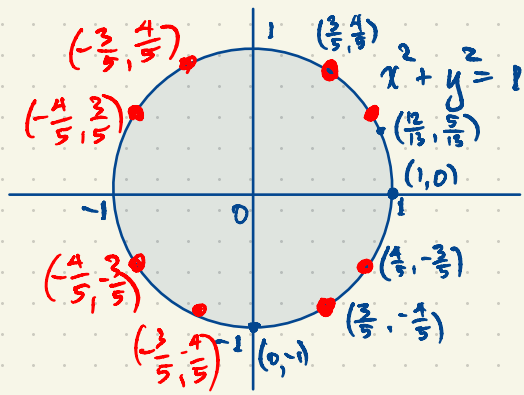


# Number Theory

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  $(9, 12, 15) = 3(3, 4, 5)$ .

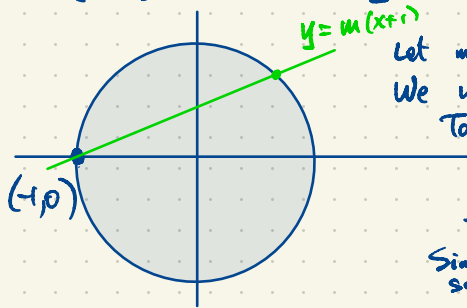
There are infinitely many primitive Pythagorean triples.

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. ↖ 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<sup>+</sup> 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).

Are there infinitely many primes of the form  $n^2+1$ ? e.g.

$$\begin{aligned} 1^2+1 &= 2 \\ 2^2+1 &= 5 \\ 4^2+1 &= 17 \\ &\text{etc.} \end{aligned}$$

We believe the answer is "yes" but the problem is open.

Goldbach's Conjecture: Is every even number  $> 2$  a sum of two primes?

e.g.  $4 = 2+2$ ,  $6 = 3+3$ ,  $8 = 3+5$ ,  $10 = 5+5 = 3+7$ ,  $12 = 5+7$ ,  $14 = 7+7 = 3+11$

The Riemann Hypothesis: more about this later this semester. (Biggest open problem in mathematics.)

There are infinitely many prime numbers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Are there infinitely many twin primes? e.g. 3, 5 5, 7 11, 13 17, 19 29, 31 etc.

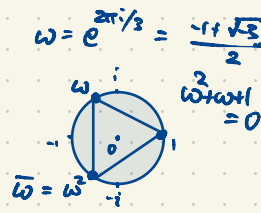
Importance of Fermat's Last Theorem:

Try to use an idea similar to proof of classification of primitive Pythagorean triples.

e.g. to show  $x^3+y^3=z^3$  has no solution in positive integers  $x, y, z \in \mathbb{N}$ :

$$y^3 = z^3 - x^3 = (z-x)(z^2+xz+x^2) = (z-x)(z-\omega x)(z-\omega^2 x)$$

Each of  $z-x = a^3$   
 $z-\omega x = b^3$   
 $z-\omega^2 x = c^3$   
 $a, b, c \in \mathbb{Z}[\omega] = \{r+s\omega : r, s \in \mathbb{Z}\}$   
is the ring of Eisenstein integers.



This leads to a contradiction, so we get a proof of Fermat's Last Theorem in the case of exponent 3.

This idea works a lot of the time so we can prove  $x^n+y^n=z^n$  has no solution for certain values of  $n$ .

The argument fails for many (most) values of  $n$  because of the failure of unique factorization.

One early goal of our course: explain why  $\mathbb{Z}$  has unique factorization and most similar rings do not have unique factorization.

Back to foundations of arithmetic of  $\mathbb{Z}$ . See handout on the integers on the course website.

$a, b, c, \dots$  are integers:  $a, b, c, \dots \in \mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$

We say  $a$  divides  $b$  if  $b = ka$  for some  $k \in \mathbb{Z}$ . (written  $a \mid b$ ).

- eg.
- 3 divides  $6 = 3 \cdot 2$
  - 3 divides  $3 = 3 \cdot 1$
  - 3 divides  $-12 = -4 \cdot 3$
  - 3 divides  $0 = 0 \cdot 3$
  - 3 does not divide 5.

$$a \mid b \iff a \text{ divides } b$$

$\iff b$  is a multiple of  $a$

$\iff a$  is a divisor of  $b$

$\iff a$  is a "factor" of  $b$ .

The divisors of 12 are  $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$ . There are exactly twelve numbers that divide 12: i.e.  $-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$ .

The divisors of 10 are  $\pm 1, \pm 2, \pm 5, \pm 10$ . (There are eight divisors of 10).

The divisors of -14 are  $\pm 1, \pm 2, \pm 7, \pm 14$ .

The divisors of 5 are  $\pm 1, \pm 5$ .

The divisors of 1 are  $\pm 1$ . (two divisors)

The divisors of 0 are  $0, \pm 1, \pm 2, \pm 3, \pm 4, \dots$

$$0 = 17 \cdot 0$$

Given two integers  $a, b$ , their common divisors:

The divisors of 68 are  $\pm 1, \pm 2, \pm 4, \pm 17, \pm 34, \pm 68$

The divisors of 10 are  $\pm 1, \pm 2, \pm 5, \pm 10$ .

The common divisors of 68 and 10 are  $\pm 1, \pm 2$  i.e.  $-2, -1, 1, 2$ .

The greatest common divisor of 68 and 10 is 2.

Range of difficulty of computational problems  
add, subtract, multiply: easy (with modest computational tools)

factorization: hard

find gcd: easy

testing primality: easy

Compute  $\text{gcd}(a, b)$  efficiently using Euclid's Algorithm

$$\text{gcd}(68, 0) = 68$$

$\text{gcd}(0, 0)$  is undefined

Divisors of 68:  $\pm 1, \pm 2, \pm 4, \pm 17, \pm 34, \pm 68$

Divisors of 0:  $0, \pm 1, \pm 2, \pm 3, \pm 4, \dots$

Common divisors of 68 and 0:  $\pm 1, \pm 2, \pm 4, \pm 17, \pm 34, \pm 68$

Greatest common divisor: 68

Computing  $\gcd(513, 381) = 3$

$$513 = 1 \times 381 + 132$$

$$381 = 2 \times 132 + 117$$

$$132 = 1 \times 117 + 15$$

$$117 = 7 \times 15 + 12$$

$$15 = 1 \times 12 + 3$$

$$12 = 4 \times 3 + 0$$

Division Algorithm: Given  $a, d \in \mathbb{Z}$  with  $d > 0$ , there exist unique  $q, r \in \mathbb{Z}$  such that  $a = qd + r$ ,  $0 \leq r < d$ .  
(If  $r = 0$  we say  $d$  divides  $a$ , i.e.  $d \mid a$ .)  
 $r$  is the remainder;  $q$  is the quotient.

The  $\gcd(a, b)$  is the last nonzero remainder

The extended form of Euclid's Algorithm:

$(a, b \in \mathbb{Z}, \text{ not both zero})$

$$3 = 513r + 381s, \quad r, s \in \mathbb{Z}.$$

We can write  $\gcd(a, b)$  as an integer linear combination of  $a$  and  $b$ .

$$3 = 513 \times 26 + 381 \times (-35)$$

This tells us:  $\{513r + 381s : r, s \in \mathbb{Z}\} = \{3t : t \in \mathbb{Z}\} = \{\dots, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}$

Shortcut:

513	381	
1	0	513
0	1	381
1	-1	132
-2	3	117
3	-4	15
-23	31	12
26	-35	<b>3</b>
*	*	0

$$\text{i.e. } 1 \times 513 + 0 \times 381 = 513$$

$$\text{i.e. } 1 \times 513 - 1 \times 381 = 132$$

$$\text{i.e. } -2 \times 513 + 3 \times 381 = 117$$

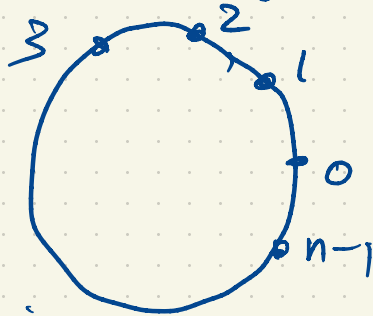
$$\text{i.e. } \gcd(513, 381) = 3 = 26 \times 513 - 35 \times 381$$

## Congruences; modular arithmetic

If  $n$  is a positive integer then we write  $a \equiv b \pmod{n}$  whenever  $a-b$  is divisible by  $n$

$$\Leftrightarrow n \mid a-b$$

$\Leftrightarrow a-b$  is a multiple of  $n$



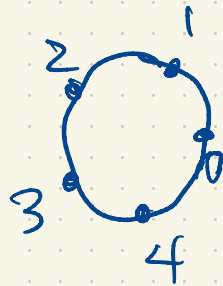
eg. integers mod 5: Every  $a \in \mathbb{Z}$  is congruent mod 5 to exactly one of 0, 1, 2, 3 or 4

$7 \times 8 = 56 \equiv 1 \pmod{5}$  (56 is congruent to 1 mod 5 because  $56-1=55$  is divisible by 5).

$33 \equiv 78 \pmod{5}$  because  $33-78$  is divisible by 5.

$$33 \equiv -7 \pmod{5}$$

$33 \not\equiv 6$  because  $33-6=27$  is not divisible by 5.



Look in early chapters of textbook and my handouts including integers

If  $(a, b, c)$  is a primitive Pythagorean triple then  $c \equiv 1 \pmod{4}$ .

( $c = m^2 + n^2$  where  $m, n$  are integers of opposite parity so  $c \equiv 0^2 + 1^2 \equiv 1 \pmod{4}$ )

Solve for  $x, y \in \mathbb{Z}$ : 
$$\begin{aligned} 3x + 5y &\equiv 1 \pmod{7} \\ 4x + y &\equiv 3 \pmod{7} \end{aligned}$$

Solution:  $x \equiv 0, y \equiv 3 \pmod{7}$ .

Check: 
$$\begin{aligned} 3 \cdot 0 + 5 \cdot 3 &\equiv 1 \pmod{7} \\ 4 \cdot 0 + 3 &\equiv 3 \pmod{7}. \end{aligned}$$

i.e.  $(x, y) \in \{(0, 3), (7, 3), (-7, -4), (-7, 10), \dots\}$   
infinitely many solutions in  $\mathbb{Z}^2$ .  
(satisfying our congruences)

x	y	
3	5	1
4	1	3
0	6	4
0	1	3
3	0	-14
3	0	0
1	0	0

i.e.  $3x + 5y \equiv 1 \pmod{7}$

i.e.  $6y \equiv 4 \pmod{7}$

i.e.  $3x \equiv -14 \equiv 0 \pmod{7}$

$$\mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \{0, 1, 2, \dots, 6\}$$
 abbreviated for simplicity

$$\bar{0} = [0] = \{\dots, -14, -7, 0, 7, 14, 21, \dots\}$$

$$\bar{1} = [1] = \{\dots, -13, -6, 1, 8, 15, 22, \dots\}$$
  
etc.

$$5 \times 6 = 2 \text{ in } \mathbb{Z}/7\mathbb{Z}$$

i.e.  $5 \times 6 = 2$

$$5 \times 6 \equiv 2 \pmod{7} \text{ in } \mathbb{Z}$$

Solve: 
$$\begin{aligned} 3x + 5y &= 1 \\ 4x + y &= 3 \end{aligned}$$
 for  $x, y \in \mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7 = \{0, 1, 2, \dots, 6\}$  finite field of order 7

Answer:  $(x, y) = (0, 3)$  is the unique solution in  $\mathbb{F}_7^2 = \{(x, y) : x, y \in \mathbb{F}_7\}$ .

Equivalently: Solve 
$$\begin{cases} 3x + 5y \equiv 1 \pmod{7} \\ 4x + y \equiv 3 \pmod{7} \end{cases}$$
 for  $x, y \in \mathbb{Z}$ .

There are infinitely many solutions of this system of two linear congruences in two unknowns  $x, y \in \mathbb{Z}$ , namely  $x \equiv 0 \pmod{7}, y \equiv 3 \pmod{7}$ . i.e.  $x \in \{\dots, -14, -7, 0, 7, 14, 21, \dots\}, y \in \{\dots, -11, -4, 3, 10, 17, 24, \dots\}$

Solve  $4x = 5$  for  $x \in \mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$  (integers mod 7).

If we were working in  $\mathbb{R}$  or in  $\mathbb{Q}$ ,  $x = \frac{5}{4}$ . In  $\mathbb{F}_7$ , the answer  $x = \frac{5}{4}$  is technically correct but this is not simplified.

$x$	0	1	2	3	4	5	6
$4x$	0	4	1	5	2	6	3

The unique solution is  $x = \frac{5}{4} = 3$ .

$$\frac{5}{4} = \frac{12}{4} = \frac{6}{2} = 3$$

In  $\mathbb{Z}$ , solve the congruence  $4x \equiv 5 \pmod{7}$ . Solution:  $x \equiv 3 \pmod{7}$  i.e.  $x \in \{\dots, -11, -4, 3, 10, 17, \dots\}$

If  $x$  is a positive integer such that the last two decimal digits of  $41x$  are 01 i.e.  $41x = \square\square\square\square\square\square 01$ , what are the last two digits of  $x$ ?

Solve  $41x \equiv 1 \pmod{100}$ . We need the inverse of 41 in  $\mathbb{Z}/100\mathbb{Z} = \{0, 1, 2, \dots, 99\}$

$$\gcd(100, 41) = 1 = (16) \cdot 100 + (-39) \cdot 41 = 1600 - 1599$$

check:

100	41	
1	0	100
0	1	41
1	-2	18
-2	5	5
7	-17	3
-9	22	2
16	-39	<span style="border: 1px solid black; padding: 2px;">1</span>
*	*	0

$$1 \equiv 41 \times (-39) \equiv 41 \times 61$$

Solution:  $x \equiv 61 \pmod{100}$

i.e. the last two decimal digits of  $x$  are 61.

Note:  $45x \equiv 1 \pmod{100}$  has no solution for  $x \in \mathbb{Z}$ .  
 $15x \equiv 5 \pmod{100}$  has multiple solutions mod 100.

$$\gcd(45, 100) = 5 \neq 1.$$

Important fact:  $\mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7$  is a field: every nonzero element has an inverse.

This is because 7 is a prime number.

If  $p$  is prime then every one of  $1, 2, \dots, p-1$  has an inverse mod  $p$ .

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$  is a field. Every nonzero element has an inverse.

Use Euclid's algorithm to find inverses.

$\mathbb{Z}/100\mathbb{Z}$  is not a field. It's only a ring.