MATH 314 Fall 2023 - Class Notes

10/17/2023

Scribe: Ian Scanlon

Summary: This Class covers Euler Phi Function and Chinese Remainder Theorem as well as Modular Exponentiation.

Notes: Phi can be shown as ϕ or φ , $\varphi(n)$ count how many residues $\pmod{n}$ have an inverse, equivalently it counts integers $0 \leq a \leq n$ where $gcd(a, n) = 1$

- $\varphi(5) = 4$
- $\varphi(26) = 12$
- $\varphi(9) = 6$

Chinese Remainder Theorem:

Notes: If m and n have $gcd(m, n) = 1$ then for any residues $a \pmod{n}$ and $b \pmod{n}$, we can find exactly one residue $X \pmod{n}$ in both residue classes

Ex1: Find $X \equiv 3 \pmod{5}$, $X \equiv 9 \pmod{11}$ if $x \leq 55$ is $\equiv 9 \pmod{11}$ then $X \equiv 9, 20, 31, 42, 53$ $(9 + 11 = 20, 20 + 11 = 31, 31 + 11 = 42, ...)$

$x = 53$ is the only solution to both equations $\pmod{55}$

General Algorithm to find x: Use Euclids extended algorithm to find m' and n' such that $1 \equiv m'm + n'n$ then $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ the solution is $X \equiv bm'man'n \pmod{mn}$

Note the theorm is false if $gcd(m, n) \neq 1$

What does this mean for the φ function?
Suppose we're computing $\varphi(m - n)$ where $gcd(m, n) = 1$, $x \pmod{mn}$ has an inverse if both $x \pmod{m}$ has an inverse <u>and</u> $x \pmod{n}$ has an inverse.

Chinese Remainder theorem says that each residue $\pmod{m}$ can be combined what a residue $\pmod{n}$ to get a unique residue $\pmod{mn}$

$\varphi(mn) = \varphi(m)\varphi(n)$ only when $gcd(m, n) = 1$

Ex2: If p is prime then $\varphi(p) = p - 1$
$\varphi(10) = \varphi(5 * 2) = \varphi(5)\varphi(2)$
$= \varphi(2-1)\varphi(5-1) = 1 * 4 = 4$

Ex3: $\varphi(70) = \varphi(7) * \varphi(10) = \varphi(7)\varphi(5)\varphi(2)$
$= \varphi(7-1)\varphi(5-1)\varphi(2-1) = 6 * 4 * 1 = 24$

$\varphi(9) = 6$ not $(9-1)$
Because the rule for prime powers is $\varphi(p^k) = p^k(1 - 1/p)$
$\varphi(p^1) = p^1 - p^0 = p - 1$
so, $\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$

Ex4: $\varphi(200) = \varphi(8)\varphi(25) = \varphi(2^3 * 5^2)$
$= \varphi(2^3)\varphi(5^2) = \varphi(2^3 - 2^2) * \varphi(5^2 - 5^1) = (8-4) * (25-5) = 4 * 20 = 80$

Modular Exponentiation: by using repeated squaring we can compute (a^{2^i}) very fast.

Ex1: 5^{16}
we know that $5^2 \equiv 25 \pmod{26}$
Therefore $(5^2)^2 \equiv (25)^2 \pmod{26}$
$5^4 \equiv (-1)^2 \equiv 1 \pmod{26}$
$(5^4)^2 = 1^2$
$5^8 \equiv 1 \pmod{26}$

So... $a^{2^i} \pmod{m}$ can be computed by using only i multiplication.

$2^{16} \pmod{13}$
$2^2 = 4 \pmod{13}$
$2^4 \equiv 4^2 \equiv 16 \equiv 3 \pmod{13}$
$2^8 \equiv (2^4)^2 \equiv 3^2 \equiv 9 \pmod{13}$
$2^16 \equiv (2^8)^2 \equiv 9^2 \equiv 81 \pmod{13} \equiv 3 \pmod{13}$