Exercise 1 ([1, Exercise 13.2]). Let \( p \) be a prime and \( k \) a positive integer.

(a) Show that if \( x \) is an integer such that \( x^2 \equiv x \mod p \), then \( x \equiv 0 \) or \( 1 \mod p \).

(b) Show that if \( x \) is an integer such that \( x^2 \equiv x \mod p^k \), then \( x \equiv 0 \) or \( 1 \mod p^k \).

Solution. Let \( x \) be an integer such that \( x^2 \equiv x \mod p^k \). Then

\[
x^2 - x = p^k n
\]

for some integer \( n \). Since \( \gcd(x - 1, x) = 1 \), it follows from [1, Proposition 10.5] that

- either \( p \mid x \),
- or \( p \mid (x - 1) \),

because \( x(x - 1) = p^k n \).

Suppose that \( p \mid x \). Then \( p \) does not divide \( (x - 1) \), since \( \gcd(x - 1, x) = 1 \). Then

\[
\frac{x}{p}(x - 1) = p^{k-1}n,
\]

which implies that \( p^{k-1} \) divides \( x/p \) by [1, Proposition 10.5], because \( \gcd(x - 1, p^{k-1}) = 1 \), since \( p \) does not divide \( (x - 1) \). Thus, we see that \( x \) is divisible by \( p^k \). Then \( x \equiv 0 \mod p^k \).

Suppose now that \( p \mid (x - 1) \). Then \( p \) does not divide \( x \), since \( \gcd(x - 1, x) = 1 \). Then

\[
\frac{x - 1}{p}x = p^{k-1}n,
\]

which implies that \( p^{k-1} \) divides \( (x - 1)/p \) by [1, Proposition 10.5], because \( \gcd(x, p^{k-1}) = 1 \), since \( p \) does not divide \( x \). Thus, we see that \( (x - 1) \) is divisible by \( p^k \). Then \( x \equiv 1 \mod p^k \).

Thus, we proved that if \( x \) is an integer such that \( x^2 \equiv x \mod p^k \),

then \( x \equiv 0 \) or \( 1 \mod p^k \).

Exercise 2 ([1, Exercise 13.4]). (a) Prove the “rule of 9”: an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

(b) Prove the “rule of 11” stated in [1, Example 13.6]. Use this rule to decide in you head whether the number 82918073579 is divisible by 11.

Solution. Let \( N \) be an integer. Then its decimal representation is

\[
\pm a_na_{n-1}a_{n-2} \ldots a_3a_2a_1a_0,
\]

where \( a_i \) is a digit in \( \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \), and \( n \) is a positive integer. Then

\[
N = \pm \sum_{i=0}^{N} a_i10^i.
\]
Since $10 \equiv 1 \mod 9$, we have
\[ N \equiv \pm \sum_{i=0}^{N} a_i 10^i \equiv \pm \sum_{i=0}^{N} a_i \mod 9, \]
which implies that
\[ N \equiv 0 \mod 9 \iff \sum_{i=0}^{N} a_i \equiv 0 \mod 9, \]
which implies that $N$ is divisible by 9 if and only if the sum of its digits is divisible by 9.
Thus, we proved the “rule of 9”. Let us prove the “rule of 11” stated in [1, Example 13.6].
Since $10 \equiv -1 \mod 11$, we have
\[ N \equiv \pm \sum_{i=0}^{N} a_i 10^i \equiv \pm \sum_{i=0}^{N} (-1)^i a_i \mod 11, \]
which implies that
\[ N \equiv 0 \mod 11 \iff \sum_{i=0}^{N} (-1)^i a_i \equiv 0 \mod 11, \]
which implies that $N$ is divisible by 11 if and only if
\[ a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \]
is divisible by 11.
Since we have $8 - 2 + 9 - 1 + 8 - 0 + 7 - 3 + 5 - 7 + 9 = 33$ and 33 is divisible by 11, we see that 82918073579 is also divisible by 11.

**Exercise 3 ([1, Exercise 13.10])**: Construct the addition and multiplication table for $\mathbb{Z}_6$.
Find all solutions in $\mathbb{Z}_6$ of the equation $x^2 + x = 0$.

**Solution.** Recall that $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. The addition table for $\mathbb{Z}_6$ is
\[
+ \begin{array}{cccccc}
0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 & 0 \\
2 & 2 & 3 & 4 & 5 & 0 & 1 \\
3 & 3 & 4 & 5 & 0 & 1 & 2 \\
4 & 4 & 5 & 0 & 1 & 2 & 3 \\
5 & 5 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
\]

and the multiplication table for $\mathbb{Z}_6$ is
\[
\times \begin{array}{cccccc}
0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 \\
2 & 0 & 2 & 4 & 0 & 2 & 4 \\
3 & 0 & 3 & 0 & 3 & 0 & 3 \\
4 & 0 & 4 & 2 & 0 & 4 & 2 \\
5 & 0 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\]
Let us find all solutions in \( \mathbb{Z}_6 \) of the equation \( x^2 + x = 0 \). Since 
\[
0^2 + 0 \equiv 0 \pmod{6},
\]
we see that 0 is a solution. Since 
\[
1^2 + 1 \equiv 2 \not\equiv 0 \pmod{6},
\]
we see that 1 is not a solution. Since 
\[
2^2 + 2 \equiv 0 \pmod{6},
\]
we see that 2 is a solution. Since 
\[
3^2 + 3 \equiv 0 \pmod{6},
\]
we see that 3 is a solution. Since 
\[
4^2 + 4 \equiv 2 \not\equiv 0 \pmod{6},
\]
we see that 4 is not a solution. Since 
\[
5^2 + 5 \equiv 0 \pmod{6},
\]
we see that 5 is a solution. Then 0, 2, 3, 5 are all solutions in \( \mathbb{Z}_6 \) of the equation \( x^2 + x = 0 \).

**Exercise 4** ([1, Exercise 14.2]). Let \( a, b \) be integers, and let \( p \) be a prime not dividing \( a \). Show that the solution of the congruence equation \( ax \equiv b \pmod{p} \) is 
\[
x \equiv a^{p-1}b \pmod{p}.
\]

**Solution.** Since \( p \) does not divide \( a \), we have
\[
a^{p-1} \equiv 1 \pmod{p}.
\]

by [1, Theorem 14.1] (Fermat’s Little Theorem). Then
\[
ax \equiv b \pmod{p} \iff a^{p-2}ax \equiv a^{p-2}b \pmod{p} \iff x \equiv a^{p-2}b \pmod{p}
\]

by [1, Proposition 13.2] and [1, Proposition 13.5]. This implies that
\[
x \equiv a^{p-2}b \pmod{p}
\]
is the solution of the congruence equation \( ax \equiv b \pmod{p} \).

**Exercise 5** ([1, Exercise 14.4]). Let \( p \) be a prime and \( k \) a positive integer.

(a) Show that if \( p \) is odd and \( x \) is an integer such that \( x^2 \equiv 1 \pmod{p^k} \), then \( x \equiv \pm 1 \pmod{p^k} \).

(b) Find the solutions of the congruence equation \( x^2 \equiv 1 \pmod{2^k} \).

**Solution.** Suppose that \( p \) is odd. Let \( x \) be an integer such that \( x^2 \equiv 1 \pmod{p^k} \). Then 
\[
(x-1)(x+1) = x^2 - 1 = p^kn
\]
for some integer \( n \). Since 
\[
x + 1 = x - 1 + 2,
\]
we see that either \( \gcd(x - 1, x + 1) = 1 \) or \( \gcd(x - 1, x + 1) = 2 \). Then
- either \( p|(x + 1) \)
- or \( p|(x - 1) \)

by [1, Proposition 10.5], since \((x + 1)(x - 1) = p^kn\). Suppose that \( p|(x + 1) \). Then \( p \) does not divide \((x - 1)\), since \( \gcd(x - 1, x + 1) \in \{1, 2\} \) and \( p \neq 2 \). Hence, we have
\[
\frac{x + 1}{p}(x - 1) = p^{k-1}n,
\]
which implies that \( p^{k-1} \) divides \((x + 1)/p\) by [1, Proposition 10.5], because
\[
\gcd(x - 1, p^{k-1}) = 1,
\]
since \( p \) does not divide \((x-1)\). Thus, we see that \( x+1 \) is divisible by \( p^k \). Then
\[
x \equiv -1 \mod p^k.
\]

Suppose now that \( p \mid (x-1) \). Then \( p \) does not divide \((x+1)\), since \( \gcd(x-1, x+1) \in \{1, 2\} \) and \( p \neq 2 \). Hence, we have
\[
\frac{x-1}{p} (x+1) = p^{k-1}n,
\]
which implies that \( p^{k-1} \) divides \((x-1)/p\) by [1, Proposition 10.5], because
\[
\gcd(x+1, p^{k-1}) = 1,
\]
since \( p \) does not divide \((x+1)\). Thus, we see that \( x-1 \) is divisible by \( p^k \). Then
\[
x \equiv 1 \mod p^k.
\]

Thus, we proved that if \( p \) is odd and \( x \) is an integer such that \( x^2 \equiv 1 \mod p^k \), then
\[
x \equiv \pm 1 \mod p^k.
\]

Now let us find the solutions of the congruence equation \( x^2 \equiv 1 \mod 2^k \).

Any odd integer \( x \) is a solution of the congruence equation \( x^2 \equiv 1 \mod 2 \) (obvious), and
any odd integer \( x \) is a solution of the congruence equation \( x^2 \equiv 1 \mod 4 \), since
\[
(2m+1)^2 = 4m^2 + 4m + 1 \equiv 1 \mod 4
\]
for any integer \( m \). Thus, in order to find all solutions of the congruence equation
\[
x^2 \equiv 1 \mod 2^k,
\]
we may assume that \( k \geq 3 \).

Let \( x \) be an integer such that \( x^2 \equiv 1 \mod 2^k \). Then
\[
(x-1)(x+1) = x^2 - 1 = 2^k n
\]
for some \( n \in \mathbb{Z} \). Then \( x \) must be odd, since otherwise both \((x-1)\) and \((x+1)\) would be odd, which is impossible, because \((x-1)(x+1) = 2^k n\) is even. Since
\[
x + 1 = x - 1 + 2,
\]
we see that \( \gcd(x-1, x+1) = 2 \).

There is an integer \( t \) such that \( x = 2t - 1 \). Then \( x+1 = 2t \) and \( x-1 = 2t-2 \). Then
\[
4t(t-1) = (x-1)(x+1) = x^2 - 1 = 2^k n,
\]
which implies that \( t(t-1) = 2^{k-2} n \). Note that \( k - 2 \geq 1 \) by assumption. Then
\[
t^2 \equiv t \mod 2^{k-2},
\]
which implies that either \( t \equiv 0 \mod 2^{k-2} \) or \( t \equiv 0 \mod 2^{k-2} \) (see Exercise 1).

Thus, there is an integer \( a \) such that either \( t = 2^{k-2} a \) or \( t = 1 + 2^{k-2} a \). Then
\[
x \equiv \pm 1 \mod 2^{k-1}.
\]

Vice versa, if \( k \geq 3 \) and \( x = \pm 1 + 2^{k-1} m \) for some integer \( m \), then
\[
\left( \pm 1 + 2^{k-1} m \right)^2 = 1 \pm 2^k m + 2^{2k-2} m^2 \equiv 1 \mod 2^k.
\]

Thus, the congruence equation \( x^2 \equiv 1 \mod 2^k \) have the following solutions:
\[
\bullet \ x \text{ is any odd integer if } k \leq 2,
\bullet \ x \text{ is any integer } x \text{ such that } x \equiv \pm 1 \mod 2^{k-1}.
\]

Another way of given the same answer is to say that the solutions of the congruence equation \( x^2 \equiv 1 \mod 2^k \) are
\[
\bullet \ x \equiv 1 \mod 2^k \text{ if } k = 1 \text{ (one solution modulo } 2^k),
\bullet \ x \equiv \pm 1 \mod 2^k \text{ if } k = 2 \text{ (two solutions modulo } 2^k),
\]
\begin{itemize}
  \item $x \equiv \pm 1 \mod 2^k$ and $x \equiv \pm 1 + 2^{k-1} \mod 2^k$ if $k \leq 3$ (four solutions modulo $2^k$).
\end{itemize}

\textbf{References}

[1] M. Liebeck, \textit{A concise introduction to pure mathematics}
Third edition (2010), CRC Press