Homework 2

Evan Hughes

January 2023

1. Find the gcd of the given pair of numbers (a, b) and express at least one of the gcd's as a $\mathbb{Z}$-linear combination of a and b.
   (a) $(56, 72)$
   $8 = (-5)56 + (4)72$
   (b) $(306, 657)$
   9
   (c) $(272, 1479)$
   17
   (d) $(1103, 465)$
   1
2. Let $p \in \mathbb{Z}$ be a prime integer.
   (a) Show that if $p > 3$, them p is of the form $6k + 1$ or $6k - 1$ for some integer k.
   $p = 6k + n$ where n is one of $0, 1, 2, 3, 4, 5$. If n is 0, 2, or 4, then p is even, so p is not prime. If n is 3, then p is divisible by 3, and not prime. This only leaves 1 and 5, 5 $equiv - 1 \pmod 6$, therefore p is of the form $6k - 1$ or $6k + 1$.
   (b) If $p > 5$, show that dividing p by 10, can only leave remainders of $1, 3, 7$, or 9, and find examples of primes with these remainders.
   $p = 10k + n$ where n is one of $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. If n is 0, 2, 4, 6, or 8, then p is even, so p is not prime. If remainder is 5, then p is divisible by 5, and not prime. This only leaves $1, 3, 7$, or 9.
   $19 \pmod 1 0 = 9$
   $17 \pmod 1 0 = 7$
   $13 \pmod 1 0 = 3$
   $11 \pmod 1 0 = 1$
3. Find the smallest positive integer in the given sets.
   (a) $\{6u + 15v : u, v \in \mathbb{Z}\}$
   $3 = (3)6 + (-1)15$
   $3 =$gcd$(6, 15)$
   (b) $\{12r + 17s : r, s \in \mathbb{Z}\}$
   $1 = (10)12 + (-7)17$
   $1 =$gcd$(12, 17)$
4. Let a, b, c, d be integers.
   (a) If $a \mid c$ and $b \mid c$, is it necessary that $ab \mid c$?
   If $a = 3$ and $b = 6$, and $c = 6$, then $a \mid c$ and $b \mid c$, but ab does not divide c.
   (b) Prove that if $a \mid c$ and $b \mid c$, and $\gcd(a, b) = 1$, then $ab \mid c$.
   If $\gcd(a, b) = 1$, then $1 = am + bn$ for some integers m and n. Then $c = c(am) + (c)bn$. Because a, b divide c, $c = as$ and $c = bt$ for some integers s and t. Then $c = abns + abmt$. $c = ab(ns + mt)$, so $ab \mid c$.

(c) Prove that if $\gcd(a, b) = d$, then $ab \mid cd$.

If $\gcd(a, b) = d$, then $d = am + bn$ for some integers m and n. Then $cd = c(am + bn)$. $cd = cam + cbn$. Not sure where to continue this proof.

5. Let p be an integer other than 0 or ± 1. Prove that if p has the property

$$\forall b, c \in \mathbb{Z}, p \mid bc \implies p \mid c \text{ or } p \mid b$$

then p is a prime number.

Since p is prime if $-p$ is prime, we assume that $p > 1$. Suppose that $p = bc$ for some positive integers b and c. Then $0 < b \leq p$ and $0 < c \leq p$. By the given properties, $p \mid b$ or c. Thus, $b = p$ and $c = 1$ or $c = p$ and $b = 1$. This shows that the only positive divisors of p are 1 and p. Therefore, the only divisors of p are ± 1, $\pm p$; Therefore, p is prime.