MA503: Homework 2

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

Solution: The congruence $17x \equiv 3 \mod 210$ defines a linear Diophantine equation:

$$17x + 210y = 3,$$

that has a solution because $\gcd(17, 210) = 1$ divides 3. First, we solve the equation:

$$17x + 210y = \gcd(17, 210) = 1,$$

using Euclidean algorithm.

$$\begin{aligned} 210 &= 12 \cdot 17 + 6 & \Rightarrow \gcd(17, 210) &= \gcd(17, 6) \\ 17 &= 2 \cdot 6 + 5 & &= \gcd(5, 6) \\ 6 &= 1 \cdot 5 + 1 & &= \gcd(5, 1) \\ 5 &= 5 \cdot 1 + 0 & &= \gcd(0, 1) = 1. \end{aligned}$$

Hence

$$\begin{aligned} 1 &= 6 - 5 \\ &= 6 - (17 - 2 \cdot 6) = 3 \cdot 6 - 17 \\ &= 3 \cdot (210 - 12 \cdot 17) - 17 = 3 \cdot 210 - 37 \cdot 17. \end{aligned}$$

Multiplying the equality by 3 we get $3 = 9 \cdot 210 - 111 \cdot 17$. Hence, -111 is a solution. □

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

Solution: In homework #1 we found a solution $x = -47, y = 40$ for the lieaner Diophantine equation

$$1485x + 1745y = 5 = \gcd(1485, 1745).$$

Multiplying the number by 3 we get a particular solution $x_0 = -141, y_0 = 120$ for the equation

$$1485x + 1745y = 15.$$

Hence, a general solution of the given equation is

$$\begin{cases} x = -141 + \frac{1745}{5} n & = -141 + 349n \\ y = 120 - \frac{1485}{5} n & = 120 - 297n. \end{cases}$$

□

Exercise 2.3. [10pts]

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

Solution: (a)

$$\begin{aligned} U_{24} &= \{a \mid 0 \le a \le 23, \quad \gcd(a, 24) = 1\} \\ &= \{1, 5, 7, 11, 13, 17, 19, 23\}. \end{aligned}$$

It is easy to check that modulo 24 we have:

$$\begin{array}{llll} 1^{-1} = 1, & 5^{-1} = 5, & 7^{-1} = 7, & 11^{-1} = 11, \\ 13^{-1} = 13, & 17^{-1} = 17, & 19^{-1} = 19, & 23^{-1} = 23. \end{array}$$

(b) $PPF(2520) = 126 \cdot 20 = 3^2 \cdot 7 \cdot 2^3 \cdot 5$. Hence,

$$\varphi(2520) = (3^2 - 3^1) \cdot (7 - 7^0) \cdot (2^3 - 2^2) \cdot (5^1 - 5^0) = 576.$$

□

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

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

Solution: The moduli are pairwise coprime and hence the Chinese remainder theorem is applicable here.

$$\begin{array}{llll} n_1 = 7, & c_1 = 3, & m_1 = 72, & 72d_1 \equiv_7 1, & d_1 = 4 \\ n_2 = 8, & c_2 = 2, & m_2 = 63, & 63d_2 \equiv_8 1, & d_2 = -1 \\ n_3 = 9, & c_3 = 1, & m_3 = 56, & 56d_3 \equiv_9 1, & d_3 = 5 \end{array}$$

Hence, a particular solution can be found as:

$$x_0 = 3 \cdot 72 \cdot 4 + 2 \cdot 63 \cdot (-1) + 1 \cdot 56 \cdot 5 = 1018 \equiv_{7 \cdot 8 \cdot 9} 10.$$

□

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

Solution: The cipher is computed as the remainder of division of m^5 by $n = 91$.

$$9^5 = 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 = 81 \cdot 81 \cdot 9 \equiv_{91} (-10) \cdot (-10) \cdot 9 \equiv_{91} 100 \cdot 9 \equiv_{91} 9 \cdot 9 = 81.$$

Hence, $c = 81$. □

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.

Solution:

- We first factor $n = 77$ to get $p = 7$ and $q = 11$.
- Hence, $\varphi(n) = 60$.
- Then find the private exponent by solving the congruence $7d \equiv_{60} 1$. That gives $d = 43$.
- Finally, we decipher the message by taking the remainder of division of 3^{43} by 77. That gives 38.

Thus, the original message sent by Bob was 38. □

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. [+5pts] 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)
$(\mathbb{Z}, +)$			
$(\mathbb{Z}, \cdot)$			
$(\mathbb{N}, +)$			
$(\mathbb{N}, \cdot)$			
$(\mathbb{Z}_n, +)$			
$(\mathbb{Z}_n, \cdot)$			
$(\mathbb{Q}, +)$			
$(\mathbb{Q}, \cdot)$			
$(\{-1, 1\}, \cdot)$			
$(\mathbb{Q} \setminus \{0\}, \cdot)$			

Solution:

	(G1)	(G2)	(G3)
$(\mathbb{Z}, +)$	x	x	x
$(\mathbb{Z}, \cdot)$	x	x	
$(\mathbb{N}, +)$		x	
$(\mathbb{N}, \cdot)$	x	x	
$(\mathbb{Z}_n, +)$	x	x	x
$(\mathbb{Z}_n, \cdot)$	x	x	
$(\mathbb{Q}, +)$	x	x	x
$(\mathbb{Q}, \cdot)$	x	x	
$(\{-1, 1\}, \cdot)$	x	x	x
$(\mathbb{Q} \setminus \{0\}, \cdot)$	x	x	x

$\square$