ETH Zürich, D-INFK
HS 2017, 5. Oktober 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik
Solution 3

Part 1: Predicate logic

3.1 Quantifiers and predicates

a)

i) $\forall m\, \forall n\, \big(0 < m \cdot n \rightarrow (0 < m \vee 0 < n)\big)$ *(2 Points)*
This statement is false. For example, $(-2) \cdot (-2) = 4$.

ii) $\forall m\, \big(0 < m \rightarrow \exists n\big(0 < n \wedge m < n \wedge (\exists k\, n = 3 \cdot k)\big)\big)$ *(2 Points)*
This statement is true. For any n, one of the numbers $n+1$, $n+2$, $n+3$ must be divisible by 3.

In the formula above, we assumed that 0 is not a natural number. An (equally good) solution for the case when 0 is a natural number would be
$\forall m\, \big(-1 < m \rightarrow \exists n\big(-1 < n \wedge m < n \wedge (\exists k\, n = 3 \cdot k)\big)\big)$

It is also allowed to drop the condition $0 < n$ (respectively, $-1 < n$), since it is implied by $m < n$.

iii) $\forall n\, \big(((\exists k\, n = 2 \cdot k) \wedge 2 < n) \rightarrow \exists p\, \exists q\, (\texttt{prime}(p) \wedge \texttt{prime}(q) \wedge n = p + q)\big)$ *(2 Points)*
This statement is known as the (strong) Goldbach conjecture. It is not known whether it is true.

b) There are many equally good ways to describe given formulas using words. We only give examples:

i) "For every integer x, there exists an integer y, such that xy is equal to 1." *(1 Point)*

An alternative solution would be "Each integer has a multiplicative inverse."

This statement is false. For example, there is no integer that will give 1 when multiplied by 5. *(1 Point)*

ii) "There exists an integer x, such that for all integers y, the product xy is not equal to 1, and such that there exists an integer greater than 0." *(1 Point)*

This statement is true. For $x = 0$, we have that for any integer y, the product xy is not equal to 1, and that there exists a positive integer, namely 42. *(1 Point)*

Be careful, the following interpretation is *not* correct (Why?):

"There exists an integer x, such that for all integers y, the product xy is not equal to 1 and y is positive."

3.2 Transitivity of quantifiers

a) Assume that the formula $\exists y\, \forall x\, P(x, y)$ is true. By the definition of $\exists$, there exists at least one y such that $\forall x\, P(x, y)$ is true. Let y^* be such a y. By the definition of $\forall$, we have that $P(x, y^*)$ is true for all x.
Therefore, we have that for all x there exists a y, namely y^*, for which $P(x, y)$ is true. This means exactly that $\forall x\, \exists y\, P(x, y)$ is true.

b) Consider the following counterexample: the universe is the set $\mathbb{Z}$ of all integers and P is the predicate `less`. In this interpretation, it is true that $\forall x\, \exists y \quad x < y$, but the statement $\exists y\, \forall x \quad x < y$ is false.

3.3 Winning strategy

a) The numbers announced by Alice cannot depend on Bob's choice for b_1 and b_2. Therefore, the statement can be described by the following formula:

$$\exists a_1 \exists a_2 \forall b_1 \forall b_2 \ \left(a_1 + (a_2 + b_1)^{|b_2|+1} = 1\right).$$

The above statement is false, because for each tuple (a_1, a_2), there exists a tuple $(b_1, b_2) := (2 - a_2 - a_1, 0)$ such that

$$a_1 + (a_2 + b_1)^{|b_2|+1} = a_1 + (a_2 + 2 - a_2 - a_1) = 2.$$

Therefore, Alice does not have a winning strategy.

b) In this case, Alice's choice for a_2 can depend on b_1. Therefore, the statement can be described by the following formula:

$$\exists a_1 \forall b_1 \exists a_2 \forall b_2 \ \left(a_1 + (a_2 + b_1)^{|b_2|+1} = 1\right).$$

This statement is true. A possible winning strategy for Alice is to choose $a_1 = 1$ and $a_2 = -b_1$. For such choice, we have

$$a_1 + (a_2 + b_1)^{|b_2|+1} = 1 + 0^{|b_2|+1} = 1.$$

Part 2: Proof techniques

3.4 Direct Proof of an Implication (2.4.3)

a) Let m and n be any two even natural numbers. Therefore, there must also exist two natural numbers a and b such that $m = 2a$ and $n = 2b$. We have $nm = (2a)(2b) = 4ab = 2(2ab)$. Thus, the product mn is also even, because there exists a natural number c, namely $c = 2ab$, such that $mn = 2c$.

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

Statement S**:** n and m are even natural numbers.

Statement T**:** nm is an even natural number.

Direct proof:
n and m are even natural numbers.
$\Rightarrow$ There exist two natural numbers, call them a and b, such that $n = 2a$ and $m = 2b$.
$\Rightarrow$ We have $nm = (2a)(2b) = 4ab = 2(2ab)$.
$\Rightarrow$ There exists a natural number c, namely $c = 2ab$, such that $nm = 2c$.
$\Rightarrow$ nm is an even natural number.

3.5 Indirect Proof of an Implication (2.4.4)

a) 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.

Formal solution:
We consider two statements S and T. We have to show that $S \implies T$ 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.
$\Rightarrow$ n is even.
$\Rightarrow$ There exists a natural number, call it k, such that $k > 0$ and $n = 2k$.
$\Rightarrow$ We have $42^n - 1 = 42^{2k} - 1 = (42^k + 1)(42^k - 1)$ for $k > 0$.
$\Rightarrow$ There exist two non-trivial divisors of $42^n - 1$, namely $(42^k + 1)$ and $(42^k - 1)$.
$\Rightarrow$ $42^n - 1$ is not a prime.

b) Assume that n is even. By the subtask 3.4 a), it follows that $n^2 = n \cdot n$ is also even.

Formal solution:

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

Statement T**:** n is odd.

Indirect proof:
n is not odd.
$\Rightarrow$ n is even.
$\Rightarrow$ $n \cdot n$ is even. (by subtask 3.4 a))
$\Rightarrow$ n^2 is even.

3.6 Case Distinction (2.4.7)

a) We can distinguish two cases, each of which we prove using a direct proof of an implication:

n **is even:** If n is even, then also $5n^2$ and $3n$ are even. Since the sum of even numbers is also even, $5n^2 + 3n + 42$ must be even. Thus, the claim holds in this case.

n **is odd:** If n is odd, then $5n^2$ and $3n$ are also odd. Since the sum of two odd numbers is even, $5n^2 + 3n$ must be even. Therefore, $5n^2 + 3n + 42$ is even as well. Thus, the claim holds in this case also.

Since the above cases cover all integers, the claim holds.

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.