Algorithmic Foundations 2

Assessed Exercise 2

Notes for guidance

1. There are two assessed exercises. Each is worth 10% of your final grade for this module. Your answers must be the result of your own individual efforts.
2. Please use the latex template and submit your the generated pdf via moodle (do not submit the latex source file).
3. Please ensure you have filled out your tutorial group, name and student id.
4. **Failure to follow the submission instructions will lead to a penalty for non-adherence to submission instructions of 2 bands**.
5. As stated on the cover sheet deadline for completing this assessed exercise is **16:30 Monday, November 23, 2020**.
6. The exercise is marked out of 30 using the included marking scheme. Credit will be given for partial answers.

---

1. (a) Show that if n divides m where m and n are positive integers greater than 1, then $a \equiv b \pmod{m}$ implies $a \equiv b \pmod{n}$ for any positive integers a and b. [4]

Solution: Suppose n divides m where m and n are positive integers greater than 1 and a and b are positive integers such that $a \equiv b \pmod{m}$. Now by definition we have $m = k{\cdot}n$ for some positive integer k and m divides $a{-}b$, i.e. there exists l such that $a{-}b = l{\cdot}m$. Combing these facts we have $a{-}b = (l{\cdot}k){\cdot}n$, and hence $a \equiv b \pmod{n}$ as required.

(b) Show that $a{\cdot}c \equiv b{\cdot}c \pmod{m}$ with a, b, c and m integers with $m{\geq}2$ does not imply $a \equiv b \pmod{m}$. [3]

Solution: Consider $a = 2$, $b = 1$, $c = 2$ and $m = 2$, then 2 divides $a{\cdot}c - b{\cdot}c = 2$, while it does not divide $a - b = 1$. Hence we have $a{\cdot}c \equiv b{\cdot}c \pmod{m}$ while $a \not\equiv b \pmod{m}$.

(c) Using the Euclidean Algorithm, find $\texttt{gcd}(3084, 1424)$. Show your working. [3]

Solution:

$$
\begin{aligned}
3084 &= 1424{\cdot}2 + 236 \\
1424 &= 236{\cdot}6 + 8 \\
236 &= 8{\cdot}29 + 4 \\
8 &= 4{\cdot}2 + 0
\end{aligned}
$$

Therefore $\texttt{gcd}(3084, 1424) = 4$.

2. A company has a contract to cover the four walls, ceiling, and floor of a factory building with fire-retardant material. The building is rectangular where of width 280m, length 336m and height 168m. Square panels can be manufactured in any size of whole metres. For safety reasons, the building must be covered in complete panels (i.e. panels cannot be cut). What is the minimum number of equally sized square panels that are required to line the interior of the building? Explain your answer. [5]

Solution: The maximum size of square tiles (and therefore minimum number of tiles) is equal to $\texttt{gcd}(280, \texttt{gcd}(168, 336))$ where $\texttt{gcd}$ is the greatest common divisor.

Using the Euclidean algorithm, computing $\texttt{gcd}(168, 336)$, we have

$$336 = 168{\cdot}2 + 0$$

and hence $\texttt{gcd}(336, 168) = 168$. Next, considering $\texttt{gcd}(280, 168)$:

$$\begin{aligned} 280 &= 168{\cdot}1 + 112 \\ 168 &= 112{\cdot}1 + 56 \\ 112 &= 56{\cdot}2 + 0 \end{aligned}$$

yielding $\texttt{gcd}(280, 168) = 56$, and therefore $\texttt{gcd}(280, \texttt{gcd}(168, 336)) = 56$.

Since the maximim size of square tiles equals 56m, the minimum number of tiles we required equals

$$2{\cdot}((280/56){\cdot}(168/56) + (168/56){\cdot}(336/56) + (280/56){\cdot}(336/56))$$

i.e. the number of tiles for the two walls of size $280{\times}168$, two walls of size $336{\times}168$ and the floor and ceiling both of size $280{\times}336$. This yields 126 tiles in total.

3. Prove that least significant digit of the square of an even integer is either 0, 4, or 6. [5]

Hint: considering splitting into cases where integers are of the form $a{\cdot}k{+}b$ or $-(a{\cdot}k{+}b)$ for $k \in \mathbb{N}$ where a and b are fixed for a given case, b varies over the cases and the least significant digit of the integer depends on only b.

Note: the *least significant digit* of an integer is the digit farthest to the right in a integer. For example, the least significant digits of 1007 and 26 are 7 and 6 respectively.

Solution: We prove the property by cases. An even integer n can be expressed as $10{\cdot}k + 0$, $-(10{\cdot}k + 0)$, $10{\cdot}k + 2$, $-(10{\cdot}k + 2)$, $10{\cdot}k + 4$, $-(10{\cdot}k + 4)$, $10{\cdot}k + 6$, $-(10{\cdot}k + 6)$, $10{\cdot}k + 8$, or $-(10{\cdot}k + 8)$ where $k \in \mathbb{N}$. Considering the different cases and the fact that for any $l \in \mathbb{N}$ we have $(-l)^2 = l^2$ we have:

- $(10{\cdot}k)^2 = (-10{\cdot}k)^2 = 100{\cdot}k^2$, and therefore ends in 0;
- $(10{\cdot}k + 2)^2 = (-(10{\cdot}k + 2))^2 = 100{\cdot}k^2 + 40{\cdot}k + 4$, and therefore ends in 4;
- $(10{\cdot}k + 4)^2 = (-(10{\cdot}k + 4))^2 = 100{\cdot}k^2 + 80{\cdot}k + 16$, and therefore ends in 6;
- $(10{\cdot}k + 6)^2 = (-(10{\cdot}k + 6))^2 = 100{\cdot}k^2 + 120{\cdot}k + 36$, and therefore ends in 6
- $(10{\cdot}k + 8)^2 = (-(10{\cdot}k + 8))^2 = 100{\cdot}k^2 + 160{\cdot}k + 64$, and therefore ends in 4.

Since these are all the cases to consider, the square of an even integers ends in 0, 4, or 6 as required.

4. Use mathematical induction to show that for any $n \in \mathbb{N}$, if $n \geq 2$, then [5]

$$\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2 \cdot n} \,.$$

Solution: Let $P(n)$ be the proposition given in the question.

Basis cases: The cases when $n = 0$ and $n = 1$ trivially hold, while if n=2, then

$$1 - \frac{1}{2^2} = \frac{3}{4} = \frac{2+1}{2 \cdot 2}$$

and therefore $P(2)$ holds.

Inductive step: suppose $P(n)$ for some $n \geq 2$, considering n+1 we have:

$$\begin{aligned}
\prod_{i=2}^{n+1} \left(1 - \frac{1}{i^2}\right) &= \left(\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right)\right) \cdot \left(1 - \frac{1}{(n+1)^2}\right) \\
&= \left(\frac{n+1}{2 \cdot n}\right) \cdot \left(1 - \frac{1}{(n+1)^2}\right) && \text{by the inductive hypothesis} \\
&= \left(\frac{n+1}{2 \cdot n}\right) \cdot \left(\frac{(n+1)^2 - 1}{(n+1)^2}\right) && \text{rearranging} \\
&= \left(\frac{n+1}{2 \cdot n}\right) \cdot \left(\frac{n^2 + 2 \cdot n + 1 - 1}{(n+1)^2}\right) && \text{expanding} \\
&= \left(\frac{n+1}{2 \cdot n}\right) \cdot \left(\frac{n \cdot (n+2)}{(n+1)^2}\right) && \text{simplifying} \\
&= \frac{n+2}{2 \cdot (n+1)} && \text{simplifying again} \\
&= \frac{(n+1)+1}{2 \cdot (n+1)} && \text{rearranging.}
\end{aligned}$$

Therefore by the principle of induction we have proved that $P(n)$ holds for all $n \in \mathbb{N}$.

5. Use mathematical induction to show that 2 divides $n^2 - n$ for all $n \in \mathbb{N}$. [5]

Solution: Let $P(n)$ be the proposition 2 divides $n^2 - n$.

Base case: $P(0)$ hold since 2 divides $0 = 0^2 - 0$.

Inductive step: Suppose $n \geq 0$ and $P(n)$ holds. Considering $P(n{+}1)$ we have:

$$\begin{aligned}
(n{+}1)^2 - (n{+}1) &= n^2 + 2{\cdot}n + 1 - n - 1 & \\
&= n^2 + n & \text{simplifying} \\
&= (n^2 - n) + 2{\cdot}n & \text{rearranging}
\end{aligned}$$

By the inductive hypothesis, we have 2 divides $n^2 - n$ and, since clearly 2 divides $2{\cdot}n$, it follows that 2 divides $(n{+}1)^2 - (n{+}1)$, and hence $P(n{+}1)$ holds.

Therefore by the principle of induction we have proved that $P(n)$ holds for all $n \in \mathbb{N}$.