Number Theory 102

Graham Middle School Math Olympiad Team

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 prove.

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 the 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:

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

What is 6547 on *Planet 51*?

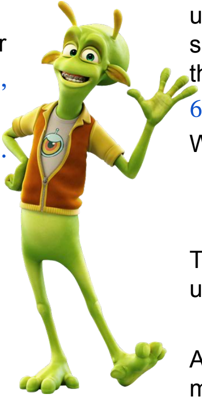
We, earthlings, use the positional numeral system, which was invented between the 1st and 4th centuries by Indian mathematicians.
In English, we read 6547 as *six thousand five hundred forty-seven*, or

$$6547 = 6\times1000+5\times100+4\times10+7,$$

in short writing:

$$6547 = 6\times10^3+5\times10^2+4\times10+7.$$

There
10 is the essential piece of how we understand our numbers. We called our system the **base-ten positional numeral system** or short **decimal**.
Moreover we have just 10 *digits*:
0, 1, 2, 3, 4, 5, 6, 7, 8, and 9.



But 10 is just the number of fingers on our hands, some random result of evolution on the Earth. Does it mean that an alien from *Planet 51*, who has 8 fingers on their hands, can't count? But if they also use the positional system, aliens may use only 8 digits. We will translate them into our spelling as 0, 1, 2, 3, 4, 5, 6, and 7. As a result, they may treat the number like this:

$$6547 \text{ (on Planet 51)} = 6\times8^3+5\times8^2+4\times8+7.$$

Which in our world would mean:

$$6547 \text{ (on Planet 51)} =$$
$$= 6\times512+5\times64+4\times8+7 = 3431.$$

To distinguish "our" numbers from "their," we will use subscript with the base of the system, so

$$6547_8 = 3431_{10}.$$

And now we can communicate with aliens without misunderstanding.

BASE 2

However, we don't need to fly to a faraway planet to find aliens using non 10 based numeral systems. Other creatures around us use another numeral system. We call them *computers*, and since they only can distinguish the presence of electricity or its absence, they may use only 2 digits - 0 and 1, where 0 - no electricity and 1 - there is electricity.

We call the numeral system with base 2 **binary**.

Present 6547_{10} in the binary system?

Let's write down the first powers of 2: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096 and so on. Since digits can be only 0 and 1, the number would be sum of some powers of 2:

$$6547_{10} = 4096+2048+256+128+16+2+1 =$$
$$= 2^{12} + 22^{11} + 2^8 + 2^7 + 2^4 + 2^1 + 2^0 =$$
$$= 1100110010011_2$$

Instead of 4 digits, the binary system uses 12 to represent 6547, but they can sum and multiply numbers much faster. The reason is the binary addition and multiplication tables.

$+$	0	1
0	0	1
1	1	10

$\times$	0	1
0	0	0
1	0	1

For example:

$$\begin{array}{r} 10011 \\ +\,1010 \\ \hline 11101 \end{array}$$

$$\begin{array}{r} 1011 \\ \times\,101 \\ \hline 1011 \\ 1011 \\ \hline 110111 \end{array}$$

In programming, we often use the **hexadecimal system** (base 16). Since we use only 10 digits, and base 16 system need 16, we use letters as digits $10 = A$, $11 = B$, $12 = C$, $13 = D$, $14 = E$, $15 = F$. For example

$$7A_{16} = 7 \times 16 + 10 = 122_{10}$$

CONVERTING BETWEEN BASES

Convert 6547_{10} to 9-base numeral system?

The natural approach is to find out all needed powers of 9: 9, 81, 729, 6561, and so on. Then find the biggest power of 9 lower than our number and divide it with reminder:

$$
\begin{aligned}
6547 &= \mathbf{8} \times 729 + 715, \\
715 &= \mathbf{8} \times 81 + 67, \\
67 &= \mathbf{7} \times 9 + 4, \\
4 &= \mathbf{4} \times 1 + 0,
\end{aligned}
$$

and we get $6547 = 8 \times 9^3 + 8 \times 9^2 + 7 \times 9 + 4$. So

$$6547_{10} = 8874_9$$

Convert 6547_9 to *decimal* numeral system?

$$
\begin{aligned}
6547_9 &= 6 \times 9^3 + 5 \times 9^2 + 4 \times 9 + 7 = \\
&= 6 \times 729 + 5 \times 81 + 4 \times 9 + 7 = 4822.
\end{aligned}
$$

But there is another approach: lets rewrite

$$6547_{10} = 8 \times 9^3 + 8 \times 9^2 + 7 \times 9 + 4.$$

as

$$6547_{10} = ((8 \times 9 + 8) \times 9 + 7) \times 9 + 4.$$

and it gives us the second method:

$$
\begin{aligned}
6547 &= 727 * 9 + \mathbf{4}, \\
727 &= 80 * 9 + \mathbf{7}, \\
80 &= 8 * 9 + \mathbf{8}, \\
8 &= \mathbf{8}.
\end{aligned}
$$

and we get our number in reverse order.
It also may be written this way (from bottom to top)

$$
\begin{array}{rl}
0 & \mathrm{R}\ \mathbf{8} \\
9\,\big)\,\overline{8} & \mathrm{R}\ \mathbf{8} \\
9\,\big)\,\overline{8\,0} & \mathrm{R}\ \mathbf{7} \\
9\,\big)\,\overline{7\,2\,7} & \mathrm{R}\ \mathbf{4} \\
9\,\big)\,\overline{6\,5\,4\,7} &
\end{array}
$$

THE LAST DIGIT

Find the last digit of $743 + 24$?

Let's write our numbers as $74 \times 10 + 3$ and $2 \times 10 + 4$ and find the sum:

$$743+\mathbf{24} = (74\times10+\mathbf{3})+(2\times10+\mathbf{4}) = (76\times10)+\mathbf{7}.$$

As we see, every multiple of 10 does not contribute to the last digit because all they can apply is tenth and higher.

The same is true for multiplication.

Find the last digit of 743×24?

$$743 \times \mathbf{24} = (74 \times 10 + \mathbf{3})(2 \times 10 + \mathbf{4}) =$$
$$= 74 \times 2 \times 100 + 74 \times 4 \times 10 +$$
$$+ 3 \times 2 \times 10 + \mathbf{3} \times \mathbf{4} =$$
$$= \text{something}\times10+\mathbf{12} = (\text{something}+1)\times10+\mathbf{2}.$$

The **last digit** of a sum, difference, or product *depends only* on the **last digit** of terms.

Find the last digit of 7^{42}?

As usual for problems with big numbers, it is sometimes fruitful to start with small numbers and look for a pattern.

$7^1 = 7$, $7^2 = ...9$, $7^3 = ...3$, $7^4 = ...1$, $7^5 = ...7$, $7^6 = ...9$, $7^7 = ...3$. And the last digits start repeating. Indeed, as soon as we get a digit we already met, the next digit would be produced by the same operation since we always multiply by 7.

As a result, the numbers will form a repeated pattern with period 4.

To find the last digit of 7^{42}, we need to find a reminder of 42 divided by 4. $42 = 10 \times 4 + 2$, so the last digit of 7^{42} will be the same as of 7^2. That means that the last digit of 7^{42} is 9.

TERMINAL ZEROES

The **factorial** $n!$ is the product of all positive integers less than or equal to n.

Count the number of trailing zeros in $7!$.

We may count $7!$ as

$$7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5{,}040.$$

So the number of trailing zeros of $7!$ is 1.

But what to do for numbers much bigger?

Count the number of trailing zeros in $78!$.

Even the computer will have trouble counting $78!$, but we don't need the whole number. Instead, we need only trailing zeros. How do they appear? Let's look from another side. What does it mean a number has n trailing zeros? We may think of that as the number is n times divisible by 10. So the number is divisible by 10^n.

A number is divisible by 10 if its prime factorization has 2 and 5.

And to be divisible by 10^n it needs to have n times factors 2 and 5. So, let's count how many 2 has prime factorization of $78!$. Every even number in $78!$ give at least one 2, so we already have $78 \div 2 = 39$ twos. Also, every multiple of 4 gives us an additional 2, so we will have additional 19 twos. Multiples of 8: 9 twos, multiples of 16: 4 twos, and multiples of 32 and 64: 2 and 1 twos.

$$39 + 19 + 9 + 4 + 2 + 1 = 74$$

And this means $78!$ is divisible by 2^{74}.

What about 5^n. $78!$ has 15 multiples of 5 and 3 multiples of 25. So $78!$ is divisible by 5^{18}. As we see, the power of 5 is much *smaller* then the power of 2.

$n!$ factorial has the same number of trailing zeroes as **maximal power** of 5 it is *divisible*.

EXERCISES

1. Convert to the base 7 the number 532_8 ?
2. What is the last digit in 7^{149} ?
3. How many trailing zeros in $144!$?
4. $R + RR = BOW$. What is the last digit of $F \times A \times I \times N \times T \times I \times N \times G$?
5. What is the largest power of 2 that is a divisor of $13^4 - 11^4$?
6. What is the smallest positive integer greater than 1 that leaves a remainder of 1 when divided by 4, 5, and 6?
7. What is the largest integer n for which 5^n is a factor of the sum $98! + 99! + 100!$?
8. Starting with some gold coins and some empty treasure chests, I tried to put 9 gold coins in each treasure chest, but that left 2 treasure chests empty. So instead I put 6 gold coins in each treasure chest, but then I had 3 gold coins left over. How many gold coins did I have?

CHALLENGE PROBLEMS

1. The digits 1, 2, 3, 4, and 5 are each used once to write a five-digit number $PQRST$. The three-digit number PQR is divisible by 4, the three-digit number QRS is divisible by 5, and the three-digit number RST is divisible by 3. What is P?
2. What is the greatest possible sum of the digits in the base-seven representation of a positive integer less than 2022?
3. The base-ten representation for $19!$ is $121{,}6T5{,}100{,}40M{,}832{,}H00$, where T, M, and H denote digits that are not given. What is $T+M+H$?
4. There are 6 boxes of apples in a store, weighting 15, 16, 18, 19, 20, and 31 pounds. Two customers purchased 5 boxes, and one customer purchased twice as many apples as the second customer. Which box has been left?