APPENDIX G

Modular Arithmetic

Let n, a, b be any integer. We define

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

(pronounced "a is congruent to b modulo n") provided $a - b$ is divisible by n (i.e., $(a - b)/n$ is an integer). For instance

$7 \equiv 3 \pmod 4$ $\quad 7 \equiv 2 \pmod 5$ $\quad 7 \equiv 1 \pmod 3$ $\quad 7 \equiv 1 \pmod 2$

$12 \equiv 0 \pmod 4$ $17 \equiv -3 \pmod 5$ $\quad -7 \equiv 1 \pmod 4$ $\quad -7 \equiv -4 \pmod 3$

$7x \equiv 3x \pmod 4$ $\quad 7x \equiv 2x \pmod 5$ $\quad 7x \equiv x \pmod 3$ $\quad -17x \equiv -x \pmod{16}$

where x is also any integer.

If p is a prime integer then *arithmetic modulo* p consists of the integers $\{0, 1, 2, \ldots, p\text{-}1\}$, subject to the usual four arithmetic operations, with the added stipulation that equality is to be replaced by congruence. Thus, in arithmetic modulo 5,

$$3 + 4 \equiv 2 \qquad 3 \cdot 4 \equiv 2 \qquad 3 - 4 \equiv 4 \qquad 4x + 4x \equiv 3x$$

and $2 \div 4 \equiv 3$ (because $3 \cdot 4 \equiv 2$),

whereas in arithmetic modulo 7,

$$3 + 4 \equiv 0 \qquad 3 \cdot 4 \equiv 5 \qquad 3 - 4 \equiv 6 \qquad 4x + 4x \equiv x$$

and $5 \div 4 \equiv 3$ (because $3 \cdot 4 \equiv 5$),

Arithmetic modulo a prime p is very similar to the standard arithmetic. The operations of addition and multiplication are commutative, associative, and distributive. Additive and multiplicative identities and inverses exist and are unique. The additive inverse of a is, of course $p - a$. The multiplicative inverse, on the other hand, is harder to find. Fortunatley, for the purposes of this text, it suffices to know that in arithmetic modulo p each of the numbers $\{1, 2, \ldots, p\text{-}1\}$ has a mutliplicative inverse.

EXERCISES H

1. Evaluate the following in modulo 5 arithmetic:

   a) $2 + 4$ b) $2 \cdot 4$ c) $2 - 4$ d) $3 + 4$

   e) $3 - 4$ f) $3 \cdot 4$ g) $3 \cdot 3$ h) $4 \cdot 4$

2. Evaluate the following in modulo 7 arithmetic:

   a) $4 + 5$ b) $4 - 5$ c) $4 \cdot 5$ d) $3 + 5$

   e) $3 - 5$ f) $3 \cdot 5$ g) $4 \cdot 4$ h) $5 \cdot 5$

3. Evaluate the following in modulo 11 arithmetic:

   a) $4 + 8$ b) $4 - 8$ c) $4 \cdot 8$ d) $3 + 10$

   e) $3 - 10$ f) $3 \cdot 10$ g) $4 \cdot 4$ h) $5 \cdot 5$

4. Simplify the following expressions in modulo 5 arithmetic:

   a) $2x + 4x$ b) $2x + 3y - 3x - y$ c) $2x - 3y - (4x - y)$

   d) $3x - y + 4z + 2(x - 2y + 3z)$ e) $3(2x - 3y + 4z) - 2(4x - y + 3z)$

5. Simplify the following expressions in modulo 7 arithmetic:

   a) $2x + 6x$ b) $2x + 3y - 3x - y$ c) $2x - 3y - (4x - y)$

   d) $3x - y + 4z + 3(x - 2y + 3z)$ e) $4(2x - 3y + 4z) - 3(4x - y + 3z)$

6. Simplify the following expressions in modulo 3 arithmetic:

   a) $2x + 2x$ b) $2x + y - x - 2y$ c) $2x - y - (2x - y)$

   d) $2x - y + 2z + 2(x - 2y + z)$ e) $2(2x - y + 2z) - (2x - y + 2z)$