A Friendly Introduction to Number Theory by Silverman

Frosty

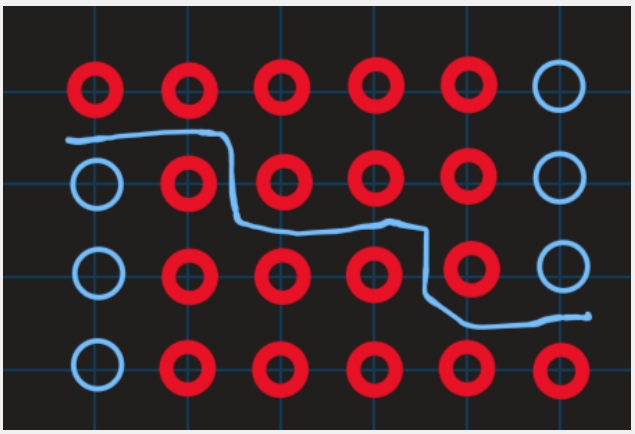
January 29, 2026

Contents

1 What is Number Theory

Problem 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.



Proof. We add up the first few odd numbers.

1. $1 = 1 = 1^2$
2. $1 + 3 = 4 = 2^2$
3. $1 + 3 + 5 = 9 = 3^2$
4. $1 + 3 + 5 + 7 = 16 = 4^2$

Please view the image above. The number of dots in the lower red triangle is what we are trying to discover a formula for. We first add k dots to the left of the triangle. Then we double the triangle and combine it with

the first to make a rectangle with width $2k$ and height $k+1$. Therefore the total number of dots is $2k^2+2k$. Now we doubled the triangle so we must remove dots to discover the number of dots in the original lower left triangle. We first halve the number of dots, $\frac{2k^2+2k}{2} = k^2+k$. We also added k redundant blue dots, thus our total number of dots is $k^2+k-k=k^2$. ∎

Problem 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?

Proof. Consider the sequence

$$p, p+1, p+2, p+3, p+4$$

There are three cases for the remainders of each term in the sequence when divided by 3. They are as follows

$$0, 1, 2, 0, 1$$

In which case $3 \mid p$.

$$1, 2, 0, 1, 2$$

In which case $3 \mid p+2$.

$$2, 0, 1, 2, 0$$

In which case $3 \mid p+4$. Thus there is only one set of prime triplets. ∎

Problem 4

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

1. Do you think there are infinitely many primes of the form N^2-1?
2. How about of the form N^2-3? How about N^2-4.
3. Which values of a do you think give infinitely many primes of the form N^2-a.

Solution (a): No, since $N^2-1=(N+1)(N-1)$, which is composite for all $N>2$.

Solution (b): For N^2-3 I think it does, and $N^2-4=(N+2)(N-2)$, so there are finitely many primes.

Solution (c): Values of a such that N^2-a cannot be factored as a difference of squares $(N-b)(N+b)$ for some integer b.

2 Pythagorean Triples

Problem 1

1. 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.
2. By examining the above list of primitive triples, make a guess about when a, b, or c is a multiple of 5. Try to show that your guess is correct.

Proof. Notice for $k \in \mathbb{Z}$:

1. $(3k)^2 = 9k^2 \equiv 0 \pmod 3$.
2. $(3k+1)^2 = 9k^2+6k+1 \equiv 1 \pmod 3$.
3. $(3k+2)^2 = 9k^2+12k+4 \equiv 1 \pmod 3$.

Then if $3 \nmid a, b$

$$(1 \pmod 3) + (1 \pmod 3) \equiv 2 \pmod 3 = c^2.$$

But no integer squared has remainder 2 modulo 3, which is a contradiction. ∎

Proof. Notice for $k \in \mathbb{Z}$:

1. $(5k)^2 \equiv 0 \pmod 5$,
2. $(5k \pm 1)^2 = 25k^2 \pm 10k + 1 \equiv 1 \pmod 5$,
3. $(5k \pm 2)^2 = 25k^2 \pm 20k + 4 \equiv 4 \pmod 5$.

Then if $5 \nmid a, b, c$

$$a^2, b^2, c^2 \equiv 1 \text{ or } 4 \pmod 5.$$

Checking all possibilities,

$$1 + 1 \equiv 2, \quad 1 + 4 \equiv 0, \quad 4 + 4 \equiv 3 \pmod 5.$$

Since $a^2 + b^2 = c^2$, the only possible case is

$$a^2 + b^2 \equiv 0 \pmod 5,$$

thus $5 \mid c^2$ and therefore $5 \mid c$, which is a contradiction. ∎

Problem 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 $m + n$.

Proof. Suppose d divides both m and n. Thus there exists k_1, k_2 such that $m = k_1 d$ and $n = k_2 d$. Then $m - n = k_1 d - k_2 d = (k_1 - k_2)d$. Thus $d \mid m - n$. Similarly, $m + n = k_1 d + k_2 d = (k_1 + k_2)d$. Thus $d \mid m + n$. ∎

Problem 6

If you look at the table of 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.

1. Find two more primitive Pythagorean triples (a, b, c) have $c = a + 2$.
2. Find a primitive Pythagorean triple (a, b, c) having $c = a + 2$ and $c > 100$.
3. Try to find a formula that describes all primitive Pythagorean triples (a, b, c) having $c = a + 2$.

Solution (a):

1. $(99, 20, 101)$
2. $(143, 24, 145)$
3. $(195, 28, 197)$
4. $(255, 32, 257)$
5. $(323, 36, 325)$
6. $(399, 40, 401)$
7. $(483, 44, 485)$
8. $(575, 48, 577)$
9. $(675, 52, 677)$

10. $(783, 56, 785)$
11. $(899, 60, 901)$

Solution (b): All previous solutions have $c > 100$.

Proof. We require $a^2 + b^2 = c^2$ with $c = a + 2$. Thus

$$a^2 + b^2 = (a+2)^2 \iff b^2 = (a+2)^2 - a^2 \iff b^2 = a^2 + 4a + 4 - a^2 \iff b^2 = 4a + 4 = 4(a+1).$$

Thus $4 \mid b^2$ and therefore $2 \mid b$. Then $b = 2k$ for some integer k. Then

$$4k^2 = 4(a+1) \iff k^2 = a + 1.$$

Thus $a = k^2 - 1$ and $c = a + 2 = k^2 + 1$. Therefore $(a, b, c) = (k^2 - 1,\ 2k,\ k^2 + 1)$ satisfies $a^2 + b^2 = c^2$. ∎

Problem 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:

1. $(3, 4, 5)$ then $2c - 2a = 2(5) - 2(3) = 10 - 6 = 4$.
2. $(5, 12, 13)$ then $2c - 2a = 2(13) - 2(5) = 26 - 10 = 16$.
3. $(7, 24, 25)$ then $2c - 2a = 2(25) - 2(7) = 50 - 14 = 36$.
4. $(9, 40, 41)$ then $2c - 2a = 2(41) - 2(9) = 82 - 18 = 64$.
5. $(15, 8, 17)$ then $2c - 2a = 2(17) - 2(15) = 34 - 30 = 4$.
6. $(21, 20, 29)$ then $2c - 2a = 2(29) - 2(21) = 58 - 42 = 16$.
7. $(35, 12, 37)$ then $2c - 2a = 2(37) - 2(35) = 74 - 70 = 4$.
8. $(45, 28, 53)$ then $2c - 2a = 2(53) - 2(45) = 106 - 90 = 16$.
9. $(63, 16, 65)$ then $2c - 2a = 2(65) - 2(63) = 130 - 126 = 4$.

Those are all perfect squares.

Proof. We know that for $s > t > 1$ we have

$$a = st \quad \text{and} \quad c = \frac{s^2 + t^2}{2}.$$

Then

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

Thus $2c - 2a$ is a perfect square. ∎

Problem 9

1. Read about the Babylonian number system and write a short description, including the symbols from 1 to 10 and the multiples of 10 from 20 to 50.
2. Read about the Babylonian tablet called 'Plimpton 322' and write a brief report, including its approximate date of origin.
3. 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 b so that (a, b, c) is a Pythagorean triple.

The Babylonians used a sexagesimal (base-60) positional numeral system. This system was inherited from either the Sumerian or Akkadian civilizations. However, neither of these predecessors used a positional system. In other words, they did not have a convention for which "end" of the numeral represented the units. The system first appeared around 2000 BC. It is credited as being the first known positional numeral system in which the digit itself and its position within the number reflect its value.

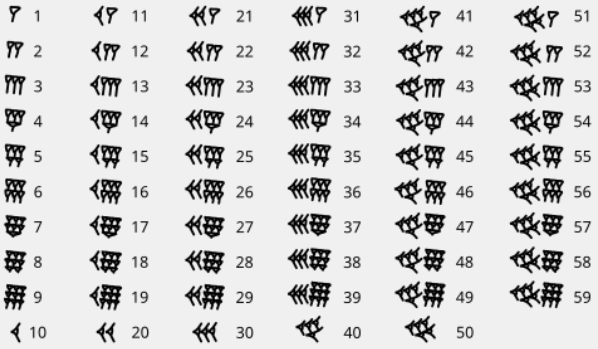


Figure 1: Babylonian numerals from 1 to 50

Figure 1 shows the numbers 1–50. The Babylonians did not have a digit for the number zero.

Figure 2: The Babylonian tablet *Plimpton 322*

Figure 2 shows a tablet named *Plimpton 322*. It was made of clay and is believed to have been written around 1800 BC. Each row of the table corresponds to a Pythagorean triple. In other words, each row corresponds to three integers, say (a, b, c), such that $a^2 + b^2 = c^2$. The tablet was written approximately 13–15 centuries prior to the Greek discoveries in geometry. The table exclusively lists numbers in which the longer leg has prime factors only 2, 3, or 5. Thus, the other two sides have exact terminating representations in the Mesopotamian sexagesimal number system. The purpose of the table is unknown.

On the table, the second and third columns of *Plimpton 322* give pairs (a, c) such that $c^2 - a^2$ is a perfect square. For example, one row corresponds to $a = 119$ and $c = 169$. Then

$$b^2 = c^2 - a^2 = 169^2 - 119^2 = 28561 - 14161 = 14400 = 120^2,$$

thus $b = 120$ and it follows that $(119, 120, 169)$ is a Pythagorean triple. Another row shows $a = 65$ and $c = 97$. Then

$$b^2 = 97^2 - 65^2 = 5184 = 72^2,$$

so $(65, 72, 97)$ is also a Pythagorean triple. These examples show that the pairs listed on *Plimpton 322* generate valid Pythagorean triples.

References

1. Wikipedia, *Babylonian cuneiform numerals*. `https://en.wikipedia.org/wiki/Babylonian_cuneiform_numerals`
2. Wikipedia, *Plimpton 322*. `https://en.wikipedia.org/wiki/Plimpton_322`

3 Pythagorean Triples and the Unit Circle

Problem 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 u and v. For example $(u, v) = (2, 1)$ gives the smallest triple $(3, 4, 5)$.

1. If u and v have a common factor, explain why (a, b, c) will not be a primitive Pythagorean triple.
2. 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.
3. Make a table of the Pythagorean triples that arise when you substitute in all values of u and v with $1 \leq v \leq 10$.
4. Using your table from (c), find some simple conditions on u and v that ensures the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is primitive.
5. Prove that your conditions in (d) really work.

Proof. Suppose u and v have a common factor $a > 1$. Thus we can write $u = k_1 a$ and $v = k_2 a$ where $k_1, k_2 \in \mathbb{Z}$. Then

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2) = ((k_1 a)^2 - (k_2 a)^2), 2(k_1 a)(k_2 a), (k_1 a)^2 + (k_2 a)^2 = (a(k_1 a - k_2 a), a(2k_1 k_2), a(k_1 a + k_2 a)).$$

Thus (a, b, c) is not a primitive. ∎

Solution (2): Take $u = 3, v = 1$.

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2) = (8, 6, 10).$$

Solution (3):

Problem 2

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

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

   whose coordinates are rational numbers.
2. What goes wrong if you try to apply the same procedure to find all points on the circle $x^2 + y^2 = 3$ with rational coordinates.

Problem 3

Find a formula for all the points on the hyperbola

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

u	v	$a = u^2 - v^2$	$b = 2uv$	$c = u^2 + v^2$	Primitive?
2	1	3	4	5	Yes
3	1	8	6	10	No
3	2	5	12	13	Yes
4	1	15	8	17	Yes
4	2	12	16	20	No
4	3	7	24	25	Yes
5	1	24	10	26	No
5	2	21	20	29	Yes
5	3	16	30	34	No
5	4	9	40	41	Yes
6	1	35	12	37	Yes
6	2	32	24	40	No
6	3	27	36	45	No
6	4	20	48	52	No
6	5	11	60	61	Yes
7	1	48	14	50	No
7	2	45	28	53	Yes
7	3	40	42	58	No
7	4	33	56	65	Yes
7	5	24	70	74	No
7	6	13	84	85	Yes
8	1	63	16	65	Yes
8	2	60	32	68	No
8	3	55	48	73	Yes
8	4	48	64	80	No
8	5	39	80	89	Yes
8	6	28	96	100	No
8	7	15	112	113	Yes
9	1	80	18	82	No
9	2	77	36	85	Yes
9	3	72	54	90	No
9	4	65	72	97	Yes
9	5	56	90	106	No
9	6	45	108	117	No
9	7	32	126	145	Yes
9	8	17	144	145	Yes
10	1	99	20	101	Yes
10	2	96	40	104	No
10	3	91	60	109	Yes
10	4	84	80	116	No
10	5	75	100	125	No
10	6	64	120	136	No
10	7	51	140	149	Yes
10	8	36	160	164	No
10	9	19	180	181	Yes

Table 1: Pythagorean triples generated by $1 \leq v \leq 10$ and $u > v$.

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.]

Problem 4

The curve

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

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