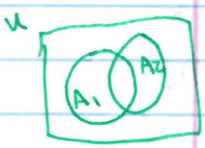
Mat 202 - Tutorial #5

Def^n: Given a positive integer m, the **Euler totient Function** $\phi(m)$ is the number of elements of $[m]$ relatively prime to m.

1. Find $\phi(35)$.

$35 = 5 \cdot 7$. A_1 = multiples of 5. $|A_1| = \frac{35}{5} = 7$.
A_2 = multiples of 7. $|A_2| = 35/7 = 5$.
$A_1 \wedge A_2$ = multiples of 5 & 7 (i.e. 35). $\frac{35}{35} = 1 = |A_1 \wedge A_2|$.



By inclusion-exclusion, $\phi(35) = U - (|A_1| + A_2) + |A_1 \wedge A_2|$
$= 35 - (7+5) + 1 = 24$.

Notice: $\phi(5) = 4$, $\phi(7) = 6$, & $4 \cdot 6 = 24$.
↳ coincidence? No!

Theorem [10.30]: If p & q are distinct prime numbers, then $\phi(pq) = \phi(p)\,\phi(q)$.

2. Prove $\phi(pq) = \phi(p)\,\phi(q)$.

A_1 = mult. of p. $|A_1| = \frac{pq}{p} = q$.
A_2 = mult. of q. $|A_2| = \frac{pq}{q} = p$.
$A_1 \wedge A_2$ = mult. of p & q. $|A_1 \wedge A_2| = \frac{pq}{pq} = 1$.

$\phi(pq) = pq - (p+q) + 1 = \underbrace{(p-1)}_{\phi(p)}\underbrace{(q-1)}_{\phi(q)} = \phi(p)\,\phi(q)$.

Theorem: $\phi(m) = m \prod_{p \in P(m)} (1 - \frac{1}{p})$, where $P(m)$ denotes the set of distinct prime factors of m.

3. Find $\phi(360)$ using [a] Inclusion-Exclusion [b] The theorem above.

[a] $360 = 2^3 \cdot 3^2 \cdot 5$.

$$\phi(360) = 360 - \left(\frac{360}{2} + \frac{360}{3} + \frac{360}{5}\right) + \left(\frac{360}{6} + \frac{360}{10} + \frac{360}{15}\right) - \frac{360}{30}$$
$$= 360 - (180 + 120 + 72) + (60 + 36 + 24) - 12$$
$$= 360 - 372 + 120 - 12 = 96.$$

[b] $\phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$

$$= 360\left(\frac{8}{30}\right) = 12 \cdot 8 = 96.$$

4. Compute [a] $\phi(143)$, [b] $\phi(72)$, [c] $\phi(30)$.

[a] $143 = 11 \cdot 13$. $\phi(143) = \phi(11 \cdot 13) = \phi(11)\phi(13) = (10)(12) = 120$.

[b] $72 = 2^3 \cdot 3^2$. $\phi(72) = 72\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$

$$= 72\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = \frac{72}{3} = 24.$$

[c] $30 = 2 \cdot 3 \cdot 5$. $\phi(30) = 30\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

$$= 15\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 5 \cdot \frac{8}{5} = 8.$$

5. (7.25): Prove that the first 6 powers of 10 belong to distinct congruence classes modulo 7.

$10 \equiv 3 \bmod 7$.

$10^2 = 100 = 30 + 70 \equiv 30 = 28 + 2 \equiv 2 \bmod 7$.

$10^3 = 1000 = 300 + 700 \equiv 300 = 42 \cdot 7 + 6 \equiv 6 \bmod 7$.

$10^4 = 10{,}000 = 7 \cdot 1428 + 4 \equiv 4 \bmod 7$.

$10^5 = 100{,}000 = 14285 \cdot 7 + 5 \equiv 5 \bmod 7$.

$10^6 = 1{,}000{,}000 = 142857 \cdot 7 + 1 \equiv 1 \bmod 7$.

6. Find 2^{402} modulo 11.

Recall: If $a \equiv r \bmod n$ & $b \equiv s \bmod n$, then $a+b \equiv r+s \bmod n$ and $a \cdot b \equiv r \cdot s \bmod n$. [Lemma 7.19]

Fermat's Little Theorem: If p is prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \bmod p$. [Theorem 7.36]

- Here we want to use the fact that $2^{10} \equiv 1 \bmod 11$.

$$2^{402} = 2^{10 \cdot 40 + 2} = (2^{10})^{40} 2^2 \equiv (1)^{40} \cdot 4 \equiv 4 \bmod 11.$$