Number Theory

Number theory studies the properties of integers. Number theory answers questions such as

Question 1. What is the last digit of 2025^{2025}?

Which would be impossible to do by hand if we try to calculate 2025^{2025} and then look at the last digit.

The study of number theory starts with doing arithmetic, factoring numbers, and goes up to many famous unsolved problems.

For example,

Question 2 (**Brocard's problem**)**.** We notice

$$1 \cdot 2 \cdot 3 \cdot 4 + 1 = 25 = 5^2 \text{ is a square;}$$
$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 1 = 121 = 11^2 \text{ is a square;}$$
$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 + 1 = 5041 = 71^2 \text{ is a square;}$$

Is there another number n besides 4, 5, 7 such that $(1 \cdot 2 \cdot \cdots \cdot n) + 1$ is a square?

As of now, we have not found such an n, but it hasn't been proved that no other number n has this property. Mathematicians have tried many ways, again using number theory, to search through potential values of n faster than the current computing power allows. They have checked all n up to 10^{12} and have not found another solution.

Arithmetic with Remainder

Imagine someone showed you a calculation:

$$398 \cdot 179 = 71244.$$

Can you tell if there's a mistake? With number theory, you can. The numbers on the left side multiply to something that should end in 2, but the last digit on the right side is an 4.

Let's expand the calculations to show why we expect the final digits to match:

$$398 \cdot 179 = (390 + 8)(170 + 9) = 66300 + 3510 + 1360 + 72$$

The first three terms, $66300, 3510, 1360$ are all multiples of 10, so they do not affect the last digit. So the last digit should match up with the last digit of $8 \cdot 9 = 72$, which is 2.

In general, we only need to look at the last digits of two numbers to know the last digit of their product. If we write two numbers, e and f, as $e = 10a + c$ and $f = 10b + d$, where c and d are their last digits respectively, and a and b are the integers you get after erasing the last digit of e and f then:

$$(10a + c)(10b + d) = 100ab + 10ad + 10bc + cd \tag{1}$$

Since $100ab$, $10ad$, $10bc$ would all have zero as their final digit (why?), the last digit of $ef = (10a + c)(10b + d)$ is the same as the last digit of cd.

Similar patterns are true when you do long division with remainders with other numbers:

Question 3. When you divide a number by 3, you get a remainder of 0, 1, or 2.

If I know $484 = 3 \cdot 161 + 1$, and $1076 = 3 \cdot 358 + 2$, what is the remainder of $520784 = 484 \cdot 1076$ when divided by 3?

Mod and Congruence

Writing every number as $(10a + c)$ and $(10b + d)$ when you only want to find the last digit is a lot of clutter. Ideally, we want to pretend that $10a + c$ is just c, and $10b + d$ is just d.

Similarly, in the solution of Question 3, it would be nice if we can pretend $3 \cdot 161 + 1$ is the same as 1, and $3 \cdot 358 + 2$ is the same as 2, when we only care about the remainder when divided by 3.

In fact, there is a new equal sign "≡" for pretending a number is the same as its remainder "modulo" the divisor, because mathematicians love shorthands:

$$10a + c \equiv c \pmod{10}, \quad 10b + d \equiv d \pmod{10}, \quad 3a + 1 \equiv 1 \pmod{3}, \quad 3b + 2 \equiv 2 \pmod{3}.$$

The "mod" in "mod 3" or "mod 10" is short for *modulo*. The word *modulo* is introduced by Gauss in 1801. It comes from Latin *modulus*, which means "a small measure". For integers a, b, and n, we write $a \equiv b \pmod{n}$ (you can read it out loud as "a is congruent to b modulo n") if a and b has the same remainder when divided by n, or equivalently $(a - b)$ is a multiple of n. [Wik24]

Now let's try to write a few new "equations" with this notation.

Question 4. (a) Find the remainder when you divide 10 by 7.

(b) What if you divide 100 by 7?

(c) What about 10000? (you don't have to do long division!)