Exercise 1 For each of the following pairs of integers \( a \) and \( b \),

(i) \( a=20, \ b=13 \)

(ii) \( a=792, \ b=275 \)

(iii) \( a=11391, \ b=1567 \)

determine the greatest common divisor \((a, b)\) and write \((a, b)\) in the form \( ax + by \) for some integers \( x \) and \( y \).

Solution.

(i) Using the Euclidean algorithm, we have

\[
\begin{align*}
20 &= 1 \cdot 13 + 7 \\
13 &= 1 \cdot 7 + 6 \\
7 &= 1 \cdot 6 + 1 \\
6 &= 6 \cdot 1 + 0,
\end{align*}
\]

so \((20, 13) = 1\). Furthermore, \(20 \cdot 2 + 13 \cdot (-3) = 1\).

(ii) Again, using the Euclidean algorithm, we have

\[
\begin{align*}
792 &= 2 \cdot 275 + 242 \\
275 &= 1 \cdot 242 + 33 \\
242 &= 7 \cdot 33 + 11 \\
33 &= 3 \cdot 11 + 0,
\end{align*}
\]

so \((792, 275) = 11\). Moreover, \(792 \cdot 8 + 275 \cdot (-23) = 11\).

(iii) Finally, by the Euclidean algorithm, we have

\[
\begin{align*}
11391 &= 7 \cdot 1567 + 422 \\
1567 &= 3 \cdot 422 + 301 \\
422 &= 1 \cdot 301 + 121 \\
301 &= 2 \cdot 121 + 59 \\
121 &= 2 \cdot 59 + 3 \\
59 &= 19 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0,
\end{align*}
\]

so \((11391, 1567) = 1\). Also, \(11391 \cdot 531 + 1567 \cdot (-3860) = 1\).■
Exercise 2 Show that if the integer $k$ divides the integers $a$ and $b$ then $k$ divides $as + bt$ for each pair of integers $s$ and $t$.

Proof. If $k|a$ and $k|b$, then $a = mk$ and $b = nk$ for some integers $m$ and $n$. It follows that $as = (ms)k$ and $bt = (nt)k$, so $as + bt = msk + ntk = k(ms + nt)$. Since $ms + nt$ is an integer, we have by definition that $k|(as + bt)$.

Exercise 3 Let $a, b$ be nonzero integers and let $p$ be a prime such that $p$ divides $ab$. Show that $p$ divides either $a$ or $b$.

Proof. Without loss of generality, suppose $p$ does not divide $a$. Since the only positive divisors of $p$ are 1 and $p$, $(a, p) = 1$. By a result proved in class using the Euclidean algorithm, there are integers $s$ and $t$ such that $as + pt = 1$. It follows that $abs + bpt = b$. Further, since $p|ab$, $ab = pn$ for some integer $n$. Thus, $b = (pn)s + bpt = p(ns + bt)$, so by definition $p|b$.

Exercise 4 Prove that if $a = a_n10^n + a_{n-1}10^{n-1} + \cdots + a_110 + a_0$ is any positive integer, then $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}$.

Proof. We will first need a brief preliminary result:

Lemma For any $n \in \mathbb{N}$, $10^n - 1 = 9(10^{n-1} + 10^{n-2} + \cdots + 10 + 1)$.

Proof of Lemma. The result is obvious when $n = 1$. Thus, suppose $10^n - 1 = 9(10^{n-1} + 10^{n-2} + \cdots + 10 + 1)$. Then

\[
9(10^n + 10^{n-1} + 10^{n-2} + \cdots + 10 + 1) = (10 - 1)(10^n + 10^{n-1} + 10^{n-2} + \cdots + 10 + 1)
= (10 - 1)10^n + 9(10^{n-1} + 10^{n-2} + \cdots + 10 + 1)
= 10^{n+1} - 10^n + (10^n - 1)
= 10^{n+1} - 1.
\]

For the sake of brevity, let $T_n = 10^n + 10^{n-1} + \cdots + 10 + 1$. Now, note that

\[
a - (a_n + a_{n-1} + \cdots + a_1 + a_0) = a_n10^n + a_{n-1}10^{n-1} + \cdots + a_110 + a_0 - (a_n + a_{n-1} + \cdots + a_1 + a_0)
= (a_n(10^n - 1) + a_{n-1}(10^{n-1} - 1) + \cdots + a_1(10 - 1)
= 9a_nT_{n-1} + 9a_{n-1}T_{n-2} + \cdots + 9a_1T_0
= 9(a_nT_{n-1} + a_{n-1}T_{n-2} + \cdots + a_1T_0).
\]

Hence, we have that $a - (a_n + a_{n-1} + \cdots + a_1 + a_0)$ is divisible by 9, so by definition, $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}$.
Exercise 5 Compute the remainder when $37^{100}$ is divided by 29.

Solution. To rephrase the problem, we want to find an integer $0 \leq a < 29$ such that $a \equiv 37^{100} \pmod{29}$. First, since $37 \equiv 8 \pmod{29}$, $37^{100} \equiv 8^{100}$. Now,

$$8^2 = 64 \equiv 35 \equiv 6 \pmod{29},$$
$$8^4 = 6^2 = 36 \equiv 7 \pmod{29},$$
$$8^8 = 7^2 = 49 \equiv 20 \pmod{29},$$
$$8^{16} = 20^2 = 400 \equiv 23 \pmod{29}.$$  

It follows that

$$8^{28} = 8^{16}8^4$$
$$\equiv 23 \cdot 20 \cdot 7 \pmod{29}$$
$$= 3220 \pmod{29}$$
$$= 29 \cdot 111 + 1 \pmod{29}$$
$$\equiv 1 \pmod{29}.$$  

Further,

$$8^{100} = 8^{28 \cdot 3 + 16}$$
$$= (8^{28})^3 \cdot 8^{16}$$
$$\equiv 1^3 \cdot 23 \pmod{29}$$
$$= 23 \pmod{29}.$$  

Hence, the remainder is 23 when $37^{100}$ is divided by 29. ■

Exercise 6 (a) Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $0$ and $1$.

(b) Using part (a), prove for any integers $a$ and $b$ that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4.

Proof.

(a) Since $\mathbb{Z}/4\mathbb{Z}$ has only four elements, we can easily prove this by cases.

$$\bar{0}^2 = \bar{0}^2 = \bar{0},$$
$$\bar{1}^2 = \bar{1}^2 = \bar{1},$$
$$\bar{2}^2 = \bar{2}^2 = \bar{4} = \bar{0},$$
$$\bar{3}^2 = \bar{3}^2 = \bar{9} = \bar{1}.$$
(b) To rephrase the question, we want to show (in \( \mathbb{Z}/4\mathbb{Z} \)) that for all integers \( a \) and \( b \), \( a^2 + b^2 \neq 3 \). Since by (a), \( a^2 \) and \( b^2 \) can only be either 0 or 1, we can again do a proof by cases.

If \( a^2 = 0 \) and \( b^2 = 0 \), then \( a^2 + b^2 = a^2 + b^2 = 0 + 0 = 0 \).

If \( a^2 = 1 \) and \( b^2 = 0 \), then \( a^2 + b^2 = a^2 + b^2 = 1 + 0 = 1 \).

If \( a^2 = 0 \) and \( b^2 = 1 \), then \( a^2 + b^2 = a^2 + b^2 = 0 + 1 = 1 \).

If \( a^2 = 1 \) and \( b^2 = 1 \), then \( a^2 + b^2 = a^2 + b^2 = 1 + 1 = 2 \).

In all cases, \( a^2 + b^2 \neq 3 \), so \( a^2 + b^2 \) never leaves a remainder of 3 when divided by 4. ■

Exercise 7 Prove that if \( \bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times \), then \( \bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times \).

Proof. Since \( \bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times \), we know \( \bar{a}^{-1}, \bar{b}^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times \) as well. Now,

\[
(\bar{a} \cdot \bar{b})(\bar{b}^{-1} \bar{a}^{-1}) = \bar{a}(\bar{b} \cdot \bar{b}^{-1})\bar{a}^{-1} = \bar{a} \cdot e \cdot \bar{a}^{-1} = \bar{a} \cdot \bar{a}^{-1} = e,
\]

where \( e \) is the identity element of \( \mathbb{Z}/n\mathbb{Z} \). Similarly, \( (\bar{b}^{-1} \cdot \bar{a}^{-1})(\bar{a} \cdot \bar{b}) = e \), so \( \bar{a} \cdot \bar{b} \) has an inverse, and \( (\bar{a} \cdot \bar{b})^{-1} = \bar{b}^{-1} \bar{a}^{-1} \). Hence, \( \bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times \). ■

Exercise 8 For the pair of integers \( a = 13 \) and \( n = 20 \), show that \( a \) is relatively prime to \( n \) and determine the multiplicative inverse of \( \overline{13} \) in \( \mathbb{Z}/20\mathbb{Z} \).

Proof. By Exercise 1(i), 20 and 13 are relatively prime. Moreover, \( \overline{17} = (\overline{13})^{-1} \), since

\[
\overline{13} \cdot \overline{17} = \overline{13} \cdot 17 = 221 = \overline{1},
\]

which is the multiplicative identity in \( \mathbb{Z}/20\mathbb{Z} \). ■