Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 8, 2023

What we have seen last time

- Finish proving Dirichlet's approximation theorem.
- Higher Diophantine equations

Today's topics

- Higher Diophantine equations
- Modular world
    - congruence and modulus
    - modular arithmetic

Higher Diophantine equations

Question

Find all triples of integers (a, b, c) *such that*

$$a^2 + b^2 = N \cdot c^2.$$

Or, equivalently, find all rational points on the circle

$$X^2 + Y^2 = N.$$

N.B. $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. Hence, it is sufficient to consider only N = primes.

When $N = 3$, it seems impossible to find any rational point. In fact, we will show that

Theorem 12.1

There is no nontrivial triples of integers (a, b, c) such that

$$a^2 + b^2 = 3 \cdot c^2.$$

Proof. Indeed, is such a triple (a, b, c) exists, then we may assume $\gcd(a, b, c) = 1$ (since the equation is homogeneous).

$x \in \mathbb{Z}$

If x is even $\Rightarrow 4 \mid x^2$

If x is odd $\Rightarrow 4 \mid x^2 - 1$

$x = 2n+1$ $\quad (2n+1)^2 = 4n^2 + 4n + 1$

Proof. From the equation, we get

$$a^2 + b^2 + c^2 = 4 \cdot c^2.$$

Namely, $4 \mid a^2 + b^2 + c^2$.

If any of a, b, c is odd, then $4 \nmid a^2 + b^2 + c^2$

On the other hand, a square can either be divided by 4 (if the base is even), or equals a multiple of 4 plus 1 (if the base is odd). Hence, the sum $a^2 + b^2 + c^2$ is a multiple of 4 if and only if all of a, b, c are even, contradicting with $\gcd(a, b, c) = 1$. $\square$

To prove the equation $a^2 + b^2 = 3 \cdot c^2$ has no nontrivial solution, we reduce the problem to prove $a^2 + b^2 - 3 \cdot c^2$ is never a multiple of 4 except the trivial cases. Namely, we try to solve the equation in remainders after dividing by 4. Doing so, we reduce an infinite problem to finite problem.

Part V

Modular Worlds

Congruence and modulus

Definition 12.2

Let m be a positive integer (called the ***modulus***). We say two integers a and b are ***congruent modulo*** m, written as

$$a \equiv b \pmod{m},$$

if $m \mid a - b$.

$m \cdot X = a - b$ has sol. in $\mathbb{Z}$.

e.g. $\text{even}^2 \equiv 0 \bmod 4$ $\quad$ $\text{odd}^2 \equiv 1 \bmod 4$

Theorem 12.3

Fix a modulus m. "Being congruent module m" is an equivalence relation on $\mathbb{Z}$. Namely,

- (**reflexivity**) *for all integer* $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$; $m \mid a - a$
- (**symmetry**) *for all integers* $a, b \in \mathbb{Z}$, *if* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$; $m \mid a - b \Rightarrow m \mid b - a$
- (**transitivity**) *for all integers* $a, b, c \in \mathbb{Z}$, *if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

$m \mid a - b \wedge m \mid b - c \Rightarrow m \mid a - c$

Congruence and modulus

Definition 12.4

For any integer $a \in \mathbb{Z}$, the set of integers congruent to a modulo m is called the ***congruence class (modulo m)*** with ***representative*** a, written as $[a]_m$, or simply $[a]$ or $\bar{a}$ if the modulus m is clear.

Example 12.5

Take 2 to be the modulus. $[0]_2$ is the set of even numbers, while $[1]_2$ is the set of odd numbers.

Definition 12.6

The ***residue set modulo*** m, written as $\mathbb{Z}/m$, is the quotient set of $\mathbb{Z}$ up to congruence modulo m. Namely, $\mathbb{Z}/m$ is the set of congruence classes modulo m.

A priori, every integer defines a congruence class. But many of them turn out to be the same. $a \in \mathbb{Z} \rightsquigarrow [a]_m$

Example 12.7

It turns out that $\mathbb{Z}/2$ consists of only two classes: $[0]_2$, the even numbers, and $[1]_2$, the odd numbers.

a even $\Rightarrow [a]_2 = [0]_2$

odd $\Rightarrow [a]_2 = [1]_2$

Definition 12.8

Let x be an integer and m be a modulus.
The ***natural representative of*** x ***modulo*** m is the remainder r left under the division

$$x = q \cdot m + r, \quad 0 \leqslant r < m, \quad q \in \mathbb{Z}.$$

Example 12.9

- The natural representative of $1234567 \pmod{10}$ is 7.
- The natural representative of $7^{2023} \pmod{2}$ is 1.

$x = q \cdot m + r$

Note that $x \equiv r \pmod{m}$. Hence, $[r]_m = [x]_m$. Namely, r is a representative of the congruence class $[x]_m$.

Note that the natural representative depends only on the congruence class $[x]_m$, rather than the integer x.

Theorem 12.10

The set $\mathbb{Z}/m$ is finite. In fact, it is bijective to the set of remainders dividing m: $\{0, \cdots, m-1\}$.

Proof. The following process gives a bijection from $\mathbb{Z}/m$ to $\{0, \cdots, m-1\}$: for any congruence class $[x]_m$, take the natural representative r of it. $\square$

Modular Arithmetic

Theorem 12.11

Fix a modulus m. Let a, b, c, d be integers such that

$$a \equiv c \pmod{m} \qquad \text{and} \qquad b \equiv d \pmod{m}.$$

Then we have

$$a + b \equiv c + d \pmod{m} \qquad \text{and} \qquad ab \equiv cd \pmod{m}.$$

$(a+b)-(c+d) = a-c+b-d = k_1 m + k_2 m$

Proof. (Product) Suppose $a - c = k_1 m$ and $b - d = k_2 m$. Then

$$ab = (c + k_1 m)(d + k_2 m) = cd + (k_1 d + k_2 c + k_1 k_2 m)m.$$

Hence, $m \mid ab - cd$. □

$[a]=[c]$, $[b]=[d]$ $\Rightarrow$ $[a+b]=[c+d]$, $[ab]=[cd]$

The previous theorem tells us that the congruence class of the sum/product is independent of the choice of representatives. We thus are able to define the ***addition*** and ***multiplication*** of congruence classes.

Definition 12.12

* The ***sum*** of two congruence classes $[a]_m$ and $[b]_m$ is $[a+b]_m$. $=[a]_m+[b]_m$

The ***product*** of two congruence classes $[a]_m$ and $[b]_m$ is $[ab]_m$. $=[a]_m\cdot[b]_m$

Example 12.13

$[1234567]_{10}\cdot[20230208]_{10} = [7]_{10}\cdot[8]_{10} = [56]_{10} = [6]_{10}$

nat. rep.

---

*Compare this with what in Example 2.7, where we already have the notions of the sum and product of two sets. $A+B := \{a+b \mid a\in A, b\in B\}$? $A\cdot B := \{a\cdot b \mid a\in A, b\in B\}$?

Definition 12.14

The residue set $\mathbb{Z}/m$ together with the ***addition*** and ***multiplication*** of congruence classes and the neutral elements $\mathbf{0} := [0]_m$ and $\mathbf{1} := [1]_m$ of them respectively, is called the ***residue ring modulo*** m.

We have a ***residue map***:

$$\pi_m : \mathbb{Z} \longrightarrow \mathbb{Z}/m : a \mapsto [a]_m$$

respecting their structures.

addition to addition
mult. to mult.
neutrals to neutrals
(0 to 0 & 1 to 1)

- We can translate problems on $\mathbb{Z}$ through π_m. Note that this map is not bijective, hence solving problems on $\mathbb{Z}/m$ doesn't mean solving problems on $\mathbb{Z}$. Since any solution in $\mathbb{Z}$ will ***descend*** to a solution in $\mathbb{Z}/m$, it is convenient to use modular arithmetic to disprove problems on $\mathbb{Z}$.

Example 12.15

If $X^2 + Y^2 = 3Z^2$ has any integer solution, then it descends to a solution in $\mathbb{Z}/4$. But we can verify there is no such a solution in $\mathbb{Z}/4$.

$[0], [1], [2], [3]$

$(a,b,c) \neq (0,0,0)$

$a^2+b^2=3c^2 \Rightarrow [a]_4^2 + [b]_4^2 = [3]_4 \cdot [c]_4^2$

Definition 12.16

Fix a modulus m. A congruence class α is a ***unit*** in $\mathbb{Z}/m$ if there is a congruence class β such that $\alpha\beta = \mathbf{1}$. The class β is called the ***multiplicative inverse*** of α. Suppose a and b are representatives of α and β respectively. Then we say a is ***(multiplicative) invertible modulo*** m and b is a ***multiplicative inverse of*** a ***modulo*** m. $ab \equiv 1 \mod m$

Example 12.17 $[2]_5$ is a unit

$2 \cdot 3 \equiv 2 \cdot 8 \equiv 1 \pmod 5$. Hence, 2 is (multiplicative) invertible modulo 5, and 3 and 8 are two multiplicative inverse of 2 modulo 5.

Theorem 12.18

Fix a modulus m. An integer a is invertible modulo m if and only if a is coprime to m.

Proof.

$$\begin{aligned} & a \text{ is invertible modulo } m \\ \iff & \text{there is } b \in \mathbb{Z} \text{ such that } ab \equiv 1 \pmod{m} \\ \iff & \text{there is } b \in \mathbb{Z} \text{ such that } m \mid ab - 1 \\ \iff & \text{the Diophantine equation } aX + mY = 1 \text{ has integer solutions} \end{aligned}$$

The last is equivalent to $\gcd(a, m) = 1$ by the Bézout's identity. □

After Class Work

Terminology

Terminology

A ***(commutative) ring*** is a set R equipped with two monoid structures $(R, +, 0)$ and $(R, \cdot, 1)$ such that:

1. $(R, +, 0)$ is an abelian group;
2. $(R, \cdot, 1)$ is an abelian monoid;
3. The two operations $+$ and $\cdot$ are compatible in the sense of the following distributive laws:
    - (left distributive law) $\forall a, b, c \in R\colon\ a \cdot (b + c) = a \cdot b + a \cdot c$;
    - (right distributive law) $\forall a, b, c \in R\colon\ (a + b) \cdot c = a \cdot c + b \cdot c$.

Refer to the after-class part of lecture 1 and 3.

Example 12.19

- $(\mathbb{Z}, +, 0, \cdot, 1)$: the set of integers $\mathbb{Z}$ equipped with the *addition* and *multiplication* operations and their neutral elements 0 and 1 respectively, is a ring.
- $(\mathbb{Z}/m, +, 0, \cdot, 1)$: the residue set $\mathbb{Z}/m$ together with the *addition* and *multiplication* of congruence classes and their neutral elements $\mathbf{0} := [0]_m$ and $\mathbf{1} := [1]_m$ respectively, is a ring.
- The residue map $\pi_m : \mathbb{Z} \to \mathbb{Z}/m$ is a surjective homomorphism between rings.