1) For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write their greatest command divisor in the form $ax + by$ for some integers x and y

(a) $a = 60$, $b = 17$

Observe that,

$$\begin{aligned} 60 &= 3(17) + 9 \\ 17 &= 1(9) + 8 \\ 9 &= 1(8) + 1 \\ 8 &= 8(1), \end{aligned}$$

so $\gcd(60, 17) = 1$, and

$$\begin{aligned} \gcd(60, 17) = 1 &= 9 - (1 * 8) = 9 - (17 - 9) = 17 + 2(9) = -17 + 2(60 - 3 * 17) \\ &= 60(2) + 17(-7). \end{aligned}$$

Finally, we have $\operatorname{lcm}(60, 17)\gcd(60, 17) = \operatorname{lcm}(60, 17) = 60(17) = 1020$.

(b) $a = 11391$, $b = 5673$

Notice that

$$\begin{aligned} 11391 &= 2(5673) + 45 \\ 5673 &= 126(45) + 3 \\ 45 &= 15(3), \end{aligned}$$

so $\gcd(11391, 5673) = 3$, and

$$\begin{aligned} \gcd(11391, 5673) &= 5673 - 126(45) = 5673 - 126(11391 - 2 * 5673) \\ &= 11391(-126) + 5673(253). \end{aligned}$$

Finally, we have $\operatorname{lcm}(11391, 5673)\gcd(11391, 5673) = 11391(5673)$ or $\operatorname{lcm} = 21540381$.

2) Determine the value of $\varphi(n)$ for each integer $n \leq 15$, where $\varphi(n)$ denotes the Euler-φ function.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	2	2	6	4	6	4	10	4	12	6	8

3) Prove that if p is prime, then $\sqrt{p}$ is not a rational number.

Proof
Suppose that $\sqrt{p}$ is a rational number. Then $\exists a, b \in \mathbb{Z}$ with $b \neq 0$ such that $\sqrt{p} = a/b$ and $\gcd(a, b) = 1$. That is, a and b are relatively prime and have no common factors. Thus, $a^2 = pb^2$, implying $p|a^2$. It follows then that $p|a$ or $a = px$ for some integer x. Hence, $a^2 = p^2x^2 = pb^2$ or $b^2 = px^2$, implying similarly that $p|b$. This is a contradiction, however, since we assumed that $\gcd(a, b) = 1$. We thus conclude that $\sqrt{p}$ is an irrational number.

■

4) Write down explicitly all the elements in the residue class of

(a) $\mathbb{Z}/8\mathbb{Z}$

$\rightarrow \mathbb{Z}/8\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

(b) $\mathbb{Z}/10\mathbb{Z}$

$\rightarrow \mathbb{Z}/10\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$

(c) $\mathbb{Z}/18\mathbb{Z}$

$\rightarrow \mathbb{Z}/18\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}, \bar{15}, \bar{16}, \bar{17}\}$

5) Prove that there are infinitely many primes.

Proof
Suppose that there are only a finite number of primes $p_1, \ldots, p_k$. Consider the following integer,

$$M = p_1 \ldots p_i \ldots p_k + 1.$$

By the Fundamental Theorem of Arithmetic, M is a composite number, which is written as a product of primes. That is, M is divisible by at least one prime number. Notice, though, that $\gcd(M, p_i) = 1$ since $M = p_i(p_1 \ldots p_k) + 1$ for each $i = 1, \ldots, k$. Hence, we have a contradiction since M is relatively prime to each prime number, implying that the set of prime numbers is in fact not finite.

■

6) Prove that if $\bar{a}$, $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof
Since $\bar{a}$, $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, there exist $\bar{c}, \bar{d} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\bar{a} \cdot \bar{c} = \bar{b} \cdot \bar{d} = \bar{1}$. Consider then $\bar{c} \cdot \bar{d}$. We have that $(\bar{a} \cdot \bar{b}) \cdot (\bar{c} \cdot \bar{d}) = (\bar{a} \cdot \bar{c}) \cdot (\bar{b} \cdot \bar{d}) = \bar{1} \cdot \bar{1} = \bar{1}$, implying that $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

■

7[1.3.12]) Let n, m, and k all be positive integers. Assume that

$$n | mk - 1.$$

Prove that $\gcd(n, m) = 1$.

Proof
Notice that $mk - 1 = nl$ for some integer l. Hence, $1 = n(-l) + mk$. Since 1 is the least element in the positive integers and is an integer-linear combination of n, m, then $\gcd(n, m) = 1$.

■

8[1.3.13]) Let a, b, and c be integers.

(a) Prove that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Proof
Notice that $1 = ax + by$ and that $bc = an$ for some integers x, y, and n. Hence $byc = (1 - ax)c = c - acx = an$ or $c = a(cx + n)$, implying that $a|c$.

■

(b) Prove that if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

Proof
Observe that $1 = an + bm$ and $1 = ak + cl$ for some $n, m, k, l \in \mathbb{Z}$. Thus $bc(ml) = (1 - an)(1 - ak) = 1 - a(n + k - ank)$ or $1 = ax + by$ where $x, y \in \mathbb{Z}$, proving that $\gcd(a, bc) = 1$.

■

9[1.3.16]) Let a and b be positive integers. Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ where $\alpha_i, \beta_i \geq 0$ and, for $1 \leq i \leq k$, p_i are distinct primes. Show that $\gcd(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$, where $\gamma_i = \min(\alpha_i, \beta_i)$. In particular, a and b are relatively prime if and only if they do not have any common prime divisors.

Proof
Let $c = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$. It is clear that $c|a$ and $c|b$ since $\gamma_i \leq \alpha_i, \beta_i$ for each i. We now prove that if $d|a$ and $d|b$ then $d|c$. Since $d|a$ and $d|b$, then it must be true that $d = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$, where $0 \leq \delta_i \leq \alpha_i, \beta_i$ and $\delta_i \in \mathbb{Z}$ for each i. Compare now δ_i and $\gamma_i = \min(\alpha_i, \beta_i)$. It is clear then that $\delta_i \leq \min(\alpha_i, \beta_i)$ for each i, so $d|c$ since $\gamma_i - \delta_i \geq 0$. Hence, $c = \gcd(a, b)$.

If a and b are relatively prime, then $\gcd(a, b) = 1$ and $\gamma_i = 0$ for each i, meaning that α_i or β_i is zero. Hence a and b share no common prime divisors. Now suppose that a and b share no common divisors, then for each i we have that at least one of α_i or β_i is zero, meaning that $\gamma_i = 0$ and $\gcd(a, b) = 1$, implying that a and b are relatively prime.

■

10[1.3.18]) Let a and b be positive integers. What can you say about the product of $\gcd(a, b)$ and lcm(a, b)? By looking at some examples, make a conjecture. Can you prove your conjecture?

$\rightarrow$ It may be observed that $\gcd(a, b)\text{lcm(a, b)} = \text{ab}$. Consider the following examples

(a, b)	$\gcd(a, b)$	lcm(a, b)	ab
(5,10)	5	10	50
(10,11)	1	110	110
(42,15)	3	210	630

We prove the conjecture below:

Proof
Notice that by definition if $c = \gcd(a, b)$ then $a = cn$ and $b = cm$ where $\gcd(n, m) = 1$. Obviously, if $d = \text{lcm(a, b)}$ then $a|d$ and $b|d$. Hence, $d = cnm$ and $cd = c^2nm = ab$. That is, $\gcd(a, b)\text{lcm(a, b)} = \text{ab}$.

■