Homework 6

For practice: 6.2, 6.3, 6.5, 6.6, 6.8, 6.12

To turn in: 6.4, 6.11 (1st part only), 6.13, 6.17, 6.24 (1st part only).

From another book: Express the fraction 1739/4042 in lowest terms. Express $\gcd(1739, 4042)$ as an integer combination of 1739 and 4042. Don't use a calculator except to check that your integer combination is correct!

Solutions to graded problems

6.4. Clearly n divides both an and bn. Hence $n \leq \gcd(an, bn)$. On the other hand since $\gcd(a, b) = 1$, there exist $s, t \in \mathbf{Z}$ such that

$$sa + tb = 1.$$

Multiplying through by n gives

$$s(an) + t(bn) = n.$$

That is, n is an integer combination of an and bn. Since $\gcd(an, bn)$ divides both an and bn, it follows that $\gcd(an, bn)$ divides n. In particular $\gcd(an, bn) \leq n$.

In summary I have shown that $n \leq \gcd(an, bn)$ and $n \geq \gcd(an, bn)$. It follows that $n = \gcd(an, bn)$. $\square$

6.11. Suppose that the person has k of each kind of coin and that the total value of all coins is n dollars (i.e. $100n$ cents). Then

$$100n = k(1 + 5 + 10 + 25 + 50) = 91k.$$

But 100 and 91 are relatively prime ($11 \cdot 91 - 100 \cdot 100 = 1$), so it must be (Proposition 6.6) that 91 divides n. In particular, the smallest n can be is 91. I conclude that minimum value of the coins is \$91.

6.13. As in problem 6.11, we have

$$100n = k(25 + 2 \cdot 5 + 4 \cdot 10) = 75k,$$

where n is the number of dollars in the meter. This simplifies to

$$4n = 3k,$$

and since 4 and 3 are relatively prime, 4 must divide k. And if 4 does divide k, we can write $k = 4m$ for some $m \in \mathbf{N}$ and conclude that $n = 3m$ is an integer number of dollars.

Therefore the total amount of money is an integer number of dollars if and only if k is a multiple of 4.

6.17. Recall that if a number k divides both m and n, then it divides any integer combination of m and n. We apply this fact as follows. Note that

$$2a = 1 \cdot (a+b) + 1 \cdot (a-b) \text{ and } a-b = 0 \cdot (a+b) + 1 \cdot (a-b).$$

Hence $gcd(a+b, a-b)$ divides both $2a$ and $a-b$. Thus $gcd(a+b, a-b)$ divides $gcd(2a, a-b)$. In the other direction, we have

$$a+b = 1 \cdot 2a + (-1) \cdot (a-b)a-b = 0 \cdot 2a + 1 \cdot (a-b).$$

So the same reasoning shows that $gcd(2a, a-b)$ divides $gcd(a+b, a-b)$. The only way this can happen is if $gcd(2a, a-b) = gcd(a+b, a-b)$.

Showing that $gcd(a+b, a-b) = gcd(a+b, 2b)$ is completely analogous. The relevant integer combinations are

$$a+b = 1 \cdot (a+b) + 0 \cdot (a-b) \text{ and } 2b = 1 \cdot (a+b) + (-1) \cdot (a-b);$$

and

$$a+b = 1 \cdot (a+b) + 0 \cdot 2b \text{ and } a-b = 1 \cdot (a+b) + (-1) \cdot 2b.$$

6.18. I claim that if $\gcd(a,b) = 1$, then $\gcd(a^2, b^2) = 1$. (so, yes, $\gcd(a,b)$ determines $\gcd(a^2, b^2)$).

Proof. Suppose that there is some number $p > 1$ dividing both a^2, b^2. We can assume without loss of generality that p is prime. But then $p|a^2$ implies that $p|a$ (Proposition 6.7). Similarly $p|b$. It follows that $p|\gcd(a,b)$, which is impossible as the latter number is one. This shows that $\gcd(a^2, b^2) = 1$. $\square$

Now $\gcd(a,b) = 1$ does not determine $\gcd(a, 2b)$. For instance $\gcd(3,1) = \gcd(3,2) = 1$, but $1 = \gcd(2,1) \neq \gcd(2,2) = 2$.

6.24. Proof by induction.

Initial step. When $n = 1$, we have $4^n - 1 = 3$ which is clearly divisible by 3.

Induction step. Suppose that $3|(4^k - 1)$—i.e. $4^k - 1 = 3m$ for some $m \in \mathbf{N}$. I must show that $3|(4^{k+1} - 1)$. Now

$$4^{k+1} - 1 = 4 \cdot 4^k - 1 = 4 \cdot (3m+1) - 1 = 12m + 3 = 3(4m+1)$$

by the induction hypothesis. This shows that $3|(4^{k+1} - 1)$ and completes the induction step.

By induction, I conclude that $3|(4^n - 1)$ for all $n \in \mathbf{N}$. $\square$

6.28. Since $a|n$, we have $n = ak$ for some $k \in \mathbf{N}$. Hence b divides the product ak. Now a and b are relatively prime, so Proposition 6.6 tells us that b must divide k. In other words $k = b\ell$. Therefore we have

$$n = ak = ab\ell,$$

which means that $ab|n$. $\square$

6.35. Let $x = 1 + (n+1)! = 1 + (1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n+1))$. Then

$$x + 1 = 2 + (n+1)! = 2(1 + 1 \cdot 3 \cdot 4 \cdot \ldots \cdot (n+1)),$$

so $2|x+1$. Similarly if $j \leq n$, then

$$x + j = (j+1) + (n+1)! = (j+1)(1 + 1 \cdot 2 \cdot \ldots \cdot j \cdot j + 2 \cdot j + 3 \cdot \ldots \cdot (n+1),$$

so $j+1$ divides $x+j$. It follows that

$$x+1, x+2, \ldots, x+n+1$$

is a sequence of n consecutive natural numbers that are not prime.

Problem from another book. The point is to compute $\gcd(1739, 4042)$. I apply the Euclidean algorithm to do this.

$$\begin{aligned} 4042 &= 2 \cdot 1739 + 564 \\ 1739 &= 3 \cdot 564 + 47 \\ 564 &= 12 \cdot 47 + 0 \end{aligned}$$

So the end result is that $\gcd(4042, 1739) = 47$. It follows that the fraction $1739/4042$ becomes $37/86$ when expressed in lowest terms! To check this, I recycle the above work, and end by expressing 47 as a linear combination of 1739 and 4042:

$$\begin{aligned} 564 &= 1 \cdot 4042 - 2 \cdot 1739 \\ 47 &= 1 \cdot 1739 - 3 \cdot 564 = 1 \cdot 1769 - 3(1 \cdot 4042 - 2 \cdot 1739) \\ &= -3 \cdot 4042 + 7 \cdot 1739, \end{aligned}$$

which a calculator will easily verify to be true.