HW3

Sawyer Maloney

September 29, 2023

Exercise 1. Suppose $b, c \in \mathbb{Z}^+$ are relatively prime and a is a divisor of $b + c$. Prove that

$$\gcd(a, b) = 1 = \gcd(a, c).$$

Solution. Proof by contradiction.

Assume $\gcd(a, b) \neq 1 \neq \gcd(a, c)$. Since $b \neq c$, there are two unique integers, $m, n > 1 \in \mathbb{Z}$ such that $am = b, an = c$. We may rewrite the first statement to solve for a: $a = \frac{b}{m}$. Further, because a divides $b + c$, there is an integer $q \in \mathbb{Z}$ such that:

$$aq = b + c$$

Rearranging the equality for c and substituting the a with the value found above,

$$\frac{b}{m}q = b + c \implies \frac{b}{m}q - b = c$$

$\square$

Exercise 2. 1.7

Exercise 3. Prove that if n is a perfect square then n must have the form $4k$ or $4k + 1$.

Solution. Since n is a perfect square, there is $m \in \mathbb{N}^+ | m^2 = n$. By the division theorem, we may write m as:

$$m = cq + r, c, q, r \in \mathbb{N}^+$$

If we fix $c = 4$, to 'divide' m by 4, we can have four remainders for $r : r \in [0, 3]$. Now consider each remainder as an individual case:

- $r = 0$. $m = 4\delta$. If $k = \delta$, then $m = 4k$.
- $r = 1$. $m = 4\delta + 1, m^2 = 16\delta^2 + 8\delta + 1, k = 4\delta^2 + 2\delta \implies m^2 = 4k + 1$
- $r = 2$. $m = 4\delta + 2, m^2 = 16\delta^2 + 16\delta + 4, k = 4\delta^2 + 4\delta + 1 \implies m^2 = 4k$
- $r = 3$. $m = 4\delta + 3, m^2 = 16\delta^2 + 24\delta + 9, k = 4\delta^2 + 6\delta + 2 \implies m^2 = 4k + 1$

Since all cases of remainders are covered, we have proven that $n = m^2$ is always of the form $4k$ or $4k + 1$. $\square$

Exercise 4. Use Euclid's algorithm to calculate the following.

- $\gcd(83, 13)$:

$$83 = 5(13) + 8$$
$$13 = 1(8) + 8$$
$$8 = 1(5) + 3$$
$$5 = 1(3) + 2$$
$$3 = 1(2) + 1$$
$$2 = 2(1) + 0$$

  The last non-zero remainder is 1, thus $\gcd(83, 13) = 1$.

- $\gcd(735, 1421)$:

$$735 = 0(1421) + 735$$
$$1421 = 1(735) + 686$$
$$735 = 1(686) + 49$$
$$686 = 14(49) + 0$$

  The last non-zero remainder is 49, thus $\gcd(735, 1421) = 49$.

Exercise 5. Let $n, k \in \mathbb{Z}^+$. Show that $\gcd(n, nk + 1) = 1$.

Solution. Proof, directly. Apply Euclid's algorithm:

$$nk + 1 = q(n) + r, q \in \mathbb{Z}, 0 \leq r < n$$

$$nk + 1 = k(n) + 1$$
$$n = n(1) + 0$$

The last non-zero remainder is 1, thus the $\gcd(n, nk + 1) = 1$. $\square$

Exercise 6. For each of the following equatoins, either find an integer solution or show that no solution exists.

- $204x + 157y = 4$. Use Euclid's to find gcd:

$$204 = 1(157) + 47$$

$$157 = 3(47) + 16$$
$$47 = 2(16) + 15$$
$$16 = 1(15) + 1$$
$$15 = 15(1) + 0$$

Thus gcd $= 1$. Now, build back up to find an equation in terms of $204, 157$:

$$1 = 16 - 15$$

$$1 = 16 - 47 + 2(16)$$
$$1 = 3(157) - 9(47) - 47$$
$$1 = 3(157) - 10(204) + 10(157)$$
$$1 = 13(157) - 10(204)$$

Now multiply across by 4:

$$4 = 52(157) - 40(204)$$

Thus an integer solution exists, $x = -40, y = 52$

- $87x + 12y = -14$. Use Euclid's to find gcd:

$$87 = 7(12) + 3$$

$$12 = 4(3)$$

Thus gcd $= 3$. Because $3 \nmid 14$, there is no integer solution to this equation.

Exercise 7. Suppose that $a, b \in \mathbb{Z}^+$ and set $l = \frac{ab}{\gcd(a,b)}$. For simplicity, $d = \gcd(a, b)$

(a) Show that l is a common multiple of a and b.

Rearranging our supposition:

$$l = b(\frac{a}{d}), q = \frac{a}{d} \implies l = bq$$

$$l = a(\frac{b}{d}), q = \frac{b}{d} \implies l = aq$$

We know $\frac{b}{d} \in \mathbb{Z}^+$ because d is the gcd, and thus divides both a and b. These equations show that a and b divide l, thus l is a common multiple of a and b.

(b) If m is any common multiple of a and b, how that m/l is an integer.

If m is a common multiple of a and b, that means that it has all the primes of a and b in its prime factorization, plus the primes of some other number c (where $c \in \mathbb{Z}^+$ may be 1). Thus:

$$m = c(ab)$$

Now examine the statement for m/l:

$$\frac{m}{\frac{ab}{d}} \implies \frac{md}{ab}$$

Substituting the equation for m into the above:

$$\frac{c(ab)d}{ab} = cd$$

cd is an integer, since both c and d are.

(c) Deduce that

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

and that for any $m \in \mathbb{Z}$

$$m \text{ is a common multiple of } a \text{ and } b \iff m \text{ is a multiple of } \operatorname{lcm}(a, b)$$