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

Is $721{,}456$ divisible by 8?

8 is $2 \times 2 \times 2$. That means that we can multiply it by $5 \times 5 \times 5$ and get $10 \times 10 \times 10$, so $1,000$ must be divisible by 8.
Lets write down $721{,}456$ as $721{,}000 + 456$, as we know from the *addition theorem* the remainder of the division of $721{,}456$ is equal to the sum of remainders of each of summants. Since $21{,}000$ is multiple of $1{,}000$ it remainder modulo 8 is 0. So

$$721{,}456 \equiv 456 \pmod 8.$$

That means to check whether $721{,}456$ divisible by 8, we need to check, whether 456 is divisible by 8. Indeed $456 = 8 \times 57$, so $721{,}456$ is also divisible by 8.

To know whether a number is divisible by 2^n, we need to check whether the **last n digits** of the number is divisible by 2^n.

Is 6385 divisible by 25?

25 is 5×5, so multiplying it by 2×2 we will get that 25 is multiple of 100. Doing the same stuff as with divisibility by 2, we write 6385 as $6300 + 85$. 6300 is a multiple of 100 thereof it is also multiple of 25. That means we only need to check whether 85 is divisible by 25. $85 = 75 + 10$, so 6385 is not divisible by 25.

To know whether a number is divisible by 5^n, we need to check whether the **last n digits** of the number is divisible by 5^n.

Both rules are true, because 10^n is divisible by 2^n and 5^n. Using this facts allows us to exclude from consideration all numbers bigger than 10^n and that left us with the last n digits of a number.

DIVISIBILITY RULES FOR 3 AND 9

Is 5479 divisible by 9?

Let's write a number 5479 as a sum

$$5472 = 5 \cdot 1000 + 4 \cdot 100 + 7 \cdot 10 + 2.$$

And then write 1000 as a sum $999 + 1$, $100 = 99 + 1$ and $10 = 9 + 1$. So

$$5472 = 5 \cdot (999+1) + 4 \cdot (99+1) + 7 \cdot (9+1) + 9 =$$
$$= 5 \cdot 999 + 5 + 4 \cdot 99 + 4 + 7 \cdot 9 + 7 + 2.$$

And finally we can realize that 999, 99, and 9 are divisible by 9. That means that divisibility of 5479 by 9 depends on divisibility of sum $5 + 4 + 7 + 2$.

A number is divisible by 9, if the **sum of its digits** is divisible by 9.

And since 9, 99, 999, 9999 and so on is also divisible by 3, we get

A number is divisible by 3, if the **sum of its digits** is divisible by 3.

$\overline{abcd}$ is a mathematical notation that a number is written with digits a, b, c, and d. So

$$\overline{abcd} = a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d.$$

This allows us to write the rules as

$$\overline{abcd} \equiv a + b + c + d \pmod{9 \text{ or } 3}.$$

The divisibility rule by 9 allows us quickly check if our arithmetic operations are correct.

$$\begin{array}{r} 384 \\ \times \quad 56 \\ \hline 2304 \\ 1820 \\ \hline 20504 \end{array}$$

Lets see remainders of factors and product

$$384 \equiv 6 \pmod 9, \quad 56 \equiv 2 \pmod 9,$$
$$20504 \equiv 2 \pmod 9.$$

But $6 \times 2 \not\equiv 2 \pmod 9$, so there is an error.

DIVISIBILITY RULES FOR 11

The divisibility rules for 9 and 3 works because 10, 100, 1,000, and so on are all divisible by 9 with remainder 1. But what about 11?

$$1\underbrace{00\ldots0}_{\text{even zeros}}-1=\underbrace{99\ldots9}_{\text{even nines}}$$

is divisible by 11 because it is sum of

$$99\,99\ \ldots 99 = 99\cdot 10^{n}+\ldots+99$$

which all are divisible by 11.
From other hand

$$1\underbrace{00\ldots0}_{\text{odd zeros}}+1=\underbrace{99\ldots9}_{\text{even nines}}0+11$$

is also divisible by 11.

Is 3432 divisible by 11?

$$3432 = 3\cdot 1000+4\cdot 100+3\cdot 10+2 =$$
$$= 3\cdot(1001-1)+4\cdot(99+1)+3\cdot(11-1)+2\equiv$$

when we get rid of all multiples of 11

$$\equiv -3+4-3+2=0 \pmod{11}.$$

As we see our final computation is the digits of the number with alternate signs.

A number is divisible by 11 if the **difference** between the **sum of the odd-place digits** and the **sum of the even-place digits** is 0 or a multiple of 11.

The combinations of the divisibility rules may also create addition divisibility rules.
For examle to check if number is divisible by 6 we may check if it divisible by 2 and 3. This will works when the divisor may be split in product of **coprime**[a] factors.
But the rule will not work for example for $27 = 9\times 3$, since testing for 9 we already testing for 3.

[a] *coprime numbers are numbers that don't have common divisors.*

SUMMARY OF THE DIVISIBILITY RULES

An integer number n is divisible by

2. if the *last digit of n is divisble by* 2, e.g. is equal to 0, 2, 4, 6, or 8;
3. if the *sum of digits of n is divisible by* 3;
4. if the *last two digits of n is divisible by* 4.
5. if the *last digit of n is divisble by* 5, e.g. is equal to 0 or 5;
6. if n is divisible by both 2 and 3;
7. if *subtracting twice the last digit of n from the remaining digits* gives a multiple of 7;
8. if the *last three digits of n is divisible by* 8;
9. if the *sum of digits of n is divisible by* 9;
10. if n is divisible by both 2 and 5;
11. if the *difference of the alternating sum of digits of n* is a multiple of 11;
12. if n is divisible by both 3 and 4.

You might notice the strange divisibility rule for 7. The proof of this rule is not straightforward as for all other. Let's write $n = a \cdot 10 + b$, where b is the last digit and a is the number build with remaining digits. Then suppose n is divisible by 7

$$\begin{aligned} a \cdot 10 + b &\equiv 0 \pmod 7, && \text{multiply all by } 2 \\ a \cdot 20 + b \cdot 2 &\equiv 0 \pmod 7, && \text{substract } 21a \\ a \cdot (-1) + b \cdot 2 &\equiv 0 \pmod 7, && \text{multiply by } -1 \\ a - b \cdot 2 &\equiv 0 \pmod 7. \end{aligned}$$

Doing the same operations in reverse order, we can get the divisibility rule for 7. This is possible because 2 and -1 are *coprime* with 7.
The rule may be repeated several times to get a number small enough for the direct check.

Similar divisibility rules may be obtained for other primes

13. if *adding 4 times the last digit of n to the remaining digits* gives a multiple of 13;
17. if *subtracting 5 times the last digit of n from the remaining digits* gives a multiple of 17.

But these rules aren't simpler than divide by the number.

EXERCISES

1. What is the largest integer less than 100 which is congruent to $3 \pmod 5$?
2. How many integers are there between 50 and 250 inclusive which are congruent to $1 \pmod 7$?
3. Find the value of the digit represented by A in the 5-digit number $12A3B$ if that number is divisible by both 4 and 9 and A does not equal B.
4. In how many ways can a debt of $\$69$ be paid exactly using only $\$5$ and $\$2$ bills?
5. When n is divided by 5 the remainder is 1. What is the remainder when $3n$ is divided by 5?
6. The 4-digit number 4_89 is divisible by 11. What digit goes in the blank?
7. If the 5-digit number $3367\_$ is divisible by 15, what digit must go in the blank?

CHALLENGE PROBLEMS

1. The Fibonacci sequence is the sequence 1, 1, 2, 3, 5, 8, 13, $\ldots$, where every term after the second is equal to the sum of the two preceding terms. Using the addition theorem for modular arithmetic, what is the remainder when the 100^{th} term of the Fibonacci sequence is divided by 8? (Hint: *look for a repeating pattern*).
2. Prove that the square of any integer is congruent to either 0, 1, or $4 \pmod 8$.