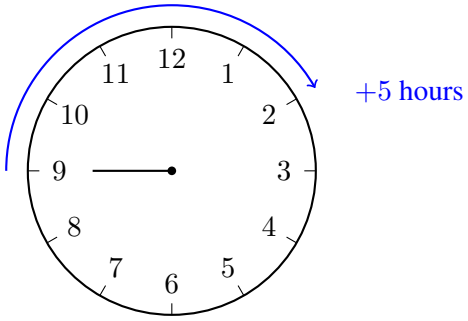
We all use a special kind of arithmetic every day without thinking about it. If it is 9 o'clock now, then in 5 hours it will not be 14 o'clock, but 2 o'clock. On a clock, after 12 we start again from the beginning. This kind of arithmetic, where numbers "wrap around," is called **modular arithmetic**, or clock arithmetic.



Example 1. It is 9 o'clock now. What time will it be in 100 hours?

Solution. Every 12 hours, the clock gets back to where it was. So we only need to know how many hours are left over after the full 12-hour rounds. We divide 100 by 12:

$$100 = 12 \cdot 8 + 4$$

After 8 full rounds the clock shows 9 o'clock again, and then 4 more hours pass. So it will be $9 + 4 = 13$, which on the clock is 1 o'clock.

The only thing that mattered in this computation was the *remainder* of 100 when divided by 12.

Definition. Let n be a positive integer. If an integer a leaves the remainder r when divided by n, we write

$$a \equiv r \pmod{n}$$

and read it as "a is congruent to r modulo n." The remainder r is always one of the numbers $0, 1, 2, \ldots, n-1$.

For example, $100 \equiv 4 \pmod{12}$, because $100 = 12 \cdot 8 + 4$. Similarly, $17 \equiv 2 \pmod{5}$, and $36 \equiv 0 \pmod{12}$, because 36 is divisible by 12.

Example 2. Today is Tuesday. What day of the week will it be 100 days from today?

Solution. The days of the week repeat every 7 days, so we need the remainder of 100 when divided by 7:

$$100 = 7 \cdot 14 + 2$$

So $100 \equiv 2 \pmod{7}$. In 98 days (14 full weeks) it will be Tuesday again, and 2 days later it will be $\boxed{\text{Thursday}}$.

Congruence

So far, the number on the right side of $\equiv$ was always a remainder. More generally, two numbers that give the same remainder are the "same" as far as the clock is concerned. For example, 14 o'clock and 2 o'clock show the same position on the clock.

© Hidegkuti, 2026

Definition. We say that a and b are **congruent** modulo n, and write

$$a \equiv b \pmod{n},$$

if a and b have the same remainder when divided by n. This happens exactly when their difference, $a - b$, is divisible by n.

For example, $14 \equiv 2 \pmod{12}$, because $14 - 2 = 12$ is divisible by 12. Also, $100 \equiv 2 \pmod{7}$, because $100 - 2 = 98 = 7 \cdot 14$. But 25 is not congruent to 4 modulo 6, because $25 - 4 = 21$ is not divisible by 6.

Negative numbers work too: on a clock, 3 hours *before* noon is 9 o'clock. Indeed, $-3 \equiv 9 \pmod{12}$, because $-3 - 9 = -12$ is divisible by 12. In general, to find the remainder of a negative number a modulo n, we keep adding n until we get one of the numbers $0, 1, \ldots, n-1$. For example, $-7 + 5 + 5 = 3$, so $-7 \equiv 3 \pmod{5}$.

Computing with Remainders

What happens to remainders when we add or multiply numbers? Let us look at an example.

Example 3. When the integer a is divided by 12, the remainder is 3. When the integer b is divided by 12, the remainder is 5. Find the remainder modulo 12 of

a) $a + b$, b) ab, c) $a^2 + b^2$.

Solution. We know that $a \equiv 3 \pmod{12}$ and $b \equiv 5 \pmod{12}$. This means that $a = 12k + 3$ and $b = 12m + 5$ for some integers k and m.

a) We add the two expressions and factor out 12 from the terms that are divisible by 12:

$$a + b = (12k + 3) + (12m + 5) = 12k + 12m + 8 = 12\,(k + m) + 8$$

So $a + b$ leaves the remainder 8 when divided by 12: $a + b \equiv 8 \pmod{12}$.

b) We multiply the two expressions.

$$\begin{aligned} ab &= (12k + 3)\,(12m + 5) = 144km + 60k + 36m + 15 \\ &= 144km + 60k + 36m + 12 + 3 = 12\,(12km + 5k + 3m + 1) + 3 \end{aligned}$$

So $ab \equiv 3 \pmod{12}$.

c) We square both expressions.

$$\begin{aligned} a^2 &= (12k + 3)^2 = 144k^2 + 72k + 9 = 12\left(12k^2 + 6k\right) + 9 \\ b^2 &= (12m + 5)^2 = 144m^2 + 120m + 25 = 12\left(12m^2 + 10m + 2\right) + 1 \end{aligned}$$

When we add these, we get $a^2 + b^2 = 12\left(12k^2 + 6k + 12m^2 + 10m + 2\right) + 10$, so $a^2 + b^2 \equiv 10 \pmod{12}$.

© Hidegkuti, 2026

Notice that we get the same answers if we work with the remainders only:

$$3+5=8, \qquad 3\cdot 5=15\equiv 3 \pmod{12}, \qquad 3^2+5^2=34\equiv 10 \pmod{12}$$

For example, if $a=27$ and $b=17$, then $a+b=44=12\cdot 3+8$, $ab=459=12\cdot 38+3$, and $a^2+b^2=1018=12\cdot 84+10$.

This is true in general: the remainder of a sum or a product depends only on the remainders of the numbers we start with.

> **Rule.** To find the remainder of a sum or a product modulo n, we may first replace each number by its remainder modulo n, then add or multiply, and finally take the remainder of the result.

Example 4. Find the last digit of $37\cdot 48$ without computing the product.

Solution. The last digit of a whole number is its remainder modulo 10. The last digits of the two factors are 7 and 8, and $7\cdot 8=56$, whose last digit is 6. So the last digit of $37\cdot 48$ is 6. We can check: $37\cdot 48=1776$.

Example 5. Find the last digit of 3^{100}.

Solution. Of course, we will not compute 3^{100}, a number with 48 digits. Instead, we only keep track of the last digit as we keep multiplying by 3:

power	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8
last digit	3	9	7	1	3	9	7	1

The last digits repeat in a cycle of length 4: $3, 9, 7, 1$. Since 100 is divisible by 4, the power 3^{100} ends at the end of a full cycle, just like 3^4 and 3^8. So the last digit of 3^{100} is 1.

Example 6. Find the remainder when 3^{100} is divided by 7.

Solution. As in Example 5, we compute the remainders of the powers of 3 one after the other. Each time, we multiply the previous remainder by 3 and take the remainder modulo 7: for example, $3^3\equiv 2\cdot 3=6$, and $3^4\equiv 6\cdot 3=18\equiv 4 \pmod 7$.

power	3^1	3^2	3^3	3^4	3^5	3^6	3^7
remainder modulo 7	3	2	6	4	5	1	3

This time the cycle has length 6, and *every* nonzero remainder, $1, 2, 3, 4, 5, 6$, appears in it before the pattern starts over. A number with this property is called a **primitive root** modulo 7. Not every number is a primitive root: for example, the powers of 6 modulo 7 are only $6, 1, 6, 1, \ldots$

Since $100=6\cdot 16+4$, after 16 full cycles we are 4 steps into the next one. So 3^{100} has the same remainder as 3^4:

$$3^{100}\equiv 3^4\equiv 4 \pmod 7$$

© Hidegkuti, 2026

Multiplication Tables

Let us write down the multiplication tables modulo 6 and modulo 7. Each entry is the remainder of the product of the row number and the column number. For example, $4 \cdot 5 = 20 \equiv 2 \pmod 6$, so the entry in row 4 and column 5 of the first table is 2.

modulo 6

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

modulo 7

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modulo 6. Look at row 2 and row 3 of the first table: $2 \cdot 3 = 6 \equiv 0 \pmod 6$. The product of two numbers that are not zero can be zero! We also have $3 \cdot 4 = 12 \equiv 0 \pmod 6$. Numbers like 2, 3, and 4 are called **zero divisors**. So the zero-product rule, "if $ab = 0$ then $a = 0$ or $b = 0$," is not true modulo 6.

Also, row 2 contains only the numbers 0, 2, and 4, each of them twice. So the equation $2x \equiv 1 \pmod 6$ has no solution at all, while $2x \equiv 4 \pmod 6$ has two solutions, $x = 2$ and $x = 5$. Modulo 6, we cannot divide by 2.

Modulo 7. The second table looks very different. There are no zero divisors: a 0 appears only in row 0 and column 0. Even better, each of the rows 1 through 6 contains every one of the nonzero remainders, $1, 2, 3, 4, 5, 6$, exactly once. In particular, every row contains a 1. This means that every nonzero number has a **reciprocal** modulo 7: a number that we can multiply it by to get 1.

number	1	2	3	4	5	6
reciprocal modulo 7	1	4	5	2	3	6

For example, $3 \cdot 5 = 15 \equiv 1 \pmod 7$, so 3 and 5 are reciprocals of each other. The same is true modulo any prime number, but not modulo 6, which is not a prime.

Example 7. Solve the equation $3x \equiv 2 \pmod 7$.

Solution. To "divide by 3," we multiply both sides by the reciprocal of 3, which is 5:

$$\begin{aligned} 5 \cdot 3x &\equiv 5 \cdot 2 \pmod 7 \\ 15x &\equiv 10 \pmod 7 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

because $15 \equiv 1$ and $10 \equiv 3$ modulo 7. We check: $3 \cdot 3 = 9 \equiv 2 \pmod 7$. We can also find the answer in the table: in row 3, the number 2 is in column 3.

© Hidegkuti, 2026



Practice Problems

1. In each congruence, find the remainder r (one of the numbers $0, 1, \ldots, n-1$).

   a) $23 \equiv r \pmod 4$ b) $100 \equiv r \pmod 9$ c) $365 \equiv r \pmod 7$ d) $48 \equiv r \pmod 6$ e) $-7 \equiv r \pmod 4$

2. It is 8 o'clock now. What time will it be in 30 hours?

3. Today is Friday. What day of the week will it be 1000 days from today?

4. A year that is not a leap year has 365 days. If January 1 is a Monday in such a year, what day of the week is January 1 of the next year?

5. Decide whether each statement is true or false.

   a) $38 \equiv 14 \pmod{12}$ b) $25 \equiv 4 \pmod 6$ c) $-1 \equiv 6 \pmod 7$

6. Find the last digit of $23 \cdot 47 \cdot 89$ without computing the product.

7. Find the last digit of 7^{50}.

8. a) List the remainders of $3^1, 3^2, 3^3, \ldots$ modulo 5 until they start to repeat. Is 3 a primitive root modulo 5?

   b) Find the remainder when 3^{50} is divided by 5.

9. Find the remainder when 2^{100} is divided by 7. (Hint: compute the remainders of $2^1, 2^2, 2^3, \ldots$ modulo 7.)

10. Use the multiplication table modulo 6 to find all solutions x (from $0, 1, \ldots, 5$) of each equation.

    a) $3x \equiv 0 \pmod 6$ b) $4x \equiv 1 \pmod 6$ c) $5x \equiv 2 \pmod 6$

11. Solve each equation, using the reciprocals modulo 7.

    a) $4x \equiv 5 \pmod 7$ b) $5x \equiv 4 \pmod 7$ c) $6x \equiv 3 \pmod 7$

12. a) Find the reciprocal modulo 11 of each of the numbers $1, 2, 3, \ldots, 10$.

    b) Use the reciprocals to solve each equation.

    $3x \equiv 5 \pmod{11}$ $7x \equiv 2 \pmod{11}$ $5x \equiv 9 \pmod{11}$ $10x \equiv 4 \pmod{11}$

© Hidegkuti, 2026



Answers

1. a) 3 b) 1 c) 1 d) 0 e) 1 (because $-7+4+4=1$)

2. $30 \equiv 6 \pmod{12}$, and $8+6=14$, so it will be 2 o'clock.

3. $1000 = 7 \cdot 142 + 6$, so it will be 6 days after Friday, which is Thursday.

4. $365 = 7 \cdot 52 + 1$, so it is one day later in the week: Tuesday.

5. a) true, because $38-14=24$ is divisible by 12 b) false, because $25-4=21$ is not divisible by 6
   c) true, because $-1-6=-7$ is divisible by 7

6. The last digits are 3, 7, and 9. $3 \cdot 7 = 21$, last digit 1; then $1 \cdot 9 = 9$. The last digit is 9. (Indeed, $23 \cdot 47 \cdot 89 = 96209$.)

7. The last digits of the powers of 7 repeat in the cycle $7, 9, 3, 1$. Since $50 = 4 \cdot 12 + 2$, the last digit of 7^{50} is the same as that of $7^2 = 49$, which is 9.

8. a) $3, 4, 2, 1$, and then the pattern repeats. All four nonzero remainders appear, so 3 is a primitive root modulo 5.
   b) $50 = 4 \cdot 12 + 2$, so $3^{50} \equiv 3^2 \equiv 4 \pmod{5}$. The remainder is 4.

9. The remainders of $2, 4, 8, 16, \ldots$ modulo 7 are $2, 4, 1, 2, 4, 1, \ldots$, a cycle of length 3. Since $100 = 3 \cdot 33 + 1$, the remainder is the same as that of 2^1, which is 2.

10. a) $x = 0$, 2, or 4 b) no solution (row 4 contains only 0, 2, and 4) c) $x = 4$

11. a) Multiply by 2: $x \equiv 10 \equiv 3 \pmod{7}$ b) Multiply by 3: $x \equiv 12 \equiv 5 \pmod{7}$ c) Multiply by 6: $x \equiv 18 \equiv 4 \pmod{7}$

12. a)

number	1	2	3	4	5	6	7	8	9	10
reciprocal modulo 11	1	6	4	3	9	2	8	7	5	10

   b) $3x \equiv 5$: multiply by 4, $x \equiv 20 \equiv 9$ $7x \equiv 2$: multiply by 8, $x \equiv 16 \equiv 5$
   $5x \equiv 9$: multiply by 9, $x \equiv 81 \equiv 4$ $10x \equiv 4$: multiply by 10, $x \equiv 40 \equiv 7$ (all modulo 11)

© Hidegkuti, 2026