Exercise 2.9.2. (a) Prove that the square a^2 of an integer a is congruent to 0 or 1 modulo 4.

(b) What are the possible values of a^2 modulo 8?

Proof of (a). We can write $a = 4k + r, 0 \leq r < 4$, then

$$a^2 \bmod 4 = r^2 \bmod 4 = 0 \text{ or } 1.$$

□

Proof of (b). Let $a = 8k + r$, then $r^2 \bmod 8$ can be 0, 1 and 4.

□

Exercise 2.9.4. Prove that every integer a is congruent to the sum of its decimal digits modulo 9.

Proof. Denote by $(a_{k-1}a_{k-2}\ldots a_0)$ the decimal form of a, that is, $a = \sum_{i=0}^{k-1} a_i \cdot 10^i$. We then have

$$a = \sum_{i=0}^{k-1} a_i \cdot 10^i \equiv \sum_{i=0}^{k-1} a_i \bmod 9.$$

□

Exercise 2.9.5. Solve the congruence $2x \equiv 5$

(a) modulo 9 and

(b) modulo 6.

Solution. (a) Since $2 \times 5 \equiv 1 \bmod 9$, $x \equiv 5 \times 5 \equiv 7 \bmod 9$.

(b) There is no solution since $2x \bmod 6$ is always an even number.

Exercise 2.9.8. Use Proposition (2.6) to prove the Chinese Remainder Theorem: Let m, n, a, b be integers, and assume that the greatest common divisor of m and n is 1. Then there is an integer x such that $x \equiv a \bmod m$ and $x \equiv b \mod n$.

Proof. Since $\gcd(m, n) = 1$, there exist s, t such that $ms - nt = b - a$, let $x := a + ms$, then $x = b + nt$, which shows $x \equiv a \bmod m$ and $x \equiv b \bmod n$.

□