Class Exercises: 2019-10-03

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

Have a copy of the lecture notes on modular arithmetic available as you work on these problems.

1. Using Euclid's GCD algorithm, compute the gcd of 276 and 437, showing your work at each step.

2. An "integer linear combination (IntLC) of a and b" is defined to be an expression of the form $ka + \ell b$, where k and ℓ are integers. For each of the following statements, indicate "true" or "false." If true, provide a concise proof. If false, provide a specific counterexample.

   For all $a, b, c, n \in \mathbb{N}^+$,

   2.1. $\gcd(a, b) \neq 1 \wedge \gcd(b, c) \neq 1 \implies \gcd(a, c) \neq 1$.

   2.2. $\gcd(ab, ac) = a \cdot \gcd(b, c)$.

   2.3. $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$.

   2.4. if an IntLC of a and b equals 1, then so does some IntLC of a and b^2.

3. Using the Inverse Existence Theorem (see the lecture notes), prove the following. If p is a prime, $b \in \mathbb{Z}_p$, and $b \neq 0$, then

   3.1. b has an inverse modulo p;

   3.2. the function $f_b : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f_b(x) = bx \bmod p$ is a bijection.