Basic Algebra (Solutions)

by Huah Chu

Exercises (§0.6, p.24)

1. Show that if p is a prime and $p|ab$ then either $p|a$ or $p|b$.

Proof. (I) Write $a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $b = \pm p_1^{\beta_1} \cdots p_n^{\beta_n}$ where $p_1, \ldots, p_n$ are prime numbers and $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ are nonnegative integers. Hence $ab = \pm p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n}$. Since $p|ab$, we have that $ab = pc$ for some integer c. Write $c = \pm q_1^{y_1} \cdots q_m^{y_m}$ where $q_1, \ldots, q_n$ are prime numbers and $y_1, \ldots, y_m$ are positive integers. Hence $\pm p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n} = \pm p \cdot q_1^{y_1} \cdots q_m^{y_m}$.

By the fundamental theorem of arithmetic, we conclude that $p = p_i$ for some i, $1 \le i \le n$, and $\alpha_i + \beta_i \ge 1$. Thus $\alpha_i \ge 1$ or $\beta_i \ge 1$ since $\alpha_i, \beta_i \ge 0$. It follows that $p = P_i|a$, if $\alpha_i \ge 1$, or $p = p_i|b$ if $\beta_i \ge 1$.

(II) Suppose $p|ab$ and $p \nmid a$. We have $(p, a) = 1$. If $b = 0$, then $p|b$ trivially. Hence we assume $b \neq 0$, then the least positive integer in $I = \{px + ay | x, y \in \mathbb{Z}\}$ is 1. So $1 = px + ay$ for some x and y. $b = pxb + aby$. ¿From $p|ab$ we have $p|b$. □

2. Define g.c.d. and l.c.m. for more than two integers and prove their existence.

Proof. (1) Let $a_1, \ldots, a_n$ be non-zero integers. An integer c is called a g.c.d. of $a_1, \ldots, a_n$ if it satisfies the following conditions

(i) $c|a_i$ for all i, $1 \le i \le n$

(ii) If d is any integer with $d|a_i$ for all i, $1 \le i \le n$, then $d|c$.

To prove the existence of a g.c.d., consider the element $b \stackrel{\text{def}}{=} \min\{a_1b_1 + a_2b_2 + \cdots + a_nb_n \in \mathbb{N} | b_1, \ldots, b_n \in \mathbb{Z}\}$. Clearly b satisfies the above condition (ii). We shall show that b satisfies the condition (i) also. In fact, write $b = a_1\beta_1 + \cdots + a_n\beta_n$ for some $\beta_i \in \mathbb{Z}$. For any a_i, suppose that $b \nmid a_i$. Write $a_i = b \cdot c + r$ with $c, r \in \mathbb{Z}$, $1 \le r \le b - 1$. Then $r = a_i - b \cdot c = a_i - (a_1\beta_1 + \cdots + a_n\beta_n)c = a_1(-\beta_1 c) + a_2(-\beta_2 c) + \cdots + a_{i-1}(-\beta_{i-1}c) + a_i(1 - \beta_i c) + a_{i+1}(-\beta_{i+1}c) + \cdots + a_n(-\beta_n c)$. A contradiction to the minimality of b.

It is easy to show that the g.c.d. is unique up to the sign, i.e., all the possible g.c.d.'s are just $\pm b$, where b is the number constructed in the proceeding section.

In general, if $a_1, \ldots, a_n$ are integers, we define a g.c.d. of $a_1, \ldots, a_n$ to be a g.c.d. of the non-zero elements in $\{a_1, \ldots, a_n\}$.

(2) We can define an l.c.m. of $a_1, \ldots, a_n$ in ad hoc ways. To prove the existence, we define b as $b = [\cdots[[a_1, a_2], a_3], \ldots, a_n]$. It is routine to check by induction on n that b satisfies the conditions (i) and (ii) in the definition of an l.c.m. □

Remark. Alternatively we can simply define an l.c.m. of $a_1, \ldots, a_n$ to be $[\cdots[[a_1, a_2], a_3],$ $\ldots, a_n]$. Hence it is desirable to show that such a definition doesn't depend on the ordering. It is the reason why we don't adopt this approach in our proof.