Introduction to Modular Arithmetic

Dave Neary

January 15, 2021

1 Modular arithmetic

Let's start with a question: 3.14159265358979323846264338327 9 is the value of π to 30 decimal places. Is the number 31415926535897932384626433832 79 the square of an integer?

Rather than attempting to answer ths question directly, let's do some exploration of squares of integers, to see if we can find some common characteristics.

n	n^2	$\text{rem}(\frac{n^2}{4})$
1	1	1
2	4	0
3	9	1
4	16	0
5	25	1
6	36	0
7	49	1

Interestingly, it seems like every even square has a remainder of 0 when we divide by 4, and every odd square has a remainder of 1 (and in fact, appears to be 1 more than a multiple of 8). We can prove that this is the case in general quite easily:

$$n = 2k \implies n^2 = 4k^2$$
$$n = 2k + 1 \implies n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

We can now return to our original question - a simple initial test for whether a number is a square of an integer is to check its remainder when divided by 4. And we only need to look at the last two digits to check because

$100n + m = 4(25n) + m$ - so we can ignore everything before the last 2 digits. In our example, $79 = 4 \times 19 + 3$, so the number at the start of this section is **not** the square of an integer.

1.1 Working with remainders

This example gives a glimpse of something called modular arithmetic - sometimes, we can draw conclusions related to a problem by looking only at the remainders when divided by a number. In terms of notation, we say that $a \equiv b \pmod{n}$ when $a = m \cdot n + b$ for some integer m. In the example above, we can write: $a^2 \equiv 0$ or $1 \pmod 4$ for all $a \in \mathbb{Z}$.

There are a few operations that hold for all numbers $\pmod n$:

Remainders are additive and multiplicative:

$$\begin{aligned} (a \pmod n) + (b \pmod n) &= (a+b) \pmod n \\ (a \pmod n) \cdot (b \pmod n) &= (a \cdot b) \pmod n \end{aligned}$$

So we can tell that if $a = 76$ and $b = 42$, when we multiply them together, the remainder when we divide the result by 5 will be $76 \pmod 5 \times 42 \pmod 5 = 1 \times 2 \pmod 5$. We say that $a \equiv b \pmod n$ (a is congruent to b mod n) if $n|(a - b)$ - that is, if we subtract one number from another, and they have the same remainder when divided by n, then their difference is a multiple of n.

Just the basics of modular arithmetic allow us to address a whole range of problems already.

Q. 1. *Prove that* $6 \cdot 4^n - 6$ *is divsible by 9 for all* n.

Proof. Let's look at the values of $6 \cdot 4^n \pmod 9$ for different values of n.

n	$4^n \pmod 9$	$6 \cdot 4^n \pmod n$
0	1	6
1	4	6
2	7	6
3	1	6

Clearly, 4^n cycles through the values 1, 4, 7 for all n, and each of these multiplied by 6 gives a remainder of 6 when divided by 9. Another way of putting this is that $4^n \equiv 1 + 3k \pmod 9$ for $n \equiv k \pmod 3$, and since $6 \cdot 3 = 18 \equiv 0 \pmod 9$ $6 \times (1 + 3k) \equiv 6 \pmod 9$ for all n. □

Q. 2. *What are the last two digits base 10 of* 6^{19}*?*

A. 1. *This is an intimidating looking question, but modular arithmetic offers us a powerful tool to simplify things.* $6^2 = 36 \pmod{100}$, $6^3 = 216 \equiv 16 \pmod{100}$, $6^4 \equiv 96 \pmod{100} \equiv -4 \pmod{100}$, $(6^4)^2 = 6^8 \equiv (-4^2) = 16 \pmod{100}$ *So we have* $6^8 \equiv 6^3 \pmod{100}$ *But now we have:*

$$\begin{aligned} 6^{19} &= (6^8)^2 \cdot 6^3 \\ &\equiv (6^3)^3 \pmod{100} \\ &\equiv 6^9 \pmod{100} \\ &\equiv 6^8 \cdot 6 \pmod{100} \\ &\equiv 6^4 \pmod{100} \\ &\equiv 96 \pmod{100} \end{aligned}$$

You can use modular arithmetic to prove common divisibility tricks.

Q. 3. *Prove that 9 divides a number if and only if it divides the sum of its digits.*

Q. 4. *Prove that a number is divisible by 8 if its last 3 digits are divisible by 8.*

Q. 5. *Prove that a number is divisible by 11 if the sum of its even digits minus the sum of its odd digits is divisible by 11.*

1.2 Fermat's Little Theorem

Fermat made an interesting observation when working with remainders modulo a prime number. If you repeatedly multiplied any number not divisible by a prime number p, and took just the remainder $\mod(p)$, that p would eventually divide $a^k - 1$ for some number, and that k always divided evenly into $p - 1$. Equivalently, for any number not divisible by p, $a^{p-1} \equiv 1 \pmod{p}$. More generally, $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$

Let's work through an example to see how it works with $p = 7$:

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

To show how we get the table entries, let's look at row 5 for example:

$$\begin{aligned} 5^2 &= 25 \equiv 4 \pmod{7} \\ 5^3 &= 5 \times 4 \equiv 6 \pmod{7} \\ 5^4 &= 5 \times 6 \equiv 2 \pmod{7} \\ 5^5 &= 5 \times 2 \equiv 3 \pmod{7} \\ 5^6 &= 5 \times 3 \equiv 1 \pmod{7} \end{aligned}$$

If you look at how many times you need to multiply a number by itself to get back to 1, you can see that for 1, the cycle length is 1, for $6 \equiv -1 \pmod{7}$ it is 2, for 2 and 4 it is 3, and for 3 and 5, it is 6. In all cases the cycle length divides $p - 1$.

In many equations where we want to prove that solutions are or are not possible for equations including prime numbers, we can do so using Fermat's Little Theorem and modular arithmetic.

Q. 6. *What is the value of* $2001^{2002} \pmod{2003}$*?*

A. 2. *There are often questions like this with year numbers in the question - it is a good idea to know if the current year (or one more than the current year) has some interesting property. In this case, let's check whether 2003 is a prime. To do so, we need to check whether it is divisible by any prime number less than* $\sqrt{2003} \approx 44$.

We can quickly see with basic divisibility tricks that it is not divisible by 2 (last digit is odd), 3 (sum of digits is not a multiple of 3), 5 (last digit is not

0 or 5), 11 (summing the alternating digits does not give the same number mod 11). So we only have to check divisibility by 7, 13, 17, 19, 23, 29, 31, 37, 41, and 43 to verify if 2003 is prime. I will leave that as an excercise.

If 2003 is prime, then by Fermat's Little Theorem, $a^2002 \equiv 1 \pmod{2003}$.

Q. 7. *What is the remainder when you divide* 4^{87} *by 17?*

A. 3. *We know by Fermat's Little Theorem that* $4^{16} \equiv 1 \pmod{17}$. *Then:*

$$\begin{aligned} 4^{87} &= (4^{16})^5 \times 4^7 \pmod{17} \\ &= (4^2)^3 \times 4 \pmod{17} \\ &= (-1)^3 \times 4 \pmod{17} \\ &= -4 \pmod{17} = 13 \pmod{17} \end{aligned}$$

Q. 8. *Find* $6^{1000} \pmod{23}$. *(AOPS)*

Q. 9. *What are the last two digits of* 7^{9999}*? (MATHCOUNTS 1986)*