ETH Zürich, D-INFK
HS 2020, 14. October 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik
Solution 4

Part 1: Proof Patterns

4.1 Indirect Proof of an Implication (2.6.3)

a) Assume that n is even. Then, $n = 2k$ for some $k \in \mathbb{N}$. We have therefore $n^2 = n \cdot n = 2k \cdot 2k = 2 \cdot 2k^2$. Hence, n^2 is even.

Detailed solution:

Statement S**:** n^2 is odd.

Statement T**:** n is odd.

Indirect proof:
n is not odd.
$\Longrightarrow$ n is even.
$\Longrightarrow$ $n = 2k$ for some $k \in \mathbb{N}$.
$\Longrightarrow$ $n \cdot n = 2k \cdot 2k$ for some $k \in \mathbb{N}$.
$\Longrightarrow$ $n \cdot n = 2 \cdot 2k^2$ for some $k \in \mathbb{N}$.
$\Longrightarrow$ $n \cdot n = 2l$ for some $l \in \mathbb{N}$.
$\Longrightarrow$ $n^2 = 2l$ for some $l \in \mathbb{N}$.
$\Longrightarrow$ n^2 is even.

b) Assume that n is even. We show that in such case $42^n - 1$ is not a prime. To this end, notice that, since n is even, there must exist a natural number $k > 0$, such that $n = 2k$. It follows that $42^n - 1 = 42^{2k} - 1 = (42^k + 1)(42^k - 1)$. Therefore, we found two non-trivial divisors of $42^n - 1$, namely $(42^k + 1)$ and $(42^k - 1)$ (they are greater than 1, because $k > 0$). Thus, $42^n - 1$ cannot be a prime.

Detailed solution:
We consider two statements S and T. We have to show that $S \Longrightarrow T$ is true. To this end, we use an indirect direct proof, that is, we assume that T is false and show that, under this assumption S, must also be false.

Statement S**:** $42^n - 1$ is a prime.

Statement T**:** n is odd.

Indirect proof:
n is not odd.
$\Longrightarrow$ n is even.
$\Longrightarrow$ There exists a natural number, call it k, such that $k > 0$ and $n = 2k$.
$\Longrightarrow$ We have $42^n - 1 = 42^{2k} - 1 = (42^k + 1)(42^k - 1)$ for $k > 0$.
$\Longrightarrow$ There exist two non-trivial divisors of $42^n - 1$, namely $(42^k + 1)$ and $(42^k - 1)$.
$\Longrightarrow$ $42^n - 1$ is not a prime.

4.2 Case Distinction (2.6.5)

a) Let n be any natural number greater or equal 0. Let $n = 3k + c$, where $0 \leq c \leq 2$ and $k \in \mathbb{N}$. We have

$$\begin{aligned} n^3 + 2n + 6 &= (3k + c)^3 + 2(3k + c) + 6 \\ &= c^3 + 9c^2k + 27ck^2 + 2c + 27k^3 + 6k + 6. \end{aligned}$$

Each summand is divisible by 3, except the term $c^3 + 2c$. Hence, we only need to show that $c^3 + 2c$ is divisible by 3 for $0 \leq c \leq 2$.

Case $c = 0$: $c^3 + 2c = 0$, which is divisible by 3.

Case $c = 1$: $c^3 + 2c = 3$, which is divisible by 3.

Case $c = 2$: $c^3 + 2c = 12$, which is divisible by 3.

Since the above cases cover all possibilities for c, we can conclude the proof.

b) In the following, we let $R_3(x)$ denote the remainder of the division of x by 3 (for example, $R_3(5) = 2$). For any prime number p, we can distinguish the following three cases:

$p = 2$: If $p = 2$, then $p^2 + 2 = 6$ is not a prime. Thus, the claim holds for $p = 2$.

$p = 3$: If $p = 3$, then $p^2 + 2 = 11$ is a prime. However, we now have $p^3 + 2 = 29$, which is also a prime. Thus, the claim also holds for $p = 3$.

$p > 3$: If $p > 3$ is a prime, then 3 cannot divide p. Therefore, we have $R_3(p) \in \{1, 2\}$. Thus, it holds that

$$R_3(p^2) = R_3(R_3(p) \cdot R_3(p)) = 1.$$

It follows that

$$R_3(p^2 + 2) = R_3(R_3(p^2) + R_3(2)) = R_3(1 + 2) = 0$$

Therefore, $p^2 + 2$ must be divisible by 3 and so it is not a prime. Thus, the claim holds also for $p > 3$.

Since the above cases cover all prime numbers, the claim holds.

4.3 Proof by Contradiction (2.6.6)

a) Let x be any irrational number and let r be any rational number. Assume that $s = x + r$ is rational. To reach a contradiction, we show that in such case x must be rational. Indeed, we have $x = s - r$. Therefore, we have that x is a difference of two rational numbers and thus, by the fact from the hint, it must also be rational. This is a contradiction with the assumption that x is irrational.

Detailed solution:
Consider a statement S. To show that S is true, we will state a false statement T, and show that if S is false, then T is true.

Fix any irrational number x and any rational number r.

Statement S: The sum $x + r$ is irrational.

Statement T**:** x is rational.

Proof by contradiction:

We show that if S is false, then T is true:

S is false.
$\implies$ It is not true that the sum $x + r$ is irrational.
$\implies$ The sum $s = x + r$ is rational.
$\implies$ $x = s - r$, where s and r are some rational numbers.
$\implies$ x is rational. (by the fact from the hint)
$\implies$ T is true.

The statement T is trivially false.

b) Assume for contradiction that $2^{\frac{1}{n}}$ is rational for some $n > 2$. That is, assume that there exist two positive integers, call them p and q, such that $2^{\frac{1}{n}} = \frac{p}{q}$. This implies that $2 = \frac{p^n}{q^n}$. Hence, we have $q^n + q^n = p^n$, which is a contradiction with Fermat's Last Theorem.

The contradiction with Fermat's Last Theorem follows from the counterexample $q^n + q^n = p^n$.

Detailed solution:

Fix any integer $n > 2$.

Statement S**:** $2^{\frac{1}{n}}$ is irrational.

Statement T**:** There exist positive integers p, q such that $q^n + q^n = p^n$.

Proof by contradiction:

We show that if S is false, then T is true:

S is false.
$\implies$ It is not true that $2^{\frac{1}{n}}$ is irrational.
$\implies$ $2^{\frac{1}{n}}$ is rational.
$\implies$ There exist positive integers p and q such that $2^{\frac{1}{n}} = \frac{p}{q}$.
$\implies$ There exist positive integers p and q such that $2 = \frac{p^n}{q^n}$.
$\implies$ There exist positive integers p and q such that $q^n + q^n = p^n$.
$\implies$ T is true.

The statement T is false, since it is a counterexample to Fermat's Last Theorem.

4.4 Pigeonhole Principle (2.6.8)

a) Let us consider the great circle[1] passing through two of the five points. There are two closed hemispheres, having this great circle as the border. Note that the two points lie on both of these hemispheres. By the pigeonhole principle, two of the remaining three points must lie on the same hemisphere (note that these hemispheres are not disjoint). Thus, this hemisphere must contain four points (together with the two on the great circle).

b) For every day i of November ($1 \leq i \leq 30$), let us consider the number a_i of bananas eaten by the monkey until that day (together with the day i). That is, on the first day it ate a_1 bananas, during the first two days it ate a_2, and so on. Further, let $b_i = a_i + 14$ for $1 \leq i \leq 30$.

First, note that for each $i \in \{1, \ldots, 30\}$, it holds that $1 \leq a_i < b_i \leq 59$ (the last inequality follows from the fact that the monkey had only 45 bananas and $45 + 14 = 59$).

[1] A great circle of a sphere is the largest circle that can be drawn on this sphere.

Hence, we have 60 numbers $a_1, \ldots, a_{30}, b_1, \ldots, b_{30}$, all between 1 and 59. By the pigeonhole principle, at least two of these numbers must be equal.

Notice now that we have $a_1 < a_2 < \cdots < a_{30}$, since the monkey ate at least one banana every day. By the definition of b_i, the same must hold for the sequence $b_1, \ldots, b_{30}$, that is $b_1 < b_2 < \cdots < b_{30}$. Therefore, the two equal numbers must be a_i and b_j for some i, j. Note further that we must have $i > j$. Otherwise, we would have $a_i = b_j$ for $i \leq j$. But since $b_j > a_j$, it would follow that $a_i > a_j$ for $i \leq j$, which is the contradiction with the fact that $a_1 < a_2 < \cdots < a_{30}$.

Thus, we have $a_i = b_j$ for some $j < i$. It follows that $a_i = 14 + a_j$ and, hence, $a_i - a_j = 14$. The value $a_i - a_j$ is exactly the amount of bananas the monkey ate between days j and i (including day i and excluding day j).

4.5 On the Soundness of a new Proof Pattern

a) $(\neg C \to A) \land (\neg C \to B) \land \neg(A \land B) \models C$.

b) Let $F = (\neg C \to A) \land (\neg C \to B) \land \neg(A \land B)$ and $G = C$. In order to decide whether $F \models G$ is true, we compute the function table of both F and G:

A	B	C	$\neg C \to A$	$\neg C \to B$	$\neg(A \land B)$	F	G
0	0	0	0	0	1	0	0
0	0	1	1	1	1	1	1
0	1	0	0	1	1	0	0
0	1	1	1	1	1	1	1
1	0	0	1	0	1	0	0
1	0	1	1	1	1	1	1
1	1	0	1	1	0	0	0
1	1	1	1	1	0	0	1

The function table shows that for any truth assignment for which F is true, G is true as well. Hence, $F \models G$ (the proof pattern is sound).

Part 2: Set Theory

4.6 Element or Subset

i)	$A \in B$ and $A \not\subseteq B$	**ii)**	$A \in B$ and $A \subseteq B$
iii)	$A \notin B$ and $A \subseteq B$	**iv)**	$A \in B$ and $A \subseteq B$

4.7 Operations on Sets

The following sets fulfill the conditions:

a) $A = \{\varnothing\}$
For $x = \varnothing$ we have $x \in A$. Also, the empty set is the subset of any other set, so $x \subseteq A$.
This is not the only solution. For example, $A = \{7, \{7\}\}$ also fulfills the given condition.

b) $A = \{\varnothing, 1\}$
We have $\mathcal{P}(A) = \{\varnothing, \{\varnothing\}, \{1\}, \{\varnothing, 1\}\}$. Since $1 \notin \mathcal{P}(A)$, it holds that $A \not\subseteq \mathcal{P}(A)$. Also, for $x = \varnothing$ we have $x \in A$ and $x \subseteq \mathcal{P}(A)$ (since the empty set is the subset of any set).

c) $A = \varnothing$
We have $\varnothing \subseteq \mathcal{P}(A)$. The second requirement is trivially fulfilled, since A has no elements.

4.8 Cardinality

First, notice that $A = \{\varnothing, \{\varnothing\}\}$. With that said, we give the solutions to individual subtasks:

i) $A \cup B = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$, $|A \cup B| = 4$

ii) $A \cap B = \{\{\varnothing\}\}$, $|A \cap B| = 1$

iii) $\varnothing \times A = \varnothing$, $|\varnothing \times A| = 0$

iv) $\{0\} \times \{3, 1\} = \{(0, 3), (0, 1)\}$, $|\{0\} \times \{3, 1\}| = 2$

v) $\{\{1, 2\}\} \times \{3\} = \{(\{1, 2\}, 3)\}$, $|\{\{1, 2\}\} \times \{3\}| = 1$

vi) $\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$, $|\mathcal{P}(\{\varnothing\})| = 2$