MA503: Homework 2

Exercise 2.1. [10pts] Solve a linear congruence $17x \equiv 3 \mod 210$.

Exercise 2.2. [5pts] Find a general solution for the linear Diophantine equation $1485x + 1745y = 15$.

Exercise 2.3. [10pts]

(a) [5pts] Find all units modulo 24. For each unit find its multiplicative inverse.
(b) [5pts] Compute $PPF(2520)$ and $\varphi(2520)$.

Exercise 2.4. [10pts] Solve the following system of congruences using $\sum c_i m_i d_i$ formula:

$$\begin{cases} x \equiv_7 3, \\ x \equiv_8 2, \\ x \equiv_9 1. \end{cases}$$

Exercise 2.5. [5pts] (RSA encryption) Let $n = 91$ and $e = 5$ be Alice's public information. Encrypt the message $m = 9$.

Exercise 2.6. [5pts] (Breaking RSA) Let $n = 77$ and $e = 7$ be Alice's public information. Let $c = 3$ be the cipher intercepted by Eve. Find the original message m.

Definition 2.1. Let G be a set and $\cdot$ a binary operation on G. The pair $(G, \cdot)$ is called a **group** if the following axioms (called group axioms) hold.

(G1) There exists $e \in G$ (called the **identity element** of G) such that $eg = ge = g$ for every $g \in G$. We often use the symbol 1 instead of e.
(G2) The binary operation $\cdot$ is **associative**.
(G3) For every $a \in G$ there exists $b \in G$ (called the **inverse** of a and denoted by a^{-1}) such that $ab = ba = e$.

For some groups we use additive notation, i.e., we use binary operation $+$. That slightly changes the axioms:

(G1) $\exists e$ such that $e + g = g + e = g$.
It is natural to use the symbol 0 instead of e for the operation $+$.
(G3) $\forall a \; \exists b$ such that $a + b = b + a = 0$.
It is natural to denote b as $-a$ in this case.

Exercise 2.7. [10pts] Check if the group axioms (G1), (G2), (G3) hold for the pairs $(G, \cdot)$ or $(G, +)$ in the table below. Put check marks in the corresponding cells. No explanation is required.

	(G1)	(G2)	(G3)
$(\mathbb{Z}, +)$			
$(\mathbb{Z}, \cdot)$			
$(\mathbb{N}, +)$			
$(\mathbb{N}, \cdot)$			
$(\mathbb{Z}_n, +)$			
$(\mathbb{Z}_n, \cdot)$			
$(\mathbb{Q}, +)$			
$(\mathbb{Q}, \cdot)$			
$(\mathbb{Q} \setminus \{0\}, +)$			
$(\mathbb{Q} \setminus \{0\}, \cdot)$			