Conjecturing Some Number Theory Results
Pre-class, Week 8

Recall the following corollary from Week 6 class activity:

Corollary: If $\gcd(a, n) = 1$ and $ax \equiv ab \pmod{n}$, then $x \equiv b \pmod{n}$.

In other words, we can "cancel" a from an equation such as $ax \equiv ab \pmod{n}$ as long as a is relatively prime to n. If a is not relatively prime to n, then the cancellation does not necessarily hold, as the above problem shows. Similarly, we saw how to define the inverse a^{-1} of an element a as long as a is relatively prime to n. In all these cases the relative primeness makes it work.

Recall how we defined the Euler ϕ-function to count all these nice a's that worked with a fixed mod n:

Given n, the number of positive integers that are less or equal to than n and relatively prime to n is denoted by $\phi(n)$. More specifically,

$$\phi(n) = |\{x : 1 \leq x \leq n \text{ and } \gcd(x, n) = 1\}| .$$

Therefore, for any given n there are $\phi(n)$ many nice a's. The question is then how big is $\phi(n)$ for an arbitrary n?

1. We already know that $\phi(p) = p - 1$ if p is prime. We also found that $\phi(pq) = (p - 1)(q - 1)$ for p, q two distinct primes. Does this formula work if $p = q$? If yes, justify. If no, can you guess the correct formula for $\phi(p^2)$? What about $\phi(p^k)$ for an unknown k?

$\phi(4) = 2 \neq (2-1)(2-1)$

$\phi(p^k) = p^{k-1}(p-1)$

$\phi(p^2) = p(p-1) = p^2 - \frac{p^2}{p}$

2. For each of the following n, find $(n - 1)! \pmod{n}$.

a. $n = 5$ $4! = 24 \equiv 4 \pmod{5}$

b. $n = 7$ $6! \equiv 6 \pmod{7}$

c. $n = 10$ $9! \equiv 0 \pmod{10}$

d. $n = 15$ $14! \equiv 0 \pmod{15}$

e. $n = 17$ $16! \equiv 16 \pmod{17}$

f. $n = 21$ $20! \equiv 0 \pmod{21}$

3. Using the results of the previous problem, make a conjecture about $(n - 1)! \pmod{n}$ for composite $n > 4$ and prove it. (Note: Consider the perfect square case separately.)

for prime p, $(p-1)! \,\%\, p \equiv p-1$	Conjecture

for composite $n > 4$, $(n-1)! \equiv 0 \pmod{n}$

if n not square, there exist 2 numbers $p, q < n \mid p \neq q$, $pq = n$
Thus $(n-1)! = pqk = nk \equiv 0 \pmod{n}$ for some k.

if n is a square then $(n-1)!$ will contain $\sqrt{n}$ and $2\sqrt{n}$ since $n > 2\sqrt{n}$ because $n > 4$. Thus $(n-1)! = 2\sqrt{n}\sqrt{n}\,k = 2nk \equiv 0 \pmod{n}$ for some k.

Over →

Recall how we defined the *order* of an element modulo n with $\gcd(a, n) = 1$:
If k is the smallest positive integer such that $a^k \equiv 1 \pmod{n}$, we call k the *order* of a modulo n.
For example, if $a = 4$, then

$$4^1 \equiv \quad \pmod{9}, 4^2 \equiv 7 \pmod{9}, 4^3 \equiv 1 \pmod{9}$$

so the order of $a = 4$ mod 9 is 3. If we let $a = 2$, the order of 2 will be 6 because $2, 2^2, 2^3, 2^4, 2^5$ are not congruent to 1 mod 9.

4. Find the order of all non-zero $a \pmod{7}$ (by hand or using a code). Any property common to all orders? (If you wrote a code, you can also try finding the orders for all $a \pmod{13}$ to get another example to help with the conjecturing.)

a	1	2	3	4	5	6	7	8	9	10	11	12
order % 7	1	3	6	3	6	2						
order % 13	1	12	3	6	4	12	12	4	3	6	12	2

order of a mod p divides p-1