 5S + i$ and t looks like $5T + j$ with i and j being integers in the set $\{1, 2, 3, 4\}$. Next we observe that

$$2b = s^2 - t^2 = (5S + i)^2 - (5T + j)^2 = 25(S^2 - T^2) + 10(Si - Tj) + i^2 - j^2.$$

If $i^2 - j^2$ is a multiple of 5, then b is a multiple of 5, and again we're done. Looking at the 16 possibilities for the pair (i, j), we see that this accounts for 8 of them, leaving the possibilities

$$(i, j) = (1, 2),\ (1, 3),\ (2, 1),\ (2, 4),\ (3, 1),\ (3, 4),\ (4, 2),\ \text{or } (4, 3).$$

Now for each of these remaining possibilities, we need to check that

$$2c = s^2 + t^2 = (5S + i)^2 + (5T + j)^2 = 25(S^2 + T^2) + 10(Si + Tj) + i^2 + j^2$$

is a multiple of 5, which means checking that $i^2 + j^2$ is a multiple of 5. This is easily accomplished:

$$1^2 + 2^2 = 5\ \ 1^2 + 3^2 = 10 \quad 2^1 + 1^2 = 5\ \ 2^2 + 4^2 = 20 \tag{2.1}$$

$$3^1 + 1^2 = 10 \quad 3^2 + 4^2 = 25 \quad 4^2 + 2^2 = 20 \quad 4^2 + 3^2 = 25. \tag{2.2}$$

.

2.2. A nonzero integer d is said to *divide* an integer m if $m = dk$ for some number k. Show that if d divides both m and n, then d also divides $m - n$ and $m + n$.

Solution to Exercise 2.2.
Both m and n are divisible by d, so $m = dk$ and $n = dk'$. Thus $m \pm n = dk \pm dk' = d(k \pm k')$, so $m + n$ and $m - n$ are divisible by d.

2.3. For each of the following questions, begin by compiling some data; next examine the data and formulate a conjecture; and finally try to prove that your conjecture is correct. (But don't worry if you can't solve every part of this problem; some parts are quite difficult.)

(a) Which odd numbers a can appear in a primitive Pythagorean triple (a, b, c)?

(b) Which even numbers b can appear in a primitive Pythagorean triple (a, b, c)?

(c) Which numbers c can appear in a primitive Pythagorean triple (a, b, c)?

Solution to Exercise 2.3.
(a) Any odd number can appear as the a in a primitive Pythagorean triple. To find such a triple, we can just take $t = a$ and $s = 1$ in the Pythagorean Triples Theorem. This gives the primitive Pythagorean triple $(a, (a^2 - 1)/2, (a^2 + 1)/2)$.
(b) Looking at the table, it seems first that b must be a multiple of 4, and second that every multiple of 4 seems to be possible. We know that b looks like $b = (s^2 - t^2)/2$ with

s and t odd. This means we can write $s = 2m + 1$ and $t = 2n + 1$. Multiplying things out gives

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

Can you see that $m(m+1)$ and $n(n+1)$ must both be even, regardless of the value of m and n? So b must be divisible by 4.

On the other hand, if b is divisible by 4, then we can write it as $b = 2^r B$ for some odd number B and some $r \geq 2$. Then we can try to find values of s and t such that $(s^2 - t^2)/2 = b$. We factor this as

$$(s-t)(s+t) = 2b = 2^{r+1}B.$$

Now both $s - t$ and $s + t$ must be even (since s and t are odd), so we might try

$$s - t = 2^r \qquad \text{and} \qquad s + t = 2B.$$

Solving for s and t gives $s = 2^{r-1} + B$ and $t = -2^{r-1} + B$. Notice that s and t are odd, since B is odd and $r \geq 2$. Then

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

This gives a primitive Pythagorean triple with the right value of b provided that $B > 2^{r-1}$. On the other hand, if $B < 2^{r-1}$, then we can just take $a = 2^{2r-2} - B^2$ instead.

(c) This part is quite difficult to prove, and it's not even that easy to make the correct conjecture. It turns out that an odd number c appears as the hypotenuse of a primitive Pythagorean triple if and only if every prime dividing c leaves a remainder of 1 when divided by 4. Thus c appears if it is divisible by the primes $5, 13, 17, 29, 37, \ldots$, but it does not appear if it is divisible by any of the primes $3, 7, 11, 19, 23, \ldots$. We will prove this in Chapter 25. Note that it is not enough that c itself leave a remainder of 1 when divided by 4. For example, neither 9 nor 21 can appear as the hypotenuse of a primitive Pythagorean triple.

2.4. In our list of examples are the two primitive Pythagorean triples

$$33^2 + 56^2 = 65^2 \qquad \text{and} \qquad 16^2 + 63^2 = 65^2.$$

Find at least one more example of two primitive Pythagorean triples with the same value of c. Can you find three primitive Pythagorean triples with the same c? Can you find more than three?

Solution to Exercise 2.4.
The next example is $c = 5 \cdot 17 = 85$. Thus

$$85^2 = 13^2 + 84^2 = 36^2 + 77^2.$$

A general rule is that if $c = p_1 p_2 \cdots p_r$ is a product of r distinct odd primes which all leave a remainder of 1 when divided by 4, then c appears as the hypotenuse in 2^{r-1} primitive Pythagorean triples. (This is counting (a, b, c) and (b, a, c) as the same triple.) So for example, $c = 5 \cdot 13 \cdot 17 = 1105$ appears in 4 triples,

$$1105^2 = 576^2 + 943^2 = 744^2 + 817^2 = 264^2 + 1073^2 = 47^2 + 1104^2.$$

But it would be difficult to prove the general rule using only the material we have developed so far.

2.5. In Chapter 1 we saw that the n^{th} triangular number T_n is given by the formula

$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

The first few triangular numbers are 1, 3, 6, and 10. In the list of the first few Pythagorean triples (a, b, c), we find $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, and $(9, 40, 41)$. Notice that in each case, the value of b is four times a triangular number.

(a) Find a primitive Pythagorean triple (a, b, c) with $b = 4T_5$. Do the same for $b = 4T_6$ and for $b = 4T_7$.

(b) Do you think that for every triangular number T_n, there is a primitive Pythagorean triple (a, b, c) with $b = 4T_n$? If you believe that this is true, then prove it. Otherwise, find some triangular number for which it is not true.

Solution to Exercise 2.5.
(a) $T_5 = 15$ and $(11, 60, 61)$. $T_6 = 21$ and $(13, 84, 85)$. $T_7 = 28$ and $(15, 112, 113)$.
(b) The primitive Pythagorean triples with b even are given by $b = (s^2 - t^2)/2$, $s > t \geq 1$, s and t odd integers, and $\gcd(s, t) = 1$. Since s is odd, we can write it as $s = 2n + 1$, and we can take $t = 1$. (The examples suggest that we want $c = b + 1$, which means we need to take $t = 1$.) Then

$$b = \frac{s^2 - t^2}{2} = \frac{(2n+1)^2 - 1}{2} = 2n^2 + 2n = 4\frac{n^2 + n}{2} = 4T_n.$$

So for every triangular number T_n, there is a Pythagorean triple

$$(2n + 1, 4T_n, 4T_n + 1).$$

(Thanks to Mike McConnell and his class for suggesting this problem.)

2.6. If you look at the table of primitive Pythagorean triples in this chapter, you will see many triples in which c is 2 greater than a. For example, the triples $(3, 4, 5)$, $(15, 8, 17)$, $(35, 12, 37)$, and $(63, 16, 65)$ all have this property.

(a) Find two more primitive Pythagorean triples (a, b, c) having $c = a + 2$.

(b) Find a primitive Pythagorean triple (a, b, c) having $c = a + 2$ and $c > 1000$.

(c) Try to find a formula that describes all primitive Pythagorean triples (a, b, c) having $c = a + 2$.

Solution to Exercise 2.6.
The next few primitive Pythagorean triples with $c = a + 2$ are

$$(99, 20, 101), \quad (143, 24, 145), \quad (195, 28, 197),$$
$$(255, 32, 257), \quad (323, 36, 325), \quad (399, 40, 401).$$

One way to find them is to notice that the b values are going up by 4 each time. An even better way is to use the Pythagorean Triples Theorem. This says that $a = st$ and $c = (s^2 + t^2)/2$. We want $c - a = 2$, so we set

$$\frac{s^2 + t^2}{2} - st = 2$$

and try to solve for s and t. Multiplying by 2 gives

$$\begin{aligned} s^2 + t^2 - 2st &= 4, \\ (s - t)^2 &= 4, \\ s - t &= \pm 2. \end{aligned}$$

The Pythagorean Triples Theorem also says to take $s > t$, so we need to have $s - t = 2$. Further, s and t are supposed to be odd. If we substitute $s = t + 2$ into the formulas for a, b, c, we get a general formula for all primitive Pythagorean triples with $c = a + 2$. Thus

$$\begin{aligned} a &= st = (t + 2)t = t^2 + 2t, \\ b &= \frac{s^2 - t^2}{2} = \frac{(t + 2)^2 - t^2}{2} = 2t + 2, \\ c &= \frac{s^2 + t^2}{2} = \frac{(t + 2)^2 + t^2}{2} = t^2 + 2t + 2. \end{aligned}$$

We will get all PPT's with $c = a + 2$ by taking $t = 1, 3, 5, 7, \ldots$ in these formulas. For example, to get one with $c > 1000$, we just need to choose t large enough to make $t^2 + 2t + 2 > 1000$. The least t which will work is $t = 31$, which gives the PPT $(1023, 64, 1025)$. The next few with $c > 1000$ are $(1155, 68, 1157)$, $(1295, 72, 1297)$, $(1443, 76, 1445)$, obtained by setting $t = 33$, 35, and 37 respectively.

2.7. For each primitive Pythagorean triple (a, b, c) in the table in this chapter, compute the quantity $2c - 2a$. Do these values seem to have some special form? Try to prove that your observation is true for all primitive Pythagorean triples.

Solution to Exercise 2.7.
First we compute $2c - 2a$ for the PPT's in the Chapter 2 table.

a	3	5	7	9	15	21	35	45	63
b	4	12	24	40	8	20	12	28	16
c	5	13	25	41	17	29	37	53	65
$2c - 2a$	4	16	36	64	4	16	4	16	4

all the differences $2c - 2a$ seem to be perfect squares. We can show that this is always the case by using the Pythagorean Triples Theorem, which says that $a = st$ and $c = (s^2 + t^2)/2$. Then

$$2c - 2a = (s^2 + t^2) - 2st = (s - t)^2,$$

so $2c - 2a$ is always a perfect square.

2.8. Let m and n be numbers that differ by 2, and write the sum $\frac{1}{m} + \frac{1}{n}$ as a fraction in lowest terms. For example, $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$ 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 the table of Pythagorean triples on page 18. Formulate a conjecture about such fractions.

(c) Prove that your conjecture is correct.

Solution to Exercise 2.8.

(a)

$$\frac{1}{4} + \frac{1}{6} = \frac{5}{12}, \quad \frac{1}{5} + \frac{1}{7} = \frac{12}{35}, \quad \frac{1}{6} + \frac{1}{8} = \frac{7}{24}.$$

(b) It appears that the numerator and denominator are always the sides of a (primitive) Pythagorean triple.

(c) This is easy to prove. Thus

$$\frac{1}{N} + \frac{1}{N+2} = \frac{2N+2}{N^2+2N}.$$

The fraction is in lowest terms if N is odd, otherwise we need to divide numerator and denominator by 2. But in any case, the numerator and denominator are part of a Pythagorean triple, since

$$(2N+2)^2 + (N^2+2N)^2 = N^4 + 4N^3 + 8N^2 + 8N + 4 = (N^2+2N+2)^2.$$

Once one suspects that $N^4 + 4N^3 + 8N^2 + 8N + 4$ should be a square, it's not hard to factor it. Thus if it's a square, it must look like $(N^2 + AN \pm 2)$ for some value of A. Now just multiply out and solve for A, then check that your answer works.

2.9. **(a)** Read about the Babylonian number system and write a short description, including the symbols for the numbers 1 to 10 and the multiples of 10 from 20 to 50.

(b) Read about the Babylonian tablet called Plimpton 322 and write a brief report, including its approximate date of origin.

(c) The second and third columns of Plimpton 322 give pairs of integers (a, c) having the property that $c^2 - a^2$ is a perfect square. Convert some of these pairs from Babylonian numbers to decimal numbers and compute the value of b so that (a, b, c) is a Pythagorean triple.

Solution to Exercise 2.9.

There is a good article in wikipedia on Plimpton 322. Another nice source for this material is

`www.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html`

Chapter 3

Pythagorean Triples and the Unit Circle

Exercises

3.1. As we have just seen, we get every Pythagorean triple (a, b, c) with b even from the formula

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$$

by substituting in different integers for u and v. For example, $(u, v) = (2, 1)$ gives the smallest triple $(3, 4, 5)$.

(a) If u and v have a common factor, explain why (a, b, c) will not be a primitive Pythagorean triple.

(b) Find an example of integers $u > v > 0$ that do not have a common factor, yet the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is not primitive.

(c) Make a table of the Pythagorean triples that arise when you substitute in all values of u and v with $1 \leq v < u \leq 10$.

(d) Using your table from (c), find some simple conditions on u and v that ensure that the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is primitive.

(e) Prove that your conditions in (d) really work.

Solution to Exercise 3.1.
(a) If $u = dU$ and $v = dV$, then a, b, and c will all be divisible by d^2, so the triple will not be primitive.
(b) Take $(u, v) = (3, 1)$. Then $(a, b, c) = (8, 6, 10)$ is not primitive.

(c)

$u\backslash v$	1	2	3	4	5	6	7	8	9
2	(3,4,5)								
3	(8,6,10)	(5,12,13)							
4	(15,8,17)	(12,16,20)	(7,24,25)						
5	(24,10,26)	(21,20,29)	(16,30,34)	(9,40,41)					
6	(35,12,37)	(32,24,40)	(27,36,45)	(20,48,52)	(11,60,61)				
7	(48,14,50)	(45,28,53)	(40,42,58)	(33,56,65)	(24,70,74)	(13,84,85)			
8	(63,16,65)	(60,32,68)	(55,48,73)	(48,64,80)	(39,80,89)	(28,96,100)	(15,112,113)		
9	(80,18,82)	(77,36,85)	(72,54,90)	(65,72,97)	(56,90,106)	(45,108,117)	(32,126,130)	(17,144,145)	
10	(99,20,101)	(96,40,104)	(91,60,109)	(84,80,116)	(75,100,125)	(64,120,136)	(51,140,149)	(36,160,164)	(19,180,181)

(d) $(u^2 - v^2, 2uv, u^2 + v^2)$ will be primitive if and only if $u > v$ and u and v have no common factor and one of u or v is even.

(e) If both u and v are odd, then all three numbers are even, so the triple is not primitive. We already saw that if u and v have a common factor, then the triple is not primitive. And we do not allow nonpositive numbers in primitive triples, so we can't have $u \leq v$. This proves one direction.

To prove the other direction, suppose that the triple is not primitive, so there is a number $d \geq 2$ that divides all three terms. Then d divides the sums

$$(u^2 - v^2) + (u^2 + v^2) = 2u^2 \quad \text{and} \quad (u^2 - v^2) - (u^2 + v^2) = 2v^2,$$

so either $d = 2$ or else d divides both u and v. In the latter case we are done, since u and v have a common factor. On the other hand, if $d = 2$ and u and v have no common factor, then at least one of them is odd, so the fact that 2 divides $u^2 - v^2$ tells us that they are both odd.

3.2. (a) Use the lines through the point $(1, 1)$ to describe all the points on the circle

$$x^2 + y^2 = 2$$

whose coordinates are rational numbers.

(b) What goes wrong if you try to apply the same procedure to find all the points on the circle $x^2 + y^2 = 3$ with rational coordinates?

Solution to Exercise 3.2.
(a) Let C be the circle $x^2 + y^2 = 2$. Take the line L with slope m through $(1, 1)$, where m is a rational number. The equation of L is

$$y - 1 = m(x - 1), \qquad \text{so} \qquad y = mx - m + 1.$$

To find the intersection $L \cap C$, we substitute and solve:

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

We know that $x = 1$ is a solution, so $x - 1$ has to be a factor. Dividing by $x - 1$ gives the factorization

$$\begin{aligned}(m^2+1)x^2 - 2(m^2-m)x + (m^2-2m-1)\\ = (x-1)\big((m^2+1)x - (m^2-2m-1)\big),\end{aligned}$$

so the other root is $x = (m^2-2m-1)/(m^2+1)$. Then we can use the fact that the point lies on the line $y = mx - m + 1$ to get the y-coordinate,

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

So the rational points on the circle $x^2 + y^2 = 2$ are obtained by taking rational numbers m and substituting them into the formula

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

(b) The circle $x^2 + y^2 = 3$ doesn't have any points with rational coordinates, and we need at least one rational point to start the procedure.

3.3. Find a formula for all the points on the hyperbola

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

whose coordinates are rational numbers. [*Hint*. Take the line through the point $(-1, 0)$ having rational slope m and find a formula in terms of m for the second point where the line intersects the hyperbola.]

Solution to Exercise 3.3.
Let H be the hyperbola $x^2 - y^2 = 1$, and let L be the line through $(-1, 0)$ having slope m. The equation of L is $y = m(x + 1)$. To find the intersection of H and L, we substitute the equation for L into the equation for H.

$$\begin{aligned}x^2 - (m(x+1))^2 &= 1\\ (1-m^2)x^2 - 2m^2x - (1+m^2) &= 0.\end{aligned}$$

One solution is $x = -1$, so dividing by $x+1$ allows us to find the other solution $x = \frac{1+m^2}{1-m^2}$, and then substituting this into $y = m(x + 1)$ gives the formula $y = \frac{2m}{1-m^2}$. So for every rational number m we get a point

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

with rational coordinates on the hyperbola. On the other hand, if we start with any point (x_1, y_1) with rational coordinates on the hyperbola, then the line through $(-1, 0)$ and (x_1, y_1) will have slope a rational number (namely $y_1/(x_1 + 1)$), so we will get every such point.

3.4. The curve

$$y^2 = x^3 + 8$$

contains the points $(1, -3)$ and $(-7/4, 13/8)$. The line through these two points intersects the curve in exactly one other point. Find this third point. Can you explain why the coordinates of this third point are rational numbers?

Solution to Exercise 3.4.
Let E be the curve $y^2 = x^3 + 8$. The line L through $(1, -3)$ and $(-7/4, 13/8)$ has slope $-37/22$ and equation $y = -\frac{37}{22}x - \frac{29}{22}$. To find where E intersects L, we substitute the equation of L into the equation of E and solve for x. Thus

$$\begin{aligned} \left(-\frac{37}{22}x - \frac{29}{22}\right)^2 &= x^3 + 8 \\ \frac{1369}{484}x^2 + \frac{1073}{242}x + \frac{841}{484} &= x^3 + 8 \\ 484x^3 - 1369x^2 - 2146x + 3031 &= 0. \end{aligned}$$

We already know two solutions to this last equation, namely $x = 1$ and $x = -7/4$, since these are the x-coordinates of the two known points where L and E intersect. So this last cubic polynomial must factor as

$$(x - 1)(x + 7/4)(x - \text{“something”}),$$

and a little bit of algebra shows that in fact

$$484x^3 - 1369x^2 - 2146x + 3031 = 484(x - 1)(x + 7/4)(x - 433/121).$$

So the third point has x-coordinate $x = 433/121$. Finally, substituting this value of x into the equation of the line L gives the corresponding y-coordinate,

$$y = -(37/22)(433/121) - 29/22 = -9765/1331.$$

Thus E and L intersect at the three points

$$(1, -3), \quad (-7/4, 13/8), \quad \text{and} \quad (433/121, -9765/1331).$$

For an explanation of why the third point has rational coordinates, see the discussion in Chapter 41.

3.5. Numbers that are both square and triangular numbers were introduced in Chapter 1, and you studied them in Exercise 1.1.

(a) Show that every square–triangular number can be described using the solutions in positive integers to the equation $x^2 - 2y^2 = 1$. [*Hint*. Rearrange the equation $m^2 = \frac{1}{2}(n^2 + n)$.]

(b) The curve $x^2 - 2y^2 = 1$ includes the point $(1, 0)$. Let L be the line through $(1, 0)$ having slope m. Find the other point where L intersects the curve.

(c) Suppose that you take m to equal $m = v/u$, where (u, v) is a solution to $u^2 - 2v^2 = 1$. Show that the other point that you found in (b) has integer coordinates. Further, changing the signs of the coordinates if necessary, show that you get a solution to $x^2 - 2y^2 = 1$ in positive integers.

(d) Starting with the solution $(3, 2)$ to $x^2 - 2y^2 = 1$, apply (b) and (c) repeatedly to find several more solutions to $x^2 - 2y^2 = 1$. Then use those solutions to find additional examples of square–triangular numbers.

(e) Prove that this procedure leads to infinitely many different square-triangular numbers.

(f) Prove that every square–triangular number can be constructed in this way. (This part is very difficult. Don't worry if you can't solve it.)

Solution to Exercise 3.5.
(a) From $m^2 = \frac{1}{2}(n^2 + n)$ we get $8m^2 = 4n^2 + 4n = (2n + 1)^2 - 1$. Thus $(2n + 1)^2 - 2(2m)^2 = 1$. So we want to solve $x^2 - 2y^2 = 1$ with x odd and y even.
(b) We intersect $x^2 - 2y^2 = 1$ with $y = m(x - 1)$. After some algebra, we find that

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

(c) Writing $m = v/u$, the other point becomes

$$(x, y) = \left(\frac{2v^2 + u^2}{2v^2 - u^2}, \frac{2vu}{2v^2 - u^2} \right).$$

In particular, if $u^2 - 2v^2 = 1$, the other point (after changing signs) is $(x, y) = (2v^2 + u^2, 2vu)$.
(d) Starting with $(u, v) = (3, 2)$, the formula from (c) gives $(x, y) = (17, 12)$. Taking $(17, 12)$ as our new (u, v), the formula from (c) gives $(577, 408)$. And one more repetition gives $(665857, 470832)$.

To get square–triangular numbers, we set $2n + 1 = x$ and $2m = y$, so $n = \frac{1}{2}(x - 1)$ and $m = \frac{1}{2}y$, and the square–triangular number is $m^2 = \frac{1}{2}(n^2 + n)$. The first few values are

x	y	n	m	m^2
3	2	1	1	1
17	12	8	6	36
577	408	288	204	41616
665857	470832	332928	235416	55420693056

(e) If we start with a solution (x_0, y_0) to $x^2 - 2y^2 = 1$, then the new solution that we get has y-coordinate equal to $2y_0x_0$. Thus the new y-coordinate is larger than the old one, so each time we get a new solution.
(f) This can be done by the method of descent as described in Chapters 29 and 30, where we study equations of the form $x^2 - Dy^2 = 1$.