

1. Show that if  $a \mid b$  and  $b \mid a$ , where  $a$  and  $b$  are integers, then  $a = b$  or  $a = -b$ .
2. Show that if  $a$ ,  $b$ , and  $c$  are integers, where  $a \neq 0$  and  $c \neq 0$ , such that  $ac \mid bc$ , then  $a \mid b$ .

3. Suppose that  $a$  and  $b$  are integers,  $a \equiv 4 \pmod{13}$ , and  $b \equiv 9 \pmod{13}$ . Find the integer  $c$  with  $0 \leq c \leq 12$  such that

**a)**  $c \equiv 9a \pmod{13}$ .

**b)**  $c \equiv 11b \pmod{13}$ .

**c)**  $c \equiv a + b \pmod{13}$ .

**d)**  $c \equiv 2a + 3b \pmod{13}$ .

**e)**  $c \equiv a^2 + b^2 \pmod{13}$ .

**f)**  $c \equiv a^3 - b^3 \pmod{13}$ .

4. Convert the binary expansion of each of these integers to a decimal expansion.

**a)**  $(1\ 1111)_2$

**b)**  $(10\ 0000\ 0001)_2$

**c)**  $(1\ 0101\ 0101)_2$

**d)**  $(110\ 1001\ 0001\ 0000)_2$

5. Convert the hexadecimal expansion of each of these integers to a binary expansion.

**a)**  $(80E)_{16}$

**b)**  $(135AB)_{16}$

**c)**  $(ABBA)_{16}$

**d)**  $(DEFACED)_{16}$

6. Use the Euclidean algorithm to find

**a)**  $\gcd(12, 18)$ .

**b)**  $\gcd(111, 201)$ .

**c)**  $\gcd(1001, 1331)$ .

**d)**  $\gcd(12345, 54321)$ .

**e)**  $\gcd(1000, 5040)$ .

**f)**  $\gcd(9888, 6060)$ .

7. Use the extended Euclidean algorithm to express  $\gcd(26, 91)$  as a linear combination of 26 and 91.

7. Find all solutions, if any, to the system of congruences  $x \equiv 7 \pmod{9}$ ,  $x \equiv 4 \pmod{12}$ , and  $x \equiv 16 \pmod{21}$ .

8. Show that 15 is an inverse of 7 modulo 26.

9. Which memory locations are assigned by the hashing function  $h(k) = k \bmod 97$  to the records of insurance company customers with these Social Security numbers?
- |              |              |
|--------------|--------------|
| a) 034567981 | b) 183211232 |
| c) 220195744 | d) 987255335 |
10. What is the original message encrypted using the RSA system with  $n = 43 \cdot 59$  and  $e = 13$  if the encrypted message is 0667 1947 0671? (To decrypt, first find the decryption exponent  $d$  which is the inverse of  $e = 13$  modulo  $42 \cdot 58$ .)