CS 235: Algebraic Algorithms, Spring 2021

Practice Exercises Before Midterm

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

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

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.

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.

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.