Homework 5 Solutions

Problem 1. Find all solutions in $\mathbb{Z}/243\mathbb{Z}$ to the following equations:

a) $18x = 27$,

b) $3x = 3$,

c) $5x = 17$,

d) $6x = 19$.

Is it a valid strategy to simplify such an equation by dividing both sides by the greatest common divisor, for example replacing $18x = 27$ by $2x = 3$? Why/why not?

Solution 1. The equations $18x = 27$ and $2x = 3$ are not entirely equivalent: for example, the first one has 9 solutions and the second one has only a single solution.

However, in a slightly different sense they can be thought of as equivalent: say we want to solve the equation $ax = b$ in $\mathbb{Z}/m\mathbb{Z}$. Let $d = (a, m)$. If $d \nmid b$ there are no solutions, so assume $d \mid b$. So d is a common divisor of a, m and b. Define $a' = a/d$, $b' = b/d$ and $m' = m/d$, and let z be an integer. Then $[z]_m$ is a solution of $ax = b$ if and only if $m \mid (az - b)$, or equivalently $dm' \mid d(a'z - b')$. This is equivalent to $m' \mid a'z - b'$, hence to $[z]_{m'}$ being a solution of $a'x = b'$. The unique solution in fact, since $(a', m') = 1$. So to find the solutions of $ax = b$, it is enough to find the unique solution x of $a'x = b'$ in $\mathbb{Z}/m'\mathbb{Z}$. Once we have it, its lifts to $\mathbb{Z}/m\mathbb{Z}$ are exactly the solutions to $ax = b$.

a) $(18, 243) = 9$ and $9 \mid 27$, so there are 9 solutions. By the above, we can find a solution by instead solving $2x = 3$ in $\mathbb{Z}/27\mathbb{Z}$. It is easy to guess that $x = [15]_{27}$ solves this. So the solutions to $18x = 27$ in $\mathbb{Z}/243\mathbb{Z}$ are

$$[15], [42], [69], [96], [123], [150], [177], [204], [231].$$

b) $(3, 243) = 3$ and $3 \mid 3$, so there are 3 solutions. Clearly $[1]$ is a solution, so all three of them are

$$[1], [82], [163]$$

c) $(5, 243) = 1$, so there is a unique solution. We can get it by computing Bezout coefficients of 243 and 5: $2 \cdot 243 - 97 \cdot 5 = 1$. Multiplying this by 17, we get that $[17 \cdot (-97)]_{243} = [52]_{243}$ is the unique solution.

d) $(6, 243) = 3$ and $3 \nmid 19$, so there is no solution.

Problem 2. Let p be an odd prime and $a \in \mathbb{Z}/p\mathbb{Z}$ with $a \neq 0 \bmod p$. A *square root* of a is a solution $x \in \mathbb{Z}/p\mathbb{Z}$ of the equation $x^2 = a$.

a) Show that every $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0 \bmod p\}$ has either none or exactly two square roots.

b) Conclude that $\mathbb{Z}/p\mathbb{Z}$ has exactly two elements which are their own inverses.

c) Find the square roots of all elements of $\mathbb{Z}/7\mathbb{Z}$, if they exist.

d) Is the statement of a) still true if p is not prime?

Solution 2.

a) Assume that x is a square root of a, that is $x^2 = a$. Then $(-x)^2 = x^2 = a$, so $-x$ is also a square root of a. We claim that $x \neq -x$. Indeed, if $x = -x$, then $2x = [0]_p$, so $x = [0]_p$ because $[2]_p$ is invertible. So if a has a square root, it has at least two of them.

   Now let $y \in \mathbb{Z}/p\mathbb{Z}$ be another square root of a, i.e. $y^2 = a = x^2$. Then $(y-x)(y+x) = 0$. As $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, this means either $y = x$ or $y = -x$. This shows that there are no other square roots than $\pm x$.

b) Being its own inverse is equivalent to being a square root of 1. So by part a) either no elements of $\mathbb{Z}/p\mathbb{Z}$ are their own inverses, or exactly two of them. But we know that $[1]$ is its own inverse, so the first case is impossible, and exactly two elements of $\mathbb{Z}/p\mathbb{Z}$ are their own inverse ($[1]$ and $[-1]$).

c) We just compute

$$[0]^2 = [0], \quad [1]^2 = [1], \quad [2]^2 = [4], \quad [3]^2 = [2], \quad [4]^2 = [2], \quad [5]^2 = [4], \quad [6]^2 = [1],$$

   so only $[1]$, $[4]$, and $[2]$ have square roots (we excluded $[0]$ in the definition). The square roots of $[1]$ are $[1]$ and $[6]$, the square roots of $[4]$ are $[2]$ and $[5]$, and the square roots of $[2]$ are $[3]$ and $[4]$.

d) No. For example, in $\mathbb{Z}/6\mathbb{Z}$ we have

$$[0]^2 = [0], \quad [1]^2 = [1], \quad [2]^2 = [4], \quad [3]^2 = [3], \quad [4]^2 = [4], \quad [5]^2 = [1],$$

   so $[3]$ has only a single square root. On the other hand, in $\mathbb{Z}/8\mathbb{Z}$ we have

$$[1]^2 = [3]^2 = [5]^2 = [7]^2 = [1],$$

   so $[1]$ has four different square roots.

Problem 3. Show that the equation $x^2 = 1$ has one solution in $\mathbb{Z}/2\mathbb{Z}$, two solutions in $\mathbb{Z}/4\mathbb{Z}$ and four solutions in $\mathbb{Z}/2^k\mathbb{Z}$ for all integers $k > 2$.

Solution 3. Assume that $k > 2$. Let $x = [a]_{2^k}$ be such that $x^2 = 1$. Then $(x-1)(x+1) = [0]_{2^k}$, so $2^k \mid (a-1)(a+1)$. This means that for some integer $0 \leq n \leq k$ we have $2^n \mid (a-1)$ and $2^{k-n} \mid (a+1)$. Let $m = \min\{n, k-n\}$. Then 2^m divides both $a-1$ and $a+1$, so it also divides their sum, 2. So $m \in \{0, 1\}$, and therefore $n \in \{0, 1, k-1, k\}$.

If $n = k-1$ then $2^{k-1} \mid (a+1)$. If $n = k$ then $2^k \mid (a+1)$, so also $2^{k-1} \mid (a+1)$. This means that $a = 2^{k-1}q - 1$ for some integer q, so $x = [a]_{2^k} \in \{[-1]_{2^k}, [2^{k-1}-1]_{2^k}\}$.

Similarly, if $n = 0$ or $n = 1$ then $2^{k-1} \mid (a-1)$. So $a = 2^{k-1}q + 1$ for some integer q, and $x \in \{[1]_{2^k}, [2^{k-1}+1]_{2^k}\}$.

So in summary, if $x^2 = 1$ then

$$x \in \{[1], [-1], [2^{k-1}+1], [2^{k-1}-1]\}.$$

We can directly check that each of these is indeed a solution, and they are all different.

The cases of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ and easy to check directly.

Problem 4. Let $a, b, c \in \mathbb{N}$ with

$$a \bmod c = b \bmod c.$$

Show that

$$(2^a - 1) \bmod (2^c - 1) = (2^b - 1) \bmod (2^c - 1).$$

Solution 4. Assume without loss of generality that $a \geq b$. Then $c \mid (a-b)$, so $a-b = kc$ for some (non–negative) integer k. We know that, for any $x \in \mathbb{Z}$,

$$(x-1)(1 + x + \cdots + x^{k-1}) = x^k - 1,$$

so $(x-1) \mid (x^k - 1)$. In particular, for $x = 2^c$ we get that $2^c - 1$ divides $2^{kc} - 1 = 2^{a-b} - 1$, so it also divides

$$(2^a - 1) - (2^b - 1) = 2^a - 2^b = (2^{a-b} - 1)2^b.$$

Problem 5. Find inverses of [1], [2], [3], [4] and [5] in $\mathbb{Z}/8512\mathbb{Z}$, if they exist.

Solution 5. Note that $8512 = 2^6 \cdot 7 \cdot 19$, so $(2, 8512) = 2$ and $(4, 8512) = 4$. So $[2]$ and $[4]$ are not invertible. On the other hand,

$$[1]^{-1} = [1], \qquad [3]^{-1} = [5675], \qquad [5]^{-1} = [3405].$$

These can be found for example by computing the Bezout coefficients:

$$1 = 8512 - 2837 \cdot 3, \qquad 1 = -2 \cdot 8512 + 3405 \cdot 5.$$

So

$$[1] = [-2837] \cdot [3], \qquad [1] = [3405] \cdot [5].$$

Here $[-2837] = [5675]$.