EXERCISES: ELEMENTARY NUMBER THEORY

Margherita Maria Ferrari

1. *Find the quotient and the remainder in the division of* -33 *by* 12.

   Solution:
   We want to determine the integers q and r such that $-33 = 12 \cdot q + r$, where $0 \leq r < b$.
   From $33 = 12 \cdot 2 + 9$, we get $-33 = 12 \cdot (-2) - 9$. Since the remainder must be non-negative, we sum and substract 12 from the right side of the last equation; thus
   $$-33 = 12 \cdot (-3) + 3.$$
   Hence $q = -3$ and $r = 3$.

   We can obtain the same result using the following formulas:
   $$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{-33}{12} \right\rfloor = \lfloor -2.75 \rfloor = -3;$$
   and
   $$r = a - b \cdot \left\lfloor \frac{a}{b} \right\rfloor = -33 - 12 \cdot \left\lfloor \frac{-33}{12} \right\rfloor = -33 + 36 = 3.$$

2. *Represent* $(36, 10)$ *as integral linear combination of* 36 *and* 10.

   Solution:
   We want to find two integers x and y such that $(36, 10)$, the greatest common divisor of 36 and 10, can be written as
   $$(36, 10) = 36 \cdot x + 10 \cdot y.$$
   First of all we compute $(36, 10)$ using the Euclidean Algorithm:
   $$36 = 10 \cdot 3 + 6,$$
   $$10 = 6 \cdot 1 + 4$$
   $$6 = 4 \cdot 1 + 2,$$
   $$4 = 2 \cdot 2.$$
   Since $n = 4$, $(36, 10) = r_3 = 2$.
   We now reverse the steps of the Euclidean Algorithm to compute the required integers x and y.
   From the previous calculations we get:
   $$r_1 = 6 = 36 - 10 \cdot 3; \tag{1}$$
   $$r_2 = 4 = 10 - 6 \cdot 1; \tag{2}$$
   $$r_3 = 2 = 6 - 4 \cdot 1. \tag{3}$$

As a consequence

$$\begin{aligned}
2 &\underset{(3)}{=} 6 - 4 \cdot 1 \\
&\underset{(2)}{=} 6 - (10 - 6 \cdot 1) \\
&= 2 \cdot 6 - 10 \\
&\underset{(1)}{=} 2 \cdot (36 - 10 \cdot 3) - 10 \\
&= 2 \cdot 36 - 7 \cdot 10
\end{aligned}$$

Hence $x = 2$ and $y = -7$.

3. *Prove that a positive integer n is divisible by 2 (respectively 5) if and only if its unit digit is divisible by 2 (respectively 5).*

   Solution:
   We begin by establishing the condition about divisibility by 2.
   A positive integer $n \in \mathbb{N}$ can be written in the following way

   $$n = a_m a_{m-1} \cdots a_1 a_0,$$

   where each $a_i \in \mathbb{N}$ represents a digit of n.
   Moreover any positive integer n can be written in expanded base 10 form as

   $$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10^1 + a_0.$$

   Since $10 \equiv 0 \pmod 2$, we get

   $$n \equiv a_m \cdot 0^m + a_{m-1} \cdot 0^{m-1} + \cdots + a_1 \cdot 0^1 + a_0 \pmod 2;$$

   that is

   $$n \equiv a_0 \pmod 2.$$

   The last relation is equivalent to $n \bmod 2 = a_0 \bmod 2$.
   If $2|n$, then $n \bmod 2 = 0$, and so $a_0 \bmod 2 = 0$; which means $2|a_0$.
   If $2|a_0$, then $a_0 \bmod 2 = 0$, and so $n \bmod 2 = 0$; which means $2|n$.

   Since $10 \equiv 0 \pmod 5$, we can repeat the same argument to prove the result for 5.

4. *Prove that a positive integer n is divisible by 3 (respectively 9) if and only if the sum of its digits is divisible by 3 (respectively 9).*

   Hint: use the same argument of Exercise 3 together with the relation $10 \equiv 1 \pmod 3$ (respectively $10 \equiv 1 \pmod 9$).

5. *Compute $3^{54} \bmod 11$.*

   Solution:
   We want to compute the remainder in the division of 3^{54} by 11.
   Since 11 is a prime number and $(3, 11) = 1$, we have that $3^{10} = 1$ in $\mathbb{Z}_{11}$ (by Fermat's Little Theorem).
   We now note that

   $$3^{54} = 3^{10} \cdot 3^{10} \cdot 3^{10} \cdot 3^{10} \cdot 3^{10} \cdot 3^4 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 4 \pmod{11}$$

   because $3^4 = 81 \equiv 4 \pmod{11}$ and $3^{10} \equiv 1 \pmod{11}$. As a consquence $3^{54} \equiv 4 \pmod{11}$ and this implies that $3^{54} \bmod 11 = 4 \bmod 11 = 4$.

6. *Compute the inverse of* 2 *in* $\mathbb{Z}_7$

   Solution:
   Since 7 is prime, the element $2 \in \mathbb{Z}_7$ is invertible; which means that exists a (unique) element $x \in \mathbb{Z}_7$ such that $2 \otimes x = 1$ in $\mathbb{Z}_7$. Such element x is called the inverse of 2 and denoted 2^{-1}.
   To compute the inverse of 2 we can apply the following result:

   Let $a, m \in \mathbb{Z}$, with $m > 0$. If $(a, m) = 1$, then $a^{\phi(m)-1}$ is the inverse of a in $\mathbb{Z}_m$, where $\phi(m)$ denotes the number of integers x in the range $1 \leq x \leq n$ such that x and m are coprime.

   Thus in our case we get
   $$2^{-1} = 2^{\phi(7)-1},$$
   where $\phi(7) = |\{a : 1 \leq a \leq 7 \text{ and } (a, 7) = 1\}|$.
   Since 7 is prime, $\phi(7) = 6$. As a consequence we obtain that
   $$2^{-1} = 2^{6-1} = 2^5 = 32 \equiv 4 \pmod{7};$$
   hence $2^{-1} = 4$ in $\mathbb{Z}_7$.

7. *Determine the solution of the system of linear congruences*
   $$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \end{cases}$$

   Solution:
   To solve the exercise we apply the Chinese Remainder Theorem. In this case $b_1 = 1$, $b_2 = 2$, $m_1 = 3$, $m_2 = 5$, $M = m_1 \cdot m_2 = 15$, $M_1 = \frac{M}{m_1} = 5$ and $M_2 = \frac{M}{m_2} = 3$. Since $(m_1, m_2) = 1$, the system has a unique solution modulo M that is
   $$b_1 x_1 M_1 + b_2 x_2 M_2,$$
   where x_i is the inverse of M_i in $\mathbb{Z}_{m_i}$, for $i = 1, 2$. The inverse of 5 in $\mathbb{Z}_3$ is $x_1 = 2$ and the inverse of 3 in $\mathbb{Z}_5$ is $x_2 = 2$. Thus the solution is
   $$b_1 x_1 M_1 + b_2 x_2 M_2 = 1 \cdot 2 \cdot 5 + 2 \cdot 2 \cdot 3 = 22 \equiv 7 \pmod{15}.$$