

SOLUTIONS TO THE REVIEW PROBLEMS

1. Find $\gcd(7605, 5733)$, and express it as a linear combination of 7605 and 5733.

Solution: Use the matrix form of the Euclidean algorithm: $\begin{bmatrix} 1 & 0 & 7605 \\ 0 & 1 & 5733 \end{bmatrix} \rightsquigarrow$

$$\begin{bmatrix} 1 & -1 & 1872 \\ 0 & 1 & 5733 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 1872 \\ -3 & 4 & 117 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 49 & -65 & 0 \\ -3 & 4 & 117 \end{bmatrix}. \text{ Thus}$$

$\gcd(7605, 5733) = 117$, and $117 = (-3) \cdot 7605 + 4 \cdot 5733$.

2. For $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, prove that $\omega^n = 1$ if and only if $3|n$, for any integer n .

Solution: Calculations in the introduction to Chapter 1 show that $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, and $\omega^3 = 1$. If $n \in \mathbf{Z}$, and $3|n$, then $n = 3q$ for some $q \in \mathbf{Z}$. Then $\omega^n = \omega^{3q} = (\omega^3)^q = 1^q = 1$. Conversely, if $n \in \mathbf{Z}$ and $\omega^n = 1$, use the division algorithm to write $n = q \cdot 3 + r$, where the remainder satisfies $0 \leq r < 3$. Then $1 = \omega^n = \omega^{3q+r} = (\omega^3)^q \omega^r = \omega^r$. Since $r = 0, 1, 2$ and we have shown that $\omega \neq 1$ and $\omega^2 \neq 1$, the only possibility is $r = 0$, and therefore $3|n$.

3. Solve the congruence $24x \equiv 168 \pmod{200}$.

Solution: First we find that $\gcd(24, 200) = 8$, and $8 | 168$, so the congruence has a solution. The next step is to reduce the congruence by dividing each term by 8, which gives $3x \equiv 21 \pmod{25}$. To solve the congruence $3x \equiv 21 \pmod{25}$ we could find the multiplicative inverse of 3 modulo 25. Trial and error shows it to be -8 , we can multiply both sides of the congruence by -8 , and proceed with the solution.

$$\begin{array}{rcl} 24x & \equiv & 168 \pmod{200} \\ 3x & \equiv & 21 \pmod{25} \\ -24x & \equiv & -168 \pmod{25} \\ x & \equiv & 7 \pmod{25} \end{array}$$

The solution is $x \equiv 7, 32, 57, 82, 107, 132, 157, 182 \pmod{200}$.

4. Solve the system of congruences $2x \equiv 9 \pmod{15}$ $x \equiv 8 \pmod{11}$.

Solution: Write $x = 8 + 11q$ for some $q \in \mathbf{Z}$, and substitute to get $16 + 22q \equiv 9 \pmod{15}$, which reduces to $7q \equiv -7 \pmod{15}$, so $q \equiv -1 \pmod{15}$. This gives $x \equiv -3 \pmod{11 \cdot 15}$.

5. List the elements of \mathbf{Z}_{15}^\times . For each element, find its multiplicative inverse, and find its multiplicative order.

Solution: There should be 8 elements since $\varphi(15) = 8$. By Problem 39, the multiplicative order of any nontrivial element is 2, 4, or 8. The elements are $[1], [2], [4], [7], [8], [11], [13],$ and $[14]$.

Computing powers, we have $[2]^2 = [4]$, $[2]^3 = [8]$, and $[2]^4 = [1]$. This shows not only that the multiplicative order of $[2]$ is 4, but that the multiplicative order of $[4]$ is 2. The same computation shows that $[2]^{-1} = [8]$ and $[4]^{-1} = [4]$. We can also deduce that $[13] = [-2]$ has multiplicative order 4, that $[13]^{-1} = [-2]^{-1} = [-8] = [7]$, and that $[11]^{-1} = [-4]^{-1} = [-4] = [11]$.

Next, we have $[7]^2 = [4]$, so $[7]$ has multiplicative order 4 because $[7]^4 = [4]^2 = [1]$.

To compute the multiplicative order of $[8]$, we can rewrite it as $[2]^3$, and then it is clear that the first positive integer k with $([2]^3)^k = [1]$ is $k = 4$, since $3k$ must be a multiple of 4. (This can also be shown by rewriting $[8]$ as $[-7]$.) Similarly, $[11] = [-4]$ has multiplicative order 2, and $[13] = [-2]$ has multiplicative order 4.

6. Show that if $n > 1$ is an odd integer, then $\varphi(2n) = \varphi(n)$.

Solution: Since n is odd, the prime 2 does not occur in its prime factorization. The formula in Proposition 1.4.8 shows that to compute $\varphi(2n)$ in terms of $\varphi(n)$ we need to add $2 \cdot (1 - \frac{1}{2})$, and this does not change the computation.

Second solution: Since n is odd, the integers n and $2n$ are relatively prime, and so it follows from Exercise 1.4.27 of the text that $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$.