Congruences: What is the remainder?

What is the last digit of $10^{1000}$ in decimal?

Yes, it is 0, but why?

Because $10^{1000} \equiv 0 \pmod{10}$

The congruence notation $a \equiv b \pmod{m}$ states that $m \mid a-b$. It is useful because we can specify equivalence classes of integers

$$x \equiv 1 \pmod{m} \iff x \in \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m} \} = \{1 + km \mid k \in \mathbb{Z}\}$$

Further, $a \equiv b \pmod{m} \iff a \mod m \equiv b \mod m$. Congruences observe certain algebraic laws which make them nice to work with.

What is the last decimal digit of $9^{1000}$?

We can do the multiplication or we can use properties of modular arithmetic.
What is \( 9^{1000} \mod 10 \)?

We observe that \( 9 \equiv -1 \pmod{10} \).

Thus this is equivalent to \((-1)^{1000} \pmod{10}\).

If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then
\[ ac \equiv bd \pmod{m} \]

This is true because
\[ ac - bd = (a-b)c + b(c-d) \]

So since \( m \mid (a-b) + m \mid (c-d) \), then \( m \mid (ac - bd) \).

As a corollary, by applying this repeatedly,
\[ a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m} \]

So:
\[ 9^{1000} \equiv (-1)^{1000} \equiv 1 \pmod{10} \]

The last digit must be 1.

\[ 9^{1001} \equiv -1^{1001} \equiv -1 \pmod{10} \]

So the last digit must be \( 10 + 1 = 9 \).

Thus we have shown that \( 9^n \) must have a last digit of 1 or 9.
What is \(2^{741} \pmod{5}\)?

Observe \(2^2 = 4 \equiv -1 \pmod{5}\).

Thus \(2^{741} = 2 \cdot 4^{370} \equiv 2 \cdot (-1)^{370} \equiv 2 \pmod{5}\)

Powers of 0, 1, -1 are easiest to work with, so if we can get close to the modulus with some power, our computation is easy.

What is the last digit of \(2^{753}\) in decimal?

\(2^3 \pmod{10} = -2\) \quad | \quad (-2)^3 \pmod{10} = 2

Thus
\[2^{753} = (-2)^{251} \cdot 4^3 \equiv 2 \cdot 2^9 \equiv 2 \cdot (-2)^3 \equiv -4 \cdot 512 \equiv 6 \cdot 2 \pmod{10}\]

\[= 2\]

It is impressive to be able to work with such large numbers so easily. This should convince you that modular arithmetic can be useful in computation.
What is $2^{573} + 3^{752} \pmod{7}$?

We know how to find each of these separately - can we just add and subtract congruences?

Yes, $a \equiv b$ and $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$

**Proof:**

$m \mid a - b + n \mid c - d$, so $m \mid a - b + c - d$

$m \mid (a + c) - (b + d) \Rightarrow (a + c) \equiv (b + d) \pmod{m}$.

- $2^{573} \equiv 191 \equiv 1 \pmod{7}$
- $752 \equiv 3^2 \equiv 2 \pmod{7}$

- $2^{573} + 3^{752} \equiv 1 + 2 \equiv 3 \pmod{7}$

We have addition, subtraction and multiplication of congruences. What about division?

- $3 \cdot 2 \equiv 5 \cdot 2 \pmod{4}$

So we just can't cancel across congruences.

- $3 \equiv 5 \pmod{4}$
We can cancel congruences when \( d \perp m \).

\[ ad \equiv bd \quad \Leftrightarrow \quad a \equiv b \pmod{m} \quad \text{for integer} \quad d \perp m \]

So

\[ 2 \underset{5}{\equiv} 2 \pmod{5} \Rightarrow 3 \cdot 2 \underset{5}{\equiv} 2 \cdot 3 \pmod{5} \]

**Proof:**

If \( d \perp m \), \( \gcd(d, m) = 1 \)

Thus \( \exists d', m' \) such that \( d'd + m'm = 1 \).

\[ ad \equiv bd \Rightarrow add' \equiv bdd' \quad \text{since} \quad d \parallel d' \]

Note \( d'd \equiv 1 \pmod{m} \), since \( M' = 1 - d'd \).

Thus

\[ a(d'd) \equiv a \pmod{m} \quad \text{and} \quad b(d'd) \equiv b \pmod{m} \]

So:

\[ a dd' \equiv a \equiv b dd' \equiv b \pmod{m} \]

Clearly \( ad \equiv bd \pmod{md} \Leftrightarrow a \equiv b \pmod{m} \)

\[ \frac{ad - bd}{md} \Leftrightarrow \frac{a - b}{n} \]
$2^{573} \equiv -(3^{952}) \pmod{7}$ implies
$5 \cdot 2^{573} \equiv -(3^{952}) \cdot 5^x \pmod{7}$ and with $x = 952$.

Since when $d \perp m$ we can divide by $d$ without changing the modulus and when $d \mid m$, we can divide by the $d$ by changing the modulus to $m/d$,

$$ad \equiv bd \pmod{m} \iff a \equiv b \pmod{\frac{m}{\gcd(m,d)}}$$

because $d/\gcd(m,d) \perp m$. 
Probabilistic Primality Testing

To test if an integer \( n \) is composite or prime, we can divide by all possible factors up to \( \sqrt{n} \), but this is very slow for large \( n \).

A better way is to find some property which holds true for all primes and then test it several times using \( n \) in the role of the prime. If it fails, \( n \) must be composite; if not, \( n \) is probably prime.

**Fermat's Theorem:** \( N^{p-1} \equiv 1 \pmod{p} \) if \( N \) is not prime.

if \( N \neq p \), and \( p \) is a prime, \( N \) is prime.

So is \( p = 753 \) prime?

The only values of \( N \leq 752 \) such that \( N^{752} \equiv 1 \pmod{753} \) are \( N = 1, 250, 503 \) and 752. Thus, the number of false witnesses we encounter are very small!
Proof that \( N^{p-1} \equiv 1 \pmod{p} \), \( N \perp p \), for all prime \( p \).

This is simple with the fact that \( n \mod p, 2n \mod p, \ldots, n(p-1) \mod p \) are a permutation of \( 1, 2, \ldots, p-1 \), when \( N \not\mid p \) since:

\[
(N)(2n)\cdots((p-1)n \equiv (p-1)! \pmod{p} \\
(p-1)! \cdot N^{p-1} \equiv (p-1)! \pmod{p}.
\]

Since \( p \) is prime, \( GCD((p-1)!, p) = 1 \), \( N^{p-1} \equiv 1 \pmod{p} \).

But why do we get a permutation?

Ex: \( p = 7, n = 1 \) → obvious 0, 1, 2, 3, 4, 5, 6

\( p = 7, n = 2 \)

\begin{align*}
0 \mod 7 &= 0 \\
2 \mod 7 &= 2 \\
4 \mod 7 &= 4 \\
6 \mod 7 &= 6 \\
8 \mod 7 &= 1 \\
10 \mod 7 &= 3 \\
12 \mod 7 &= 5
\end{align*}

\( p = 7, n = 3 \)

0 3 6 2 5 1 4
Suppose that \( kn \equiv kn \pmod{p} \) did not describe a permutation for \( 0 \leq k \leq p-1 \). Since there are \( p \) values, this means that \( an \equiv bn \pmod{p} \), for \( 0 \leq a < b \leq p-1 \).

By the division rule,
\[
\frac{a}{b} \equiv \frac{b}{a} \pmod{\frac{p}{\gcd(p,n)}}
\]
Since \( N \perp p \), \( \gcd(p,n) = 1 \), so
\[
a \equiv b \pmod{p}
\]
which is a contradiction since \( a \neq b \) and both are between \( 0 \) and \( p-1 \). \( \square \)

Thus if \( C \perp M \), \( Cx \equiv (\pmod{m}) \) gives distinct values for all \( 0 \leq x \leq n-1 \).
Ari Kaufman’s Congruence

As final evidence that modular arithmetic is useful, the congruence
\[ k = (5x + 3y + z) \mod 517 \]
arises in an architecture for computer graphics. Where does it come from?

Suppose you have an \( N \times N \times N \) array of elements, which you would like to store in \( N \) memories, so they can be accessed in parallel.

The most common access patterns will be all elements in a row, column, or axle \( (x, y, k), 1 \leq k \leq N \).
They use the congruence \( k = (5x + 3y + 2) \mod 2517 \)
to partition elements \((x, y, z), 1 \leq x, y, z \leq 512\) into 517 memories.

Since \( 1 \perp 2517, 3 \perp 2517, 5 \perp 2517 \), and for any access where two of \( x, y, z \) are constant, the equation reduces to
\[
(cX + d \pmod{m})
\]
where \( c \perp m \) and \( d \) is a constant which acts as an offset.

Thus for any orthogonal query, the \( n \) elements are in distinct memories, allowing parallel access!

In fact, a stronger condition holds. All major + minor diagonal accesses are also contention free!
What happens on a major diagonal query?

\[(x+k, y+k, k), \ 1 \leq k \leq n\]

These elements will be in memories

\[k = (5(x+k) + 3(y+k) + k) \mod 517\]

\[= (5x + 3y + 9k) \mod 517\]

\[
\text{constant } 9 \per 517
\]

The coefficients 5, 3, 1 were selected so any sum or difference combination is relatively prime to 517 and unique

\[5 \neq 3, \ 5 \neq 1, \ 5 + 3 \neq 1, \ 5 \neq 3 \times 1, \ 3 \neq 1\]