Puzzle. $3^{519} \pmod{11}$ $\qquad 3^{10} \equiv 1 \pmod{11}$ $\qquad 3^5 \equiv 1 \pmod{11}$

$\Downarrow$

If you know $3^5 \equiv 1 \pmod{11}$

3x $\qquad$ square twice 2x

$$3^{519} \equiv (3^5)^{103} 3^4 \equiv 1^{103} 3^4 \equiv 81 \equiv 4$$

$$3^4 \cdot 3 \equiv 1$$

$$3^4 \equiv 3^{-1}$$

$$3^{-1} 3^{520} \equiv 3^{-1} \cdot 1^{104} \equiv 3^4 \equiv 4$$

Successive Squaring (Efficient Modular Exponentiation)

Q: Compute $b^e \pmod{n}$ for large e.

① Compute $b, b^2, b^4, b^8, \ldots, b^{2^k}, \ldots$ by successive squaring. until we get $\lfloor \log_2(e) \rfloor$ powers.

② Write e in binary

$$e = 2^a + 2^b + \cdots + 2^z$$

and multiply as needed:

$$b^e = b^{2^a} \cdot b^{2^b} \cdot \cdots \cdot b^{2^z}$$

Example $\quad 3^{18} \bmod 11.$

$$3, \boxed{3^2 \equiv 9}, 3^4 \equiv 9^2 \equiv 81 \equiv 4$$

$$3^8 \equiv (3^4)^2 \equiv 4^2 \equiv 16 \equiv 5$$

$$\boxed{3^{16} \equiv (5)^2 \equiv 25 \equiv 3}$$

$(18 = 16 + 2)$

$$3^{18} \equiv 3^{16} \cdot 3^2 \equiv 3 \cdot 9 \equiv 27 \equiv 5$$

Greatest Common Divisor $a, b \in \mathbb{Z}$

$\gcd(a,b)$ is largest positive integer that divides both a and b.

eg.

$$\gcd(3, 15) = 3$$

$$\gcd(20, 15) = 5$$

$$\gcd(3, 5) = 1 \quad \text{"coprime"}$$

$$\gcd(8, 25) = 1$$

Prop^n. An element $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible iff (if and only if) $\gcd(a,n) = 1$

Proof. If a is invertible, then $aa^{-1} \equiv 1 \pmod{n}$

So $aa^{-1} + kn = 1$

Let $g = \gcd(a,n)$. Then $g \mid a$ and $g \mid n$ so $g \mid aa^{-1} + kn$

$\Rightarrow g \mid 1. \Rightarrow g = 1.$

If a is not invertible, then $x \mapsto ax$ doesn't hit 1.

$\Rightarrow x \mapsto ax$ is not bijective.

$\Rightarrow x \mapsto ax$ is not injective.

So $ab \equiv ab' \pmod{n}$ where $b \not\equiv b' \pmod{n} \Rightarrow n \nmid b - b'$

So $a(b - b') = kn$ for some $k \in \mathbb{Z}$. $\Rightarrow \gcd(a,n) > 1$ $\blacksquare$

Recall: a is invertible if $\exists\, b \in \mathbb{Z}/n\mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$

Recall: if $|A| = |B|$ finite then $f: A \to B$ is injective iff surjective.

Def^n. The set of invertible elements of $\mathbb{Z}/n\mathbb{Z}$ is denoted $(\mathbb{Z}/n\mathbb{Z})^*$.

"unit group"

$$(\mathbb{Z}/n\mathbb{Z})^* = \{ a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1 \}$$

$\gcd(0,3) = 3$

Example. $(\mathbb{Z}/3\mathbb{Z}) = \{0,1,2\}$ $\quad (\mathbb{Z}/3\mathbb{Z})^* = \{1,2\}$

$(\mathbb{Z}/10\mathbb{Z}) = \{0,1,\dots,9\}$ $\quad (\mathbb{Z}/10\mathbb{Z})^* = \{\underline{1,3,7,9}\}$

When n is prime $\quad |(\mathbb{Z}/n\mathbb{Z})^*| = n-1$

$$(\mathbb{Z}/n\mathbb{Z})^* = \{1,2,\dots,n-1\}.$$

all except 0

$$\cancel{0},\ 1,\ \cancel{2},\ 3,\ \cancel{4},\ \cancel{5},\ \cancel{6},\ 7,\ \cancel{8},\ 9$$

removes every 2nd

removes every 5th

$$10 = 2 \cdot 5$$

Sps $n = p_1 p_2 \cdots p_s$ (distinct primes)

$$\left|(\mathbb{Z}/n\mathbb{Z})^*\right| = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)$$

$$= \varphi(n) \qquad 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$$

euler totient function