CS 235: Algebraic Algorithms, Spring 2021

Discussion 1

Date: Tuesday, February 02, 2021.

Problem 1. For all integers $a, b, c > 0$. Show that:

(a) $\gcd(ca, cb) = c\ \gcd(a, b)$ and $\operatorname{lcm}(ca, cb) = c\operatorname{lcm}(a, b)$

(b) $d = \gcd(a, b) \neq 0$ if and only if $\gcd(a/d, b/d) = 1$

Hint: recall from the lecture, if $d = \gcd(a, b)$ then we can express d as a linear combination of a, b, namely, $ax + by = d$ for some $x, y \in \mathbb{Z}$

Problem 2. Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $a \equiv b \pmod{n}$ Show that $\gcd(a, n) = \gcd(b, n)$.

Problem 3. Let $a \in \mathbb{Z}$, show that: $a^2 \not\equiv 2 \pmod 4$ or $a^2 \not\equiv 3 \pmod 4$

Hint: consider we have $a \equiv n \pmod 4$, then what are the possible values for n? Then, for each n, how can we express a in terms of some $x \in \mathbb{Z}$? At this point, what is special about a^2 in terms of x?