MODULAR ARITHMETIC

PETER MCNAMRA

Bucknell University

and Trinity College Dublin

Motivating Problems.

(a) Find the remainder when 2^{123} is divided by 29.

(b) Do there exist integer solutions to

$$x^2 + y^2 = z^2 \ ?$$

Yes: solutions are side-lengths of right-angled triangles, such as $3, 4, 5$ or $5, 12, 13$.

(c) Do there exist integer solutions to

$$x^n + y^n = z^n \ \text{ for } n > 2 \ ?$$

This is Fermat's Last Theorem.

Pierre de Fermat 1637: conjectured "no."

Andrew Wiles 1994: proved "no."

Google "Nova the proof" for documentary (49 minutes)

or read "Fermat's Last Theorem" by Simon Singh.

(d) Show there are no integer solutions to

$$x^2 + y^2 = 10^z - 1 \ \text{ for } z > 1.$$

This is an example of an *exponential Diophantine equation*. (Diophantus of Alexandria, 3rd century)

1. MODULAR ARITHMETIC

Main definition. Integers a, b, m with $m \neq 0$.

We say "a is congruent to b modulo m" and write

$$a \equiv b \pmod{m} \quad \text{if}$$

$$m \mid a - b \quad \text{i.e. } m \text{ divides } a - b.$$

Examples.

$4 \equiv 9 \pmod{5}$.

$23 \equiv 1 \pmod{2}$.

$-5 \equiv 3 \pmod{4}$.

In other words...

$$\text{We say} \quad a \equiv b \pmod{m} \quad \text{if}$$

- a and b have the same remainder when divided by m, or
- there exists an integer k such that $a - b = km$.

Properties.

1. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then

$$a \equiv c \pmod{m}.$$

e.g. $2013 \equiv 13 \pmod{4}$ and $13 \equiv 1 \pmod{4}$ so

$$2013 \equiv 1 \pmod{4}.$$

2. Suppose $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$ then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}, \quad \text{and}$$

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

Proof of $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

We have $m \mid a_1 - b_1$ and $m \mid a_2 - b_2$ and we wish to show that $m \mid a_1 a_2 - b_1 b_2$.

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= a_1 a_2 \mathbf{- b_1 a_2 + b_1 a_2} - b_1 b_2 \\ &= a_2(a_1 - b_1) + b_1(a_2 - b_2). \end{aligned}$$

Problem 1: just an example of previous identity. Find the remainder of 46×23 (a.k.a. $46 \,.\, 23$) on division by 7.

Solution. $46 \equiv 4 \pmod{7}$ and $23 \equiv 2 \pmod{7}$ so

$$46 \,.\, 23 \equiv 4 \,.\, 2 \equiv 8 \equiv 1 \pmod{7}.$$

Problem 2: look for a small partner. Compute $13^8 \pmod{7}$. What does this mean? The unique remainder r satisfying $0 \leq r < 7$.

Easiest solution. $13^8 \equiv (-1)^8 \equiv 1 \pmod{7}$.

Problem 3: multiple steps. Compute $2^{123} \pmod{29}$.

Solution. Find a power of 2 that has a small remainder mod 29.

$$2^5 \equiv 3 \pmod{29}.$$

So

$$(2^5)^k \equiv 3^k \pmod{29}.$$

Repeat this idea:

$$3^3 \equiv 27 \equiv -2 \pmod{29}.$$

Now we have something useful:

$$2^{15} \equiv (2^5)^3 \equiv 3^3 \equiv -2 \pmod{29}.$$

Next,

$$2^{120} \equiv (2^{15})^8 \equiv (-2)^8 \pmod{29}.$$

To save ourselves computing $(-2)^8 \pmod{29}$, we can say

$$(-2)^8 \equiv (-2)^3(-2)^5 \equiv (-8)(-32) \equiv (-8)(-3) \equiv 24 \equiv -5$$

Finally,

$$2^{123} \equiv 2^{120} \,.\, 2^3 \equiv -5 \,.\, 8 \equiv -40 \equiv -11 \equiv 18 \pmod{29}.$$

Answer: 18.

This page was added after the lecture.

A student asked the following question.

Question. Why does m dividing $a - b$ mean that a and b have the same remainer under division by m?

Answer. This is a good question since it requires some work to give a complete proof.

By the definition of a "remainder," we can write

$$a = im + r_1,$$

where r_1 is the remainder under division by m and satisfies

$$0 \leq r_1 \leq m - 1.$$

Similarly,

$$b = jm + r_2 \quad \text{with} \quad 0 \leq r_2 \leq m - 1.$$

Then if m divides $a - b$, this means that m divides

$$im + r_1 - jm - r_2 = m(i - j) + r_1 - r_2.$$

Since m clearly divides $m(i - j)$, we get that m divides $r_1 - r_2$. We know that r_1 and r_2 are both between 0 and $m - 1$ inclusive, which means that $r_1 - r_2$ is between $-(m - 1)$ and $m - 1$ inclusive. Therefore, the only possibility is that $r_1 - r_2 = 0$, so $r_1 = r_2$.

2. DIOPHANTINE EQUATIONS.

Main trick for today: pick an appropriate modulus.

Problem 4. Show there are no integer solutions to

$$x^2 + y^2 = 10^z - 1 \text{ for } z > 1.$$

Solution. Exercise in seats: find all possible values of $x^2 \pmod 4$.

$$0^2 \equiv 0 \pmod 4.$$

$$1^2 \equiv 1 \pmod 4.$$

$$2^2 \equiv 0 \pmod 4.$$

$$3^2 \equiv 1 \pmod 4.$$

$$4^2 \equiv 0 \pmod 4.$$

$$\vdots$$

$$(i + km)^2 \equiv i^2 + 2ikm + k^2m^2 \equiv i^2 \pmod m.$$

Key point:

$$x^2 + y^2 \equiv 0, 1 \text{ or } 2 \pmod 4.$$

Meanwhile,

$$10^z - 1 \equiv 10^2 \,.\, 10^{z-2} - 1 \equiv -1 \equiv 3 \pmod 4.$$

Since the mod 4 values are different, there are no solutions.

Why modulus 4? Because it works! (4 is good for squares, but there's not really a hard and fast rule.)

3. FERMAT'S LITTLE THEOREM.

Exercise in seats: pick any integers a and p. Then compute $a^{p-1} \pmod{p}$.

Fermat's Little Theorem. For any prime p and any integer a such that $p \nmid a$ (i.e. p does not divide a),

$$a^{p-1} \equiv 1 \pmod{p}.$$

Lots of nice proofs (Art of Problem Solving wiki has 4). Simple one in Group Theory (college).

Example. $a = 57$ and $b = 29$:

$$57^{28} \equiv 1 \pmod{29}.$$

Problem 5. (1989 AIME) One of Euler's conjectures was disproved in the 1960s by two American mathematicians when they showed there exists a positive integer n such that

$$133^5 + 110^5 + 84^5 + 27^5 = n^5.$$

Find the value of n.

Question. How do we apply Fermat's Little Theorem here?

Fermat's Little Theorem restated. For any prime p and any integer a,

$$a^p \equiv a \pmod{p}.$$

To see that it's the same theorem as before note that:

◦ The case when $p \mid a$ is trivial. So can assume $p \nmid a$.

◦ p divides $a^{p-1} - 1$ if and only if p divides $a^p - a = a(a^{p-1} - 1)$.

Solution to Problem 5.

First, apply Fermat's Little Theorem:

$$133^5 + 110^5 + 84^5 + 27^5 \equiv 133 + 110 + 84 + 27 \equiv 4 \pmod 5.$$

Try mod 2. LHS is even so n must be even.

Try mod 3.

$$133^5 + 110^5 + 84^5 + 27^5 \equiv 1^5 + (-1)^5 + 0^5 + 0^5 \equiv 0 \pmod 3.$$

So n is divisible by 2 and 3, has remainder 4 mod 5, and

must be greater than 133.

$$138, \mathbf{144}, 150, 156, 162, 168, \mathbf{174}, \ldots .$$

(preview of Chinese Remainder Theorem)

We'd like to show 174 is too big. One way:

$$174^5 = (133 + 41)^5 = 133^5 + 5 \,.\, 133^4 \,.\, 41 + \text{other stuff} + 41^5.$$

$$133^5 = 133^5.$$

$$41^5 > 27^5.$$

$$5 \,.\, 133^4 \,.\, 41 = 205 \,.\, 133^4 > 110 \,.\, 133^4 + 84 \,.\, 133^4 > 110^5 + 84^5.$$

Answer: $n = 144$.

For the road...

Problem 6. Suppose $13 \not| m$. Show that $m^4 + 8$ is not the cube of an integer (use arithmetic modulo 13).

Problem 7. Show that there are no integer solutions to

$$w^6 + x^6 + y^6 + z^6 = 10^{12} + 7$$

or

$$w^6 + x^6 + y^6 + z^6 = 10^{12} + 4.$$

(Pick an appropriate modulus for each.)

Problem 8. Now that you know Fermat's Little Theorem, solve Problem 3 in a (mildly) simpler way than before.

Problem 9.

(a) Show that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

(b) Show that an integer is divisible by 11 if and only if the alternating sum (add the first digit, subtract the second, add the third, subtract the fourth, etc.) of its digits is divisible by 11.

Problem 10. It's nice when the number of things in a list is divisible by 10. Discuss.