Math 235 (Fall 2012)
Assignment 1 solutions

Luiz Kazuo Takei

September 25, 2012

Exercise 1

a) $x^3 + 3x + 1$

In this case, the discriminant is

$$1^2 + 4\frac{3^3}{27} > 0$$

which means there is only one real solution.

b) $x^3 - 3x + 1$

In this case, the discriminant is

$$1^2 + 4\frac{(-3)^3}{27} = -3 < 0$$

which means there are more than 1 solution. The solutions are given by

$$u + v$$

where u^3, v^3 are roots of

$$y^2 + y + 1$$

and

$$uv = 1.$$

The roots of

$$y^2 + y + 1$$

(computed using the quadratic formula) are given by

$$e^{i\frac{2\pi}{3}} \quad \text{and} \quad -e^{i\frac{\pi}{3}} = e^{i\frac{4\pi}{3}}.$$

The cube roots of $e^{i\frac{\pi}{3}}$ are given by

$$e^{i\frac{2\pi}{9}} \quad , \quad e^{i\frac{2\pi}{9}}e^{i\frac{2\pi}{3}} = e^{i\frac{8\pi}{9}} \quad \text{and} \quad e^{i\frac{2\pi}{9}}e^{i\frac{4\pi}{3}} = e^{i\frac{14\pi}{9}}.$$

Similarly, the cube roots of $e^{i\frac{4\pi}{3}}$ are given by

$$e^{i\frac{4\pi}{9}} \quad , \quad e^{i\frac{4\pi}{9}}e^{i\frac{2\pi}{3}} = e^{i\frac{10\pi}{9}} \quad \text{and} \quad e^{i\frac{4\pi}{9}}e^{i\frac{4\pi}{3}} = e^{i\frac{16\pi}{9}}.$$

So the solutions are

$$\zeta + \zeta^{-1} \quad , \quad \zeta^4 + \zeta^{-4} \quad \text{and} \quad \zeta^7 + \zeta^{-7}$$

where

$$\zeta := e^{i\frac{2\pi}{9}}.$$

In other words, the solutions are

$$\begin{gathered}
(\cos(\tfrac{2\pi}{9}) + i\sin(\tfrac{2\pi}{9})) + (\cos(\tfrac{2\pi}{9}) - i\sin(\tfrac{2\pi}{9})) \\
(\cos(\tfrac{2\pi}{9}) + i\sin(\tfrac{2\pi}{9}))^4 + (\cos(\tfrac{2\pi}{9}) - i\sin(\tfrac{2\pi}{9}))^{-4} \\
(\cos(\tfrac{2\pi}{9}) + i\sin(\tfrac{2\pi}{9}))^7 + (\cos(\tfrac{2\pi}{9}) - i\sin(\tfrac{2\pi}{9}))^{-7}.
\end{gathered}$$

or, written in a different way,

$$2\cos(\tfrac{2\pi}{9}) \quad , \quad 2\cos(\tfrac{8\pi}{9}) \quad \text{and} \quad 2\cos(\tfrac{14\pi}{9})$$

Exercise 2

a

To define a function from S to T, we need to define the images of each element of S. So, for instance, $a \in S$ could be mapped to either x or y (both in T). The same applies to $b, c \in S$. Therefore, we have $2^3 = 8$ functions $S \to T$.

b

For a function to be injective, the target must be at least of the same size as the domain. Since $|S| > |T|$, there is no injective function $S \to T$.

c

To be surjective, the image of the function must be equal to its target, which in our case is $T = \{x, y\}$. So there must be at least one element of S being mapped to x and one being mapped to y.

Since $|S| = 3$, there are two possibilities for such a surjective function:

(i) there are exactly 2 points being mapped to x (and, hence, 1 point being mapped to y); or

(ii) there is exactly 1 point being mapped to x (and, hence, 2 points being mapped to y).

To count how many possibilities falling in the first case, we need to count in how many times we can split the set S in two subsets, one having 2 elements and the other one having 1 element. This is the same as counting how many subsets of S having 2 elements there are. And the answer to this question is

$$\binom{3}{2} = \frac{3!}{2! \cdot 1!} = 3.$$

Similarly, the number of possibilities in the second case is also

$$\binom{3}{2} = \frac{3!}{2! \cdot 1!} = 3.$$

So, there are 6 surjective functions $S \to T$.

Exercise 3

a

Notice that, by definition, $fg = f \circ g$, where

$$(f \circ g)(x) = f(g(x)).$$

To prove two functions are the same, it is enough to show they are equal when evaluated at each point. Now,

$$[f(gh)](x) = [f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x))),$$

and

$$[(fg)h](x) = [(f \circ g) \circ h)](x) = (f \circ g)(h(x)) = f(g(h(x))).$$

This proves $f(gh) = (fg)h$.

b

Define $f, g : \mathbb{N} \to \mathbb{N}$ by

$$f(n) := n^2 \quad \text{and} \quad g(n) := n + 1.$$

Then

$$(fg)(n) = f(g(n)) = f(n+1) = (n+1)^2 \quad \text{and} \quad (gf)(n) = g(f(n)) = g(n^2) = n^2 + 1.$$

And therefore

$$(fg)(1) = (1+1)^2 = 4 \quad \text{and} \quad (gf)(1) = 1^2 + 1 = 2.$$

shows that $fg \neq gf$.

Exercise 4

Let $z := 1 + \sqrt{3}i$ and notice that the polar representation of z is given by

$$z = 2e^{i\frac{\pi}{3}}.$$

Thus

$$z^{111} = 2^{111}e^{i\frac{\pi}{3}111} = 2^{111}e^{i37\pi}.$$

Since

$$37\pi = 18(2\pi) + \pi,$$

we obtain that

$$z^{111} = 2^{111} \cdot (e^{i2\pi})^{18} \cdot e^{i\pi} = 2^{111} \cdot (1) \cdot (-1) = -2^{111}$$

is an integer.

Exercise 5

We are going to use the following fact (which can itself be proved by induction):

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Now we prove by induction that for all $n \geq 1$

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

The base case $n = 1$ is trivial.
We therefore assume it holds for n and prove it for $n + 1$.

$$\begin{aligned}
1^3 + 2^3 + \cdots + +n^3 + (n+1)^3 &= (1 + 2 + \cdots + n)^2 + (n+1)^3 \\
&= \tfrac{n^2(n+1)^2}{2^2} + (n+1)^3 \\
&= (n+1)^2 \left[\tfrac{n^2}{4} + (n+1)\right] \\
&= (n+1)^2 \left[\tfrac{(n+2)^2}{4}\right] \\
&= \tfrac{(n+1)^2(n+2)^2}{2^2} \\
&= (1 + 2 + \cdots + (n+1))^2.
\end{aligned}$$

Exercise 6

$$\begin{aligned}
910091 &= 3619 \cdot 251 + 1722 \\
3619 &= 1722 \cdot 2 + 175 \\
1722 &= 175 \cdot 9 + 147 \\
175 &= 147 \cdot 1 + 28 \\
147 &= 28 \cdot 5 + 7 \\
28 &= 7 \cdot 4 + 0
\end{aligned}$$

Since 7 is the last non-zero remainder,

$$\gcd(910091, 3619) = 7.$$

Exercise 7

First we show that 7 divides $8^n - 1$ for all $n \geq 0$.

It is known that

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

for every number x (cf. example 2.3.5 in notes).

Therefore

$$8^n - 1 = 7 \cdot (8^{n-1} + 8^{n-2} + \cdots + 8 + 1)$$

is clearly divisible by 7.

We now prove by induction that 49 divides $8^n - 7n - 1$ for all $n \geq 0$.

As usual, the base case $n = 0$ is trivial. We now assume it holds for n and show it for $n+1$.

We know 49 divides

$$8^n - 7n - 1 = 7(8^{n-1} + \cdots + 8 + 1) - 7n = 7(8^{n-1} + \cdots + 8 + 1 - n).$$

Hence, 7 divides $8^{n-1} + \cdots + 8 + 1 - n$.

We now want to show that 49 divides

$$8^{n+1} - 7(n+1) - 1 = 7(8^n + \cdots + 8 + 1 - (n+1)),$$

which is equivalent to proving that 7 divides

$$8^n + \cdots + 8 + 1 - (n+1) = (8^{n-1} + \cdots + 8 + 1 - n) + (8^n - 1).$$

But the first term on the right-hand side is divisible by 7 by the induction hypothesis and the second term is divisible by 7 by the first part of this exercise.

This finishes the solution of this exercise.

Exercise 8

Recall that the addition law was defined on $\mathbb{N}$ as follows:

$$0 + m := m \quad \text{and} \quad S(n) + m := S(n+m).$$

Moreover, it was proved in class that this addition is commutative (i.e., $n + m = m + n$).

We now want to show it is associative, i.e.,

$$(r+s) + t = r + (s+t)$$

for all $r, s, t \in \mathbb{N}$.

To prove this, we fix s and t and use induction on r.

Let's prove the base case $r = 0$:

$$(0+s) + t = s + t = 0 + (s+t).$$

Now we assume it holds for r and show it for $S(r)$:

$$\begin{aligned}(S(r)+s)+t &= S(r+s)+t = S((r+s)+t) = S(r+(s+t)) \\ &= S(r)+(s+t),\end{aligned}$$

where the third equality follows from the induction hypothesis and the other ones follow from the definition of addition on $\mathbb{N}$.

Exercise 9

To show that $|A| < |2^A|$, we need to show that $|A| \leq |2^A|$ and $|A| \neq |2^A|$.

It is easy to show that $|A| \leq |2^A|$. In fact, construct the injection $f : A \to 2^A$ given by $f(a) := \{a\}$.

Now we need to show that $|A| \neq |2^A|$, i.e., we need to show that there is no bijection $A \to 2^A$. To prove this, we take a function $g : A \to 2^A$ and show it can't be surjective. Given a function $g : A \to 2^A$, we may construct the following subset of A:

$$X := \{a \in A \mid a \notin g(a)\} \in 2^A$$

(note this makes sense because $g(a)$, being an element of 2^A, is a subset of A).

Claim. X is not in the image of g.

Proof. Suppose X is in the image of g. Then, there exists $a_0 \in A$ such that $X = g(a_0)$.

We may ask ourselves: is $a_0 \in X$?

If $a_0 \in X$, it satisfies the condition to be in X, namely: $a_0 \notin g(a_0)$. But $g(a_0) = X$. So $a_0 \notin X$.

On the other hand, if $a_0 \notin X$, it does not satisfies the condition to be in X, namely: $a_0 \in g(a_0) = X$.

The conclusion is, if there is $a_0 \in A$ such that $X = g(a_0)$, then it satisfies the following:

$$a_0 \in X \Leftrightarrow a_0 \notin X,$$

which is obviously impossible (unless you live in a crazy logical world...). □

We showed that if we have a function $g : A \to 2^A$, it can't be surjective. In particular, there is no bijective function $A \to 2^A$, meaning $|A| \neq |2^A|$ as we wanted to show.

Exercise 10

We first prove that if the decimal expansion of a number becomes periodic, then it is a rational number.

The first step is to note that if the decimal expansion stops, then it is rational. Indeed, if

$$x = m.a_1 \cdots a_r,$$

for $m \in \mathbb{Z}$ and $a_i \in \{0, \ldots, 9\}$, then

$$10^r x = u \in \mathbb{Z}$$

and, thus,

$$x = \frac{u}{10^r} \in \mathbb{Q}.$$

Now, if x is any number whose decimal expansion becomes periodic, we may write x as

$$x = y + 10^{-s} z$$

where y is a number whose decimal expansion stops (hence, rational) and z is a number whose decimal expansion is periodic and satisfies $0 < z < 1$.

So, it remains only to show that z is rational (since a sum of rational numbers is again rational).

Suppose

$$z = 0.a_1 a_2 \cdots a_t a_1 a_2 \cdots a_t \ldots,$$

i.e., the digits $a_1 \cdots a_t$ just keep repeating in the expansion of z.

Then it is easy to see that

$$10^t z = w + z,$$

where w is the integer whose digits are $a_0 \cdots a_t$, i.e., $w = a_1 10^{t-1} + \cdots + a_{t-1} 10 + a_t$ and, so,

$$z = \frac{w}{10^t - 1} \in \mathbb{Q}.$$

We now prove the converse: if a number is rational, then its decimal expansion becomes periodic.

For this, we need to understand how to write the decimal expansion of a rational number $\frac{m}{n}$. We may assume $0 < m < n$ (the other cases can be reduced to this one). So

$$\frac{m}{n} = 0.a_1 a_2 \ldots .$$

To find a_1, we use Euclidean division for $10m$ and n, i.e.,

$$10m = a_1 \cdot n + r_1$$

where $0 \leq r_1 < n$.

To find a_2, we use Euclidean division for $10r_1$ and n, i.e.,

$$10r_1 = a_2 \cdot n + r_2$$

where $0 \leq r_2 < n$.

In general, to find a_i, we use Euclidean division for $10r_{i-1}$ and n, i.e.,

$$10r_{i-1} = a_i \cdot n + r_i$$

where $0 \leq r_i < n$.

So, the digit a_i depends only on the remainders of the divisions by n of the previous step. Since these remainders can only be one of the

$$0, 1, \ldots, n-1$$

it follows that at some point, the remainder will start repeating and then the digit a_i will start repeating.