**Exercise 1.9**. Suppose we run Algorithm ExtEuclid on input (117,67). Show the steps of the computation by giving the data corresponding to that shown in in the table in Example 1.2.

**Exercise 1.10**. Show that if a ≥ b > 0, then the values s and t computed by ExtEuclid(a, b) satisfy |s| ≤ b/d and |t| ≤ a/d.
Hint: prove by induction on b—be careful, you have to stop the induction before b gets to zero, so the last step to consider is when b | a.
**Exercise 1.11.** Suppose that a, b are integers with d := gcd(a, b) ̸= 0.

(a) Show that a/d and b/d are relatively prime.

(b) Show that if s and t are integers such that as + bt = d, then s and t are relatively prime.

**Exercise 1.12**. Let n be an integer. Show that if a, b are relatively prime integers, each of which divides n, then ab divides n.

**Exercise 2.7.** Let n be a positive integer. For x ∈ {0, . . . , 2n −1}, let x ̃ denote the integer obtained by inverting the bits in the n-bit, binary representation of x (note that x ̃ ∈ {0, . . . , 2n − 1}). Show that x ̃ + 1 ≡ −x (mod 2n). This justifies the usual rule for computing negatives in 2’s complement arithmetic.

Hint: what is x + x ̃?

**Exercise 2.11.** For each of the following congruences, determine all the integer solutions z ∈ {0, . . . , 999}. To so this, you should first put the congruence in the form az = b (mod 1000), as we did in going from (2.2) to (2.3) in Example 2.3. Then follow the steps outlined in §2.2.3. Show all your steps (but you may use a calculator to help with the multiplications). Use the extended Euclidean algorithm to compute modular inverses, where necessary.

(a) 100z + 200 ≡ 93z + 171 (mod 1000)

(b) 115z + 130 ≡ 100z + 165 (mod 1000)

 (c) 115z + 132 ≡ 100z + 140 (mod 1000)

(d) 119z + 132 ≡ 113z + 140 (mod 1000)

**Exercise 2.25.** Calculate the order of 9 mod 100. Show your work by building a table of powers 9^i mod 100. In addition, from this table, identify the multiplicative inverse of 9 mod 100.

**Exercise 2.30.** Compute 399 mod 100 using the repeated squaring algorithm. Show your work.

**Exercise 3.3.** Consider the field F = Z5. Let f = X3 +X+[1] ∈ F[X], g = [2]X2 +[3]X+[4] ∈ F[X], and h = [3]X2 + [2]X + [1] ∈ F [X]. Compute (gh) mod f . Show your work. That is, you should compute the product polynomial P = gh ∈ F [X], and then use polynomial division with remainder to compute P mod f. Along the way, you the coefficients of any polynomials you compute should be reduced mod 5.

**Exercise 3.4.** Consider the field F = Z5. Use the Lagrange interpolation formula to compute the coefficients of the polynomial g ∈ F [X] of degree less than 3 such that g([1]) = [3], g([2]) = [4], g([3]) = [1].

Show your work.