Modular Arithmetic

Graham Middle School Math Olympiad Team

MODULAR ARITHMETIC

Now is $4:00$ *pm*, what time will be 100 hours from now?

4 days is equal to $4 \times 24 = 96$ hours, so 100 hours is equal to 4 days and 4 hours. That means in 96 hours we will have the same time. After 4 hours it will be $8:00$ *pm*.

Modular arithmetic is a type of arithmetic that deals with remainders of numbers.

In modular arithmetic, numbers ”wrap around” upon reaching a given number (this given number is known as the **modulus**) to leave a remainder.

The value $a \pmod{m}$ is a shorthand way of saying *“the remainder when a is divided by m”*, and is from 0 to $m-1$.

We say that two numbers a and b are **congruent modulo** m if $b-a$ is divisible by m. That is,

$$a \equiv b \pmod{m}$$

if and only if $b-a=mk$ for some integer k.

38 is congruent to $14 \pmod{12}$, because $38-14=24$, which is a multiple of 12, or, equivalently, because both 38 and 14 have the same remainder 2 when divided by 12. We use a triple equal sign to represent *congruence*:

$$38 \equiv 14 \pmod{12}.$$

The same rule holds for negative values:

$$-8 \equiv 7 \pmod{5};$$

$$2 \equiv -3 \pmod{5};$$

$$-3 \equiv -8 \pmod{5}.$$

In contests, you will often find modular arithmetic a useful tool for solving problems involving remainders or divisibility.

ADDITION AND MULTIPLICATION THEOREMS FOR MODULAR ARITHMETIC

If $a + b = c$, then

$$a \pmod{n} + b \pmod{n} \equiv c \pmod{n}.$$

To find the **remainder of the sum** of a and b, we can instead **sum the remainders** of the two terms.

The proof is straightforward:
Let's write a, b and c as $q_a n + r_a$, $q_b n + r_b$ and $q_a n + r_a$ where q_a, q_b, and q_c are *quotients* and r_a, r_b, and r_c are *remainders* of division by n. Then

$$a + b = q_a n + r_a + q_b n + r_b = (q_a + q_b)n + (r_a + r_b)$$

That means we can ignore $(q_a + q_b)n$ and $q_c n$ when considering numbers *modulo* n. So we have

$$r_a + r_b \equiv r_c \pmod{n}.$$

Which we wanted to proof.

For example:

$$2021 \equiv 2000 + 20 + 1 \pmod{n}$$

If $a \times b = c$, then

$$a \pmod{n} \times b \pmod{n} \equiv c \pmod{n}.$$

To find the **remainder of the product** of a and b, we can instead **multiply the remainders** of the two factors.

Doing the same substitution as in proof of the *addition theorem*

$$a \times b = (q_a n + r_a)(q_b n + r_b) =$$
$$= q_a q_b n^2 + (q_a r_b + q_b r_a)n + r_a r_b.$$

We can ignore $q_a q_b n^2$, $(q_a r_b + q_b r_a)n$, and $q_c n$ because all of them is divisible by n. So we have

$$r_a \times r_b \equiv r_c \pmod{n}.$$

For example:

$$2021 \times 2022 \equiv 21 \times 22 \equiv 462 \equiv 62 \pmod{100};$$
$$42 \times 24 \equiv 3 \times -2 \equiv -6 \equiv 7 \pmod{13}.$$

DIVISIBILITY RULES FOR POWERS OF 2 AND 5

In elementary school you learned that all even numbers are divisible by 2. So you only need to know the last digit of a number to know if it is divisible by 2. We can prove that's true. Let a, b, c, d, e be the digits of a 5-digit number.

$$\overline{abcde} = a\times10^4+b\times10^3+c\times10^2+d\times10^1+e\times10^0.$$

With the exception of the units digit term, each term in this sum must have a value of zero $\pmod 2$ because all multiples of 10 are divisible by 2. By the addition theorem of modular arithmetic

$$\overline{abcde} \pmod 2 \equiv \overline{abcd0} \pmod 2 + e \pmod 2 \equiv e\ (\text{mod } 2$$

note also that

$$\overline{abcde} \pmod 5 \equiv \overline{abcd0} \pmod 5 + e \pmod 5 \equiv e\ (\text{mod } 5$$

since all powers of 10 are divisible by 5.

What about divisibility by 4? Ten is not divisible by 4, but every power of 10 greater than 100 is, so all multiples of 100 have a value of $0 \pmod 4$. Hence, the value of any number greater than $100 \pmod 4$ is equal to the value $\pmod 4$ of its last 2 digits. This gives us the divisibility rule for 4: a number is divisible by 4 if the number formed by its last two digits is divisible by 4. In fact, the remainder of any number divided by 4 is the remainder of the number formed by its last two digits. Going to the next power of 2,