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

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

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

where each pair (κ, ℓ) represents the system of congruences

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

Solution.

(a) a must satisfy

$$\left.\begin{array}{l} a \equiv 0 \mod 4 \\ a \equiv 0 \mod 7 \end{array}\right\}$$

which obviously has $a = 0$ as solution. This solution is unique in the given range $0 \leq a < 28$ by the Chinese rimender theorem.

(b) In this case we must consider the system

$$\left.\begin{array}{l} a \equiv 1 \mod 4 \\ a \equiv 1 \mod 7 \end{array}\right\}$$

which, by the same reason as in (a) has solution $a = 1$.

(c) Now a must satisfy

$$\left.\begin{array}{l} a \equiv 2 \mod 4 \\ a \equiv 1 \mod 7 \end{array}\right\}.$$

Imitating the proof of the Chinese rimeinder theorem, a solution is given by $a = 4\alpha + 7\beta$ where

$$7\beta \equiv 2 \mod 4 \tag{1}$$

and

$$4\alpha \equiv 1 \mod 7. \tag{2}$$

Since $7 \equiv 3 \mod 4$, (1) is equivalent to $3\beta \equiv 2 \mod 4$ and hence

$$\beta \underset{\substack{\uparrow \\ 9\equiv 1 \mod 4}}{\equiv} 9\beta \underset{\substack{\uparrow \\ 3\beta\equiv 2 \mod 4}}{\equiv} 3 \cdot 2 = 6 \equiv 2 \mod 4.$$

For (2) we have

$$\alpha \underset{\substack{\uparrow \\ 8\equiv 1 \mod 7}}{\equiv} 8\alpha \underset{\substack{\uparrow \\ \text{by (2)}}}{\equiv} 2 \mod 7.$$

Thus, taking $\alpha = 2$ and $\beta = 2$ we have $a = 4\alpha + 7\beta = 22$ (again, according to the Chinese reminder theorem, this is the unique solution in the range $0 \leq a < 28$).

(d) Next we look at the system

$$\left.\begin{array}{l} a \equiv 3 \mod 4 \\ a \equiv 5 \mod 7 \end{array}\right\}.$$

Proceeding as in part (c) we look for a solution of the form $a = 4\alpha + 7\beta$ so that

$$7\beta \equiv 3 \mod 4 \tag{3}$$

and

$$4\alpha \equiv 5 \mod 7. \tag{4}$$

As before, from (3) we have

$$\beta \equiv 3 \cdot 3 = 9 \equiv 1 \mod 4,$$

and from (4)

$$\alpha \equiv 2 \cdot 5 = 10 \equiv 3 \mod 7.$$

This, with $\alpha = 3$ and $\beta = 1$, gives $a = 4\alpha + 7\beta = 19$. □

---

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

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

Solution. Note first that the given moduli $42 = 2 \cdot 3 \cdot 7$ and that by Fermat's theorem

$$n^7 = n \cdot \left(n^2\right)^3 \equiv n \cdot n^3 = n^4 = \left(n^2\right)^2 \equiv n^2 \equiv n \mod 2,$$

$$n^7 = n \cdot \left(n^3\right)^2 \equiv n \cdot n^2 = n^3 \equiv n \mod 3,$$

and

$$n^7 \equiv n \mod 7.$$

This means that $2 \mid n^7 - n$, $3 \mid n^7 - n$ and $7 \mid n^7 - n$ which implies that $42 \mid n^7 - n$ because $2, 3$ and 7 are primes. This is the same as $n^7 \equiv n \mod 42$ as we wanted. □

---

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

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

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

Solution. By the Chinese remainder theorem we only need to show that if the given system has always solutions then m_1 and m_2 must be relatively prime. To do so, note that if we can solve for a pair of given integers a and b then

$$\begin{cases} x = a + \kappa m_1 \\ x = b + \ell m_2 \end{cases} \Rightarrow \quad b - a = \kappa m_1 - \ell m_2 \quad \Rightarrow \quad \gcd(m_1, m_2) \mid (b - a).$$

Since a and b can be chosen arbitrarily we conclude that $\gcd(m_1, m_2) = 1$ (just take $a = 0$ and $b = 1$ for example). $\square$

---

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

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

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

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

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

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

Solution.

   (a) An integer $1 \le k \le p^\kappa$ will not be relatiely prime to p^κ if it is of the form $k = \ell \cdot p$. The restriction for ℓ is then $1 \le \ell \le p^{\kappa-1}$ which give us $p^{\kappa-1}$ such $k's$. Therefore

$$\varphi(p^\kappa) = p^\kappa - p^{\kappa-1} = p^{\kappa-1}(p-1).$$

(*b*) Since φ is multiplicative

$$\begin{aligned}\varphi(m) &= \varphi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\right) = \varphi\left(p_1^{\alpha_1}\right)\cdot\varphi\left(p_2^{\alpha_2}\right)\cdot\ldots\cdot\varphi\left(p_k^{\alpha_k}\right)\\ &\underset{\substack{\uparrow\\ \text{by }(a)}}{=} p_1^{\alpha_1-1}(p_1-1)\cdot p_2^{\alpha_2-1}(p_2-1)\cdot\ldots\cdot p_k^{\alpha_k-1}(p_k-1)\\ &= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\cdot p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)\\ &= p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)\\ &= m\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right).\end{aligned}$$

(*c*) Since $m^\kappa = p_1^{\kappa\alpha_1}\cdot p_2^{\kappa\alpha_2}\cdot\ldots\cdot p_k^{\kappa\alpha_k}$ is the prime factorization of m^κ if $m = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ is that of m, by (*b*) we have

$$\begin{aligned}\varphi\left(m^\kappa\right) &= m^\kappa\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)\\ &= m^{\kappa-1}\cdot m\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)\\ &= m^{\kappa-1}\cdot\varphi(m).\end{aligned}$$

□

---

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

$$a^r \equiv a \mod m.$$

Solution. Since $r \equiv 1 \mod (p-1)$ there exists an integer κ such that $r = 1+\kappa(p-1)$. Hence, by Fermat's little theorem, if $p \nmid a$ we have

$$a^r = a^{1+\kappa(p-1)} = a\left(a^{p-1}\right)^\kappa = a \mod p,$$

and so $p \mid (a^r - a)$. Trivially $p \mid (a^r - a)$ when $p \mid a$ and so $p \mid (a^r - a)$ for any integer a. Likewise $q \mid (a^r - a)$ and since p and q are distinct primes we conclude that $m = pq \mid (a^r - a)$. This means that $a^r \equiv a \mod m$ as was to be shown. □

Remark. The result in this exercise also holds if $m = p_1\cdot p_2\cdot\ldots\cdot p_k$ is the product of k distinct primes and $r \equiv 1 \mod p_i$ for all $i = 1, 2\ldots, k$. Note now that exercise 2 follows from this with $p_1 = 2$, $p_2 = 3$ and $p_3 = 7$.