Math 345-504
2–9–2018

Solutions to Problem Set 7

1. Find the greatest common divisor $(831, 240)$ of 831 and 240.

Then write $(831, 240)$ as a linear combination of 831 and 240 with integer coefficients.

831	-	45
240	3	13
111	2	6
18	6	1
3	6	0

$$3 = (831, 240) = 13 \cdot 831 + (-45) \cdot 240. \quad \square$$

---

2. (a) Find $(103, 83)$ and write it as a linear combination with integer coefficients of 103 and 83.

(b) Using the result of (a) and without using trial and error, find specific integers x and y such that

$$103x + 83y = 55.$$

(a)

103	-	36
83	1	29
20	4	7
3	6	1
2	1	1
1	2	0

$$103 \cdot (-29) + 83 \cdot 36 = 1 = (103, 83). \quad \square$$

(b) Multiplying the equation in (a) by 55, I obtain

$$103 \cdot (-1595) + 83 \cdot 1980 = 55.$$

Thus, $x = -1595$, $y = 1980$ is a solution to the equation.
In fact, there are infinitely many solutions of the form:

$$x = -1595 + 83t, \quad y = 1980 - 103t. \quad \square$$

---

3. Prove that if n is an integer, then $5n^2 + 6$ and $6n^2 + 7$ are relatively prime.

$$6(5n^2 + 6) + (-5)(6n^2 + 7) = 1, \quad \text{so} \quad (5n^2 + 6, 6n^2 + 7) = 1. \quad \square$$

4. (a) Let $x, m, n \in \mathbb{Z}$. Prove that if $(m, n) = 1$ and $m \mid x$ and $n \mid x$, then $mn \mid x$.

(b) Give a counterexample to show that if $x, m, n \in \mathbb{Z}$ and $m \mid x$ and $n \mid x$, it does not necessarily follow that $mn \mid x$. (Note the difference in assumptions between (a) and (b)!)

(a) If $m \mid x$ and $n \mid x$, then $mj = x$ and $nk = x$ for some $j, k \in \mathbb{Z}$.
If $(m, n) = 1$, there are integers a and b such that

$$am + bn = 1.$$

Multiply by x and substitute:

$$\begin{aligned} amx + bnx &= x \\ am(kn) + bn(jm) &= x \\ mn(ak + bj) &= x \end{aligned}$$

Hence, $mn \mid x$. $\square$

(b) $4 \mid 12$ and $6 \mid 12$, but $4 \cdot 6 \not\mid 12$. $\square$

MATH 504]

5. Let G be a group and let $x \in G$. Suppose that $(m, n) = 1$ and

$$x^m = 1 \quad \text{and} \quad x^n = 1.$$

Prove that $x = 1$.

Since $(m, n) = 1$, I have

$$am + bn = 1 \quad \text{for some} \quad a, b, \in \mathbb{Z}.$$

Then

$$x = x^1 = x^{(am+bn)} = (x^m)^a \cdot (x^n)^b = 1 \cdot 1 = 1. \quad \square$$

It is now, and in this world, that we must live. - André Gide