1 Additional Exercises: Modular Arithmetic

1. (a) Prove 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?
2. (a) Prove that 2 has no multiplicative inverse modulo 6.
   (b) Determine all integers n such that 2 has a multiplicative inverse modulo n.
3. Solve the congruence $2x \equiv 5$
   (a) modulo 9
   (b) modulo 6
4. Determine the integers n for which the system of congruences $x + y \equiv 2$ (modulo n) and $2x - 3y \equiv 3$ (modulo n) has a solution.
5. Use the theorem about subgroups of $\mathbf{Z}$ we proved earlier to prove the *Chinese Remainder Theorem.*

   Theorem 1 (Earlier Result) *Let a, b be integers, not both zero, and let d be the positive integer which generates the subgroup $aZ + bZ$. Then*

Theorem 2 *1. (a) d can be written in the form $d = ar + bs$*

(b) d divides both a and b

(c) If an integer c divided both a and b, then it also divides d.

1. **Theorem 3 (Chinese Remainder Theorem)** *Let m, n, α, β be integers and assume* $\gcd(m, n) = 1$. *Then there is an integer x such that $x \equiv \alpha$ (modulo m) and $x \equiv \beta$ (modulo n).*