Problem Set 2: GCDs and The Euclidean Algorithm

5) Find an integer solution to the following Diophantine equations:
   (a) \(4x + 15y = 1\)  \((try\ this\ one\ without\ the\ Euclidean\ algorithm - can\ you\ quickly\ guess\ \(x\)\ and\ \(y\)?)\)
   (b) \(7x + 9y = 1\)
   (c) \(26x + 38y = 6\)

6) Compute the following inverses in \(\mathbb{Z}_n\). You will want to use your work in Question 5) for all of these!
   (a) \(4^{-1}\) in \(\mathbb{Z}_{15}\)
   (b) \(7^{-1}\) in \(\mathbb{Z}_9\)
   (c) \(2^{-1}\) in \(\mathbb{Z}_7\)
   (d) \(13^{-1}\) in \(\mathbb{Z}_{19}\)

7) The extended Euclidean algorithm applied to \(a\) and \(b\) provides one solution to the equation \(ax + by = g\) where \(g = \gcd(a, b)\), but there are many more solutions! To this end, find three different pairs of integers \((x, y)\) such that \(4x + 3y = 1\).

8) For a positive integer \(d\) and an integer \(n\), remember that if \(n \equiv r \pmod{d}\) where \(0 \leq r < d\), then \(n = qd + r\) for some \(q \in \mathbb{Z}\).
   Let \(n \in \mathbb{Z}\) be positive and set \(d = 2\). Prove the following statements:
   (a) If \(n \equiv 0 \pmod{2}\), then \(\gcd(n, n + 2) = 2\). \((if\ n \equiv 0 \pmod{2},\ what\ kind\ of\ number\ is\ n?)\)
   (b) If \(n \equiv 1 \pmod{2}\), then \(\gcd(n, n + 2) = 1\). \((if\ n \equiv 1 \pmod{2},\ what\ kind\ of\ number\ is\ n?)\)

9) For \(a, d \in \mathbb{Z}\) where \(d \neq 0\), restate the definition of \(d \mid a\) in the language of modular arithmetic.

10) Prove that \(\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p - 1\}\).

11) Prove the following for \(a, b, d \in \mathbb{Z}\):
   (a) If \(d \mid a\) then \(d \mid ca\) for any \(c \in \mathbb{Z}\).
   (b) If \(d \mid a\) and \(d \mid b\) then \(d \mid (a + b)\).
   (c) If \(d \mid a\) and \(d \mid b\) then \(d \mid (ax + by)\) for any \(x, y \in \mathbb{Z}\).
   (d) Let \(k \in \mathbb{Z}\) be a common divisor of \(a\) and \(b\); that is, \(k \mid a\) and \(k \mid b\). Prove that \(k \mid \gcd(a, b)\).  
      \(Hint:\ Modular\ arithmetic\ won't\ be\ as\ helpful\ here.\)

12) In \(\mathbb{Z}_n\), we can’t divide by any number that has a common factor with \(n\). However, we CAN divide congruences by common factors!
   Suppose that \(a, b, n \in \mathbb{Z}\) have a common factor of \(k\), where \(k \in \mathbb{Z}, k \neq 0,\ and\ n \neq 0\). Prove the following statement:
   \[
   \text{If } a \equiv b \pmod{n}, \text{ then } \frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{n}{k}}
   \]

13) Prove that the Euclidean algorithm always results in the greatest common divisor!
mini Problem Set 3: Quadratic Residues Part 1

14) (a) List all of the squares and non-squares in $\mathbb{Z}_{13}$ and $\mathbb{Z}_{19}$.

(b) For primes $p \in \{7, 11, 13, 17, 19\}$, which ones have $-1$ as a square in $\mathbb{Z}_p$?

(c) Which of the primes $p \in \{7, 11, 13, 17, 19\}$ can be written as $x^2 + y^2$ for non-zero $x, y \in \mathbb{Z}$?

(d) Any pattern connecting parts (b) and (c)?

15) (a) For each prime $p < 43$, determine whether or not $p$ can be written in the form $x^2 + 3y^2$ for positive integers $x$ and $y$.

(b) For each prime $p < 43$, determine whether or not $-3$ is a square modulo $p$.

(c) Any pattern connecting parts (a) and (b)?

(d) Can you find a similar connection for primes $p$ which can be written in the form $x^2 + 5y^2$ for positive integers $x$ and $y$, and whether or not $-5$ is a square modulo $p$? Try for primes $p < 110$. 

Page 2 of 2 November 6, 2019 Problem Sets Day 2