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 $\exists a, b \in \mathbb{Z}$ 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) $\mathbb{Z}/8\mathbb{Z}$

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

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

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

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

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

5) Prove that there are infinitely many primes.

Proof
Suppose that there are only a finite number of primes.

■