Solutions of Exercises – Module II

Exercise 1. Suppose $a\,b = b\,a = c\,a = a\,c = e$

Then $b = e\,b = (c\,a)\,b = c\,(a\,b) = c\,e = c$

Exercise 2. First realize that if $a, b \in T$ then

$$(a\,b)\,(b^{-1}\,a^{-1}) = a(b\,b^{-1})a^{-1} = a\,e\,a^{-1} = e$$

and $$(b^{-1}\,a^{-1})\,(ab) = b^{-1}\,(a^{-1}\,a)\,b = b^{-1}\,e\,b = e$$

so $a\,b \in T$ and T is closed with respect to the operation. Associativity holds in T since it holds in S. Of course $e\,e = e$ implies that $e \in T$ and

$$a^{-1}\,a = a\,a^{-1} = e$$

implies that $(a^{-1})^{-1} = a$. Thus $a \in T$ implies that $a^{-1} \in T$.

Exercise 4. Since $|R| \geq 2$, $0 \neq 1$. By Exercise 3

$$a\,0 = 0 \neq 1$$

$\forall a \in R$. Then $0 \notin U$ and $U \subseteq R - \{0\}$. Note, however, that we cannot use Exercise 2, since $R - \{0\}$ may NOT be closed with respect to the operation, i.e. there may exist $a, b \in R - \{0\}$ such that $ab = 0$. NEVERTHELESS, the steps of Exercise 2 may be repeated verbatim to obtain U is a group.

Exercise 5 c) $n \mid b - c \;\Rightarrow\; b = q\,n + c$ so $d \mid b, n \;\Leftrightarrow\; d \mid c, n$

d) $p \mid a^2 - b^2 = (a - b)\,(a + b) \;\Rightarrow\; p \mid a - b$ or $p \mid a + b$

e) Suppose $f(x) = \sum_{i=0}^{m} a_i\, x^i$ and $\sum_{i=0}^{m} a_i\, a^i \equiv k \pmod n$

Consider $\sum_{i=0}^{m} a_i (a + tn)^i$. If $i \geq 1$

$$(a + tn)^i = a^i + \sum_{j=1}^{i} \binom{i}{j} t^j\, n^j a^{i=j}$$

$$\equiv a^i \pmod n$$

Thus $\sum_{i=0}^{m} a_i(a+t\,n)^i = a_0 + \sum_{i=1}^{m} a_i(a+t\,n)^i$

$$\equiv a_0(\text{mod } n) + \sum_{i=1}^{m} \left[a_i\; a^i(\text{mod } n)\right]$$
$$= f(a)\ (\text{mod } n)$$
$$= \ k\ (\text{mod } n)$$

Exercise 6a) $Z_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$

Exercise 7) Observe that $n = 420$, $\left(\frac{n}{5}\right)^{-1}$ mod $5 = 4$, $\left(\frac{n}{7}\right)^{-1}$ mod $7 = 2$

and $\left(\frac{n}{12}\right)^{-1}$ mod $12 = 11$. Therefore

$$\hat{x} = 3(84)(4) + 3\,(60)(2) + 5\,(35)\,(11) = 3293$$

so that $x = 353$.

Exercise 9) We assume that if ord a_1, ord a_2,.., ord a_{k-1} are pairwise relatively prime and $a_1, a_2, .., a_{k-1}$ commute in pairs then

$$\text{ord}\ (a_1\ a_2,..,\ a_{k-1}) = \prod_{i=1}^{k-1} \text{ord}\ a_i$$

Next consider $a_1,\ a_2,..,\ a_{k-1},\ a_k$ which commute in pairs and have orders which are pairwise relatively prime.

Suppose

$$d = \gcd\ (\text{ord}(\prod_{i=1}^{k-1} a_i),\ \text{ord}\ a_k).$$

Then, since

$$\text{ord}(\prod_{i=0}^{k-1} a_i) = \prod_{i=1}^{k-1} \text{ord}\ (a_i)$$

and $\text{ord}(a),..,\ \text{ord}(a_k)$, are pairwise relatively prime

$\exists i$ such that $d \mid \text{ord}\ a_i$. But then $d \mid \text{ord}\ a_i,\ \text{ord}\ a_k \Rightarrow d = 1$

Also

$$(a_1\ a_2 \cdots a_{k-1})a_k = a_1 \cdot\cdot a_{k-2}\ a_k\ a_{k-1}$$
$$= \cdots = a_k \cdot (a_1,.., a_{k-1})$$

by induction so we may conclude from the $k = 2$ case that

$$\text{ord}\ (a_1 \cdots a_{k-1}\ a_k) = \text{ord}(a_1 \cdots a_{k-1})\ \text{ord}(a_k)$$
$$= (\prod_{i=1}^{k-1} \text{ord}\ (a_i)$$

9.54

Solutions of Submitted Exercises from Module II
(Exercise 3; 5a and b)

Exercise 3 First

$$a\,0 = a(0+0) = a\,0 + a\,0$$

so

$$\begin{aligned} 0 = a\,0 + (-(a\,0)) &= (a\cdot 0 + a\,0) + (-(a\,0)) \\ &= a\cdot 0 + (a\,0 + (-(a\,0))) \\ &= a\,0 + 0 \\ &= a\,0 \end{aligned}$$

Similarly $0\,a = 0$

Next suppose $|R| \geq 2$ so $\exists\, a \in R$ such that $a \neq 0$. If $1 = 0$ then $a = a\,1 = a\,0 = 0$ - a contradiction

Exercise 5 a) *i)* $a \equiv b \pmod{n} \Leftrightarrow n \mid a-b \Leftrightarrow n \mid b-a$

$\Leftrightarrow b \equiv a \pmod{n}$. Also

$n \mid a-b \Leftrightarrow n \mid (a-b)-0 \Leftrightarrow a-b \equiv 0 \pmod{n}$

ii) $n \mid a-b$ and $n \mid b-c \Rightarrow n \mid a-c = (a-b)+(b-c)$

iii) $a+c-(b+d) = (a-b)+(c-d)$

so $n \mid a-b$ and $n \mid c\text{-}d \Rightarrow n \mid [a+c-(b+d)]$

$a\,c - db = (a-b)\,c + b(c-d)$

$\Rightarrow n \mid (ac\text{-}bd)$

iv) $n \mid a-b$ and $d \mid n \Rightarrow d \mid a-b$

v) $n \mid a-b \Rightarrow n\,c \mid ac-bc = (a-b)c$

Exercise 5 b) *i)* Let $n = \alpha \gcd(a, n)$

Suppose $x \equiv y \pmod{\alpha}$ i.e. $\alpha \mid x\text{-}y$

But $\gcd(a, n) \mid a$ so

$n = \alpha \gcd(a, n) \mid ax - ay = a(x-y)$

Conversely if $n = \alpha \gcd(a, n)$ and $a = \beta \gcd(a,n)$ then $\gcd(\alpha,\beta) = 1$. Now $\exists\, \delta \in Z$ such that

$\beta\gcd(a,n)\,(x-y) = a, (x-y) = \delta\, \alpha \gcd(a, n)$. Hence $\beta(x-y) = \alpha\delta$

so $\alpha \mid \beta(x-y)$ and therefore $\alpha \mid x-y$ i.e. $x \equiv y \bmod (\alpha)$

ii) follows immediately from i)

iii)If $n_i \mid x - y \quad i = 1,.., k$ then $x - y$ is a common multiple of each n_i.
Hence $x - y$ is a multiple of $\ell cm\,(n_1,..,n_k)$

Conversely $\ell cm\,(n_1,..,n_k) \mid x - y$

and $n_i \mid \ell cm(n_1,.., n_k) \Rightarrow n_i \mid x - y \quad i = 1,.., k$

iv) follows from *iii*) and $\ell cm(n_1,.., n_k) = \prod_{i=1}^{k} n_i$ when the n_i are pairwise relatively prime.

Exercise 5 a) Base case: $k = 2$. Suppose $a_1 | b$, $a_2 | b$ and $\gcd(a_1, a_2) = 1$.

Then $\ell cm(a_1, a_2) = a_1 a_2$ so $a_1 a_2 | b$ because the least common multiple must divide every other common multiple.

<u>Induction hypothesis:</u> If $\gcd(a_i, a_j) = 1$ for $1 \le i < j \le k$ and $a_i | b$ for $i = 1, \ldots, k$ then $\prod_{i=1}^{k} a_i | b$.

<u>Induction step:</u> Suppose $\gcd(a_i, a_j) = 1$ for $1 \le i < j \le k+1$ and $a_i | b$ for $i = 1, \ldots, k, k+1$. Then $\prod_{i=1}^{k} a_i | b$ by the hypothesis

But $\gcd(\prod_{i=1}^{k} a_i, a_{k+1}) = 1$ by Exercise 4 so $\prod_{i=1}^{k+1} a_i | b$ by the result for $k = 2$.

Exercise 6 b) Here we apply the extended Euclidean algorithm:

STEPS	q_3	r	x_3	y_3	a	b	x_2	x_1	y_2	y_1
2					3587	1819	0	1	1	0
1st 3	1	1768	1	−1	1819	1768	1	0	−1	1
2nd 3	1	51	-1	2	1768	51	-1	1	2	-1
3rd 3	34	34	35	−69	51	34	35	−1	−69	2
4th 3	1	17	−36	71	34	17	−36	35	71	−69
5th 3	2	0			17	0		-36		71

so $d = 17$, $x = -36$, $y = 71$

Check: $\frac{3587}{17} = 211$, $\frac{1819}{17} = 1$

$(3587)(-36) + (1819)(71) = -129132 + 129\,149 = 17$

An Application of the Chinese Remainder Theorem

A person's age can be determined to within a congruence by the following procedure:

Determine the remainders r_3, r_4 and r_5 obtained by dividing the age x by 3, 4 and 5 respectively

Then

$$x \equiv$$

Proof Consider

$$x \equiv r_3 \pmod 3$$

$$x \equiv r_4 \pmod 4$$

$$x \equiv r_5 \pmod 5$$

Then, by the Chinese Remainder Theorem,

$$x \equiv r_3 (20)(20^{-1} \bmod 3) + r_4 (15)(15^{-1} \bmod 4)$$

$$+ r_5 (12)(12^{-1} \bmod 5)$$

$$= 40 r_3 + 45 r_4 + 36 r_5$$

Example Age $= 40$ so $r_3 = 1, r_4 = 0, r_5 = 0$

and $x = 40 \equiv 40$