ETH Zürich, D-INFK
HS 2023, 10. November 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Solution 7

7.1 The Greatest Common Divisor

Let $a, b, u, v \in \mathbb{Z} \setminus \{0\}$ be such that $ua + vb = 1$ and let $d = \gcd(a, b)$. By the definition of $\gcd$, we have $d \mid a$ and $d \mid b$. That is, there exist $k, l \in \mathbb{Z}$ such that $a = kd$ and $b = ld$.

Hence, $1 = ua + vb = ukd + vld = (uk + vl)d$. Thus, $d \mid 1$.

Since 1 is the only positive divisor of 1, it follows that $d = 1$.

7.2 Geometric Interpretation of the Greatest Common Divisor

Remark: a proof that assumes the steps in the footnotes without proof would still be considered valid in an exam situation.

Consider the line in the Cartesian plane through $(0, 0)$ and (a, b) which has equation

$$y = \frac{b}{a}x.$$

Let $d = \gcd(a, b)$. By definition, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, so that we can write $a = d \cdot k_1$ and $b = d \cdot k_2$ for some $k_1, k_2 \in \mathbb{Z}$. Since a, b are positive and d is positive, then k_1 and k_2 must be positive. Therefore. we get

$$y = \frac{b}{a}x \iff y = \frac{k_2}{k_1}x.$$

Observe that $\gcd(k_1, k_2) = 1$.[1] Assume that (x, y) is an integer solution to the equation. This means that $k_1 \cdot y = k_2 \cdot x$, or that in other words $k_1 \mid x \cdot k_2$. Since $\gcd(k_1, k_2) = 1$, this implies $k_1 \mid x$.[2] We are only interested in points lying in the segment with endpoints $(0, 0)$ and (a, b), so that necessarily $0 \leq x \leq a = k_1 \cdot d$. There are exactly $d + 1$ multiples of k_1 between 0 and $k_1 \cdot d$, namely

$$\{0, k_1, 2 \cdot k_1, \ldots, d \cdot k_1\}.$$

This shows that there are *at most* $\gcd(a, b)+1$ integer solutions to the equation above. However, clearly we can plug each of these values for x in the equation to find a corresponding point on the segment with integer coordinates. This proves the claim.

[1] Indeed, assume that this is not true, and let $1 < e = \gcd(k_1, k_2)$. By definition, $\gcd(k_1, k_2) \mid k_2$ and $\gcd(k_1, k_2) \mid k_2$, so that we can write $k_1 = e \cdot k_3$ and $k_2 = e \cdot k_4$ for some $k_3, k_3 \in \mathbb{Z}$. We have $a = k_1 \cdot d = (k_3 \cdot e) \cdot d = k_3 \cdot d^2$ and $a = k_1 \cdot d = (k_4 \cdot e) \cdot d = k_4 \cdot d^2$. Therefore, $e \cdot d \mid a$ and $e \cdot d \mid b$, which means that $e \cdot d \mid d$ by definition of $\gcd$. However, since $e > 1$ we have $e \cdot d > d$, a contradiction. This proves $\gcd(k_1, k_2) = 1$.

[2] This is easily seen by considering the prime factorizations of k_1, k_2, x, and $k_2 \cdot x$. Indeed, by the uniqueness of the factorization each prime factor of k_1 must be a factor of either k_2 or x. It cannot be a factor of k_2 because this would contradict $\gcd(k_1, k_2) = 1$, and therefore it must be a factor of x.

7.3 Properties of Greatest Common Divisor

Consider the unique prime factorizations $a = \prod_i p_i^{e_i}$, $b = \prod_i p_i^{f_i}$, and $c = \prod_i p_i^{g_i}$ (notice that only finitely many exponents are non-zero). We have

$$\begin{aligned}
\gcd\big(a, \operatorname{lcm}(b,c)\big) &= \gcd\left(a, \prod_i p_i^{\max(f_i,g_i)}\right) && \text{(Section 4.3.3)}\\
&= \prod_i p_i^{\min\left(e_i, \max(f_i,g_i)\right)} && \text{(Section 4.3.3)}\\
&= \prod_i p_i^{\max\left(\min(e_i,f_i), \min(e_i,g_i)\right)} && (*)\\
&= \operatorname{lcm}\left(\prod_i p_i^{\min(e_i,f_i)}, \prod_i p_i^{\min(e_i,g_i)}\right) && \text{(Section 4.3.3)}\\
&= \operatorname{lcm}\big(\gcd(a,b), \gcd(a,c)\big). && \text{(Section 4.3.3)}
\end{aligned}$$

Proof of $(*)$**:** we show that for all $x, y, z \in \mathbb{N}$

$$\min\big(x, \max(y,z)\big) = \max\big(\min(x,y), \min(x,z)\big). \tag{1}$$

Suppose, without loss of generality that $y \leq z$ (else, replace y by z). We distinguish a few cases:

- ($x \leq y$) Since $y \leq x$ in this case the left hand side of equation (1) is $\min(x,z) = x$. On the right hand side we get $\max(x,x) = x$.
- ($y \leq x \leq z$). In this case, since $\max(y,z) = z$, on the left hand side of equation 1 we get $\min(x,z) = x$. On the right hand side we get $\max(y,x)$ which is again x.
- ($y \leq z \leq x$). In this case, on the left hand side of the equation we get $\min(x,z) = z$. On the right hand side we get $\max(y,z)$ which is again z.

This concludes the proof of $(*)$.

7.4 Congruences

a) Take arbitrary $m, n \in \mathbb{N}$. By Lemma 4.14 we have

$$123^m - 33^n \equiv_{10} 3^m - 3^n.$$

Assume without loss of generality that $m \leq n$. If $m \equiv_4 n$, then there exists a $k \in \mathbb{N}$, such that $n - m = 4k$ and by Lemma 4.14, we have:

$$\begin{aligned}
3^m - 3^n &\equiv_{10} 3^m(1 - 3^{n-m}) \equiv_{10} 3^m(1 - 3^{4k}) \equiv_{10} 3^m(1 - 9^{2k})\\
&\equiv_{10} 3^m(1 - (-1)^{2k}) \equiv_{10} 3^m(1 - 1^k) \equiv_{10} 3^m \cdot 0 \equiv_{10} 0.
\end{aligned}$$

b) Take any $a, b, c, d, m \in \mathbb{Z}$, such that $m > 0$. Assume that $a \equiv_m b$ and $c \equiv_m d$. Then, there exist $s, t \in \mathbb{Z}$ such that $a - b = ms$ and $c - d = mt$. It follows that

$$ac = (ms + b)(mt + d) = m^2st + msd + mtb + bd = m(mst + sd + tb) + bd.$$

Therefore, $m \mid ac - bd$, so $ac \equiv_m bd$.

c) Consider all possible remainders $R_{11}(n^5 + 7)$ and $R_{11}(m^2)$ when $m, n \in \mathbb{Z}$. By Corollary 4.17, we have $R_{11}(n^5 + 7) = R_{11}((R_{11}(n))^5 + 7)$ and $R_{11}(m^2) = R_{11}((R_{11}(m))^2)$. By trying all ten possibilities for $R_{11}(n)$ and, respectively, for $R_{11}(m)$, we get that $R_{11}(n^5 + 7) \in \{6, 7, 8\}$ and $R_{11}(m^2) \in \{0, 1, 3, 4, 5, 9\}$. Since these sets are disjoint, $n^5 + 7$ cannot be equal to m^2.

7.5 Modular Arithmetic

a) Take any even $n \geq 0$ and let $k \in \mathbb{N}$ be such that $n = 2k$. By Corollary 4.17, we have $R_7(13^n+6) = R_7(R_7(13)^n+6) = R_7(R_7(-1)^n+6) = R_7((-1)^n+6) = R_7((-1)^{2k}+6) = R_7(7) = 0$. Hence, $7 \mid 13^n + 6$.

b) Let $a, e, m, n \in \mathbb{N} \setminus \{0\}$ and assume that $R_m(a^e) = 1$. By Theorem 4.1, there exists a $q \in \mathbb{N}$, such that $n = qe + R_e(n)$. Therefore,

$$\begin{aligned}
R_m(a^n) &= R_m\left(a^{qe+R_e(n)}\right) \\
&= R_m\left((a^e)^q \cdot a^{R_e(n)}\right) \\
&= R_m\left(\left(R_m\left(a^e\right)\right)^q \cdot R_m\left(a^{R_e(n)}\right)\right) && \text{(Corollary 4.17)} \\
&= R_m\left(1^q \cdot R_m\left(a^{R_e(n)}\right)\right) && (R_m(a^e) = 1) \\
&= R_m\left(R_m(1)^q \cdot R_m\left(a^{R_e(n)}\right)\right) \\
&= R_m\left(a^{R_e(n)}\right). && \text{(Corollary 4.17)}
\end{aligned}$$

c) We first compute $2023 \equiv_{12} 2023 - 1800 \equiv_{12} 223 \equiv_{12} 223 - 180 \equiv_{12} 43 \equiv_{12} 7$. By Subtask b), $R_{13}(2^{2023}) = R_{13}(2^{R_{12}(2023)}) = R_{13}(2^7)$. Now we have $2^7 \equiv_{13} 128 \equiv_{13} 11$.

7.6 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

$$553 = 3 \cdot 142 + 127. \tag{2}$$

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

$$142 = 127 + 15 \tag{3}$$

$$127 = 8 \cdot 15 + 7 \tag{4}$$

$$15 = 2 \cdot 7 + 1 \tag{5}$$

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).

7.7 Solution of a Congruence Equation

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

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

7.8 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 $a \equiv_n b \ \wedge \ a \equiv_m b \iff a \equiv_n R_n(b) \ \wedge \ a \equiv_m R_m(b)$. 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:

$$x \equiv_a R_a(y_1)$$
$$x \equiv_b R_b(y_1)$$
$$x \equiv_c R_c(y_2)$$

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 $0 \leq x < nm$.