3. For a positive integer n, define $\phi(n)$ to be the number of positive integers $a < n$ such that $\text{hcf}(a,n) = 1$. (For example, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$.)

   Work out $\phi(n)$ for $n = 5, 6, \ldots, 10$.

   If p is a prime, show that $\phi(p) = p - 1$, and more generally, that $\phi(p^r) = p^r - p^{r-1}$.

4. There has been quite a bit of work over the years on trying to find a nice formula that takes many prime values. For example, $x^2 + x + 41$ is prime for all integers x such that $-40 \leq x < 40$. (You may like to check this!) However:

   Find an integer x coprime to 41 such that $x^2 + x + 41$ is not prime.

5. Use the idea of the proof of Euclid's Theorem 13.1 to prove that there are infinitely many primes of the form $4k + 3$ (where k is an integer).

6. On his release from prison, critic Ivor Smallbrain rushes out to see the latest film, *Prime and Prejudice*. During the film Ivor attempts to think of ten consecutive positive integers, none of which is prime. He fails.

   Help Ivor by showing that if $N = 11! + 2$, then none of the numbers $N, N+1, N+2, \ldots, N+9$ is prime.

   More generally, show that for any $n \in \mathbb{N}$ there is a sequence of n consecutive positive integers, none of which is prime. (Hence, there are arbitrarily large "gaps" in the sequence of primes.)

Chapter 14

Congruence of Integers

In this chapter we introduce another method for studying the integers, called congruence. Let us go straight into the definition.

DEFINITION *Let m be a positive integer. For $a, b \in \mathbb{Z}$, if m divides $b - a$ we write $a \equiv b \mod m$, and say a is congruent to b modulo m.*

For example,

$$5 \equiv 1 \mod 2, \quad 12 \equiv 17 \mod 5, \quad 91 \equiv -17 \mod 12, \quad 531 \not\equiv 0 \mod 4 .$$

PROPOSITION 14.1
Every integer is congruent to exactly one of the numbers $0, 1, 2, \ldots, m-1$ modulo m.

PROOF Let $x \in \mathbb{Z}$. By Proposition 11.1, there are integers q, r such that

$$x = qm + r \quad \text{with} \quad 0 \leq r < m .$$

Then $x - r = qm$, so m divides $x - r$, and hence by the above definition, $x \equiv r \mod m$. Since r is one of the numbers $0, 1, 2, \ldots, m-1$, the proposition follows. ∎

Example 14.1

(1) Every integer is congruent to 0 or 1 modulo 2. Indeed, all even integers are congruent to 0 modulo 2, and all odd integers to 1 modulo 2.

(2) Every integer is congruent to 0, 1, 2 or 3 modulo 4. More specifically, every even integer is congruent to 0 or 2 modulo 4, and every odd integer to 1 or 3 modulo 4.

(3) My clock is now showing the time as 2.00 A.M. What time will it be showing in 4803 hours? Since $4803 = 3 \mod 24$, it will be showing a