CSC3001 Discrete Mathematics: Tutorial 6

Presented by Rybin Dmitry
dmitryrybin@link.cuhk.edu.cn

The Chinese University of Hong Kong, Shenzhen

October 26, 2022

Tough problems for bored students

1. When is $6^{n-2} + 3^{n-2} + 2^{n-2} - 1$ divisible by n?
2. Show that

$$x^3 + y^4 = z^5$$

has infinitely many solutions in positive integers. Same for

$$x^k + y^{k+1} = z^{k+2},$$

where k is positive integer.
Does the same hold for

$$x^{2k} + y^{2k+2} = z^{2k+4}?$$

Number Theory recap

1. Since multiplication is invertible, it follows that multiplying by number a permutes residues $1, 2, ..., p-1$. Hence product of numbers $1, 2, ..., p-1$ modulo p is equal to the product of numbers $a, 2a, 3a, ..., (p-1)a$. Hence

$$a^{p-1} = 1 \mod p$$

2.

Number Theory recap

1. (GCD as a linear combination) The most important property of $d = \gcd(a, b)$ of two numbers a, b is that it is the smallest positive integral combination formed by a and b

$$d = ma + nb = \min\{x > 0 | x = ma + nb, n, m \in \mathbb{Z}\}$$

2. In particular, for coprime numbers a, b we have $\gcd(a, b) = 1$ and hence

$$1 = ma + nb$$

which means

$$1 = ma \mod b$$

3. (multiplication modulo b) Previous identity shows that a is invertible modulo b if it is coprime to b
4. (multiplication modulo prime p) In particular, the numbers $1, 2, ..., p - 1$ are all invertible modulo p.

Exercise 1

Do modular multiplications

$$12345 \cdot 67890 \mod 17$$

$$2^7 9 \mod 17$$

Solution to Exercise 1

To simplify calculations we just need to keep finding numbers divisible by 17

$$12345 = 123 \cdot 100 + 45 = (119 + 4) \cdot 100 + 45 = 4 \cdot 15 + 11 = 71 = 3 \mod 17$$

$$67890 = 68000 - 110 = -110 = 9 \mod 17$$

$$3 \cdot 9 = 27 = 10 \mod 17$$

Answer is 10.

$$2^{79} = 2^{80-1} = (2^{16})^5 \cdot 2^{-1} = 1 \cdot 9 = 9 \mod 17$$

Exercise 2

Compute

$$(2p)!/p^2 \mod p$$

Solution to Exercise 2

First, without division by p^2 the answer would evidently be equal to 0

$$(2p)! = 0 \mod p$$

We will use Wilson theorem

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) = -1 \mod p$$

It implies that

$$(p+1) \cdot (p+2) \cdot (p+3) \cdot ... \cdot (2p-1) = -1 \mod p$$

We now only need to note that

$$(p \cdot 2p)/p^2 = 1 \cdot 2.$$

Then the whole answer is

$$(1 \cdot 2 \cdot .... \cdot (p-1)) \cdot 1 \cdot ((p+1) \cdot (p+2) \cdot (p+3) \cdot ... \cdot (2p-1)) \cdot 2 = 2 \mod p$$

Exercise 3

Prove that for any residues p, q, r modulo $3, 5$ and 7 there is always an integer n such that

$$n = p \mod 3$$

$$n = q \mod 5$$

$$n = r \mod 7$$

Solution to Exercise 3

This is a statement of chinese remainer theorem. Let us think about this theorem more.

1. Clearly, it is enough to consider n modulo $3 \times 5 \times 7 = 105$
2. We want to show that the map
$$\mathbb{Z}_{105} \to \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$
$$n \mapsto (n \mod 3, n \mod 5, n \mod 7)$$
covers all triplets.
3. We prove that sizes of both sets are 105 (obvious)
4. We prove that only 0 is mapped to $(0, 0, 0)$ (obvious)
5. Since map is linear, it is injective, hence bijective (kind of obvious).

Exercise 4

Plot a directed graph with vertices given by residues $\bmod 7$:

$$0, 1, 2, 3, ..., 6$$

and edges given by

$$x \mapsto 3x$$

What can you conclude from this graph?

Solution to Exercise 4

The graph is a cycle

$$1 \to 3 \to 2 \to 6 \to 4 \to 5 \to 1$$

plus an isolated loop $0 \to 0$. It follows that

$$3^6 = 1 \mod 7$$

It also follows that powers of 3 generate all residues $\mod 7$.

Thank You

Thank you for your attention!