Modular Arithmetic and Divisibility Rules

Graham Middle School Math Olympiad Team

Modular Arithmetic

- M**odular arithmetic** is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the **modulus** (plural **moduli**). The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in his book *Disquisitiones Arithmeticae*, published in 1801.
- A familiar use of modular arithmetic is in the 12-hour clock, in which the day is divided into two 12-hour periods. If the time is 7:00 now, then 8 hours later it will be 3:00. Usual addition would suggest that the later time should be 7 + 8 = 15, but this is not the answer because clock time "wraps around" every 12 hours. Because the hour number starts over after it reaches 12, this is arithmetic *modulo* 12. According to the definition below, 12 is **congruent** not only to 12 itself, but also to 0, so the time called "12:00" could also be called "0:00", since 12 is congruent to 0 modulo 12

Examples

- 38 is congruent to 14 (mod 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 THEOREM 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 **add the remainders** of the two terms.

The proof of this theorem is trivial. You might never have considered if this is true, but it has to be because

a/N + b/N = (a + b)/N

Example:

$2021 \equiv 2000 + 20 + 1 \pmod{10}$;

DIVISIBILITY RULES FOR POWERS OF 2

If a number is divisible by 2^n, then the number formed by the last n digits of the given number is also divisible by 2^n; and the converse is true.

Proof

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.

$$ABCDE = A \times 10^4 + B \times 10^3 + C \times 10^2 + D \times 10^1 + E \times 10^0$$

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

$ABCDE \pmod 2 \equiv ABCD0 \pmod 2 + E \pmod 2 \equiv E \pmod 2$ note also that
$ABCDE \pmod 5 \equiv ABCD0 \pmod 5 + E \pmod 5 \equiv E \pmod 5$ since all powers of 10 are divisible by 5.

Therefore, a number is divisible by 2 if its last digit is even, and a number is divisible by 5 if its last digit is 0 or 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 (mod 4). Hence, the value of any number greater than 100 (mod 4) is equal to the value (mod 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, $100 \equiv 4 \pmod 8$, but $1000 \equiv 0 \pmod 8$, so the divisibility rule for 8 requires us to check if the last 3 digits of a number are divisible by 8. In fact, $10^n = 5^n 2^n$, so 10^n is always evenly divisible by 2^n, and never evenly divisible by 2^{n+1}. To the find the remainder of any number when it is divided by 2^n, we only have to look at the last n digits.

Example

Is 421,235,264 divisible by 16?

Ans: 16 is 2^4, so we only need check if the number formed by the last 4 digits, namely 5264, is divisible by 16. In fact, 5264 is easily shown to be 329x16, so the statement is true.

MULTIPLICATION THEOREM FOR MODULAR ARITHMETIC

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

Proof

Let

$$a \pmod n = a', \quad b \pmod n = b', \quad c \pmod n = c'.$$

Since $a \pmod n = a'$, a must be equal to some integer multiple of n plus a'. The similar relationships hold between b and b' and c and c'. In other words:

$$a = k_a n + a', \quad b = k_b n + b', \quad c = k_c n + c',$$

where k_a, k_b, and k_c are some integers.

$$a \times b = c$$

can now be written as

$$(k_a n + a') \times (k_b n + b') = c = k_c n + c'.$$

By the distributive property we multiply out the terms:

$$k_a k_b n^2 + a' k_b n + b' k_a n + a' b' = k_c n + c'.$$

When we evaluate all the terms mod n, all the terms with factors of n are congruent to 0 (mod n), and we see that

$$a' b' \equiv c' \pmod n.$$

Q.E.D.

Note: Q.E.D. is an abbreviation for the Latin phrase *quod erat demonstrandum* (which was to be proved). It is placed to signify that a conjecture has been proven.

Examples

$2021 \times 2022 \equiv 21 \times 22 \equiv 462 \equiv 62 \pmod{100}$;

$42 \times 24 \equiv 3 \times -2 \equiv -6 \equiv 7 \pmod{13}$;

$99^{99} \equiv (-1)^{99} \equiv -1 \equiv 9 \pmod{10}$;

$38 \times 173 \times 619 \equiv 0 \times 173 \times 619 \equiv 0 \pmod{19}$.

Side note. The Power of Proof

One of the really cool things about mathematics that you don't get exposed to much until geometry in Math 8.2 is how you can prove one theorem, and then another, and subsequent theorems are built upon those proofs in a beautiful, logical, self-consistent framework. In this unit, by proving the addition and multiplication theorems for modular arithmetic, we can now go on to prove many of the divisibility rules you learned in elementary school, but until now, those rules may have seemed like mysterious, hidden truths. I have always found it extremely satisfying to understand why something is true or valid. In mathematics, it is through proofs that we understand the why.

REMAINDER TEST FOR 11

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**

Proof

Any base 10 number can be broken into the sum of its digits times increasing powers of 10 (1, 10, 100, 1000, etc.)
For example, ABCDE = A x 10^4 + B x 10^3 + C x 10^2 + D x 10^1 + E x 10^0
1 (mod 11) is 1
10 (mod 11) is 10 which is congruent to -1 (This is the key realization in this proof)
100 (mod 11) is 1
1000 (mod 11) is -1
10000 (mod 11) is 1 and the pattern continues to alternate between -1 and 1. We know this is true from the product theorem for modular arithmetic. Since 10 (mod 11) ≡ -1, the value (mod 11) of increasing powers of 10 will alternate between 1 and -1.

Hence to calculate the value of any counting number (mod 11), sum the digits in the 1's, 100's, etc. places, and from that subtract the sum of the digits in the 10's, 1000's, etc. places. When this value is 0 (mod 11), the number is evenly divisible by 11, and we see how we obtain the divisibility rule for 11.
ABCDE (mod 11) = A (mod 11) x 10^4 (mod 11) + B (mod 11) x 10^3 (mod 11) + C (mod 11) x 10^2 (mod 11) + D (mod 11) x 10 (mod 11) + E (mod 11). Of course, any single digit number (mod 11) is equal to itself, so ABCDE (mod 11) = (A – B + C – D + E) (mod 11).

Examples

Is 22231 divisible by 11?

Ans: We highlight the odd place digits in green, and the even place digits in red: 22231. (2+2+1) – (2+3) = 0, therefore 22231 is divisible by 11 (in fact it is 2021x11);

What is the remainder when 75479 is divided by 11?

Ans: You could do long division, but it is perhaps easier to use modular arithmetic. (7+4+9) – (5+7) = 8

What is the remainder when 15482 is divided by 11?

Ans: (1+4+2) – (5 + 8) = -6. Of course −6 ≡ 5 (mod 11), so the remainder (which must be a positive integer less than 11) is 5;

What is the remainder when 92819 is divided by 11?

Ans: (9+8+9) – (2+1) = 23. 23 ≡ 1 (mod 11), so the remainder is 1.

REMAINDER TEST FOR 9

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

Proof

Now that we know modular arithmetic, we can see where the divisibility rule for 9 comes from.
1 (mod 9) is 1
10 (mod 9) is 1
100 (mod 9) is 1
1000 (mod 9) is 1
In fact, it is obvious that any power of 10 (mod 9) is 1, since it would be 1 larger than a number whose digits are all 9, and therefore is evenly divisible by 9.

The remainder when any number (…EDCBA) is divided by 9 is (using the sum and product theorems)
…EDCBA (mod 9) = A (mod 9) + 10 (mod 9)xB (mod 9) + 100 (mod 9)xC (mod 9) + 1000 (mod 9)xD (mod 9) …
= A (mod 9) + B (mod 9) + C (mod 9) + D (mod 9) + …
In other words, it is the sum of digits. Note that since 9 (mod 9) is zero, when summing the digits, you can actually skip any 9's since adding multiples of 9 to the sum of the other digits won't change if that sum is divisible by 9.

.

Examples

Is 22231 divisible by 9?

Ans: Summing the digits, we get 10. $10 \equiv 1 \pmod 9$ so the remainder is 1 when 22231 is divided by 9;

What is the remainder when 75479 is divided by 9?

Ans: 7+5+4+7 = 23 (note that you don't need to worry about adding that last 9). $23 \equiv 5 \pmod 9$, so the remainder is 5.

.

REMAINDER TEST FOR 3

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

Proof

This proof is very similar to the remainder test for 9, but summing the digits can be made even simpler. 1 (mod 3) is 1; 10 (mod 3) is 1; 100 (mod 3) is 1; 1000 (mod 3) is 1
In fact, it is obvious that any power of 10 (mod 3) is 1, since it would be 1 larger than a number whose digits are all 9, and therefore is evenly divisible by 3.

Hence the remainder when any number (…EDCBA) is divided by 3 is (using the sum and product theorems)
…EDCBA (mod 3) = A (mod 3) + 10 (mod 3)xB (mod 3) + 100 (mod 3)xC (mod3) + 1000 (mod 3)xD (mod 3) …
= A (mod 3) + B (mod 3) + C (mod 3) + D (mod 3) + …

Therefore, if the sum of the digits is divisible by 3, the number is divisible by 3.

Note, however, that summing the digits becomes even easier when you know that you actually only have to sum them (mod 3).
0, 3, 6, or 9 ≡ 0 (mod 3)
1, 4, or 7 ≡ 1 (mod 3)
2, 5, or 8 ≡ 2 ≡-1 (mod 3)

Examples

Is the number 1234567899876543 21 divisible by 3?

Ans: You could add up all of the digits and get 90 and see that is divisible by 3. Or you could sum the digits (mod 3):
1 -1 0 1 -1 0 1 -1 0 0 -1 1 0 -1 1 0 -1 1 and get zero and reach the same result even faster.

What is the remainder when 7^{77} is divided by 3?

Ans: 7 ≡ 1 (mod 3). By the product theorem of modular arithmetic, 7 multiplied by itself any integer number of times will result in a product congruent to 1 (mod 3). Therefore, the remainder is 1.

SUMMARY OF THE DIVISIBILITY RULES

1. **If a number is divisible by 2^n, then the number formed by the last n digits of the given number is also divisible by 2^n; and the converse is true.**
   Example: 7,292,536 is divisible by 2 (or 2^1) because 6 is divisible by 2
   Example: 7,292,536 is divisible by 4 (or 2^2) because 36 is divisible by 4.
   Example: 7,292,536 is divisible by 8 (or 2^3) because 536 is divisible by 8.
2. **If the sum of the digits of a number is divisible by 3, then the number is divisible by 3**
3. **If the sum of the digits of a number is divisible by 9, then the number is divisible by 9.**
   Example: 323,745 is divisible by 3 because 3+2+3+7+4+5 = 24 which is a multiple of 3.
   Example: 658,773 is divisible by 9 because 6+5+8+7+7+3 = 36 which is a multiple of 9.
4. **A number is divisible by 5 if its units digit is 5 or 0.**
5. **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**.
   Example: 90,728 is divisible by 11 because (9+7+8) – (0+2) = 24 – 2 = 22, which is a multiple of 11.
6. **A number is divisible by the product of two co-prime numbers if it is divisible by each of those co-prime numbers.**
   Example: A number is divisible by 6 if it is divisible by both 2 and 3.
   Example: A number is divisible by 15 if it is divisible by both 3 and 5.
   Example: A number is not necessarily divisible by 24 if it is divisible by both 2 and 12, because 2 is a factor of 12.

Exercises (2 points each)

1. What is the largest integer less than 100 which is congruent to 3 (*mod* 5)?

2. How many integers are there between 50 and 250 inclusive which are congruent to 1 (*mod* 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 (5 points each)

8. The Fibonacci sequence is the sequence 1, 1, 2, 3, 5, 8, 13, …, 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*).

9. Prove that the square of any integer is congruent to either 0, 1, or 4 (*mod* 8).