DMMR Tutorial sheet 4

Inductions, Modulo, Primes

October 14, 2014

Some of the exercises for this tutorial are taken from the book: Kenneth Rosen, Discrete Mathematics and its Applications, 7th Edition, McGraw-Hill, 2012.

1. Prove the following claim by induction: "Every positive integer $n \in \mathbb{N}, n > 1$ is divisible by a prime number"

   Solution:
   We prove this statement by strong induction: **Base Case** $n = 2$**:** 2 is a prime number itself and therefore divisible by the prime number 2. **Induction Hypothesis:** Let $n \in \mathbb{N}, n > 2$ such that all $k \in \mathbb{N}$ with $2 < k < n$ are divisible by a prime number. **Induction Step:** We now look at n itself. If n is a prime number than n is trivially divisible by the prime number n. If n is not a prime number, then by definition of prime, it is divisible by a number $k < n$. For k we have the induction hypothesis and therefore k is divisible by a prime number. By transitivity of the definition of "divide" we get that n is divisible by this prime number as well. □

2. Use strong induction to show that every positive integer n can be written as a sum of distinct powers of two, that is, as a sum of a subset of the integers $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, and so on. [Hint: For the inductive step at stage $k + 1$, separately consider the case where $k + 1$ is even and where it is odd. When it is even, note that $(k + 1)/2$ is an integer.]

   Before beginning your proof, state the property (the one you are asked to prove for every integer n) in completely formal notation with all quantifiers.

   Solution:
   The sentence we are required to prove can be stated formally as follows:

   $$\forall\, n \in \mathbb{Z}^+ \;\exists\, a_1, a_2, a_3, \ldots, a_m \in \mathbb{N}$$
   $$[(\forall\, i, j \in \{1, \ldots, m\}\; i \neq j \longrightarrow a_i \neq a_j) \wedge n = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}]$$

   or more concisely as follows:

   $$\forall\, n \in \mathbb{Z}^+ \;\exists\, S \subseteq \mathbb{N} \left(n = \sum_{a \in S} 2^a \right)$$

   Base case: The sum with a single element 2^0 equals 1.

   Inductive Hypothesis: We assume that every l, with $l \leq k$, is the sum of distinct powers of two and then prove it for $k + 1$ by splitting in cases where $k + 1$ is even and when it is odd.

   Inductive Step: *Case 1:* If $k+1$ is even then $(k+1)/2$ is an integer and $(k+1)/2 \leq k$. Using the inductive hypothesis we can write $(k + 1)/2$ as $2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}$ where all a_i's are distinct.

Then,

$$\begin{aligned} k+1 &= 2(2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}) \\ &= 2 \cdot 2^{a_1} + 2 \cdot 2^{a_2} + \cdots + 2 \cdot 2^{a_m} \\ &= 2^{a_1+1} + 2^{a_2+1} + \cdots + 2^{a_m+1} \end{aligned}$$

These are clearly distinct powers of two, thus we have proved what we wanted.

Case 2: If $k+1$ is odd we apply the inductive hypothesis to k to get $k = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}$. However, we know that $a_i \neq 0$ for every i with $1 \leq i \leq m$ because otherwise exactly one element of the sum would be $2^0 = 1$ and the rest would be even numbers, and thus k would be odd. Therefore,

$$\begin{aligned} k+1 &= 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m} + 1 \\ &= 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m} + 2^0 \end{aligned}$$

and $\{2^{a_1}, 2^{a_2}, \cdots, 2^{a_m}, 2^0\}$ are all distinct. □

3. What is wrong with this "proof"?

   "Theorem" For every positive integer n, if x and y are positive integers with $\max(x, y) = n$, then $x = y$.

   Base case: Suppose that $n = 1$. If $\max(x, y) = 1$ and x and y are positive integers, we have $x = 1$ and $y = 1$.

   Inductive Hypothesis: Let k be a positive integer. Assume that whenever $\max(x, y) = k$ and x and y are positive integers, then $x = y$. Now let $\max(x, y) = k + 1$, where x and y are positive integers.

   Inductive Step: Then $\max(x - 1, y - 1) = k$, so by the inductive hypothesis, $x - 1 = y - 1$. It follows that $x = y$, completing the inductive step.

   Solution:
   The result is clearly false, so the proof must be wrong. The base case proof is correct, so the problem has to be in the inductive step. The inductive hypothesis is stated correctly and it is true that if $\max(x, y) = k + 1$ then $\max(x - 1, y - 1) = k$, so the problem must be in *applying* the inductive hypothesis. Analysing the inductive hypothesis we see that it requires the numbers to be positive integers to conclude that they are equal. However, it is applied to the predecessors $x - 1$ and $y - 1$ of two positive integers, which are not necessarily positive. By incrementing the size of k starting from its value in the base case (1) we can find the place where the chain of dominoes first *breaks*. For $k = 2$ take $x = 2$ and $y = 1$. Then, $max(x, y) = 2$. However, $x - 1 = 1$ and $y - 1 = 0$. These numbers are not the values of x and y that we used for the base case; and if 0 had been allowed we would not have been able to prove the base case. Thus, the inductive chain breaks after the first domino. □

4. Let a, b, c, d, m be integers. Find counter examples to each of the following statements about congruences:

   (a) if $ac \equiv bc \pmod{m}$ with $m \geq 2$, then $a \equiv b \pmod{m}$

   (b) if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$

   Solution:

(a) With $m = c = 2$ and $a = 0, b = 1$ we get $ac \equiv 0 \cdot 2 \equiv 0 \equiv 2 \equiv 1 \cdot 2 \equiv bc \pmod 2$, but $0 \mod 2 = 0 \neq 1 = 1 \mod 2$ and therefore $1 \not\equiv 0 \pmod 2$

(b) With $m = 3$, $a = 2 \equiv 5 = b \pmod 3$ and $c = 1 \equiv 4 \pmod 3$ we get $a^c \mod 3 = 2^4 \mod 3 = 16 \mod 3 = 1$, but $b^d \mod 3 = 5^1 \mod 3 = 5 \mod 3 = 2$. Since $2 \neq 1$ it follows that $a^c \not\equiv b^d \pmod m$

□

5. Let $n \geq 0$ be an integer. Prove by induction:

(a) 8 divides $3^{2n+2} + 7$

(b) 64 divides $3^{2n+2} + 56n + 55$

Solution:

(a) 5 points. We prove this as induction over n:
Base case: For $n = 0$ we get $3^2 + 7 = 9 + 7 = 16$. 8 divides 16 since $16 = 2 \cdot 8$
Induction Hypothesis: Assume 8 divides $3^{2n+2} + 7$.
Induction Step: with (n+1) we get

$$\begin{aligned} & 3^{2(n+1)+2} + 7 \\ =& 3^{2n+2+2} + 7 \\ =& 3^{2n+2} \cdot 9 + 7 \\ =& 3^{2n+2} \cdot 8 + 3^{2n+2} + 7 \end{aligned}$$

By the IH we know that $3^{2n+2} + 7$ is presentable as $c \cdot 8$. Therefore we get $3^{2(n+1)+2} + 7 = (3^{2n+2} + c) \cdot 8$. Since $(3^{2n+2} + c) \in \mathbb{Z}$ this means 8 divides $3^{2(n+1)+2} + 7$ by definition.
By the induction principle 8 divides $(3^{2n+2} + 7)$ for every $n \geq 0$

(b) 6 points. Proof by induction over n:
Base case: For $n = 0$ we get $3^2 + 55 = 9 + 55 = 64$. 64 divides 64 since $64 \cdot 1 = 64$.
Induction Hypothesis: Assume 64 divides $3^{2n+2} + 56n + 55$ for some $n \geq 0$
Induction Step: For $n + 1$ we get:

$$\begin{aligned} & 3^{2(n+1)+2} + 56(n+1) + 55 \\ =& 3^{2n+2} + 56n + 55 + 3^{2n+2} \cdot 8 + 56 \\ =& 3^{2n+2} + 56n + 55 + (3^{2n+2} + 7) \cdot 8 \end{aligned}$$

For the IH we know 8 divides $3^{2n+2} + 56n + 55$ and therefore $3^{2n+2} + 56n + 55 = 64 \cdot c$ for some $c \in \mathbb{Z}$. From a) we know that 8 divides $(3^{2n+2} + 7)$ and therefore $(3^{2n+2} + 7) = 8 \cdot c'$ for some $c' \in \mathbb{Z}$. This means $(3^{2n+2} + 7) \cdot 8 = c' \cdot 8 \cdot 8 = c' \cdot 64$. Together we get $3^{2(n+1)+2} + 56(n+1) + 55 = 64 \cdot (c + c')$. Since $c + c' \in \mathbb{Z}$ this means 64 divides $3^{2(n+1)+2} + 56(n+1) + 55$ by definition.
By the induction principle 64 divides $(3^{2n+2} + 56n + 55)$ for every $n \geq 0$

□

Solutions (to the last question on the sheet) must be handed in on paper at the ITO by Wednesday, 21 October, 4:00pm. Please post it into the grey metal box on the wall outside the ITO.