Exercise 6

1. Let a_1 and a_2 be relatively prime positive integers. Let $\mathcal{M}$ be the set of all integers n such that $0 \le n \le a_1a_2 - a_1 - a_2$ and n can be written in the form $n = a_1x_1 + a_2x_2$, where x_1 and x_2 are nonnegative integers. Let $\mathcal{N}$ be the set of all integers n such that $0 \le n \le a_1a_2 - a_1 - a_2$ and n cannot be written in the form $n = a_1x_1 + a_2x_2$, where x_1 and x_2 are nonnegative integers. Then $|\mathcal{N}| = N(a_1, a_2)$ and $|\mathcal{M}| + |\mathcal{N}| = (a_1 - 1)(a_2 - 1)$. Let $n \in [0, a_1a_2 - a_1 - a_2]$, and write n in the form

$$n = a_1x_1 + a_2x_2, \quad \text{where } 0 \le x_1 \le a_2 - 1.$$

This representation is unique. Define the function f by

$$f(n) = a_1a_2 - a_1 - a_2 - n = a_1(a_2 - 1 - x_1) - a_2(x_2 + 1).$$

Prove that f is an involution that maps $\mathcal{M}$ onto $\mathcal{N}$ and $\mathcal{N}$ onto $\mathcal{M}$, and so

$$|\mathcal{M}| = |\mathcal{N}| = \frac{(a_1 - 1)(a_2 - 1)}{2} \quad \text{and} \quad \frac{N(a_1, a_2)}{G(a_1, a_2)} = \frac{1}{2}.$$

2. Find all solutions in integers x_1, x_2, and x_3 of the system of linear diophantine equations

$$3x_1 + 5x_2 + 7x_3 = 560, \qquad 9x_1 + 25x_2 + 49x_3 = 2920.$$

3. Find all solutions of the *Ramanujan-Nagell diophantine equation*

$$x^2 + 7 = 2^n$$

with $x \le 1000$.

4. Find all solutions of the *Ljunggren diophantine equation*

$$x^2 - 2y^4 = -1$$

with $x \le 1000$.

5. When is the sum of a geometric progression equal to a power? Equivalently, what are the solutions of the exponential diophantine equation

$$1 + x + x^2 + \cdots + x^m = y^n \tag{1.6}$$

in integers x, m, y, n greater than 2? Check that

$$1 + 3 + 3^2 + 3^3 + 3^4 = 11^2, \;\; 1 + 7 + 7^2 + 7^3 = 20^2, \;\; 1 + 18 + 18^2 = 7^3.$$

These are the only known solutions of (1.6).

6. Construct the multiplication table for the ring $\mathbf{Z}/5\mathbf{Z}$.

7. Construct the multiplication table for the ring $\mathbf{Z}/6\mathbf{Z}$.

8. Prove that if a is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

9. Let d be a positive integer that is a common divisor of a, b, and m. Prove that

$$a \equiv b \pmod{m}$$

if and only if

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

10. Prove that $a_1 \equiv a_2 \pmod{m}$ implies $a_1^k \equiv a_2^k \pmod{m}$ for all $k \geq 1$. Prove that if $f(x)$ is a polynomial with integer coefficients and $a_1 \equiv a_2 \pmod{m}$, then $f(a_1) \equiv f(a_2) \pmod{m}$.

11. Let n be a positive integer such that $n \equiv 3 \pmod{4}$. Prove that n cannot be written as the sum of two squares.

12. Prove that every integer belongs to at least one of the following 6 congruence classes:

$$\begin{array}{rl} 0 & \pmod{2} \\ 0 & \pmod{3} \\ 1 & \pmod{4} \\ 3 & \pmod{8} \\ 7 & \pmod{12} \\ 23 & \pmod{24}. \end{array}$$

13. Let p be prime, $m \geq 1$, and $0 \leq k \leq p-1$. Prove that

$$N = \binom{mp+k}{p} \equiv m \pmod{p}.$$

Hint: Consider the integer $(p-1)!N$ modulo p.

14. Let G be the subset of $M_2(\mathbf{C})$ consisting of the four matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Prove that G is a multiplicative group isomorphic to the additive group of congruence classes $\mathbf{Z}/4\mathbf{Z}$.

15. Find all solutions of the congruence $28x \equiv 35 \pmod{42}$.

16. Find all solutions of the system of congruences

$$8x + 5y \equiv 1 \pmod{13}$$

$$4x + 3y \equiv 3 \pmod{13}.$$

(A criterion for divisibility by 7.) Let n be a positive integer, and let $d_k d_{k-1} \ldots d_1 d_0$ be the usual 10-adic representation of n. Define $f(n) = d_k d_{k-1} \ldots d_1 - 2d_0$. (For example, if $n = 203$, then $d_0 = 3$, $d_1 = 0$, $d_2 = 2$, and $f(203) = 20 - 6 = 14$.) Prove that n is divisible by 7 if and only if $f(n)$ is divisible by 7. Use this criterion to determine if 7875 is divisible by 7.

Hint: Prove that $10v + u \equiv 0 \pmod{7}$ if and only if $v - 2u \equiv 0 \pmod{7}$.

17. Let $k \geq 3$. Find all solutions of the congruence

$$x^2 \equiv 1 \pmod{2^k}.$$

18. Prove that m is prime if and only if $\varphi(m) = m - 1$.

19. Prove that if m divides n, then $\varphi(m)$ divides $\varphi(n)$.