Mathematics 243, section 1 – Algebraic Structures
Suggested Solutions, Problem Set 4
October 23, 2003

2.4/10. If $b > 0$ and $a = qb + r$ (from division), then we want to show that $\gcd(a, b) = \gcd(b, r)$.

We discussed one approach in the Problem Session. Here is a rather different way to do this one. Recall that if we define $S_{a,b} = \{ma+nb|m, n \in \mathbf{Z}\}$, then the smallest (strictly) positive integer in $S_{a,b}$ is $d = \gcd(a, b)$. The same is true for any two integers, so if we can show the two sets $S_{a,b} = S_{b,r}$, then the desired result follows. To show the equality, first note that any $ma + nb \in S_{a,b}$ can be rewritten as:

$$\begin{aligned} ma + nb &= m(qb + r) + nb \\ &= (mq + n)b + mr, \end{aligned}$$

which is an element of $S_{b,r}$. Hence $S_{a,b} \subseteq S_{b,r}$. Conversely, any $m'b+n'r$ can be rewritten as:

$$\begin{aligned} m'b + n'r &= m'b + n'(a - qb) \\ &= n'a + (m' - qn')b, \end{aligned}$$

which is an element of $S_{a,b}$. Hence $S_{b,r} \subseteq S_{a,b}$. So we have $S_{b,r} = S_{a,b}$, and $\gcd(b, r) = \gcd(a, b)$.

2.4/11. The idea for this one is to consider the steps in the Euclidean algorithm and apply the result from problem 10 repeatedly:

$$\begin{aligned} a = q_1 b + r_1 &\Rightarrow \gcd(a, b) = \gcd(b, r_1) \\ b = q_2 r_1 + r_2 &\Rightarrow \gcd(b, r_1) = \gcd(r_1, r_2) \\ &\vdots \\ r_{n-2} = q_n r_{n-1} + r_n &\Rightarrow \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) \end{aligned}$$

(This can also be nicely phrased as a proof by induction!) Then assuming r_n is the last nonzero remainder, we have $r_n | r_{n-1}$ in the next step so $gcd(r_{n-1}, r_n) = r_n$. Hence putting together the whole string of equalities,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n.$$

Note that it is this argument that shows the Euclidean algorithm actually "works"(!)

2.4/20 and 21. In the problem session, we worked out some of a "slick" way to solve 20 and 21 *together*. Namely (after multiplying by -1 as necessary) we can assume $a, b > 0$, and since $d = \gcd(a, b)$ satisfies $d|(ab)$, we will have $ab = md$ for some $m \in \mathbf{Z}$. Then we

just have to prove that the integer m satisfies the properties for a least common multiple given in problem 20.

(a) If we have "adjusted" a, b to make them positive, then no divisibility properties are changed and $ab > 0$, $d > 0$ imply $m > 0$.

(b) To show that $a|m$ and $b|m$, note that $d|a$ and $d|b$, so $a = q_1 d$ and $b = q_2 d$ for some integers q_1, q_2. Then substituting from $a = q_1 d$ into the equation $ab = md$ gives $(q_1 d)b = md$. We can cancel the d on both sides (since $d > 0$) to yield $q_1 b = m$. Hence $b|m$. Similarly, substituting from $b = q_2 d$ into the equation $ab = md$ gives $a(q_2 d) = md$. We can cancel the d on both sides again to yield $aq_2 = m$. Hence $a|m$.

(c) Now assume $a|c$ and $b|c$. Then we must show $m|c$ (where m is the integer from the equation $ab = qm$). We have $c = an_1$ and $c = bn_2$ for some integers n_1, n_2 by hypothesis. Then we also know $a = q_1 d$ and $b = q_2 d$ for some integers q_1, q_2 since $d = \gcd(a, b)$. *Key observation:* in these equations q_1, q_2 must satisfy $\gcd(q_1, q_2) = 1$. (Reason: if not, then we could factor an additional common divisor of a, b out of the q's and d would not be the greatest common divisor). To use this observation, note that we can substitute for a, b in the equation $ab = dm$ to get $q_1 q_2 d^2 = dm$. Cancelling one factor of d implies:

$$q_1 q_2 d = m. \tag{1}$$

But now we also have from $c = an_1$, $c = an_2$: $dq_1 n_1 = c = dq_2 n_2$, hence

$$q_1 n_1 = q_2 n_2. \tag{2}$$

The key observation above says, for instance, that in (2) $q_2|n_1$ (q_2 has no factors > 1 in common with q_1, but it divides $q_1 n_1$. Hence $n_1 = q_2 k$ for some integer k. Therefore

$$c = an_1 = (q_1 d)(q_2 k) = (q_1 q_2 d)k = mk.$$

(using (1)). Therefore $m|c$.

To show *uniqueness*, note that if m, m' are two lcm's of a, b, then property (c) says $m|m'$ and $m'|m$, so $m = m'$ (since both are positive).

Comments:

- There is also a nice way to use the fact that $d = ma + nb$ for some integers m, n to show part (c) here.
- It is also possible to prove that there exists an integer satisfying these properties using a proof similar to what we did for the gcd: Namely, let

$$T_{a,b} = \{c \in \mathbf{Z} : a|c \text{ and } b|c\}$$

This is a set containing positive integers like the product ab. Hence the Well-Ordering property implies that $T \cap \mathbf{Z}^+$ contains a smallest element. Let's call that minimal

strictly positive element m. Properties (a) and (b) are automatic for this m from the construction to show property (c) holds, take any $c \in T_{a,b}$, and divide m into it:

$$c = mq + r, \quad 0 \leq r \leq m - 1$$

Since $r = c - mq$ and c, m are in $T_{a,b}$, it is easy to see that $a|r$ and $b|r$ (like problem 16). So $r \in T_{a,b}$. But m was the smallest strictly positive element in $T_{a,b}$, and $r \leq m - 1$. Hence $r = 0$, so $m|c$. (If you use this approach, though, then you still need to show that the formula in problem 21 holds!!!)