Math 120: Groups and Rings

http://math.stanford.edu/~church/teaching/120-S18

Homework 6 Solutions by Prof. Church

Let R denote the set of *infinite-integers*. For example, here are some elements of R:

$$\begin{aligned} a &= \cdots 000000001 \\ b &= \cdots 000000021 \\ c &= \cdots 000000049 \\ d &= \cdots 123123123 \\ e &= \cdots 593593593 \\ f &= \cdots 999999999 \\ g &= \cdots 562951413 && \text{(digits of } \pi \text{, backwards)} \end{aligned}$$

Question 1. Compute $a + f$, $c + f$, and $d + f$.

Solution.

$$\begin{array}{c} a \\ +f \\ \hline = \end{array} \quad \begin{array}{r} {\scriptstyle 11111111} \\ \cdots 000000001 \\ + \;\; \cdots 999999999 \\ \hline \cdots 000000000 \end{array} \qquad \begin{array}{c} c \\ +f \\ \hline = \end{array} \quad \begin{array}{r} {\scriptstyle 11111111} \\ \cdots 000000049 \\ + \;\; \cdots 999999999 \\ \hline \cdots 000000048 \end{array} \qquad \begin{array}{c} d \\ +f \\ \hline = \end{array} \quad \begin{array}{r} {\scriptstyle 11111111} \\ \cdots 123123123 \\ + \;\; \cdots 999999999 \\ \hline \cdots 123123122 \end{array}$$

In other words, the element $f = \cdots 999999999$ behaves like "-1".

Question 2. Find an element $h \in R$ such that $d + h = \cdots 000000000$.
Show that for any element $x \in R$, there exists some $y \in R$ such that $x + y = \cdots 000000000$.

Solution. Set $h = \cdots 876876877$. Then we can check that h behaves as "$-d$", i.e. that $d + h = 0$, as follows:

$$\begin{array}{rr} d & \cdots \overset{11111111}{123123123} \\ +\,h & + \;\; \cdots 876876877 \\ \hline = & \cdots 000000000 \end{array}$$

In general, given $x \in R$, we can produce its additive inverse $y =$ "$-x$" as follows. Let's say that x_i is the ith digit of x, starting with x_0 being the rightmost digit: $x = \cdots x_8x_7x_6x_5x_4x_3x_2x_1x_0$. Let n be the smallest number with $x_n \neq 0$, so that x ends with a string of n consecutive 0s. (so n could be zero if x ends with a nonzero digit).
Define y as follows:

- The rightmost n digits of y are 0.
- The next digit y_n is $10 - x_n$ (note that $y_n \in \{1, \ldots, 9\}$ since $x_n \neq 0$).
- For the remaining digits, we set $y_k = 9 - x_k$ for all $k > n$ (note that $y_k \in \{0, 1, \ldots, 9\}$ since $x_k \in \{0, 1, \ldots, 9\}$).

For example, if $x = \cdots 35353535000$, we would set $y = \cdots 64646465000$. When we add these, we get

$$\begin{array}{rr} x & \cdots \overset{1111111}{35353535000} \\ +\,y & + \;\; \cdots 64646465000 \\ \hline = & \cdots 00000000000 \end{array}$$

Why does this work in general? Say that y is defined in terms of x as above, and set $z = x + y$.

- The last n digits of x and y are 0, so the last n digits of z are 0.
- In the next digit we have $y_n = 10 - x_n$. When we add these, we get $x_n + y_n = 10$; therefore z_n is 0, and we carry a 1 to the next digit.
- In the next digit to the left, we have $y_{n+1} = 9 - x_{n+1}$, plus the 1 that we just carried. So we add these and get $x_{n+1} + y_{n+1} + 1 = 10$; therefore $z_{n+1} = 0$, and we carry a 1 to the next digit to the left.
- This pattern continues to all following digits; we always carry a 1 from the digit on the right, and $x_k + y_k = 9$; so $z_k = 0$ and we carry a 1 to the next digit to the left.

Therefore all the digits of $z = x + y$ are 0, as desired.

Question 3. Find an element $s \in R$ with the property that

$$\begin{array}{rr} & s \\ \times & \cdots 000003 \\ \hline = & \cdots 000001 \end{array}$$

In other words, thinking of natural numbers $n \in \mathbb{N}$ as elements of R, we're looking for a solution to the equation $s \times 3 = 1$ in R, i.e. a *multiplicative inverse* of 3 in R.

Solution. The easiest way to do this is to note that it's very easy to find an element $r \in R$ for which $r \times 3 = \cdots 999999$, namely $r = \cdots 333333$. We saw in Question 1 that $f = \cdots 999999$ behaves like -1; so if $r \times 3 = -1$, the natural guess is that $(-r) \times 3 = 1$. And we know from Question 2 how to find the additive inverse of r; it's $\cdots 666667$.

Once we've found this, we don't have to worry about whether it's legal to manipulate negatives like this (although it is); if we set

$$s = \cdots 666667,$$

we can just compute that

$$\begin{array}{r} 3 \\ \times\, s \\ \hline = \end{array} \qquad \begin{array}{rr} & \cdots 000003 \\ \times & \cdots 666667 \\ \hline & {\scriptstyle 1111} \\ & \cdots 000021 \\ & \cdots 00018 \\ & \cdots 0018 \\ & \cdots 018 \\ & \cdots 18 \\ + & \cdots 8 \\ \hline = & \cdots 000001 \end{array}$$

Question 4. Show that 2 does not have a multiplicative inverse in R;
that is, there is no element $t \in R$ satisfying $t \times 2 = 1$.

Solution. The key is to notice that the last digit of $t \times 2$ only depends on the *last digit* of t. (This is implicit in the italicized hint on page 2.) Indeed, we have the following pattern for any $t \in R$:

last digit of t	0	1	2	3	4	5	6	7	8	9
last digit of $t \times 2$	0	2	4	6	8	0	2	4	6	8

Therefore it is impossible to find any element $t \in R$ for which $t \times 2$ ends with 1.

Question 5. (Hard)
Which natural numbers $n \in \mathbb{N}$ have a multiplicative inverse in R? Can you prove it?
(Can you describe which $x \in R$ have a multiplicative inverse in R?)

Solution. It is not actually any harder to do this for general $x \in R$. The answer is that

$$x \in R \text{ has a multiplicative inverse} \qquad \Longleftrightarrow \qquad \text{the last digit of } x \text{ is a 1, 3, 7, or 9.}$$

($\Longrightarrow$): The forwards implication is the easier direction. We can prove this with the same ideas as (d). Assume that x has a multiplicative inverse y with $x \times y = 1$. The key is that the last digit of $x \times y$ only depends on the last digit of x and the last digit of y.

In particular, if the last digit of x were even (0, 2, 4, 6, or 8), then the last digit of $x \times y$ would be even. Similarly, if the last digit of x were 0 or 5, then the last digit of $x \times y$ would be 0 or 5. Therefore if $x \times y = 1$, the last digit of x must be 1, 3, 7, or 9.

($\Longleftarrow$): We now have to prove the opposite implication: if the last digit of x is 1, 3, 7, or 9, then we can find some multiplicative inverse y with $x \times y = \cdots 00000001$.

The **key idea** here is this: if we only forget about everything but the last digit, it's like we're working in $\mathbb{Z}/10\mathbb{Z}$. (After all, that's how you define modular arithmetic.) If we forget about everything but the last *two* digits, it's like we're working in $\mathbb{Z}/100\mathbb{Z}$. In general, if we forget about everything but the last k digits, it's like we're working in $\mathbb{Z}/10^k\mathbb{Z}$.

To make this more precise, let's say that $f_1 \colon R \to \mathbb{Z}/10\mathbb{Z}$ is the function that takes $x \in R$ to its last digit (modulo 10). Similarly $f_2 \colon R \to \mathbb{Z}/100\mathbb{Z}$ takes $x \in R$ to (the equivalence class of) the number formed by its last two digits.

In general, $f_k \colon R \to \mathbb{Z}/10^k\mathbb{Z}$ takes $x \in R$ to (the equivalence class of) the number formed by its last k digits (modulo 10^k). For example, if $x = \cdots 666667$ from Question 3, then $f_1(x) = \overline{7} \in \mathbb{Z}/10\mathbb{Z}$, $f_2(x) = \overline{67} \in \mathbb{Z}/100\mathbb{Z}$, $f_3(x) = \overline{667} \in \mathbb{Z}/1000\mathbb{Z}$, and so on.

In this language, our observation above about forgetting all but the last k digits says that

$$f_k(x + z) = f_k(x) + f_k(z) \quad \text{and} \quad f_k(x \times z) = f_k(x) \times f_k(z).$$

In particular, if $x \times y = \cdots 00001$, then we must have

$$f_k(x) \times f_k(y) = \overline{1} \quad \text{in } \mathbb{Z}/10^k\mathbb{Z}. \tag{$*$}$$

We know (Proposition 0.3.4) that an element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ exactly when a is relatively prime to n. In our case, this means that an element $\overline{a} \in \mathbb{Z}/10^k\mathbb{Z}$ has a multiplicative inverse if and only if a is not divisible by 2 or 5 (since the prime factors of $10^k = 2^k \cdot 5^k$ are 2 and 5). Our assumption that the last digit of x is 1, 3, 7, or 9 guarantees that $f_k(x)$ is not divisible by 2 or by 5. In other words, $f_k(x)$ lies in the group $(\mathbb{Z}/10^k\mathbb{Z})^\times$ of elements with multiplicative inverses.

Choose $n_k \in \mathbb{N}$ so that $\overline{n_k} \in (\mathbb{Z}/10^k\mathbb{Z})^\times \subset \mathbb{Z}/10^k\mathbb{Z}$ is the multiplicative inverse of $f_k(x)$:

$$f_k(x) \times \overline{n_k} = \overline{1} \quad \text{in } \mathbb{Z}/10^k\mathbb{Z}.$$

(Note that the multiplicative inverse is *unique*, since $(\mathbb{Z}/10^k\mathbb{Z})^\times$ is a group.) We define the element y by saying

$$\text{the last } k \text{ digits of } y \text{ are the last } k \text{ digits of } n_k$$

For example, say that $x = \cdots 123123123$.

- The multiplicative inverse of $\overline{3}$ in $\mathbb{Z}/10\mathbb{Z}$ is $\overline{7}$ (since $3 \cdot 7 = 2\mathbf{1}$),
  so the last digit of y would be 7;
- The multiplicative inverse of $\overline{23}$ in $\mathbb{Z}/100\mathbb{Z}$ is $\overline{87}$ (since $23 \cdot 87 = 20\mathbf{01}$),
  so the last two digits of y would be 87;
- The multiplicative inverse of $\overline{123}$ in $\mathbb{Z}/1000\mathbb{Z}$ is $\overline{187}$ (since $123 \cdot 187 = 23\mathbf{001}$),
  so the last three digits of y would be 187;
- The multiplicative inverse of $\overline{3123}$ in $\mathbb{Z}/10000\mathbb{Z}$ is $\overline{2187}$ (since $3123 \cdot 2187 = 683\mathbf{0001}$),
  so the last four digits of y would be 2187;
- and so on.

There is one possible problem here: the way I've phrased it, I use n_k to determine the last k digits of y. But what if these aren't consistent? That is, what if n_3 told me the last three digits should be 187, but n_2 told me the last two digits should be something other than 87? This is where the *uniqueness* of the inverse comes in. You can think about that, but it's fine if you didn't deal with this in your answer.

As you know, $0 \times 0 = 0$ and $1 \times 1 = 1$.
In other words, if we write t^2 for $t \times t$, this says 0 and 1 are solutions to the equation $t^2 = t$.

Question 6. (Hard) Find two other elements $x \in R$ and $y \in R$ satisfying $x^2 = x$ and $y^2 = y$.

Solution. We use the same reasoning as in Question 4 and the italicized hint at page 2: the last digit of t^2 is uniquely determined by the last digit of t; in particular they must coincide if t is to be a solution of the given equation. We compute:

last digit of t	**0**	**1**	2	3	4	**5**	**6**	7	8	9
last digit of t^2	**0**	**1**	4	9	6	**5**	**6**	9	4	1

Therefore the last digit has to be 0 or 1 or 5 or 6. Since we already found solutions whose last digit is 0 and 1, let's try to come up with a solution x whose last digit is 5.

Many students gave "algorithmic" solutions where you showed by induction that, if you have n digits that work (for $n \geq 1$), you can find an $(n+1)$-st digit that extends it (in fact uniquely). This is a great approach. For variety, I give a different one here. If you work out by hand what the last few digits of such a number x must be, you find that it must end with $\cdots 0625$. This looks suspiciously like a power of 5, so let's try that according to the following procedure:

We start with 5, we square to get 25, then we square this to get 625, we square to get 390625, of which we keep 0625; we square 0625 to get 390625, of which we keep 90625; we square 90625 to get 8212890625, of which we keep 890625; and so on.

More precisely, we start with the last digit $x_0 = 5 = 5^{2^0}$ and this needs to be $x_0 = \overline{x} \in \mathbb{Z}/10\mathbb{Z}$. We square it, to get $\left(5^{2^0}\right)^2 = 5^{2^1} = 25 = x_1x_0 = \overline{x} \in \mathbb{Z}/100\mathbb{Z}$, then we square it again, to get $\left(5^{2^1}\right)^2 = 5^{2^2} = 625 = x_2x_1x_0 = \overline{x} \in \mathbb{Z}/10^3\mathbb{Z}$, and again, to get $\left(5^{2^2}\right)^2 = 5^{2^3} = 390625 \equiv 0625 = \overline{x} \in \mathbb{Z}/10^4\mathbb{Z}$...

Clearly we are trying to "produce" some element x of R by giving $\overline{x} \in \mathbb{Z}/10^k\mathbb{Z}$ for all natural numbers k: why is this well-defined? That is to say, why do later digits do not change as I keep squaring?

Here's what we need to check: fix some m, and let $a = 5^{2^{m-1}}$ so that $\overline{a} = a_{m-1} \cdots a_2a_1a_0 \in \mathbb{Z}/10^m\mathbb{Z}$ is the number we obtain after m steps. Let $b = a^2 = 5^{2^m}$ be the next number we obtain, so that $\overline{b} = b_mb_{m-1} \cdots b_2b_1b_0 \in \mathbb{Z}/10^{m+1}\mathbb{Z}$ are the digits at the next step. We need to check we need to make sure that squaring again does not change the last m digits, i.e. that $a_{m-1} \cdots a_2a_1a_0 = b_{m-1} \cdots b_2b_1b_0$. That is to say, we need to prove that $\overline{a} = \overline{5^{2^{m-1}}} \in \mathbb{Z}/10^m\mathbb{Z}$ and $\overline{b} = \overline{\left(5^{2^{m-1}}\right)^2} = \overline{5^{2^m}} \in \mathbb{Z}/10^{m+1}\mathbb{Z}$ define the same congruence class modulo 10^m.

In other words, we need to show that the difference $d = 5^{2^m} - 5^{2^{m-1}}$ is divisible by 10^m, because this is what it means for the two numbers to define the same congruence class modulo 10^m. To check that d is divisible by 10^m, it suffices to check that d is divisible by 5^m and by 2^m.

We have

$$5^{2^m} - 5^{2^{m-1}} = 5^{2^{m-1}}\left(5^{2^m - 2^{m-1}} - 1\right) = 5^{2^{m-1}}\left(5^{2^{m-1}} - 1\right)$$

Clearly 5^m divides this product, because $m \leq 2^{m-1}$ for every positive integer m, so it remains to check that 2^m divides $5^{2^{m-1}} - 1$. We prove this by induction on m: for $m = 1$ it is obvious as $2^1 = 2$ divides $5^{2^0} - 1 = 4$, so assume that $m \geq 2$ and that we proved it for all $m - 1$.

We can write this second factor as a difference of squares:

$$5^{2^{m-1}} - 1 = \left(5^{2^{m-2}}\right)^2 - 1^2 = \left(5^{2^{m-2}} - 1\right)\left(5^{2^{m-2}} + 1\right)$$

By the induction assumption, 2^{m-1} divides the first factor. On the other hand, the second factor is obviously even (the sum of 1 and a power of 5), so 2 divides it, and then $2^{m-1} \cdot 2 = 2^m$ divides the product.

This concludes the proof that our element $x \in R$ is well-defined.

Now we claim that x is a solution of $t^2 = t$. Again, it suffices to check that x^2 and x have the same last digit for every positive integer m.

Fix then $m \in \mathbb{N}$. By construction, we know that the last m digits of x are the last m digits of $5^{2^{m-1}}$. As usual, the last m digits of x^2 are completely determined by the last m digits of x; indeed the last m digits of x^2 will be the last m digits of $\left(5^{2^{m-1}}\right)^2 = 5^{2^m}$ and we want to check that these two powers of 5 have the last m digits.
But this is *exactly* what we checked to make sure that x was well-defined. No need to re-write it again, we are done.

Finally, we need to come up with a fourth solution. Notice that if $x^2 = x$, then $(1-x)^2 = 1 - 2x + x^2 = 1 - 2x + x = 1 - x$. So $y = 1 - x = \cdots 109376$ is another solution.

Question 7. (Hard) Can you prove the equation $t^2 = t$ has only four solutions in R?
(Further thought: how about $t^5 = t$; does this have more solutions than you expect?)

Solution. We will show that if t is a solution of $t^2 = t$, then t is uniquely determined by its last digit.
In the previous question we already found four solutions, each with a different last digit - namely 0, 1, 5 and 6 - therefore the statement above will prove that there is no other solution, since again by Question 6 any solution has to end in 0, 1, 5 or 6.

Suppose s_1 and s_2 are two solutions of $t^2 = t$ with the same last digit d. If the last digit is 1, replace s_1 with $1 - s_1$ and s_2 with $1 - s_2$ to get two new solutions with last digit 0. Similarly, if the last digit is 6, replace s_1 with $1 - s_1$ and s_2 with $1 - s_2$ to get two new solutions with last digit 5. So we can assume that this same last digit d is 0 or 5.

We will prove that $s_1 - s_2$ is 0 by proving that $s_1 - s_2$ is a multiple of 10^m for all $m \geq 1$. Note that $x \in R$ is a multiple of 10 if and only if its last digit is 0 (since $10 \times \cdots x_2 x_1 = \cdots x_2 x_1 0$). In particular, $s_1 + s_2$ is a multiple of 10 (since its last digit is either $0 + 0 = 0$ or $5 + 5 = 10 \equiv 0$). Write $s_1 + s_2 = 10 \cdot a$ for some $a \in R$ (a is just $s_1 + s_2$ shifted to the right by one digit) and set $s_1 - s_2 = b$.

We now use the rather unusual factorization

$$s_1 - s_2 = s_1^2 - s_2^2 = (s_1 - s_2)(s_1 + s_2).$$

Applying this over and over, we see that

$$s_1 - s_2 = (s_1 - s_2)(s_1 + s_2) = (s_1 - s_2)(s_1 + s_2)^2 = (s_1 - s_2)(s_1 + s_2)^3 = \cdots = (s_1 - s_2)(s_1 + s_2)^m.$$

Therefore for any $m \geq 1$ we have

$$s_1 - s_2 = (s_1 - s_2)(10 \cdot a)^m = 10^m \cdot (a^m b).$$

We don't need to worry about what the digits of $a^m b$ are, because the 10^m factor tells us that at least the last m digits of $s_1 - s_2$ are 0. Since we can apply this argument for all $m \geq 1$, we conclude that *all* the digits of $s_1 - s_2$ are zero, i.e. $s_1 - s_2 = 0$. Adding s_2 to both sides shows $s_1 = s_2$ as desired.

Question 8. (Hard) Find two nonzero elements $a \in R$ and $b \in R$ whose product is zero: $a \neq 0$ and $b \neq 0$, but $a \times b = 0$.

Solution. For any $r \in R$, let's say that r is " divisible by 2^k " if the number $f_k(r)$ given by the last k digits of r is divisible by 2^k; in other words,[1] if

$$f_k(r) \in 2^k\mathbb{Z}/10^k\mathbb{Z}.$$

Define $d_2(r) \in \mathbb{N} \cup \{\infty\}$ and $d_5(r) \in \mathbb{N} \cup \{\infty\}$ by:

$$d_2(r) = \max\{k \,|\, r \text{ is divisible by } 2^k\}$$

$$d_5(r) = \max\{k \,|\, r \text{ is divisible by } 5^k\}$$

Note that it's possible to have $d_2(r) = \infty$ or $d_5(r) = \infty$; for example, the element $x = \cdots 2890625$ from Question 6 is divisible by 5^k for *all* k, so $d_5(x) = \infty$.

Note that the number of 0's at the end of r is the biggest k for which r is divisible by $10^k = 2^k 5^k$; in other words, it's the minimum of $d_2(r)$ and $d_5(r)$. For example, if $r = \cdots 12121200$, we have $d_2(r) = 4$ and $d_5(r) = 2$. In particular, $r = 0$ if and only if $d_2(r) = \infty$ and $d_5(r) = \infty$.

The key to this question is the observation:

$$d_2(a \times b) = d_2(a) + d_2(b), \qquad d_5(a \times b) = d_5(a) + d_5(b)$$

From this, we can see that two numbers a and b will satisfy $a \times b = 0$ if and only if $d_2(a) = \infty$ and $d_5(b) = \infty$ (or vice versa).

So how can we construct some $a \in R$ that is divisible by 2^k for all k? We use a similar construction as in Question 6, but reversing the roles of 2 and 5. We define a to have the last k digits equals to the last k digits of $2^{5^{k-1}}$. Since $5^{k-1} \geq k$ for all $k \geq 1$, this will obviously give us an element with $d_2(a) = \infty$ as soon as we prove that the element $a \in R$ is well-defined.

In other words, we need to show that at each step k we have made compatible choices, i.e. that at the next step, when we say that the last $k+1$ digits of a are the last $k+1$ digits of 2^{5^k}, the last k digits of 2^{5^k} coincide with the last k digits of $2^{5^{k-1}}$.

The latter fact boils down to showing that 10^k divides the difference

$$2^{5^k} - 2^{5^{k-1}} = 2^{5^{k-1}}\left(2^{5^k - 5^{k-1}} - 1\right).$$

Again, since $5^{k-1} \geq k$ for all $k \geq 1$, we have that 2^k divides the first factor on the right hand side, so it remains to check that 5^k divides $2^{5^k - 5^{k-1}} - 1 = 2^{5^{k-1}(5-1)} - 1 = 16^{5^{k-1}} - 1$.

We now proceed by induction on k, the case $k = 1$ being trivial (as 5 divides 15). We use the identity

$$a^5 - b^5 = (a-b)(a^4 + a^3b + a^2b^2 + ab^3 + b^4)$$

for $a = 16^{5^{k-2}}$ and $b = 1$. Then we have

$$16^{5^{k-1}} - 1 = \left(16^{5^{k-2}} - 1\right)\left(\left(16^{5^{k-2}}\right)^4 + \left(16^{5^{k-2}}\right)^3 + \left(16^{5^{k-2}}\right)^2 + 16^{5^{k-2}} + 1\right).$$

[1] It turns out this is equivalent to saying that $r = 2^k \times t$ for some $t \in R$, which justifies the terminology "divisible by 2^k", but we don't need that right now.

The induction assumption says that 5^{k-1} divides the left factor $\left(16^{5^{k-2}}-1\right)$, so it suffices to check that 5 divides the other factor. Note that every power of 16 will end with the digit 6, thus the last digit of the factor on the right is the last digit of $6+6+6+6+1=25$. This shows that 5 divides $\left(\left(16^{5^{k-2}}\right)^4+\left(16^{5^{k-2}}\right)^3+\left(16^{5^{k-2}}\right)^2+16^{5^{k-2}}+1\right)$ and completes the proof.

Question 9. Prove that there is no element $x \in R$ satisfying $x^2 = 7$.

Solution. We noted in the solution for Question 4, or better yet in the italicized hint on page 2, that the last digit of $t \times s$ only depends on the last digits of t and s.

In particular the last digit of t^2 depends only on the last digit of t: to show that the equation $t^2 = 7$ has no solutions in R, it suffices then to check by brute force that no last digit t_0 of t gives $t^2 = 7$ in $\mathbb{Z}/10\mathbb{Z}$.

We have, as in the solution to Question 6:

last digit of t	0	1	2	3	4	5	6	7	8	9
last digit of t^2	0	1	4	9	6	5	6	9	4	1

and this finishes the proof.

Question 10. (Hard) Prove that there *is* at least one solution $z \in R$ to the equation $z^3 = 7$.

Solution. In fact, something much more general is true:

for *any* $k \in \mathbb{N}$ that is prime to 10,
and *any* $x \in R$ whose last digit is 1, 3, 7, or 9,

x **has a unique k-th root** z

satisfying $z^k = x$.

Let G be a finite abelian group (with multiplicative notation) and consider the map "n-power"

$$p_n : G \longrightarrow G \quad g \mapsto g^n.$$

It is easy to check this is a group homomorphism: $1^n = 1$, $(gh)^n = g^n h^n$ and $\left(g^{-1}\right)^n = g^{-n} = (g^n)^{-1}$.

The kernel of p_n consists of all the elements satisfying $g^n = 1$; that is, all the elements whose order divides n.

Suppose now that n is coprime to the order of the group G: in particular by Lagrange's theorem no element $g \in G$ has order dividing n (besides the identity). Therefore, $\ker p_n = \{1_G\}$, so p_n is injective. But if p_n is an injective map from a finite set to itself, it must also be *surjective*, and thus a *bijection*. In particular, for every $g \in G$ there exists a unique $h \in G$ such that $h^n = g$.

Observe now that $|\ (\mathbb{Z}/10\mathbb{Z})^\times\ | = 4$, $|\ (\mathbb{Z}/100\mathbb{Z})^\times\ | = 40$, $|\ (\mathbb{Z}/1000\mathbb{Z})^\times\ | = 400$, and in general $\left|\ (\mathbb{Z}/10^k\mathbb{Z})^\times\ \right| = 4 \cdot 10^{k-1}$. (Indeed, as we saw in Question 5 these are all those elements whose last digits is 1, 3, 7, or 9, which is $\frac{4}{10}$ of all the elements.)

In particular, all these orders are coprime to $n = 3$, so for every $k \geq 1$ we pick the element $g_k = 7 \in \mathbb{Z}/10^k\mathbb{Z}$ - which is invertible - and we obtain a unique element $h_k \in \left(\mathbb{Z}/10^k\mathbb{Z}\right)^\times \subset \mathbb{Z}/10^k\mathbb{Z}$ such that $h_k^3 = 7$ in $\mathbb{Z}/10^k\mathbb{Z}$.

It remains to check that we can glue together all these h_k to obtain a unique, well-defined, element x of R. In other words, we define x to have the last k digits equal to h_k, and we need to show that this is well-defined.

As we have done in the previous problems, to show that x built as above is well-defined we just need to check that h_{k+1} and h_k have the same last k digits.

By construction we have $h_{k+1}^3 = 7$ in $\mathbb{Z}/10^{k+1}\mathbb{Z}$, and this equation stays true under the surjection map $\mathbb{Z}/10^{k+1}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/10^k\mathbb{Z}$. In particular, the congruence class of h_{k+1} modulo 10^k satisfies the equation $z^3 = 7$ in $\mathbb{Z}/10^k\mathbb{Z}$, but we know that $z = h_k$ is the only solution!

Therefore, h_{k+1} reduces to h_k modulo 10^k, and this means that h_{k+1} and h_k have the same last k digits, which shows that our solution x is well-defined.