Solutions to Homework 2

§1.2 #2. *You have at your disposal arbitrarily many 4-cent stamps and 7-cent stamps. What are the postages you can pay? Show in particular that you can pay all postages greater than 17 cents.*

The question can be restated as: which numbers can be written as $4m + 7n$, where m and n are non-negative integers? If we allowed negative integers, then the answer would be any mutiple of $\gcd(4, 7)$, but that's 1, so it would be any number. Thus "non-negative" is what makes it interesting.

Following Shifrin's hint, let's deal with numbers up to 17 and numbers greater than 17 separately.

If $4m + 7n \leq 17$ then $n \geq 0$ imples $4m \leq 17$, so $m \leq 4$; and $m \geq 0$ implies $7n \leq 17$, so $n \leq 2$. By brute force we find that the numbers we can get with $0 \leq m \leq 4$ and $0 \leq n \leq 2$ are 4, 7, 8, 11, 12, 14, 15, and 16, and then some numbers greater than 17 which we're not interested in yet.

Now suppose we wish to get a number $N \geq 18$. If $n = 4k$ then we use k 4-cent stamps. If $N = 4k + 1$ then we must have $k \geq 5$, so we can write

$$N = 4(k - 5) + 21 = 4(k - 5) + 3 \cdot 7.$$

If $N = 4k + 2$ then we must have $k \geq 4$, so we can write

$$N = 4(k - 3) + 14 = 4(k - 3) + 2 \cdot 7.$$

If $N = 4k + 3$ then again we must have $k \geq 4$, so we can write

$$N = 4(k - 1) + 7.$$

Thus we can get any amount greater than or equal to 18.

§1.2 #5. *Prove or give a counterexample: the integers q and r guaranteed by the division algorithm, Theorem 2.2, are unique.*

They are unique, as follows. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, and suppose that $a = qb + r$ and $a = q'b + r'$ with $0 \leq r, r' < b$. I claim that $q = q'$ and $r = r'$. We have $qb + r = q'b + r'$, so $qb - q'b = r' - r$, so $r' - r$ is a multiple of b. But the inequalities above imply that $-b < r' - r < b$, and the only multiple of b in that range is zero, so $r' - r = 0$, so $r' = r$. Then we have $qb + r = q'b + r$; subtracting r we get $qb = q'b$; and dividing by b we get $q = q'$.

§1.2 #11. *Prove that there are no integers m, n so that $(\frac{m}{n})^2 = 2$.*

One answer: If m and n have a common factor, then we can cancel it to get a solution where m and n are relatively prime. Rewrite the equation as $m^2 = 2n^2$. Then m^2 is even, so m is even (because if m were odd then m^2 would be odd). Write $m = 2k$. Then $4k^2 = 2n^2$, so $2k^2 = n^2$, so n^2 is even, so n is even. But this contradicts the assumption that m and n are relatively prime.

Another answer: Write the prime factorizations of m and n as

$$m = \pm 2^{a_1} 3^{a_2} 5^{a_3} \cdots ,$$
$$n = \pm 2^{b_1} 3^{b_2} 5^{b_3} \cdots ,$$

where the a_is and b_is are non-negative integers. If $m^2 = 2n^2$ then

$$2^{2a_1} 3^{2a_2} 5^{3a_3} \cdots = 2^{2b_1+1} 3^{2b_2} 5^{3b_3} \cdots .$$

Because prime factorizations are unique, we have $2a_1 = 2b_1 + 1$, but this is impossible because $2a_1$ is even while $2b_1 + 1$ is odd.

§1.3 #15. *If $n \equiv 7 \pmod 8$, then n is not the sum of three squares.*

(I put this problem out of order so that the next one could fit on one page.)

Modulo 8, we have $0^2 \equiv 0$, $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$, $(\pm 3)^2 \equiv 1$, and $4^2 \equiv 0$. There is no way to choose three numbers that are either 0, 1, or 4, and have their sum be congruent to 7 modulo 8.

Famously, Lagrange showed that every positive integer is the sum of four squares.

§1.2 #13. *The least common multiple of a and b is defined as the positive number μ that satisfies*

(i) $a \mid \mu$ and $b \mid \mu$, and

(ii) for all $s \in \mathbb{Z}$, if $a \mid s$ and $b \mid s$ then $\mu \mid s$.

Prove that

(a) *if* $\gcd(a, b) = 1$ *then* $\mu = ab$.

If you want you could skip this and say it's a special case of part (b), but I'll spell it out.

It is clear that $a \mid ab$ and $b \mid ab$, so we must show that for any integer s with $a \mid s$ and $b \mid s$, we have $ab \mid s$. Because $\gcd(a, b) = 1$, we can write $1 = am + bn$ for some integers m and n. Following the hint, we multiply through by s to get

$$s = ams + bns$$

Because $a \mid s$ and $b \mid s$, we can write $s = ak$ and $s = bl$ for some integers k and l. We can substitute this into the equation above to get

$$s = ambl + bnak = ab(ml + nk),$$

so $ab \mid s$ as desired.

(b) *more generally, if* $\gcd(a, b) = d$ *then* $\mu = \frac{ab}{d}$.

Because d divides b, we can write $\mu = a \cdot \frac{b}{d}$ to see that $a \mid \mu$, and because d divides a, we can write $\mu = \frac{a}{d} \cdot b$ to see that $b \mid \mu$. It remains to show that for any integer s with $a \mid s$ and $b \mid s$, we have $\mu \mid s$.

By Theorem 2.3 we can write $d = am + bn$ for some integers m and n. Divide through by d to get

$$1 = \frac{a}{d} \cdot m + \frac{b}{d} \cdot n,$$

again noting that $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Because $a \mid s$ and $b \mid s$, we can write $s = ak$ and $s = bl$ for some integers k and l. Multiplying the equation above by s, we get

$$\begin{aligned} s &= \frac{a}{d} \cdot ms + \frac{b}{d} \cdot ns \\ &= \frac{a}{d} \cdot mbl + \frac{b}{d} \cdot nak \\ &= \frac{ab}{d} \cdot (ml + nk), \end{aligned}$$

so s is a multiple of $\mu = \frac{ab}{d}$ as desired.