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

$$x \equiv 1 \pmod{m} \iff x \in \{\ldots -2m+1, -m+1, 1, m+1, 2m+1 \ldots\}$$

Further $a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$.

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 $9^{1000} \bmod 10$?

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

Thus this is equivallent to $(-1)^{1000} \pmod{10}$

if $a \equiv b$, $c \equiv d \Rightarrow ac \equiv bd \pmod{m}$

This is true because

$$ac - bd = (a-b)c + b(c-d)$$

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

As a corrollary, by applying this repeatedly,

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$$

So:

$$9^{1000} \equiv (-1)^{1000} \equiv 1 \pmod{10}$$

The last digit must be 1.

$$9^{1001} \equiv -1^{1001} = -1 \pmod{10},$$

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?

$2^3 \bmod 10 = -2 \mid (-2)^3 \bmod 10 = 2$

Thus

$$2^{753} \equiv (-2)^{251} \equiv 4 \cdot 2^{83} \equiv 2^{85} \equiv 2 \cdot (-2)^{28}$$

$$\equiv 2 \cdot -2 \cdot 2^9 \equiv -4 \cdot 512 \equiv 6 \cdot 2 \pmod{10}$$

$= \underline{2}$

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 $c \equiv d \pmod m \Rightarrow$

$$a+c \equiv b+d \pmod m$$
$$a-c \equiv b-d \pmod m$$

$$\boxed{\begin{array}{l}\underline{\text{Proof:}} \quad m \mid a-b \text{ \& } m \mid c-d, \text{ so } m \mid a-b+c-d \\ m \mid (a+c)-(b+d) \Rightarrow (a+c) \equiv (b+d) \bmod m.\end{array}}$$

$$2^{573} \equiv (1)^{191} \equiv 1 \pmod 7$$
$$3^{752} \equiv 3^2(-1)^{250} \equiv 2 \pmod 7$$

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

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

$$3 \cdot 2 \equiv 5 \cdot 2 \pmod 4$$
$$3 \not\equiv 5 \pmod 4$$

So we just can't cancel across congruences

We can cancel congruences when $d \perp m$.

$ad \equiv bd \iff a \equiv b \pmod{m}$ $\quad$ a, b, d, m are integer $d \perp m$

$\underbrace{}_{\text{relatively prime}}$

So $\quad 2^{751} \equiv 2 \pmod{5} \Rightarrow$

$$3^x \cdot 2^{751} \equiv 2 \cdot 3^x \pmod{5}$$

Proof:

If $d \perp m$, $GCD(d, m) = 1$

Thus $\exists d', m'$ $d'd + m'm = 1$.

$ad \equiv bd \Rightarrow add' \equiv bdd'$, since $d' \equiv d'$.

Note $d'd \equiv 1 \pmod{m}$, since $m'm = 1 - d'd$.

Thus $a(d'd) \equiv a \pmod{m}$ + $b(d'd) \equiv b \pmod{m}$

So: $\quad add' \equiv a \equiv bdd' \equiv b \pmod{m}$ $\square$

Clearly $ad \equiv bd \pmod{md} \Rightarrow a \equiv b \pmod{m}$

$$\frac{ad - bd}{md} \iff \frac{a - b}{m}$$

So $2^{573} \equiv -(3^{752}) \pmod{7}$ implies

$5^{x} 2^{573} \equiv -(3^{752}) 5^{x} \pmod{7}$ and visa versa.

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

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

because $d/GCD(m,d) \perp m$.

Probabalistic Primality Testing

To test if an integer N is composite or prime, we can divide by all possible factors up to the $\sqrt{N}$, 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 time using N in the role of the prime. If it fails, N must be composite, if not, N is <u>probably</u> prime.

Fermat's Theorem: $N^{P-1} \equiv 1 \pmod{P}$ if $N \perp P$.

if $N < P$, and P is a prime, $N \perp P$.

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

$N \bmod p$, $2N \bmod p$ . . . $N(p-1) \bmod p$

are a permutation of $1, 2 \ldots p-1$, when $N \perp p$

since:

$$(N)(2N)\cdots(p-1)N \equiv (p-1)! \pmod{p}$$

$$(p-1)!\, N^{p-1} \equiv (p-1)! \pmod{p}$$

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

$p = 7$, $N = 2$

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

$p = 7$, $N = 3$ 0 3 6 2 5 1 4

Suppose that $kN \pmod{p}$ did not describe a permutation for $0 \le k \le p-1$.

Since there are p values, this means that

$$aN \equiv bN \pmod{p}, \text{ for } 0 \le a < b \le p-1$$

By the division rule,

$$a \equiv b \pmod{p/\mathrm{Gcd}(p, N)}$$

Since $N \perp p$, $\mathrm{GCD}(p, N) = 1$, so

$$a \equiv b \pmod{p}$$

which is a contradiction since $a \ne b$ and both are between 0 + $p-1$. $\square$!

$$\boxed{\text{Thus if } C \perp M,\ CX \pmod{M} \text{ gives distinct values for all } 0 \le X \le M-1}$$

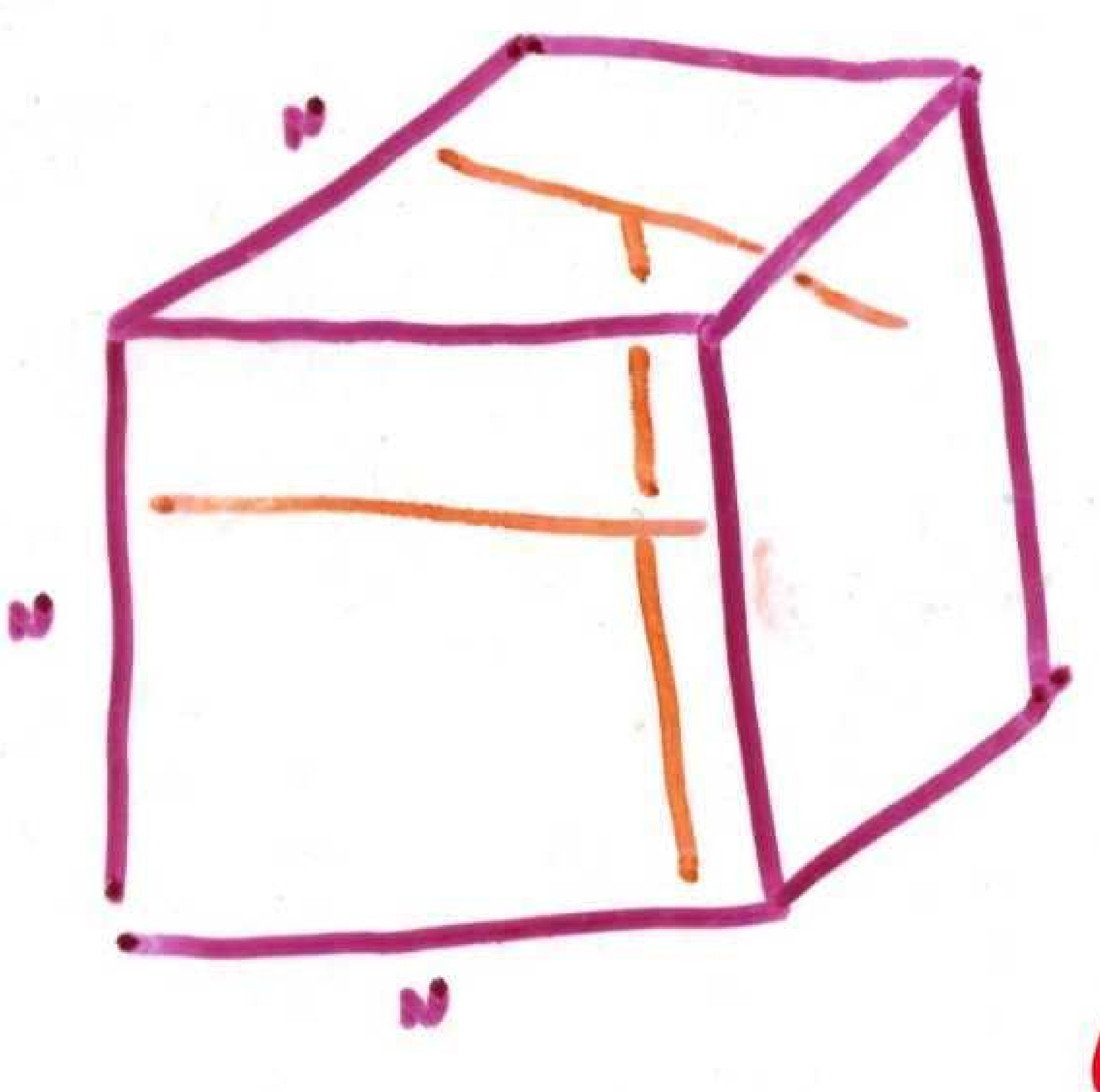
Ari Kaufman's Congruence

As final evidence that modular arithmetic is useful, the congruence

$$k = (5x + 3y + z) \bmod 517$$

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 axel

(x, y, k), $1 \le k \le N$

They use the congruence $k = (5x + 3y + z) \bmod 517$ to partition elements (x, y, z), $1 \le x, y, z \le 512$ into 517 memories.

Since $1 \perp 517$, $3 \perp 517$, $5 \perp 517$, 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?

$$(x+k,\ y+k,\ k), \quad 1 \le k \le N$$

These elements will be in memories

$$k = (5(x+k) + 3(y+k) + k) \bmod 517$$

$$= (\underbrace{5x + 3y}_{\text{constant}} + \underbrace{9k}_{9 \perp 517}) \bmod 517$$

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

$5 \ne 3$ $\quad 5 \ne 1$ $\quad 5+3 \ne 1$ $\quad 5 \ne 3+1$

$3 \ne 1$