Mathematics 243, section 1 – Algebraic Structures
Selected Solutions, Problem Set 6
October 23, 2006

2.4/7. From the given information that $\gcd(a, b) = 1$, we know that $1 = ma + nb$ for some integers m, n. Multiply both sides of this equation by c. Then

$$c = mac + nbc.$$

But now use that $a|c$ and $b|c$. We have equations $c = as$ and $c = bt$ for integers s, t. Then we can substitute from $c = bt$ into the c in the first term on the right above, and from $c = as$ into the second term:

$$c = mabt + nbas = (ab)(mt + ns).$$

Since $m, t, n, s \in \mathbf{Z}$, this implies $(ab)|c$.

Comment: The proof of 2.4/18 is almost exactly the same, except you start from $d = ma + nb$ for some $m, n \in \mathbf{Z}$.

2.4/8. If $b > 0$ and $a = qb + r$ (for instance, from division), then we want to show that $\gcd(a, b) = \gcd(b, r)$.

Proof 1: The most direct way to show this is to let $d = \gcd(a, b)$ and to show that d satisfies the properties to be $\gcd(b, r)$ also. In other words, we must show $d > 0$, $d|b$ and $d|r$, and if $c|b$ and $c|r$, then $c|d$. The first of these is automatic by the definition of $\gcd(a, b)$. From that definition, we also have $d|b$. So we must prove that $d|r$. But from the equation $a = qb + r$, we have $r = a - qb$. So if $d|a$ and $d|b$, then $d|r$ too. (Reason: write $a = ud$ and $b = vd$ for integers u, v, then $r = ud - qvd = d(u - qv)$. Since $u - qv$ is an integer, this shows $d|r$.) Finally, assume that $c|b$ and $c|r$. Then from the equation $a = qb + r$, by an argument like the one just above, we also have $c|a$. But then $c|a$ and $c|b$ so $c|d$ from the fact that $d = \gcd(a, b)$. It follows that $d = \gcd(b, r)$ also.

Proof 2: 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 $\gcd(b,r) = \gcd(a,b)$.

Comment: A number of people seemed to be thinking along these lines but proved only "half" of what you need here. Namely, if you just know that $d = ma + nb = Mb + Nr$ for *some* $M, N \in \mathbf{Z}$ then it *does not follow* that $d = \gcd(b,r)$. You also need to know that d is the *smallest* positive number in the set $S_{b,r}$. That is established here by showing that $S_{b,r} = S_{a,b}$ as sets.

2.4/9. The idea for this one is to consider the steps in the Euclidean algorithm and apply the result from problem 8 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"(!)

2.4/10. We use "complete" induction on the integer j, starting from $j = 1$. At the first step in the algorithm, we have

$$r_1 = a - q_1 b = (1)a + (-q_1)b$$

so the desired statement is true with $s_1 = 1$ and $t_1 = -q_1$ in $\mathbf{Z}$. At the second step,

$$r_1 = b - q_2 r_1 = b - q_2(a - q_1 b) = (-q_2)a + (1 + q_1 q_2)b$$

so the desired statement is true with $s_2 = -q_2$ and $t_2 = (1 + q_1 q_2)$ in $\mathbf{Z}$. So now assume that

$$\begin{aligned} r_{n-1} &= s_{n-1}a + t_{n-1}b \\ r_n &= s_n a + t_n b \end{aligned}$$

where $s_{n-1}, t_{n-1}, s_n, t_n$ are integers. Then the next step in the Euclidean Algorithm produces

$$r_{n+1} = r_{n-1} - q_{n+1} r_n$$

Substituting from the above and rearranging the terms, we see

$$r_{n+1} = s_{n-1}a + t_{n-1}b - q_{n+1}(s_n a + t_n b) = (s_{n-1} - q_{n+1}s_n)a + (t_{n-1} - q_{n+1}t_n)b$$

So the desired statement is true with $s_{n+1} = s_{n-1} - q_{n+1}s_n$ and $t_{n+1} = t_{n-1} - q_{n+1}t_n$ in $\mathbf{Z}$.

2.4/12. (by induction on the number of factors) We can take the base case as $n = 2$. If p is prime and $p|(a_1a_2)$ then $p|a_1$ or $p|a_2$ by Euclid's Lemma (Theorem 2.16 in the book, also done in class, so we don't need to repeat the proof). Now assume that whenever $p|(a_1 \cdots a_k)$, then $p|a_i$ for some i, $1 \leq i \leq k$. Consider a case where $p|(a_1 \cdot \cdots \cdot a_k a_{k+1})$. By associativity of multiplication, we can group the factors as $(a_1 \cdots a_k)a_{k+1}$. By the base case, if p divides this product, then $p|(a_1 \cdots a_k)$ or $p|a_{k+1}$. If $p|a_{k+1}$, then we have shown what we have to. If not, then p does divide $(a_1 \cdots a_k)$ and the induction hypothesis shows $p|a_i$ for some i, $1 \leq i \leq k$. Hence p divides at least one of the factors.

2.4/19. Let

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

This is a set containing positive integers. Hence the Well-Ordering Property implies that $T \cap \mathbf{N}$ contains a smallest element. Let's call that minimal strictly positive element m. Properties (1) and (2) in the problem are automatic for this m from the construction. To show property (3) holds, take any $c \in T$, and divide m into it:

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

Since $r = c - mq$ and c, m are in T, it is easy to see that $a|r$ and $b|r$. So $r \in T$. But m was the smallest strictly positive element in T, and $r < m$. Hence $r = 0$, so $m|c$.

To show *uniqueness* of the lcm, note that if m, m' are two lcm's of a, b, then property (3) says $m|m'$ (because m' is a common multiple of a and b and m is an lcm). Similarly, $m'|m$ (since m is a common multiple of a, b and m' is an lcm). Hence by 2.3/20 from last week's problem set, $m = m'$ (since both are positive).