CS 70 HW #11

Sunjay
Caleb RO - cyro@berkeley.edu

1) Fermat's Little theorem

theorem: prove $m, m^3 - m$ is divisible by 130 for all natural numbers

FLT
↳ $m^{13} - m \rightarrow 2 \times 5 \times 13 \mid m^{13} - m$

130
10 (13)
2 (5)

Factor
$m(m^{12} - 1)$

$a^3 - b^3 = (a-b)(a^2+ab+b^2)$

↳ $m(m^6+1)(m^6-1)$

↳ $m(m^3+1)(m^3-1)(m^6+1)$

↳ $m(m-1)(m^2+m+1)(m^3-(-1))(m^6+1)$

↳ $m(m-1)(m^2+m+1)(m+1)(m^2-m+1)((m^2)^3-(-1))$

↳ $m(m-1)(m^2+m+1)(m+1)(m^2-m+1)(m^2+1)(m^4-m^2+1)$

↓

Need to prove Divisible by 2, 5 and 13

By 2:

$m(m-1)(m^2+m+1)(m+1)(m^2-m+1)(m^2+1)(m^4-m^2+1)$

↳ m^2-m → Divisible by 2 ✓

By 5:

$m(m-1)(m^2+m+1)(m+1)(m^2-m+1)(m^2+1)(m^4-m^2+1)$

↳ m^5-m → Divisible by 5 ✓

By 13:

$m^{13}-m \rightarrow m^{13} = m \pmod 3 \; ; \forall m \in N$

↳ Divisible by 13 ✓

→ This theorem is True by FLT

2) Euler's totient Function

↳ $\Phi(n) = |\{ i : 1 \leq i \leq n, gcd(n,i) = 1 \}|$

where $\Phi(n)$ total number of positive integers $\leq n$ relatively prime

a) Given: p is prime Find $\Phi(p)$

* Since p is prime, all numbers ranging from 1 to $p-1$ are relatively prime to p.

↳ Thus: $\Phi(p) = p-1$

b) Given: p is prime and k is positive integer

Find $\Phi(p^k)$

* Since p is prime and we are essentially multiplying itself by k times, the only numbers that are not relatively prime to p^k are gonna be all the multiples of p

↳ number of multiples of $p = p^{k-1}$

↳ Thus: $\Phi(p^k) = p^k - p^{k-1}$ = removing numbers that are less than p^k but are not multiples of p

C) If gcd $(a, b) = 1$, then $\phi(a \cdot b) = \phi(a)\,\phi(b)$

Chinese Remainder Theorem

Since gcd $(a, b) = 1$, passes CRT condition

1) $x \equiv i \bmod (a)$; $i \% a = x$

2) $x \equiv j \bmod (b)$; $j \% b = x$

↳ $x = \bmod (a) * \bmod (b)$; x: CRT value

↳ $x = i * j$; $i = ax$, $j = bx$

↳ $x = ax * bx$

↳ $1 = a + b$

3) Euler totient Theorem

a)