Modular arithmetic

Last time: calculation rules

$+, -, \times, (\ )^{-1}$

ex: Divisibility rules

Is 12345 even? No, because the last digit is not even.
This test is about divisibility by 2

Is 12345 divisible by 5? Test: last digit
5 or 0: divisible by 5
otherwise: no

Explanation: numbers are writen in base 10

$$12345 = 1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0$$

Since $10 \equiv 0 \mod n$ ($n = 2$ or 5)

then

$$\underline{12345} \equiv 1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + \underline{5}$$

More generally, if

$$x = a_k a_{k-1} \dots a_0$$
$$= a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_0 10^0$$

then $x \equiv a_0$ (mod 2 or 5)

$$n \mid x \iff x \equiv 0 \mod n$$

So we just need to check divisibility of the last digit

a_0 mod 2 or 5

What about divisibility by 3?

Test: $x = a_k 10^k + \dots + a_0 10^0$

is divisible by 2 iff the sum of its digits is divisible by 3

$x = 12345$

$1 + 2 + 3 + 4 + 5 = \frac{5 \times 6}{2} = 15 \leftarrow$ divisible by 3!

Non-example: x = 1111
1+1+1+1=4, not divisible by 3

Proof:

$x = a_k a_{k-1} \dots a_0$

$= a_k 10^k + \dots + a_0 10^0$

Note: $10 \equiv 1 \pmod 3$

$x \equiv a_k 1^k + \dots + a_0 1^0$

$\equiv a_k + \dots + a_0 \pmod 3$

Remark: some test works for divisibility by 9 because

$$10 \equiv 1 \pmod 9$$

Speaking of powers mod n, we have seen

$$a \equiv b \pmod n \not\Rightarrow c^a \equiv c^b \pmod n$$

So what can we do with "large powers"?

ex: find 39^{42} % 12

$$39 \equiv 3 \pmod{12}$$

$$39^{42} \equiv 3^{42} \pmod{12}$$

How do we reduce the exponent? You just need to find a pattern on the powers of 3

$$3^1 \equiv 3 \pmod{12}$$

$$3^2 \equiv 9 \pmod{12}$$

$$3^3 = 9 \cdot 3 = 27 \equiv 3 \pmod{12}$$

$$3^4 = 3^3 \cdot 3 \equiv 3 \cdot 3 \equiv 9 \pmod{12}$$

repeat

We notice: $3^3 \equiv 3 \pmod{12}$

$$\Rightarrow 3^{42} \equiv 3^{3 \cdot 14}$$

$$\equiv (3^3)^{14}$$

$$\equiv 3^{14} \pmod{12}$$

Also: $14 = 12 + 2 = 3 \cdot 4 + 2$

$$3^{14} \equiv 3^{3 \cdot 4 + 2} \equiv (3^3)^4 \, 3^2$$

$$\equiv 3^4 \, 3^2$$

$$= 3^6 \equiv (3^3)^2 \equiv 3^2 \equiv 9 \mod 12$$

That works, but you still have to find the pattern (and ideally prove it).
In the case of prime modular arithmetic (where p is prime), the pattern is:

Fermat's Little Theorem (FLT)

Assume p prime

Version 1: If $a \not\equiv 0 \mod p$, then $a^{p-1} \equiv 1 \pmod p$

Version 2: $a^p \equiv a \pmod p$

ex: find $39^{42} \% 11$

11 is prime

FLT $\Rightarrow$ $a^{10} \equiv 1 \pmod{11}$ if $a \not\equiv 0$

$$39 \equiv 6 \mod 11$$

$$\begin{aligned}
39^{42} &\equiv 6^{42} \mod 11 \\
&\equiv 6^{40+2} \mod 11 \\
&\equiv (6^4)^{10}\, 6^2 \mod 11 \\
&\equiv 6^2 \mod 11 \\
&= 36 \equiv 3 \mod 11
\end{aligned}$$

Proof that version 1 is equivalent to version 2 (FLT)

$\boxed{\Rightarrow}$ case 1: $a \equiv 0$

then $a^p = 0^p \equiv 0 \equiv a \pmod p$

case 2: $a \not\equiv 0$

then $a^{p-1} \equiv 1 \pmod p$

$a^p \equiv a\, a^{p-1} \equiv a \pmod p$

$\boxed{\Leftarrow}$ Assume $a^p \equiv a \pmod p$ and $a \not\equiv 0$

then a is invertible

$$a^{-1} a^p \equiv a^{-1} a \equiv 1 \pmod p$$

Proof of V1: assume $a \not\equiv 0 \bmod p$

Consider the number

$$\{1a, 2a, 3a, \ldots, (p-1)a\}$$

these $(p-1)$ numbers are distinct mod p

$\rightarrow$ Proof: $xa \equiv ya \pmod p$

$$\Rightarrow x a a^{-1} \equiv y a a^{-1} \pmod p$$

$$x \equiv y \pmod p$$

But we know that 1,2,...,p-1 are all distinct.
Moreover no number in A is 0

$$xa \equiv 0 \pmod p$$

$$\Rightarrow x \equiv 0 \pmod p$$

Only way for this to work is:
A = {1,2,3,...,p-1} (possibly written in a different order)

Now, multiply all those numbers together

$$(1a)(2a)(3a)\ldots((p-1)a) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod p$$

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

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

$$a^{p-1} \equiv 1 \pmod p$$

The converse of FLT is also true

Theorem: suppose that $\forall a,\ 1 \leq a < n$,
we have $a^{n-1} \equiv 1 \pmod{n}$
then n is prime

Proof by contradiction

Suppose $a^{n-1} \pmod{n},\ \forall a \not\equiv 0$

and that n is not prime

Then n is composite, so it has a prime factor: p $\quad p \mid n$

by assumption

$$p^{n-1} \equiv 1 \pmod{n}$$

$$p^{n-1} = 1 + kn \quad (k \in \mathbb{Z})$$

$$1 = kn - p^{n-1}$$, but $p \mid kn$ and $p \mid p^{n-1}$

$$\Rightarrow p \mid 1$$ Contradiction!

Fermat's test: given $n \geq 2$

Randomly pick a number a $,\ 1 \leq a < n$

check $\gcd(a, n) = 1$ (otherwise n not prime)

then check that $a^{n-1} \equiv 1 \pmod{n}$
(otherwise n not prime)

If a "passes the test", there is no conclusion, but it indicates that n may be prime

Ex: $n = 9$ choose randomly $a = 2$

$\gcd(9, 2) = 1$ ✓

$$2^{9-1} = 2^8 = (2^4)^2 = 7^2 = 49 \equiv 4 \bmod 9 \not\equiv 1$$

$\Downarrow$

9 not prime!

Of course, we could have been unlucky with the random pick

ex: $a = 8$ $\quad 8 \equiv -1 \pmod 9$

$$8^8 \equiv (-1)^8 \equiv 1 \pmod 9$$

8 passes the test

When you pick a random a which passes the test, then try again with a different a (probabilistic primality test). The probability of passing the test multiple times when n is not prime is (usually) very low.

More precisely, the probability that a passes the test is (most of the time) $< \frac{1}{2}$

Repeat test 10 times:

$\Rightarrow$ Probability of passing the test 10 times when n is not prime $\leq \frac{1}{2^{10}} < \frac{1}{1000}$

$\Rightarrow$ with high probability, n is prime

There are catches:
Definition: a Fermat Pseudoprime (or armichael number) is a number n such that, for $1 \leq a < n$

$$\gcd(a, n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod n$$

ex: 561, 1105, 1729, 2465

Good news; those numbers are rare, and for all other non prime numbers, the probability is $< \frac{1}{2}$

Last year, a high school student (Daniel Larson) proved a 30 years old conjecture about the distribution of those numbers

$\forall x$ large enough, $\exists c$ pseudoprime $x < c < 2x$