WUSTL Math Circle Oct 26, 2014

The integers we use every is infinite. It keeps going and never ends:

$$1, 2, 3, 4, \ldots, 99999, 100000, 100001, \ldots$$

So have we used a number system that is finite. Of course, for example, we round up the hours to 12.

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0, 1, 2, 3, \ldots$$

In this case, we just need 12 numbers.

Let d be a fixed positive integer. For two other integers n and r, we say that

$$n \equiv r \mod m$$

which reads "n is congruent to r modulo m" or "n and r are congruent modulo m", if

$$n = m \times q + r$$

for some other integer q. For example,

$$12 \equiv 7 \mod 5,$$

which reads "12 is congruent to 7 modulo 5". But of course, modulo 5, we see that 12 and 7 is also congruent to 2. In fact, modulo m, we just need m numbers, namely

$$0, 1, 2, \ldots, m-1.$$

Such a number system is called "base m".

Here are a few simple properties of modulo arithmetics. If we have

$$\begin{aligned} a &\equiv c \mod m \\ b &\equiv d \mod m \end{aligned}$$

then it follows that

$$\begin{aligned} a + b &\equiv c + d \mod m \\ a - b &\equiv c - d \mod m \\ ab &\equiv cd \mod m \end{aligned}$$

and for positive integer e,

$$a^e \equiv b^e \mod m.$$

Exercise. Prove these properties.

To get some concrete ideas, we work out the multiplication table base 5.

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Exercise. Work out the mutiplication table base 8.

×	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							

If we are work with a number system with base greater than 10, we often use capital letters. For example, the MAC address, also known as "media access control address" or "physical IP address", uses the number system base 16, so we have 16 numbers.

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.$$

A MAC address "08-00-27-0E-25-B8" really means

$$08 - 00 - 27 - 0(14) - 25 - (11)8.$$

Exercise. Work out the mutiplication table base 11 and base 16.

×	1	2	3	4	5	6	7	8	9	A
1										
2										
3										
4										
5										
6										
7										
8										
9										
A										

×	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1															
2															
3															
4															
5															
6															
7															
8															
9															
A															
B															
C															
D															
E															
F															

Is there a pattern? Notice that 5 and 11 are prime numbers, and there are NO 0's in the multiplication table base 5 or 11. This means for every number base 5 (or base 11), we can find its reciprocal. For example,

$$4^{-1} \equiv 4 \mod 5$$
$$2^{-1} \equiv 3 \mod 5$$

On the other hand, 8 and 16 are not prime numbers, and there ARE 0's in the multiplication table base 8 or 16. This means not every number base 8 (or 16) has a reciprocal.

To generalize this observation, if p is a prime number, then in the number system base p, which we denote by

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\},$$

every number has a reciprocal.

Exercise. Prove the above claim. Hint: Use the Euclidean algorithm.

For this reason, when p is prime, we say that $\mathbb{Z}_p$, together with the addition and the multiplication, is a field. More precisely, $(\mathbb{Z}_p, +, \cdot)$ is a field of characteristic p.

Here are a few more problems for entertainment.[1]

Exercise. What is the last digit of

$$(...((7)^7)^7)...)^7$$

if there are 1000 7's as exponents and only one 7 in the middle?

Solution. First, we note that

$$(...((7)^7)^7)...)^7 = 7^{7^{1000}}$$

Notice that

$$\begin{aligned} 7^0 &\equiv 1 \mod 10 \\ 7^1 &\equiv 7 \mod 10 \\ 7^2 \equiv 49 &\equiv 9 \mod 10 \\ 7^3 \equiv 343 &\equiv 3 \mod 10 \\ 7^4 \equiv 2401 &\equiv 1 \mod 10 \end{aligned}$$

so this implies

$$7^{4n+k} \equiv 7^k \mod 10$$

On the other hand, we have

$$7 \equiv -1 \mod 4$$

this means that

$$7^{1000} \equiv (-1)^{1000} \equiv 1 \mod 4$$

Hence, $7^{1000} = 4n + 1$ for some integer n, and it follows that

$$7^{7^{1000}} \equiv 7^{4n+1} \equiv 7 \mod 10$$

That is, the last digit of $7^{7^{1000}}$ is 7.

Exercise. What are the last two digits of 7^{2014}?

Solution. Now we need the last two digits, so we recycle some of the calculation from the previous exercise, albeit with base 100.

$$\begin{aligned} 7^0 &\equiv 1 \mod 100 \\ 7^1 &\equiv 7 \mod 100 \\ 7^2 &\equiv 49 \mod 10 \\ 7^3 \equiv 343 &\equiv 43 \mod 100 \\ 7^4 \equiv 2401 &\equiv 1 \mod 100 \end{aligned}$$

This implies

$$7^{4n+k} \equiv 7^k \mod 100$$

Hence,

$$7^{2014} \equiv 7^{503\times 4+2} \equiv 7^2 \equiv 49 \mod 100$$

That is, the last two digits of 7^{2014} are 4 and 9.

[1]Source: Art Of Problem Solving Wiki page

Exercise. Can you find a number that is both a multiple of 2 but not a multiple of 4 and a perfect square?
Solution. We want to solve the integer equation.

$$4n + 2 = x^2$$

Take modulo 4, we get

$$2 \equiv x^2 \mod 4$$

However, 2 is NOT the square of any number base 4.

$$0^2 \equiv 0 \mod 4$$
$$1^2 \equiv 1 \mod 4$$
$$2^2 \equiv 0 \mod 4$$
$$3^2 \equiv 1 \mod 4$$

That is, there is NO number that is both a multiple of 2 but not a multiple of 4 and a perfect square.