Discrete Structures

Worksheet 12

Spring 2022
February 11

---

1. This question is about congruences.

   (a) Explain why the following systems of congruences have the same solutions:

   $$\begin{cases} x \equiv 2 \pmod{39} \end{cases} \qquad \begin{cases} y \equiv 2 \pmod{13} \\ y \equiv 2 \pmod{3} \end{cases}$$

   (b) Find the multiplicative inverses of 2 modulo 3, 13, 39. Show your work!

   (c) Suppose you know that $ab \equiv 1 \pmod{pq}$. Just from this, is it possible to find the multiplicative inverses of a modulo p and modulo q? The numbers p and q are prime.

2. This question is about exponents in congruences.

   (a) For what numbers $a \in \{0, 1, \ldots, 18\}$ is it possible to solve the quadratic equations:

   $$\text{(i) } x^2 \equiv a \pmod{19} \qquad \text{(ii) } x^2 + x \equiv a \pmod{19}$$

   (b) For $a = 1, 2, 3$, what are the solutions to the exponential equation:

   $$3^x \equiv a \pmod{19}$$

3. Show that $n^7 - n$ is divisible by 42 for all $n \in \mathbf{Z}$.
   Hint: Use fermat's Little theorem.

4. Let $a, b, c \in \mathbf{Z}$. Show that $\gcd(ab, c) = 1$ if and only if $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.

---

6. Complete the following tasks for next lab (Tuesday). They will be presented at the beginning of the lab.

   (a) Use induction to prove that $4^n + 5^n + 6^n$ is divisible by 15 for all odd $n \in \mathbf{N}$.

   (b) Using proof by contradiction, prove that there is no largest prime number.
   Hint: Use the uniquess of proime factorization.

   (c) Let $p = 6n + 5$ be a positive integer, for some $n \in \mathbf{Z}_{\geqslant 0}$. Show that there is at least one prime factor q of p for which also $q = 6k + 5$, for some $k \in \mathbf{Z}_{\geqslant 0}$.
   Hint: Use proof by contradiction and the fact that factors of an odd number are odd.

   (d) For all integers a, b, show that $\gcd(a, b) = \gcd(2a + b, 3a + 2b)$.