Thm 4.10: Let a and n be natural numbers, with $(a,n)=1$ and $k = \mathrm{ord}_n(a)$.

If m is a natural number, then

$$a^m \equiv 1 \pmod{n}$$

if and only if $k \mid m$.

Proof: By Division Alg., we have

$$m = q\cdot k + r, \quad \text{where } 0 \le r < k.$$

So

$$\begin{aligned} a^m &\equiv a^{qk+r} \pmod{n} \\ &\equiv (a^k)^q \cdot a^r \pmod{n} \\ &\equiv 1^q \cdot a^r \pmod{n} \\ &\equiv a^r \pmod{n} \qquad 0 \le r < k \end{aligned}$$

Hunter: The numbers $\overset{=1}{a^0}, a^1, a^2, \ldots, a^{k-1}$ $(a^k \equiv a^0 \pmod{n})$ are pairwise incongruent. In particular, only one is congruent to $1 \pmod{n}$.

So $a^m \equiv 1 \pmod{n}$ if and only if $r=0$, i.e. $k \mid m$.

Fun takeaway: If $(a, n) = 1$, $k = \text{ord}_n(a)$

When we look at powers of a modulo n, under multiplication, we just add exponents modulo k.

Reason: $a^i \equiv a^j \pmod{n}$ $\quad i \geq j$

$$(a^{i-j})\, a^j \equiv a^j \pmod{n}$$

$$a^{i-j} \equiv 1 \pmod{n}$$

Thm 4.10 $\Rightarrow k \mid (i-j) \Rightarrow i \equiv j \pmod{k}$

Ex: $a = 7$, $n = 10$

$$7^1 \equiv 7 \pmod{10}$$

$$7^2 \equiv 49 \pmod{10} \equiv 9 \pmod{10}$$

$$7^3 \equiv 7 \cdot 9 \pmod{10} \equiv 3 \pmod{10} \qquad \text{ord}_{10}(7) = 4$$

$$7^4 \equiv 7 \cdot 3 \pmod{10} \equiv 1 \pmod{10}$$

So when we work with powers of 7 modulo 10, we add exponents modulo 4.

Ex: $7^{26} \cdot 7^{41} \equiv 7^{4\cdot 6+2} \cdot 7^{4\cdot 10+1} \pmod{10}$

$$\equiv (\overset{1}{\cancel{7^4}})^6 \cdot 7^2 \cdot (\overset{1}{\cancel{7^4}})^{10} \cdot 7^1 \pmod{10}$$

$$\equiv 7^3 \pmod{10}$$

Portfolio

- Entries imported
- Turn in unfinished entries ASAP
- Volunteer for extra portfolio entries worth extra credit
  - ↳ see Canvas announcement later today

Exit Survey

- Next week
- Must respond to recieve participation grade

Final Exam

- Monday, May 10   10:30 am - 12:30 pm
- Cumulative, emphasis on Ch. 3/4

Next Week

Monday: Fun math

Wednesday: Reflection

Friday: Review