Staff Solutions to Problem Set 4

Reading: Chapter 7. on Infinite Sets and Chapter 8. on Number Theory through Section 8.9

Problem 1.
Show that the set \( \mathbb{N}^* \) of finite sequences of nonnegative integers is countable.

Solution. Define the weight of a finite string of nonnegative integers to be the larger of the length of the string and the largest integer in the string. There are only finitely many strings of any given weight, \( n \), so list the strings in order of weight, ordered within same-weight groups in some arbitrary way, say in “dictionary” order.

Problem 2.
Let \( \mathbb{N}^\omega \) be the set of infinite sequences of nonnegative integers. For example, some sequences of this kind are:

\[
\begin{align*}
(0, 1, 2, 3, 4, \ldots), \\
(2, 3, 5, 7, 11, \ldots), \\
(3, 1, 4, 5, 9, \ldots).
\end{align*}
\]

Prove that this set of sequences is uncountable.

Solution. Proof. One approach is to show that if \( \mathbb{N}^\omega \) were countable, then \( \mathcal{P}(\mathbb{N}) \) would be too, contradicting Cantor’s Theorem 7.1.6.

STAFF NOTE: If needed, offer hint: verify that \( \mathbb{N}^\omega \) is as big as \( \mathcal{P}(\mathbb{N}) \).

Namely, we can define a surjective function from \( f : \mathbb{N}^\omega \to \mathcal{P}(\mathbb{N}) \) as follows:

\[
f(s) := \{ n \in \mathbb{N} \mid s[n] = 0 \}
\]

where \( s[n] \) is the \( n \)th element of sequence \( s \).

Now if there was a surjective function from \( g : \mathbb{N} \to \mathbb{N}^\omega \), then the composition of \( f \) and \( g \) would be a surjective function from \( \mathbb{N} \) to \( \mathcal{P}(\mathbb{N}) \) contradicting Cantor’s Theorem 7.1.6.

Alternatively, to show that \( \mathbb{N}^\omega \) is uncountable, we can use a basic diagonal argument directly to show that no function from \( \mathbb{N} \) to the set of sequences \( \mathbb{N}^\omega \) is a surjection.

Proof. Let \( \sigma \) be a function from \( \mathbb{N} \) to the infinite sequences of nonnegative integers. To show that \( \sigma \) is not a surjection, we will describe a sequence, diag, of nonnegative integers that is not in the range of \( \sigma \).

Namely, define a sequence \( \text{diag} \in \mathbb{N}^\omega \) as follows:

STAFF NOTE: If needed, offer this def of diag as a hint.
Now by definition,
\[ \text{diag}[n] \neq \sigma(n)[n], \]
for all \( n \in \mathbb{N} \), proving that diag is not equal to \( \sigma(n) \) for any \( n \in \mathbb{N} \). This means that diag is not in the range of \( \sigma \), as claimed.

**Problem 3.**
The sum of the digits of the base 10 representation of an integer is congruent modulo 9 to that integer. For example
\[ 763 \equiv 7 + 6 + 3 \pmod{9}. \]
This is not always true for the hexadecimal (base 16) representation, however. For example,
\[ (763)_{16} = 7 \cdot 16^2 + 6 \cdot 16 + 3 \equiv 1 \not\equiv 7 + 6 + 3 \pmod{9}. \]

(a) For exactly what integers \( k > 1 \) is it true that the sum of the digits of the base 16 representation of an integer is congruent modulo \( k \) to that integer? Justify your answer.

**Solution.**

\[ 3, 5, 15. \]
Summing the digits mod \( k \) works iff \( 16 \equiv 1 \pmod{k} \). This is equivalent to \( k \mid 16 - 1 = 15 \). So the three factors of 15 are exactly the \( k \)'s that work.
To see why only these \( k \)'s work, just look at two-digit hex numbers \( 16c + d \) where \( c, d \in [0, 16) \). In this case the digit-sum requirement means that for all such \( c, d \),
\[ 16c + d \equiv c + d \pmod{k}, \]
so letting \( c = 1, d = 0 \) gives \( 16 \equiv 1 \pmod{k} \).

(b) Give a rule that generalizes this sum-of-digits rule from base \( b = 16 \) to an arbitrary number base \( b > 1 \), and explain why your rule is correct.

**Solution.** By the reasoning of part (a) with “16” replaced by “\( b \)” a necessary and sufficient condition for a number \( k > 1 \) to satisfy the sum-of-digits condition is that \( k \) be a divisor of \( b - 1 \).

**Problem 4.**
The set of complex numbers that are equal to \( m + n\sqrt{-5} \) for some integers \( m, n \) is called \( \mathbb{Z}[\sqrt{-5}] \). It will turn out that in \( \mathbb{Z}[\sqrt{-5}] \), not all numbers have unique factorizations.
A sum or product of numbers in \( \mathbb{Z}[\sqrt{-5}] \) is in \( \mathbb{Z}[\sqrt{-5}] \), and since \( \mathbb{Z}[\sqrt{-5}] \) is a subset of the complex numbers, all the usual rules for addition and multiplication are true for it. But some weird things do happen. For example, the prime 29 has factors:

(a) Find \( x, y \in \mathbb{Z}[\sqrt{-5}] \) such that \( xy = 29 \) and \( x \neq \pm 1 \neq y \).
Solution. Let \( x = (3 + 2\sqrt{-5}) \) and \( y = (3 - 2\sqrt{-5}) \), so
\[
(3 + 2\sqrt{-5})(3 - 2\sqrt{-5}) = 9 - 2\cdot 4 = 9 + 5\cdot 4 = 29.
\]

On the other hand, the number 3 is still a “prime” even in \( \mathbb{Z}[\sqrt{-5}] \). More precisely, a number \( p \in \mathbb{Z}[\sqrt{-5}] \) is called \textit{irreducible} over \( \mathbb{Z}[\sqrt{-5}] \) iff when \( xy = p \) for some \( x, y \in \mathbb{Z}[\sqrt{-5}] \), either \( x = \pm 1 \) or \( y = \pm 1 \).

**Claim.** The numbers \( 3, 2 + \sqrt{-5}, \text{ and } 2 - \sqrt{-5} \) are irreducible over \( \mathbb{Z}[\sqrt{-5}] \).

In particular, this Claim implies that the number 9 factors into irreducibles over \( \mathbb{Z}[\sqrt{-5}] \) in two different ways:
\[
3 \cdot 3 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).
\]
(1)

So \( \mathbb{Z}[\sqrt{-5}] \) is an example of what is called a \textit{non-unique factorization} domain.

To verify the Claim, we’ll appeal (without proof) to a familiar technical property of complex numbers given in the following Lemma.

**Definition.** For a complex number \( c = r + si \) where \( r, s \in \mathbb{R} \) and \( i \) is \( \sqrt{-1} \), the \textit{norm}, \( |c| \), of \( c \) is \( s^2 + r^2 \).

**Lemma.** For \( c, d \in \mathbb{C} \),
\[
|cd| = |c| \cdot |d|.
\]

(b) Prove that \( |x|^2 \neq 3 \) for all \( x \in \mathbb{Z}[\sqrt{-5}] \).

**Solution.** Say \( x = m + n\sqrt{-5} \) for \( m, n \in \mathbb{Z} \). Now suppose to the contrary that \( |x|^2 := m^2 + 5n^2 = 3 \). But \( m^2 + 5n^2 \geq 5 \) for \( n \neq 0 \). Hence \( n \) must be 0, in which case the integer \( m \) must be \( \pm \sqrt{3} \), a contradiction.

(c) Prove that if \( x \in \mathbb{Z}[\sqrt{-5}] \) and \( |x| = 1 \), then \( x = \pm 1 \).

**Solution.** \( \text{Proof.} \) Say \( x = m + n\sqrt{-5} \) for \( m, n \in \mathbb{Z} \). So \( |x| = \sqrt{m^2 + 5n^2} \). But \( m^2 + 5n^2 > 1 \) if \( n \neq 0 \), so \( |x| = 1 \) implies \( \sqrt{m^2} = 1 \). That is, \( x = m = \pm 1 \).

(d) Prove that if \( |xy| = 3 \) for some \( x, y \in \mathbb{Z}[\sqrt{-5}] \), then \( x = \pm 1 \) or \( y = \pm 1 \).

\textit{Hint:} \( |z|^2 \in \mathbb{N} \) for \( z \in \mathbb{Z}[\sqrt{-5}] \).

**Solution.** \( \text{Proof.} \)

\[3 = |xy| \quad \text{implies} \quad 3^2 = |xy|^2 = |x|^2 |y|^2 \quad \text{(by the Lemma)}
\]

\[\quad \quad \quad \quad \quad \text{implies} \quad |x|^2 = 1 \text{ OR } |y|^2 = 1 \text{ OR } |x|^2 = |y|^2 = 3 \]

\[\quad \quad \quad \quad \quad \quad \quad \text{(by the hint and unique factorization of } 3^2 \text{ over } \mathbb{N})
\]

\[\quad \quad \quad \quad \quad \text{implies} \quad |x|^2 = 1 \text{ OR } |x|^2 = 3 \text{ OR } |y|^2 = 1
\]

\[\quad \quad \quad \quad \quad \text{implies} \quad |x|^2 = 1 \text{ OR } |y|^2 = 1 \quad \text{(by part (b))}
\]

\[\quad \quad \quad \quad \quad \text{implies} \quad x = \pm 1 \text{ OR } y = \pm 1 \quad \text{(by part (c))}
\]

\[\text{(e) Complete the proof of the Claim.}\]
Solution. We must prove that $3$, and $2 \pm \sqrt{-5}$ are irreducible over $\mathbb{Z}[\sqrt{-5}]$. That is, suppose $xy = 3$, or $xy = 2 \pm \sqrt{-5}$, for some $x, y \in \mathbb{Z}[\sqrt{-5}]$. We must prove that either $x = \pm 1$ or $y = \pm 1$.

But by definition,

$$|2 \pm \sqrt{-5}| = \sqrt{2^2 + 5 \cdot 1^2} = \sqrt{9} = 3 = |3|.$$ 

So $|xy| = 3$ in any case, and part (d) implies $x = \pm 1$ or $y = \pm 1$, as required.