MATH 314 Spring 2024 - Class Notes

3/27/2027

Scribe: Ablolom Yohannes

Summary: What was covered in class was the Euler Phi function and Modular Exponentiation

Euler Phi Function: Tool that is helpful for public-key crypto-systems, Especially for RSA. As for the definition its the number of integers for a value m, that is relativly prime to m denoted by $\Phi(m)$

Formulas:

- $\Phi(m) = \Phi(m * n) = \Phi(m) * \Phi(n) = (m - 1) * (n - 1)$
- $\Phi(p^e) = p^e - p^{e-1}$

Ex. $\Phi(10)$
$= \Phi(5 * 2)$
$= \Phi(5) * \Phi(2)$
= (5-1) * (2-1) = 4

If the value is already prime then its m-1
Ex. $\Phi(13) = 12$

Mixups Ex. $\Phi(49)$
Wrong: $\Phi(7 * 7)$ = (7-1) * (7-1)
Right: $\Phi(7^2)$
$= 7^2 - 7^{2-1} = 49 - 7 = 42$

Harder Ex. $\Phi(240)$
$= \Phi(30)\Phi(8)$
$= \Phi(15)\Phi(2)\Phi(2^3)$
$= \Phi(3)\Phi(5)\Phi(2^4)$
$= (3 - 1)(5 - 1)(2^4 - 2^3)$
$= 64$

Modular Exponentiation: Expression: $a^b \pmod m$

How to:

- Convert b into binary

- Then use repeated squaring as such: a^{2i} for every value in the binary
- As you traverse each part of the binary, multiply the values of the binary you need

Ex. $17^{162} \pmod{19}$
Write 162 in binary = 101000010 (Which is: 128 + 32 + 2)
Now $\underline{\text{Compute } 17^9 17^7 17^2}$
Start with 17^2 and work your way up
$\underline{17^2 = -2^2 = 4 \pmod{19}}$ (You do $17 \pmod{19}$ to get easier values)
$17^4 = 4^2 = 16 \pmod{19}$
$17^8 = 16^2 = -3^2 = 9 \pmod{19}$
$17^{16} = 9^2 = 81 = 5 \pmod{19}$
$\underline{17^{32} = 5^2 = 25 = 6 \pmod{19}}$
$17^{64} = 6^2 = 36 = 17 \pmod{19}$
$\underline{17^{128} = 17^2 = 4 \pmod{19}}$
$17^{162} = 4 * 6 * 4 = 96 = \underline{1} \pmod{19}$