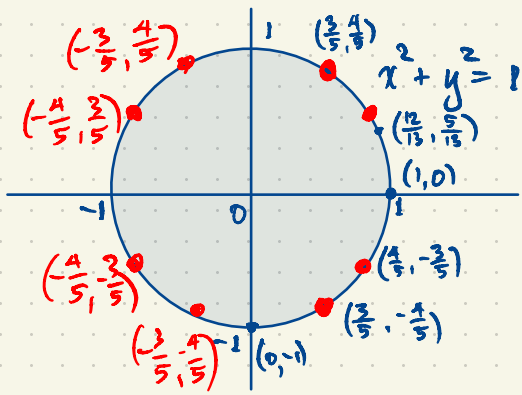


Number Theory

Book 1



How many points on the circle $x^2 + y^2 = 1$ ($x, y \in \mathbb{Q}$) have rational number coordinates?

Not $(\frac{1}{2}, \pm\frac{\sqrt{3}}{2})$

Are there infinitely many "rational points" on the unit circle?

$(\frac{3}{5}, \frac{4}{5}) \leftrightarrow 3^2 + 4^2 = 5^2$ solution of $x^2 + y^2 = z^2$ ($x, y, z \in \mathbb{Z}$)

A Pythagorean triple is a triple (a, b, c) of positive integers a, b, c , satisfying $a^2 + b^2 = c^2$.

eg. $(3, 4, 5)$, $(6, 8, 10)$, $(9, 12, 15)$, $(5, 12, 13)$, ...

A triple (a, b, c) is primitive if it is not an integer scalar multiple of a smaller triple eg. $(3, 4, 5)$ is primitive; $(6, 8, 10) = 2(3, 4, 5)$ is imprimitive, as is $(9, 12, 15) = 3(3, 4, 5)$.

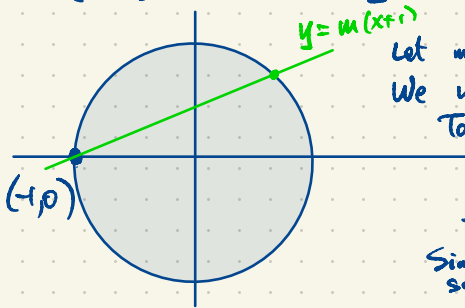
There are infinitely many primitive Pythagorean triples.

The triple $(3, 4, 5)$ yields eight rational points $(\pm\frac{3}{5}, \pm\frac{4}{5})$, $(\pm\frac{4}{5}, \pm\frac{3}{5})$. So does $(9, 3, 5)$

Theorem There are infinitely many rational points on the unit circle $x^2 + y^2 = 1$.

See Chapter 3.

Proof



Let $m \in \mathbb{Q}$. Consider the line $y = m(x+1)$ through $(-1, 0)$.

We will see that this line intersects the circle in two rational points.

To find these points, solve $\begin{cases} y = m(x+1) \\ x^2 + y^2 = 1 \end{cases}$ for (x, y) .

$x^2 + (m(x+1))^2 = 1$ (we have eliminated y from this equation)

This is a quadratic equation in x with rational coefficients.

Since $x = -1$ is one rational root, the other root must also be rational so (x, y) is rational. Every $m \in \mathbb{Q}$ gives a rational point on the unit circle.

Starting over, we give a completely algebraic approach to parameterizing the primitive Pythagorean triples.

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ ring of integers.

$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ positive integers.

\mathbb{N} has unique factorization. Every $n \in \mathbb{N}$ factors uniquely as a product of prime numbers $2, 3, 5, 7, 11, 13, (17, 19, 23, 29, 31, \dots)$

ie. if $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$ where all p_i, q_j are primes then $k = \ell$ and $p_i = q_i$ after re-indexing if necessary.

eg. $12 = 2 \times 6 = 2 \times 2 \times 3$ is a prime factorization of 12.

$$12 = 3 \times 4 = 3 \times 2 \times 2$$

$1 = 1$ is a prime factorization with 0 prime factors.

A prime number is an integer $n > 1$ which is not of the form ab ($a, b \in \mathbb{N}$, $a, b > 1$).

We'll assume unique factorization for now but later, we'll have to explain this.

$$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$$

x	x^2
0	0
1	1

$\gcd(a, b) =$ greatest common divisor of a, b

for $a, b \in \mathbb{N}$

eg. $\gcd(40, 68) = 2 \times 2 = 4$
 $2 \times 2 \times 5 \quad 2 \times 2 \times 17$

$$(3, 4, 5), (4, 3, 5)$$

Pythagorean triple (a, b, c) , a, b, c positive integers with $a^2 + b^2 = c^2$

(a, b, c) is primitive if it's not a scalar multiple (ka', kb', kc') with $k > 1$. $(6, 8, 10) = 2(3, 4, 5)$ is imprimitive.

If (a, b, c) is a primitive Pythagorean triple, what can we say about the parity of a, b, c ?

a, b, c can't all be even and they can't all be odd. In fact one must be even and the other two must be odd. \leftarrow the quality of being even or odd

Can a, b be odd and c even? No.

Integers mod 4 $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

x	x^2
0	0
1	1
2	0
3	1

If a, b are odd then $a^2 + b^2 \equiv 2 \pmod{4}$ but if c is even then $c^2 \equiv 0 \pmod{4}$

There is no Pythagorean triple (a, b, c) with a, b odd.

So every primitive Pythagorean triple is either (even, odd, odd) or (odd, even, odd).

Without loss of generality, take (odd, even, odd) ie. a, c odd, b even.

We will prove:

Theorem Every primitive Pythagorean triple has the form $(a,b,c) = (m^2-n^2, 2mn, m^2+n^2)$ for a unique pair of relatively prime integers m,n of opposite parity (i.e. one even, the other odd) with $m > n \geq 1$. (Or with a,b reversed).
Every such triple is a primitive Pythagorean triple.

Towards the proof, let's observe that in a primitive Pythagorean triple (a,b,c) , any two of a,b,c are relatively prime i.e. $\gcd(a,b) = 1 = \gcd(a,c) = \gcd(b,c)$. Why?

Suppose (a,b,c) is not primitive, i.e. $(a,b,c) = (ka, kb, kc)$ with $k \geq 2$. Then $\gcd(a,b) \neq 1$ ($\gcd(a,b) \geq k$)
 $\gcd(a,c) \neq 1$
 $\gcd(b,c) \neq 1$.

Suppose (a,b,c) is a primitive Pythagorean triple. Why must $\gcd(a,b) = 1$?
Why must $\gcd(a,c) = 1$?
Why must $\gcd(b,c) = 1$?

Aside

Subtlety: The triple $(6,10,15)$ is primitive: it is not of the form $(a,b,c) = k(a',b',c')$, $k,a',b',c' \in \mathbb{N}$, $k > 1$.
But $\gcd(6,10) = 2$, $\gcd(6,15) = 3$, $\gcd(10,15) = 5$. No two of $6,10,15$ are relatively prime.
Of course $(6,10,15)$ is not Pythagorean.

Given a primitive Pythagorean triple (a,b,c) , $a^2+b^2=c^2$ if $\gcd(a,b) > 1$ then there is a prime number p which is a factor of both a and b . But then p is a factor of a^2+b^2 so p is a factor of c^2 so p is a factor of c .
Then $a=pa'$, $b=pb'$, $c=pc'$, $(a,b,c) = p(a',b',c')$, $a',b',c' \in \mathbb{N}$. Then (a,b,c) is imprimitive.

What about $a^n+b^n=c^n$? (a,b,c,n positive integers) For $n > 2$ there are no solutions.
This was known as Fermat's Last Theorem. Proved about 30⁺ years ago by Andrew Wiles and others.

Given a primitive Pythagorean triple (a, b, c) , $a^2 + b^2 = c^2$, we have $\gcd(a, b) = 1$, $\gcd(a, c) = 1$, $\gcd(b, c) = 1$.
 Without loss of generality, a, c are odd, b is even. Then $\underbrace{b^2}_{\text{even}} = \underbrace{c^2 - a^2}_{\text{even}} = \underbrace{(c+a)}_{\text{even}} \underbrace{(c-a)}_{\text{even}}$. So $\left(\frac{b}{2}\right)^2 = \frac{c+a}{2} \cdot \frac{c-a}{2}$.
 $\frac{b}{2} \in \mathbb{N}$, $\frac{c+a}{2} \in \mathbb{N}$, $\frac{c-a}{2} \in \mathbb{N}$.

Write $m = \frac{c+a}{2}$, $n = \frac{c-a}{2}$ so $m, n \in \mathbb{N} = \{1, 2, 3, \dots\}$ positive integers.

$m > n \geq 1$. Then $\gcd(m, n) = 1$. Why? If not then there is a prime p which is a factor of both m and n . Then $m+n = c$ is a multiple of p and $m-n = a$ is a multiple of p . This is impossible since $\gcd(a, c) = 1$.

$\left(\frac{b}{2}\right)^2 = m \cdot n$ An integer squared equals mn where m, n are relatively prime.

- eg. $10^2 = 100 = mn$
- $100 = 100 \times 1$
 - ~~$= 50 \times 2$~~
 - ~~$= 25 \times 4$~~
 - ~~$= 20 \times 5$~~
 - ~~$= 10 \times 10$~~
 - ~~$= 5 \times 20$~~
 - $= 4 \times 25$
 - ~~$= 2 \times 50$~~
 - $= 1 \times 100$

Aside

Then m and n must both be squares. This fact follows directly from considering the prime factorization on both sides. We will discuss uniqueness of prime factorization later.

$m = M^2$, $n = N^2$, $M, N \in \mathbb{N}$.

$\left(\frac{b}{2}\right)^2 = M^2 N^2$
 $b^2 = 4M^2 N^2$
 $b = \pm 2MN$
 $b = 2MN$

$c = m+n = M^2 + N^2$
 $a = m-n = M^2 - N^2$

$M > N \geq 1$
 $\gcd(M, N) = 1$

If M, N are both odd then a, c would be even which is not true. So M, N must have opposite parity (one is even; the other is odd).