Solutions to Exercise Sheet 2

Solution 2.1. *Solving linear equations.*

(1) We use the Euclidean algorithm to compute $\mathrm{hcf}(140, 84)$ and decide if the equation has a solution.

$$140 = 84 \times 1 + 56;$$
$$84 = 56 \times 1 + 28;$$
$$56 = 28 \times 2 + 0.$$

Hence $\mathrm{hcf}(140, 84) = 28$, which does not divide 98. By Proposition 2.5, the equation has no solution.

(2) By Euclidean algorithm, we can find $\mathrm{hcf}(28, 116)$.

$$116 = 28 \times 4 + 4;$$
$$28 = 4 \times 7 + 0.$$

Hence $\mathrm{hcf}(28, 116) = 4$, which divides 124. So the equation has 4 solutions modulo 116. We can solve it first by cancelling 4 to get $7x \equiv 31 \pmod{29}$, which reduces to $7x \equiv 2 \pmod{29}$. Now we use Euclidean algorithm for the pair 7 and 29.

$$29 = 7 \times 4 + 1;$$
$$7 = 1 \times 7 + 0.$$

So we simply have $1 = 29 - 7 \times 4$ hence $7 \times (-4) \equiv 1 \pmod{29}$. Multiply both sides by 2 to get $7 \times (-8) \equiv 2 \pmod{29}$. Since we usually prefer to use positive numbers as representatives of congruence classes, we add 29 to -8 to get 21. Hence $x \equiv 21 \pmod{29}$. To get solutions modulo 116, we keep adding 29 to 21 until we get repeated congruence classes. So we have $x \equiv 21, 50, 79 \text{ or } 108 \pmod{116}$, which are all solutions to the original equation.

(3) We write it as a congruence equation $12x \equiv 17 \pmod{7}$. Since $\mathrm{hcf}(12, 7) = 1$, we should have a unique solution to it. To solve the equation we can add multiples of 7 to 17 until we can cancel the coefficient 12. Hence we have $12x \equiv 24 \pmod{7}$, then $x \equiv 2 \pmod{7}$. We write $x = 7k+2$ for an arbitrary $k \in \mathbb{Z}$, then substitute x in the original equation to get $12(7k+2)+7y = 17$. Therefore we have $7y = -84k-7$ thus $y = -12k - 1$. The solutions to the original equation is $x = 7k + 2, y = -12k - 1$ for an arbitrary $k \in \mathbb{Z}$.

(4) For simplicity we write $d = \mathrm{hcf}(a, b)$. For one direction, assume that $ax + by = c$ has a solution $x = x_0$ and $y = y_0$. Then $ax_0 + by_0 = c$. Since $d \mid a$ and $d \mid b$, we know $d \mid (ax + by)$, which gives $d \mid c$. For the other direction, assume $d \mid c$, then we can write $c = dc'$ for some integer c'. Since $d = \mathrm{hcf}(a, b)$, we can find

integers x_0' and y_0', such that $ax_0' + by_0' = d$ (for example, by Euclidean algorithm). Multiply both sides by c', then we get $ax_0'c' + by_0'c' = dc' = c$. Therefore $x = x_0'c'$ and $y = y_0'c'$ is a solution.

Solution 2.2. *Solving systems of linear equations.*

(1) We find a common solution to the first two equations. From the first equation we can write $x = 7q + 1$. Substituting x in the second equation to get $7q + 1 \equiv 4 \pmod 9$, hence $7q \equiv 3 \pmod 9$. Adding 18 to 3 and we get $7q \equiv 21 \pmod 9$, hence $q \equiv 3 \pmod 9$. Write $q = 9r + 3$ to get $x = 7(9r + 3) + 1 = 63r + 22$. So the solution to the first two equations is $x \equiv 22 \pmod{63}$. Now we bring the third equation into the question. By substitution we get $63r + 22 \equiv -2 \pmod 5$, hence $63r \equiv -24 \pmod 5$. We reduce it to $3r \equiv 1 \pmod 5$, hence $3r \equiv 6 \pmod 5$, which gives $r \equiv 2 \pmod 5$. Write $r = 5s+2$ to get $x = 63(5s+2)+22 = 315s+148$. So the solution to the original system is $x \equiv 148 \pmod{315}$.

(2) Since $\mathrm{hcf}(4, 13) = 1$ divides 6 and $\mathrm{hcf}(6, 8) = 2$ divides 4, both equations have solutions. From $4x \equiv 6 \pmod{13}$ we get $4x \equiv 32 \pmod{13}$ hence $x \equiv 8 \pmod{13}$. Write $x = 13q + 8$ and substitute x in the second equation to get $6(13q + 8) \equiv 4 \pmod 8$. We write it as $78q \equiv -44 \pmod 8$ and reduce it to $6q \equiv 4 \pmod 8$. By cancelling 2 we get $3q \equiv 2 \pmod 4$. By adding 4 to 2 we get $3q \equiv 6 \pmod 4$ hence $q \equiv 2 \pmod 4$. We write $q = 4r + 2$, then $x = 13(4r + 2) + 8 = 52r + 34$. So the solution is $x \equiv 34 \pmod{52}$.

Remark: you might ask if the result is consistent with the Chinese remainder theorem because the modulus is not $13 \times 8 = 104$. In fact, the solution to the first equation is $x \equiv 8 \pmod{13}$. And the second equation has two solutions $x \equiv 2 \pmod 8$ and $x \equiv 6 \pmod 8$. By the Chinese remainder theorem, they combine to give two solutions to the original system, which are $x \equiv 34 \pmod{104}$ and $x \equiv 86 \pmod{104}$. They can be represented by a single congruence $x \equiv 34 \pmod{52}$.

(3) From the first equation we can write $x = 15q + 7$. We substitute x in the second equation to get $15q + 7 \equiv 5 \pmod 9$. That is $15q \equiv -2 \pmod 9$, which reduces to $6q \equiv 7 \pmod 9$. Notice that $\mathrm{hcf}(6, 9) = 3$ which does not divide 7. By Proposition 2.5, this equation has no solution. Hence so is the original system.

Solution 2.3. *Cancellation law for congruences.*

(1) Since $k \mid m$, we can write $m = km'$ for some integer m'. For one direction, assume $ka \equiv kb \pmod m$. Then there exists some $c \in \mathbb{Z}$ such that $ka - kb = cm$. We divide both sides by k to get $a - b = cm'$, which implies $a \equiv b \pmod{m'}$, as required.

For the other direction, assume $a \equiv b \pmod{m'}$. Then there exists some $c \in \mathbb{Z}$ such that $a - b = cm'$. We multiply both sides by k to get $ka - kb = ckm' = cm$, which implies $ka \equiv kb \pmod{m}$.

(2) Since $ka \equiv kb \pmod{m}$, we know $m \mid (ka - kb) = k(a - b)$. Since $\mathrm{hcf}(k, m) = 1$, we claim that we have $m \mid (a - b)$. Indeed, using the condition $\mathrm{hcf}(k, m) = 1$, we can find some $\alpha, \beta \in \mathbb{Z}$, such that $k\alpha + m\beta = 1$. Multiply both sides by $a - b$ to get $k(a - b)\alpha + m(a - b)\beta = a - b$. Since m divides both terms on the left-hand side, we conclude that m divides the right-hand side; i.e. $m \mid (a - b)$. It follows that $a \equiv b \pmod{m}$.

For the other direction, assume $a \equiv b \pmod{m}$. Then we know $m \mid (a - b)$, hence $m \mid k(a - b) = ka - kb$. It follows that $ka \equiv kb \pmod{m}$.

(3) Since $\mathrm{hcf}(k, m) = d$, we can write $k = dk'$ and $m = dm'$. By Exercise 1.1 (2), we know $\mathrm{hcf}(k', m') = 1$. The condition $ka \equiv kb \pmod{m}$ is equivalent to $dk'a \equiv dk'b \pmod{dm'}$, which is equivalent to $k'a \equiv k'b \pmod{m'}$ by part (1), which is further equivalent to $a \equiv b \pmod{m'}$ by part (2). This proves the equivalence required in question.

Solution 2.4. *Wilson's theorem and beyond.*

(1) We write $S = \{1, 2, \cdots, p - 1\}$. For any $k \in S$, $p \nmid k$ hence $\mathrm{hcf}(k, p) = 1$, which implies $kx \equiv 1 \pmod{p}$ has a unique solution modulo p by Proposition 2.5. Since the congruence class $\overline{0}$ is not the solution, this solution must be a congruence class $\overline{b}$ for some b not divisible by p. This congruence contains exactly one element in the set S, which we call b_k. Therefore this b_k is the unique solution in S to the equation $kx \equiv 1 \pmod{p}$.

(2) When $k = 1$, it is clear that $b_k = 1$ does satisfy the equation $kb_k \equiv 1 \pmod{p}$. When $k = p - 1$, it is also clear that $b_k = p - 1$ satisfy the same equation because $kb_k = (p - 1)(p - 1) \equiv (-1)(-1) = 1 \pmod{p}$.

It remains to show that these are the only values of k which make $k = b_k$. In other words, if $k^2 \equiv 1 \pmod{p}$ is satisfied by some $k \in S$, we want to show that $k = 1$ or $k = p - 1$. Indeed, the equation $k^2 \equiv 1 \pmod{p}$ is equivalent to $p \mid (k^2 - 1) = (k + 1)(k - 1)$, which implies that either $p \mid k + 1$ or $p \mid k - 1$ because p is a prime. If $p \mid k + 1$, then $k \equiv -1 \pmod{p}$, so the only value in S is $k = p - 1$. If $p \mid k - 1$, then $k \equiv 1 \pmod{p}$, so the only value in S is $k = 1$. This shows that the only values for k which make $k = b_k$ are $k = 1$ and $k = p - 1$.

(3) By parts (1) and (2), the set $S \backslash \{1, p - 1\}$ can be divided into pairs, such that the product of the two elements in each pair is congruent to 1 modulo p. Hence the product of all elements in $S \backslash \{1, p - 1\}$ is congruent to 1 modulo p. Taking the

remaining two elements 1 and $p-1$ into consideration, the product of all elements in S is congruent to $p-1$ modulo p, or equivalently, -1 modulo p.

(4) Assume n is composite and $n \neq 4$, then we can write $n = ab$ for some $a, b \in \mathbb{Z}$, $1 < a, b < n$. There are two cases. If $a \neq b$, then a and b appear as distinct factors in $(n-1)!$. Hence $(n-1)!$ is a multiple of ab. In other words, $(n-1)! \equiv 0 \pmod{n}$. If $a = b$, then the assumption implies $a = b \geqslant 3$, hence $2a < ab = n$. Now a and $2a$ appear as distinct factors in $(n-1)!$. Hence $(n-1)!$ is a multiple of $a \cdot 2a = 2ab = 2n$, which implies $(n-1)! \equiv 0 \pmod{n}$. When $n = 4$, we have $(4-1)! = 3! = 6 \equiv 2 \pmod{4}$.

(5) The "if" part is proved in part (3) for odd primes, and is clear for $n = 2$. The contrapositive of the "only if" part is proved in part (4). Therefore the condition $(n-1)! \equiv -1 \pmod{n}$ is equivalent to n being a prime.