Exercise 1. Describe the set \((\mathbb{Z}/12\mathbb{Z})^\times\). Give an inverse for each of its elements.

Solution.

1. The units of \(\mathbb{Z}/12\mathbb{Z}\) are exactly the elements of \(\mathbb{Z}/12\mathbb{Z}\) relatively prime with 12. Therefore, \((\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}\).

2. If you used the Euclidean algorithm to compute the gcd of these numbers with 12, you can apply the reverse algorithm to find the inverses, but since the set of units is very small, its quicker to guess them directly. Answers are:
   \((1)^{-1} = 1, (5)^{-1} = 5, (7)^{-1} = 7\) and \((11)^{-1} = 11\).

Exercise 2. Check 32 is invertible modulo 1265 and compute an inverse.

Solution.

1. We have: \(32 = 2^5\) and \(2 \nmid 1265\). Therefore, 32 and 1265 are relatively prime, i.e. 32 is invertible modulo 1265.

2. An inverse of 32 can be obtained by applying the Euclidean algorithm and then reverse it:

\[
\begin{align*}
1265 &= 32 \times 39 + 17 \\
39 &= 17 \times 2 + 5 \\
17 &= 5 \times 3 + 2 \\
3 &= 2 \times 1 + 1 \\
1 &= 1 \times 1 + 0 \\
\end{align*}
\]

You can reverse from line 4, and you will obtain:

\[
32 \times 593 + 1265 \times (-15) = 1
\]

Therefore 593 is the inverse of 32 modulo 1265.

Exercise 3. 1. Find all integers \(x \in \mathbb{Z}\) satisfying \(9x \equiv 3 \pmod{5}\).

Solution. The integers 3 and 5 are relatively prime, so we can multiply by the inverse of 3 on both sides to get:

\[
3x \equiv 1 \pmod{5}
\]

We have to find the inverse of 3 modulo 5. You can observe that:
3 \times 2 = 6 \equiv 1 \pmod{5},
so that 2 is an inverse modulo 5. Multiplying by 2 on both sides of the equation, we get \( x \equiv 2 \pmod{5} \).
As a result the solution set is the set of all integers \( x \) such that \( x \equiv 2 \pmod{5} \), that is, the set \( 2 + 5\mathbb{Z} \).

2. Find all integers \( x \in \mathbb{Z} \) satisfying \( 5x + 1 \equiv 4 \pmod{26} \).

\textit{Solution.} We can write the equation:

\[ 5x \equiv 3 \pmod{26} \]

If you multiply the equation by 5 (which is relatively prime with 26), you get the equivalent equation

\[ 25x \equiv 15 \pmod{26} \]

That is:

\[ -x \equiv 15 \pmod{26} \]

Therefore, the solution is:

\[ x \equiv 11 \pmod{26} \]

The solution set is \( 11 + 26\mathbb{Z} \).

\textbf{Exercise 4.} 1. Show that for any \( a \in \mathbb{Z} \), the integer \( a^2 \) is congruent either to 0 or to 1 modulo 4.

\textit{Solution.} Let \( a \) be an integer. Then there exists \( k \) such that \( a = 2k \) (when \( a \) is even) or \( a = 2k + 1 \) (when \( a \) is odd). In the first case, we have \( a^2 = (2k)^2 = 4k^2 \equiv 0 \pmod{4} \), and in the second case, we have

\[ a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4} \]

2. Show that for any \( a, b \in \mathbb{Z} \), the integer \( a^2 + b^2 \) cannot be congruent to 3 modulo 4.

\textit{Solution.} Using the result of question 1, the possible values for \( a^2 + b^2 \) modulo 4 are 0 (when both \( a^2 \) and \( b^2 \) are congruent to 0 modulo 4), 1 (when one of them is congruent to 1 modulo 4 and the other to 0) or 2 (when both are congruent to 1 modulo 4).

3. Can 1735 be written as a sum of two squares?

\textit{Solution.} You can check that 1735 is congruent to 3 modulo 4. Therefore, according to the previous result, it can’t be written as the sum of two squares.
**Exercise 5.** Show that the square of an integer never has 2, 3, 7 or 8 as its last digit. (Hint: work modulo 10)

*Solution.* Let $x$ be the square of the integer $y$.
You can study $y$ modulo 10 to prove this. Indeed the remainder in the Euclidean division of an integer by 10 is nothing but its last digit.

If $y \equiv 0 \pmod{10}$, $x \equiv 0 \pmod{10}$.
If $y \equiv 1 \pmod{10}$, $x \equiv 1 \pmod{10}$.
If $y \equiv 2 \pmod{10}$, $x \equiv 4 \pmod{10}$.
If $y \equiv 3 \pmod{10}$, $x \equiv 9 \pmod{10}$.
If $y \equiv 4 \pmod{10}$, $x \equiv 6 \pmod{10}$.
If $y \equiv 5 \pmod{10}$, $x \equiv 5 \pmod{10}$.
If $y \equiv 6 \pmod{10}$, $x \equiv 6 \pmod{10}$.
If $y \equiv 7 \pmod{10}$, $x \equiv 9 \pmod{10}$.
If $y \equiv 8 \pmod{10}$, $x \equiv 4 \pmod{10}$.
If $y \equiv 9 \pmod{10}$, $x \equiv 1 \pmod{10}$.

(You can write all of this in the form of a table) Therefore, the last digit of a square is never 2, 3, 7 or 8.

**Exercise 6** (Divisibility criteria). Let $a \geq 1$ be an integer. We may write

$$a = 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10 a_1 + a_0$$

for some $d \geq 0$ so that $a_0, \ldots, a_d$ are integers in the set $\{0, \ldots, 9\}$, with $a_d \neq 0$. The integers $a_d, \ldots, a_0$ are the digits of the integer $a$. Show that:

1. The integer $a$ is even if and only if its last digit $a_0$ is even.

   *Solution.*
   $$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10 a_1 + a_0 \pmod{2}$$

   But all powers of 10 greater than 1 are even. Therefore:

   $$a \equiv a_0 \pmod{2}$$

   And it follows that $a$ is even if and only if $a_0$ is even.

2. The integer $a$ is divisible by 5 if and only if its last digit $a_0$ is either 0 or 5.

   *Solution.*
   $$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10 a_1 + a_0 \pmod{5}$$

   But all powers of 10 greater than 1 are multiples of 5. Therefore:

   $$a \equiv a_0 \pmod{5}$$

   And it follows that $a$ is a multiple of 5 if and only if $a_0$ is 0 or 5 (only positive multiples of 5 inferior to 10).
3. The integer $a$ is divisible by 4 if and only if the number $10a_1 + a_0$ given by its last two digits is divisible by 4.

Solution.

$$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10a_1 + a_0 \pmod{4}$$

But all powers of 10 greater than 2 are multiples of 4. Therefore:

$$a \equiv 10a_1 + a_0 \pmod{4}$$

And it follows that $a$ is a multiple of 4 if and only if $10a_1 + a_0$ is a multiple of 4.

4. The integer $a$ is divisible by 3 if and only if the sum $a_d + \ldots + a_0$ of its digits is divisible by 3.

Solution.

$$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10a_1 + a_0 \pmod{3}$$

But $10 \equiv 1 \pmod{3}$. Therefore:

$$a \equiv a_d + \ldots + a_1 + a_0 \pmod{3}$$

And it follows that $a$ is a multiple of 3 if and only if the sum of its digits is a multiple of 3.

5. The integer $a$ is divisible by 9 if and only if the sum $a_d + \ldots + a_0$ of its digits is divisible by 9.

Solution.

$$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10a_1 + a_0 \pmod{9}$$

But $10 \equiv 1 \pmod{9}$. Therefore:

$$a \equiv a_d + \ldots + a_1 + a_0 \pmod{9}$$

And it follows that $a$ is a multiple of 9 if and only if the sum of its digits is a multiple of 9.

6. The integer $a$ is divisible by 11 if and only if the alternating sum

$$\sum_{k=0}^{d} (-1)^k a_k = (-1)^d a_d + (-1)^{d-1} a_{d-1} + \ldots + (-1)a_1 + a_0$$

of its digits is divisible by 11.

Solution.

$$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10a_1 + a_0 \pmod{11}$$
But $10 \equiv -1 \pmod{11}$. Therefore:

$$a \equiv (-1)^d a_d + (-1)^{d-1} a_{d-1} + \cdots - a_1 + a_0 \pmod{11}$$

And it follows that $a$ is a multiple of 11 if and only if the alternating sum of its digits is a multiple of 11.

7. Apply these criteria to determine the decomposition into prime factors of the integer 152460.

*Solution.* You can observe that:

11 | 152460 because the alternating sum of its digit is 0, a multiple of 11.

9 | 152460 because the sum of its digits is 18, a multiple of 9.

5 | 152460 because its last digit is 0.

4 | 152460 because 4 | 60.

Therefore $4 \times 5 \times 9 \times 11 | 152460$.

And we have: $152460 = (2^2 \times 5 \times 3^2 \times 11) \times 77$

In addition $77 = 7 \times 11$.

Therefore:

$$152460 = 2^2 \times 3^2 \times 5 \times 7 \times 11^2$$