CS 235: Algebraic Algorithms, Spring 2021

Practice Exercises Before Midterm

Exam Date: Wednesday, March 10^{th}, 2021.

✓

Problem 1. Prove that $\underline{\gcd(n, (n-1)!) = 1 \text{ if and only if } n \text{ is prime}}$.

$\gcd(n, (n-1)!) = 1 \Rightarrow n$ is prime

n is prime $\Rightarrow \gcd(n, (n-1)!) = 1$

$\Rightarrow$ gcd of n and $(n-1)!$ is 1 which means
the n and $(n-1)!$ are relatively prime
so n and all integers smaller than n has to
be relative prime which is a definition of prim

" the other way around

18

Problem 2. This question has two sub-problems

(i) Find the additive inverse and multiplicative inverse of 11 in $\mathbb{Z}_{19}$. Is 11 a perfect square in $\mathbb{Z}_{19}$ (i.e. is there a value of $x \in \mathbb{Z}_{19}$ such that $x^2 \equiv 11 \pmod{19}$)?

(ii) Show that $\varphi(12^k) = \varphi(12) \cdot 12^{k-1}$ where φ is the Euler's totient function.

i) additive inverse is $19-11=8$

multiplicative inverse is ($11 \times a \bmod 19 \equiv 1 \bmod 19$) $\boxed{17}$

$x^2-11=0 \quad (x+\sqrt{11})(x+\sqrt{11})$

11 x^2 4, 9, 16, 6, 17, 11, Yes there is a value. 7

12^2

ii) $\varphi(12^k) = \varphi(12) \times 12^{k-1}$

Theorem 2.11

12^k is when factorized $(2^2)^k \cdot (3^1)^k$

so $\varphi(12^k) = \prod_{i=1}^{2} p_i^{e_i-1}(p_i-1) = 2^{2k-1}(2-1) \times 3^{k-1}(3-1)$

$= 2^{2k-1} \times 3^{k-1} \times 2$

$12^k \prod_{i=1}^{2} (1-1/p_i)$

$= 12^k \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right)$

$\varphi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$

$12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) \times 12^{k-1}$ above

A

Chinese remai

Problem 3. Let $a, b, n, n' \in \mathbb{Z}$ with $n > 0$, $n' > 0$, and $\gcd(n, n') = 1$. Show that if $a \equiv b \pmod{n}$ and $a \equiv b \pmod{n'}$, then $a \equiv b \pmod{nn'}$.

Then, use the statement above to show that $(x^{\varphi(y)} + y^{\varphi(x)}) \equiv 1 \pmod{xy}$ where x, y are distinct primes, and φ is the Euler's totient function.

1) From chinese remainder theorem
$\gcd(n, n') = 1$

$n \mid a-b$, $n' \mid a-b$ and n and n' are relatively prime,
so $a-b$ is also dived by nn'

$$x^{\varphi(y)} \equiv 1 \pmod{y} \text{ and } y^{\varphi(x)} \equiv 1 \pmod{x}$$

$$\text{so } x^{\varphi(y)} \equiv ty+1 \text{ and } y^{\varphi(x)} \equiv sx+1$$

$$x^{\varphi(y)} + y^{\varphi(x)} \equiv ty + sx + 2$$

$$x^{\varphi(y)} \equiv 1 \pmod{y}$$
$$x^{\varphi(y)} \equiv 0 \pmod{x}$$

$$x^{\varphi(y)} + y^{\varphi(x)} \equiv 1 + 0 \pmod{y}$$

$$x^{\varphi(y)} + y^{\varphi(x)} \equiv 0 + 1 \pmod{x}$$

$$\text{so } x^{\varphi(y)} + y^{\varphi(x)} \equiv 1 \pmod{xy}$$

Problem 4. Consider the system of congruences

$$x \equiv 6 \pmod{7}$$
$$x \equiv 6 \pmod{11}$$
$$x \equiv 3 \pmod{13}$$

Find one solution to the above system. Then, describe all integer solutions to the system.

Chinese remainder theorem

$x \equiv 6 \pmod{7} \rightarrow A_1$
$x \equiv 6 \pmod{11} \rightarrow B_1$
$x \equiv 3 \pmod{13} \rightarrow C_1$

so $x = A_1 + B_1 + C_1 \pmod{7 \times 11 \times 13}$

so $x = 11 \times 13 \times A_1 + 7 \times 13 \times B_1 + 7 \times 11 \times C_1 \bmod (7 \times 11 \times 13)$

$x \equiv 143A_1 + 91B_1 + 77C_1 \pmod{7 \times 11 \times 13}$

use modular inverse

$6 \bmod 7 \equiv 143 \times (143^{-1} \times 6) \bmod 7$
$6 \bmod 11 \equiv 91 \times (91^{-1} \times 6) \bmod 11$
$3 \bmod 13 \equiv 77 \times (77^{-1} \times 3) \bmod 13$

$143^{-1} \bmod 7 \Rightarrow 3^{-1} \bmod 7 \Rightarrow 5$
$91^{-1} \bmod 11 \Rightarrow 3^{-1} \bmod 11 \Rightarrow 4$
$77^{-1} \bmod 13 \Rightarrow 12^{-1} \bmod 13 \Rightarrow 12$

48 5 60

12 24 36 48 60
13 26 39 52 65 78

$A_1 \equiv 143 \times 5 \times 6$
$B_1 \equiv 91 \times 4 \times 6$
$C_1 = 77 \times 12 \times 3$

$$\begin{array}{r} 143 \\ \times 130 \\ \hline 000 \\ 429 \end{array}$$

$4290 + 2184 + 2772$

$$\begin{array}{r} 91 \\ \times 24 \\ \hline 364 \\ 182 \end{array}$$

2184

6474
2772

9246

$$\begin{array}{r} 9246 \\ 9009 \\ \hline 237 \end{array}$$

all z

$\boxed{9246, \quad 237 \bmod (1001)}$

$$\begin{array}{r} 77 \\ 13 \\ \hline 231 \\ 77 \\ \hline 1001 \end{array}$$

21 2

2 21 77 42

$$\begin{array}{r} 36 \\ \hline 462 \end{array}$$ 4

$$\frac{231}{277^2}$$