Exercise 30. Pierre de Fermat is said to have factored numbers $n$ by decomposing them as

$$n = x^2 - y^2 = (x - y)(x + y).$$

Use this method to factor the integer $n = 24003$. Describe an algorithm to determine the above $x$ and $y$. Can this method be applied in general for any $n$?

Exercise 31. Show that 1031 is invertible modulo 2227 and compute the inverse $1031^{-1}$ in the ring $\mathbb{Z}_{2227}$.

Exercise 32.

(a) Prove the Chinese Remainder Theorem:

Suppose $m_1, \ldots, m_r$ are pairwise relatively prime, $a_1, \ldots, a_r \in \mathbb{N}$. The system of $r$ congruences

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \ldots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \pmod{M},$$

where $M_i = M / m_i$, $y_i = M_i^{-1} \pmod{m_i}$, $i = 1, \ldots, r$.

(b) Solve the following system of linear congruences using the Chinese Remainder Theorem and compute the smallest positive solution.

$$x \equiv 3 \pmod{11}$$
$$x \equiv 5 \pmod{13}$$
$$x \equiv 7 \pmod{15}$$
$$x \equiv 9 \pmod{17}$$