Modular Arithmetic

The expression $a \equiv b \pmod{n}$, pronounced "a is congruent to b modulo n," means that $a - b$ is a multiple of n. For instance, $(-43) - 37 = -80$ so that $-43 \equiv 37 \pmod{4}$. Given a, there is only one value b between 0 and $n-1$ so that $a \equiv b \pmod{n}$. We call b the residue of a modulo n and write $b = (a \mod n)$.

Quick facts:

- A number and its negative are usually not congruent: $2 \not\equiv (-2) \pmod{9}$, since $2 - (-2) = 4$ is not a multiple of 9. This is the source of many mistakes.
- Suppose $a \equiv b$ and $c \equiv d \pmod{n}$. Then
$$a + c \equiv b + d \pmod{n} \quad \text{and} \quad a \cdot c \equiv b \cdot d \pmod{n}$$
- Dividing is not so simple:

  $6 \equiv 36 \pmod{10}$, but dividing by 2 would give $3 \equiv 18 \pmod{10}$ which is not true!

  The problem above is that 2 divides 10 (think about it). We can do two things:
  - Divide by a number k relatively prime to n: $6 \equiv 36 \pmod{10}$ so dividing by 3 gives $2 \equiv 12 \pmod{10}$.
  - Divide all three numbers by a number k which is a divisor of n: $6 \equiv 36 \pmod{10}$ so dividing by 2 gives $3 \equiv 18 \pmod{5}$.
- You can also reduce n alone: $7 \equiv 13 \pmod{6} \implies 7 \equiv 13 \pmod{3}$. But this does not work in the opposite direction: $13 \equiv 16 \pmod{3}$, but $13 \not\equiv 16 \pmod{6}$.
- To compute exponents we use Euler's Theorem:

  $$\boxed{\text{If } a \text{ is relatively prime to } n, \text{ then } a^{\varphi(n)} \equiv 1 \pmod{n}.}$$

  (Here, $\varphi(a)$ is the number of integers between 1 and n, relatively prime to n.)
- A useful result concerning factorials is Wilson's Theorem:

  $$\boxed{\text{The number } p \text{ is a prime if and only if } (p-1)! \equiv -1 \pmod{p}.}$$

Examples: (a) If $p = 6$, Wilson's Theorem fails:

$$(6-1)! = 120 \equiv 0 \pmod{6}.$$

But if $p = 7$,

$$(7-1)! = 720 = 102 \cdot 7 + 6 \equiv 6 \equiv (-1) \pmod{7}.$$

(b) To compute the residue $4444^{4444} \mod 18$, we notice $4444 \equiv 16 \pmod{18}$.

$$4444^{4444} \equiv 16^{4444} \equiv (-2)^{4444} \equiv 4^{2222} \pmod{18}$$

We cannot use Euler's Theorem because 4 and 18 are not relatively prime, but we can break the above into two congruences (note that $\varphi(9) = 6$):

$$4^{2222} \equiv 0 \pmod{2} \quad , \quad 4^{2222} \equiv 4^{370 \cdot 6 + 2} \equiv 1 \cdot 4^2 \equiv 7 \pmod{9}$$

so the residue modulo 18 we seek is even and congruent to 7 modulo 9:

$$4444^{4444} \equiv 16 \pmod{18}.$$

Inverses: The other use of Euler's Theorem is to compute inverses modulo n. For instance, if we need to find a value b such that $3 \cdot b \equiv 1 \pmod{29}$, we recall that $3^{\varphi(29)} \equiv 1 \pmod{29}$ and $\varphi(29) = 28$, to get $3 \cdot 3^{27} \equiv 1 \pmod{29}$ so $b = 3^{27}$ does the trick. There are two serious difficulties.

- Not all numbers a have an inverse modulo n. Since we rely on Euler's Theorem, it is necessary that a and n are relatively prime: $2 \cdot b \equiv 1 \pmod{4}$ is impossible.
- The number 3^{27} is too big!! The fastest way to reduce such an exponent is to express it in binary, $3^{27} \equiv 3^{16+8+2+1}$, and then compute the residues of consecutive squares:

$$\begin{array}{lll} 3^2 & & \equiv 9 \pmod{29} \\ 3^4 & = 9^2 = 81 & \equiv -6 \pmod{29} \\ 3^8 & \equiv (-6)^2 = 36 & \equiv 7 \pmod{29} \\ 3^{16} & \equiv 7^2 = 49 & \equiv 20 \pmod{29} \end{array}$$

Then we simply compute

$$3^{27} = 3^{16} \cdot 3^8 \cdot 3^2 \cdot 3^1 \equiv 20 \cdot 7 \cdot 9 \cdot 3 = 3780 \equiv 10 \pmod{29}$$

and sure enough, $3 \cdot 10 \equiv 1 \pmod{29}$, so $b = 10$ is a (small and manageable) inverse of 3 modulo 29.

The inverse of a modulo n is usually written $\left(\frac{1}{a}\right)_n$, but remember that this actually represents an integer.

Chinese Remainder Theorem:

Let $n_1, \ldots, n_r$ be pairwise relatively prime positive integers. Then there is a solution to the system of equations

$$\begin{array}{rcl} x \equiv & b_1 & \pmod{n_1} \\ \vdots & & \vdots \\ x \equiv & b_r & \pmod{n_r} \end{array}$$

Here is an example of how to construct the solution. Find an integer x such that

$$\begin{array}{rcl} x \equiv & 3 & \pmod{5} \\ x \equiv & 7 & \pmod{8} \\ x \equiv & 2 & \pmod{11}. \end{array}$$

A solution will be

$$x = 3 \cdot (8 \cdot 11) \cdot \left(\tfrac{1}{8 \cdot 11}\right)_5 + 7 \cdot (5 \cdot 11) \cdot \left(\tfrac{1}{5 \cdot 11}\right)_8 + 2 \cdot (8 \cdot 5) \cdot \left(\tfrac{1}{8 \cdot 5}\right)_{11}$$

To confirm this, check the residue of x modulo 5 (to test the first equation). The first term is congruent to 3 because $8 \cdot 11$ cancels with its inverse. The other two terms are 0 becase they contain the factor 5. Then $x \equiv 3 \pmod{5}$ and the other two equations are satisfied similarily.

Now we just need to compute all the inverses to obtain the value of x.

$$\begin{array}{rcll} \left(\frac{1}{8 \cdot 11}\right)_5 \equiv & (8 \cdot 11)^3 = 88^3 \equiv 3^3 = 27 & \equiv 2 & \pmod{5} \\ \left(\frac{1}{5 \cdot 11}\right)_8 \equiv & (5 \cdot 11)^3 = 55^3 = (-1)^3 & = 7 & \pmod{8} \\ \left(\frac{1}{8 \cdot 5}\right)_{11} \equiv & (8 \cdot 5)^9 = 40^9 \equiv 7^9 = 49^4 \cdot 7 \equiv 5^4 \cdot 7 = 25^2 \cdot 7 \equiv 3^2 \cdot 7 = 63 & \equiv 8 & \pmod{11} \end{array}$$

Then $x = (3 \cdot 8 \cdot 11 \cdot 2) + (7 \cdot 5 \cdot 11 \cdot 7) + (2 \cdot 8 \cdot 5 \cdot 8) = 3863$. The smallest solution is the residue of 3863 modulo $5 \cdot 8 \cdot 11 = 440$; that is, 343. Try it!

1. Compute the residue obtained when dividing $1! + 2! + \ldots + 100!$ by 15.

2. Let $p \geq 5$ be a prime. Show that $p^2 - 1$ is divisible by 24.

3. Suppose that n is an integer divisible by 24. Show that the sum of all the positive divisors of $n - 1$ (including 1 and $n - 1$) is also divisible by 24.

4. A perfect square has *tail* n if its last n digits in base 10 are the same and non-zero. What is the longest possible tail? What is the smallest square with this tail?

5. Let T be a set of 20 numbers selected from $\{1, 4, 7, 10, 13, 16, \ldots, 100\}$. Show that we can find two distinct elements of T whose sum is 104.

6. Find the smallest natural number n which ends in 6 when written in base 10, and such that if the final 6 is moved to the front of the number, the result is $4n$.

7. (a) Find all natural numbers n for which 7 divides $2^n - 1$.
   (b) Prove that there is no natural number n for which 7 divides $2^n + 1$.

8. Find all positive integers n such that the set $\{n, n+1, n+2, n+3, n+4, n+5\}$ can be partitioned into two subsets so that the product of the numbers in each subset is equal.

9. The sequence a_n is defined by $a_1 = 2$, $a_{n+1} = a_n^2 - a_n + 1$. Show that any pair of values in the sequence are relatively prime.

10. Let a_n be the sequence defined by $a_1 = 3$, $a_{n+1} = 3^{a_n}$. Let b_n be the remainder when a_n is divided by 100. What is b_{2004}?