ETH Zürich, D-INFK
HS 2020, 11. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Solution 8

8.1 Multiplicative Inverses

a) The inverse of a is $R_m(u)$, because $a \cdot R_m(u) \equiv_m au \equiv_m 1 - vm \equiv_m 1$.

b) We first compute $\gcd(142, 553)$, using Lemma 4.2. Notice that dividing 553 by 142, we get

$$553 = 3 \cdot 142 + 127. \tag{1}$$

Hence, by Lemma 4.2 (setting $m = 142$ and $n = 553$), we have $\gcd(142, 553) = \gcd(142, 127)$. We then repeat this trick:

$$142 = 127 + 15 \tag{2}$$

$$127 = 8 \cdot 15 + 7 \tag{3}$$

$$15 = 2 \cdot 7 + 1 \tag{4}$$

Therefore, $\gcd(142, 553) = \gcd(142, 127) = \gcd(127, 15) = \gcd(15, 7) = \gcd(7, 1) = 1$. We now notice that rearranging Equations (1) to (4) allows us to find u and v such that $1 = 142u + 553v$ as follows:

$$\begin{aligned}
1 &\overset{(4)}{=} 15 - 2 \cdot 7 \\
&\overset{(3)}{=} 15 - 2 \cdot (127 - 8 \cdot 15) = (-2) \cdot 127 + 17 \cdot 15 \\
&\overset{(2)}{=} (-2) \cdot 127 + 17 \cdot (142 - 127) = 17 \cdot 142 - 19 \cdot 127 \\
&\overset{(1)}{=} 17 \cdot 142 - 19 \cdot (553 - 3 \cdot 142) = 74 \cdot 142 - 19 \cdot 553
\end{aligned}$$

Therefore, the multiplicative inverse of 142 modulo 553 is $R_{553}(74) = 74$.

Note: The above method can be generalized to efficiently compute, for any given a and b, values u and v, such that $\gcd(a, b) = ua + vb$. The resulting algorithm is called the extended Euclid's gcd-algorithm. Moreover, since an integer a has the multiplicative inverse modulo m if and only if $\gcd(a, m) = 1$, this algorithm allows to efficiently compute the multiplicative inverse of any number (or conclude that the inverse does not exist).

8.2 Adding Digits of q-ary Numbers

a) The claim is trivially true for $q = 2$, since we have $R_1(n) = 0$ for all $n \in \mathbb{N}$. For $q > 2$, we use modular arithmetic (Corollary 4.17) to see that

$$\begin{aligned} R_{q-1}(n) &= R_{q-1}\left(\sum_{i\in\{0,\ldots,k\}} q^i \cdot a_i\right) \\ &= R_{q-1}\left(\sum_{i\in\{0,\ldots,k\}} R_{q-1}(q)^i \cdot a_i\right) \\ &= R_{q-1}\left(\sum_{i\in\{0,\ldots,k\}} 1^i \cdot a_i\right) \\ &= R_{q-1}\left(\sum_{i\in\{0,\ldots,k\}} a_i\right). \end{aligned}$$

b) We have

$$\begin{aligned} &\sum_{i\in\{0,\ldots,k\}} a_i = \sum_{i\in\{0,\ldots,k\}} b_i \\ &\qquad\Longrightarrow R_{q-1}(n) = R_{q-1}(2n) && \text{(Subtask a))} \\ &\qquad\Longrightarrow n \equiv_{q-1} 2n && \text{(Lemma 4.16)} \\ &\qquad\Longrightarrow (q-1) \mid (n-2n) && \text{(Def. } \equiv_{q-1}\text{)} \\ &\qquad\Longrightarrow (q-1) \mid -n \\ &\qquad\Longrightarrow (q-1) \mid n. \end{aligned}$$

8.3 Solution of a Congruence Equation

a) Take any $a, b, m \in \mathbb{Z}$, such that $m > 0$.

$$\begin{aligned} &ax \equiv_m b \text{ for some } x \in \mathbb{Z} \\ &\qquad\Longleftrightarrow ax - b = km \text{ for some } x, k \in \mathbb{Z} && \text{(def. } \equiv_m\text{)} \\ &\qquad\Longleftrightarrow ax + (-k)m = b \text{ for some } x, k \in \mathbb{Z} \\ &\qquad\Longleftrightarrow b \in (a, m) && \text{(def. of the ideal)} \\ &\qquad\Longleftrightarrow b \in (d), \text{ where } d = \gcd(a, m) && \text{(Lemmas 4.3 and 4.4)} \\ &\qquad\Longleftrightarrow b = u \cdot \gcd(a, m) \text{ for some } u \in \mathbb{Z} && \text{(def. of the ideal)} \\ &\qquad\Longleftrightarrow \gcd(a, m) \mid b \end{aligned}$$

8.4 The Chinese Remainder Theorem

a) $\Longrightarrow$: Assume that $a \equiv_{nm} b$. This means that there exists a $k \in \mathbb{Z}$ such that $a - b = k(nm)$. Therefore, $a - b = (km)n$ and, thus, $a \equiv_n b$. Analogously, we get $a \equiv_m b$.

$\Longleftarrow$: Assume that $a \equiv_n b \wedge a \equiv_m b$. Now consider the system of congruence equations $x \equiv_n R_n(b) \ \wedge \ x \equiv_m R_m(b)$. By Lemma 4.16, we have $a \equiv_n b \ \wedge \ a \equiv_m b \Longleftrightarrow a \equiv_n$

$R_n(b) \;\wedge\; a \equiv_m R_m(b)$. Hence, by the assumption, $x = a$ is a solution to the system of congruence equations. Analogously, $x = b$ is also a valid solution.

Since $\gcd(n, m) = 1$, it follows from the Chinese Remainder Theorem that all solutions for x are congruent modulo nm. Therefore, we must have $a \equiv_{nm} b$.

b) Since m and n are not relatively prime, we cannot apply directly the Chinese Remainder Theorem. Therefore, we will transform the system of congruence equations.

By subtask a), the following system of congruence equations is equivalent:

$$x \equiv_a y_1 \tag{1}$$
$$x \equiv_b y_1 \tag{2}$$
$$x \equiv_a y_2 \tag{3}$$
$$x \equiv_c y_2 \tag{4}$$

If $y_1 \not\equiv_a y_2$, there are clearly no solutions. Otherwise, the equations (1) and (3) are equivalent and we can remove (3). By Lemma 4.16, we get the following equivalent system of congruence equations:

$$\begin{aligned} x &\equiv_a R_a(y_1) \\ x &\equiv_b R_b(y_1) \\ x &\equiv_c R_c(y_2) \end{aligned}$$

Since a, b, c are pairwise relatively prime, the Chinese Remainder Theorem guarantees that there exists a unique solution x_0 such that $0 \leq x_0 < abc$. All remaining solutions must be of the form $x_0 + k(abc)$ for $k \in \mathbb{N}$. Since $nm = a^2bc$, there exist exactly a solutions x such that $0 \leq x < nm$.

8.5 Algebras

a) $\langle \mathbb{Z}; \star \rangle$ is neither a group nor a monoid, because $\star$ is not associative. The counterexample is the following:

$$2 \star (0 \star 0) = 2 \star 0 = 4 \neq 16 = 4 \star 0 = (2 \star 0) \star 0$$

b) $\langle \mathcal{P}(X); \cup \rangle$ is a commutative monoid but not a group.

Associativity and commutativity of $\cup$ follow directly from Theorem 3.4. The neutral element is $\varnothing$, because (1) $A \cup \varnothing = \varnothing \cup A = A$ for all A and (2) $\varnothing \in \mathcal{P}(X)$, since $\varnothing \subseteq X$ for any X.

To prove that it is not a group, we give a counterexample to **G3**. Since $X \neq \varnothing$, there exists an $x \in X$. Therefore, $\{x\} \in \mathcal{P}(X)$. Assume for contradiction that there exists an inverse element of $\{x\}$, that is, assume that there exists an $A \in \mathcal{P}(X)$ such that $\{x\} \cup A = \varnothing$. But since $x \in \{x\} \cup A$, this is a contradiction.

8.6 Facts About Groups

a) We have to show that e is also a left neutral element. For any $a \in G$, we have

$$e * a \overset{\textbf{G3}}{=} (a * \widehat{a}) * a \overset{\textbf{G1}}{=} a * (\widehat{a} * a) \overset{\textbf{G3}}{=} a * e \overset{\textbf{G2'}}{=} a$$

b) We have to show that $\widehat{b} * \widehat{a}$ is the right inverse of $a * b$, that is, that $(a * b) * (\widehat{b} * \widehat{a}) = e$ (as proved in the lecture notes, this implies that $(\widehat{b} * \widehat{a}) * (a * b) = e$).

$$(a * b) * (\widehat{b} * \widehat{a}) \overset{\textbf{G1}}{=} a * \Big(b * (\widehat{b} * \widehat{a})\Big) \overset{\textbf{G1}}{=} a * \Big((b * \widehat{b}) * \widehat{a}\Big) \overset{\textbf{G3}}{=} a * (e * \widehat{a}) \overset{\textbf{G2}}{=} a * \widehat{a} \overset{\textbf{G3}}{=} e$$

c) For any $a, b, c \in G$, we have

$$\begin{aligned} a * b = a * c &\overset{\textbf{G3}}{\Longrightarrow} \widehat{a} * (a * b) = \widehat{a} * (a * c) \\ &\overset{\textbf{G1}}{\Longrightarrow} (\widehat{a} * a) * b = (\widehat{a} * a) * c \\ &\overset{\textbf{G3}}{\Longrightarrow} e * b = e * c \\ &\overset{\textbf{G2}}{\Longrightarrow} b = c \end{aligned}$$