

1. Find the nonnegative integer  $a < 28$  which is represented by the following pairs

$$(a) (0, 0) \qquad (b) (1, 1)$$

$$(c) (2, 1) \qquad (d) (3, 5)$$

where each pair  $(\kappa, \ell)$  represents the system of congruences

$$\left. \begin{array}{l} a \equiv \kappa \pmod{4} \\ a \equiv \ell \pmod{7} \end{array} \right\}.$$

2. Using Fermat's little theorem show that if  $n$  is a positive integer,  $n^7 \equiv n \pmod{42}$ .

*Note:* Fermat's little theorem will be stated and proved next Tuesday in class. It states that  $a^{p-1} \equiv 1 \pmod{p}$  for any prime  $p$  and any integer  $a$  so that  $p \nmid a$ . Equivalently  $a^p \equiv a \pmod{p}$  for any integer  $a$ .

3. Let  $m_1, m_2 > 1$ . Show that the system of linear congruences

$$\left. \begin{array}{l} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{array} \right\}$$

has solutions **for any** integers  $a$  and  $b$  if, and only if,  $m_1$  and  $m_2$  are relatively prime.

4. Let  $\varphi(m) = \{1 \leq k < m \mid \gcd(k, m) = 1\}$  be Euler's function. Show that:

(a) For any prime  $p$  and any integer  $\kappa \geq 1$ ,  $\varphi(p^\kappa) = p^{\kappa-1}(p-1)$ .

(b) Use the multiplicative property of  $\varphi$  to prove that if  $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  is the prime factorization of  $m$ , then

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right).$$

(c) Use (b) to show that, in particular, for any integer  $\kappa \geq 1$ ,  $\varphi(m^\kappa) = m^{\kappa-1}\varphi(m)$ .

*Note:* Recall that  $\varphi$  being multiplicative means that  $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$  if  $m, n \geq 1$  are relatively prime.

5. Let  $p$  and  $q$  be two different primes, put  $m = pq$  and suppose that  $r \equiv 1 \pmod{p-1}$  and  $r \equiv 1 \pmod{q-1}$ . Show that for any integer  $a$ ,

$$a^r \equiv a \pmod{m}.$$