Staff Solutions to Midterm Exam March 19

In answering the following questions, you may use without proof any of the results from class or text.

Problem 1 (10 points).

Use the Well Ordering Principle to prove that there is no solution over the positive integers to the equation:

\[4a^3 + 2b^3 = c^3.\]

Solution. We use contradiction and the Well Ordering principle. Let \(S\) be the set of all positive integers, \(a\), such that there exist positive integers, \(b\), and, \(c\), that satisfy the equation.

Assume for the purpose of obtaining a contradiction that \(S\) is nonempty. Then \(S\) contains a smallest element, \(a_0\), by the well-ordering principle. By the definition of \(S\), there exist corresponding positive integers, \(b_0\), and, \(c_0\), such that:

\[4a_0^3 + 2b_0^3 = c_0^3.\]

The left side of this equation is even, so \(c_0^3\) is even, and therefore \(c_0\) is also even. Thus, there exists an integer, \(c_1\), such that \(c_0 = 2c_1\). Substituting into the preceding equation and then dividing both sides by 2 gives:

\[2a_0^3 + b_0^3 = 4c_1^3.\]

Now \(b_0^3\) must be even, so \(b_0\) is even. Thus, there exists an integer, \(b_1\), such that \(b_0 = 2b_1\). Substituting into the preceding equation and dividing both sides by 2 again gives:

\[a_0^3 + 4b_1^3 = 2c_1^3.\]

From this equation, we know that \(a_0^3\) is even, so \(a_0\) is also even. Thus, there exists an integer, \(a_1\), such that \(a_0 = 2a_1\). Substituting into the previous equation one last time and dividing by 2 one last time gives:

\[4a_1^3 + 2b_1^3 = c_1^3.\]

So \(a = a_1, b = b_1,\) and \(c = c_1\) is another solution to the original equation, and so \(a_1\) is an element of \(S\). But this is a contradiction, because \(a_1 < a_0\) and \(a_0\) was defined to be the smallest element of \(S\). Therefore, our assumption was wrong, and the original equation has no solutions over the positive integers.

Problem 2 (10 points).

We define the sequence of numbers

\[a_n = \begin{cases} a_{n-1} + a_{n-2} + a_{n-3} + a_{n-4} & \text{if } n \geq 4, \\ 1 & \text{if } 0 \leq n \leq 3. \end{cases}\]

Prove that \(a_n \equiv 1 \pmod{3}\) for all \(n \geq 0\).

Solution. Proof by strong induction with induction hypothesis

\[P(n) ::= a_n \equiv 1 \pmod{3}.\]
Base case \((0 \leq n \leq 3): a_n = 1\) and is therefore \(\equiv 1 \pmod{3}\), so \(P(n)\) holds.

Inductive step: For \(n \geq 3\), assume \(P(k)\) for \(0 \leq k < n\) in order to prove \(P(n)\). In particular, \(P(k)\) holds for \(k = n - 4, n - 3, n - 2\) and \(n - 1\), each of \(a_{n-4}, a_{n-3}, a_{n-2}\) and \(a_{n-1}\) is \(\equiv 1 \pmod{3}\), so their sum, \(a_n\), is \(\equiv 1 + 1 + 1 + 1 = 4 \equiv 1 \pmod{3}\). That is, \(a_n \equiv 1 \pmod{3}\), which means \(P(n)\) holds.

Problem 3 (10 points).
Suppose \(P(n)\) is a predicate on nonnegative integers and suppose
\[
\forall k. P(k) \implies P(k + 2). \tag{1}
\]
For each of the assertions below, determine whether it:

- Can hold (holds for some, but not all, \(P\) satisfying (1))
- Always holds (for any such \(P\)), or
- Never holds (for any such \(P\)).

Indicate which case applies by circling the correct letter.

(a) \(\neg(P(0))\) AND \(\forall n \geq 1. P(n)\) C A N

Solution. C. This formula says that \(P\) is false at 0, but true everywhere else. So \(P(k) \implies P(k + 2)\) still always holds because \(P(k + 2)\) is still always true. So this assertion can hold, but not always, since (1) can hold when \(P(0)\) is true.

(b) \([\exists n. P(2n)] \implies \forall n. P(2n + 2)\) C A N

Solution. C. We see the case is possible by considering \(P(n)\) that is always true. A counterexample is \(P(n)\) that holds iff \(n > 3\), where the \(\exists n\) is satisfied with \(n = 2\), but the \(\forall n\) fails for \(n = 0\).

(c) \(P(1) \implies \forall n. P(2n + 1)\) C A N

Solution. A. This assertion says that if \(P(1)\) holds, then \(P(n)\) holds for all odd \(n\). This case is always true.

(d) \(\exists n. \exists m > n. [P(2n) \text{ AND } \neg(P(2m))]\) C A N

Solution. N. This assertion says that \(P\) holds for some even number, \(2n\), but not for some other larger even number, \(2m\). However, if \(P(2n)\) holds, we can apply (1) \(n - m\) times to conclude \(P(2m)\) also holds. This case is impossible.

(e) \([\exists n. P(n)] \implies \forall n. \exists m > n. P(m)\) C A N

Solution. A. This assertion says that if \(P\) holds for some \(n\), then for every number, there is a larger number, \(m\), for which \(P\) also holds. Since (1) implies that if there is one \(n\) for which \(P(n)\) holds, there are an infinite, increasing chain of \(k\)'s for which \(P(k)\) holds, this case is always true.

(f) \(\neg(P(0)) \implies \forall n. \neg(P(2n))\) C A N
Solution. C. If for all $n$, $P(n)$ is false, then the statement is true. If $P(0)$ is false but $P(2)$ is true, then the statement is false.

Problem 4 (5 points).
Find an example for $A$ and $B$, such that $\mathbb{N}$ strict $A$ strict $B$. ($X$ strict $Y$ means there exists a surjective function from $Y$ to $X$, but no surjective function exists from $X$ to $Y$.)

Solution. $A$: real numbers; $B$: powerset of real numbers.

Problem 5 (5 points).
There is a mistake in the following proof, where all the congruences are taken with modulus 29:

\[
35^{86} \equiv 6^{86} \quad \text{(since $35 \equiv 6 \pmod{29}$)} \quad (2) \\
\equiv 6^{28} \quad \text{(since $86 \equiv 28 \pmod{29}$)} \quad (3) \\
\equiv 1 \quad \text{(by Fermat’s Little Theorem)} \quad (4)
\]

Identify the exact line containing the mistake and explain the logical error.

Solution. The mistake occurs at line (3).

Exponents can be replaced by their remainders on division by 28, not on division by 29. So the “explanation” that $86 \equiv 28 \pmod{29}$ on the third line is true, but does not justify that mistaken step.