

1.1 SOLUTIONS

22. Find $\gcd(435, 377)$, and express it as a linear combination of 435 and 377.

Solution: We will use the Euclidean algorithm. Divide the larger number by the smaller, which should give you a quotient of 1 and a remainder of 58. Then divide the remainder 58 into 377, and continue the Euclidean algorithm as in Example 1.1.4 in the text. That should give you the following equations.

$$\begin{array}{rcl} 435 & = & 1 \cdot 377 + 58 \\ 377 & = & 6 \cdot 58 + 29 \\ 58 & = & 2 \cdot 29 \end{array} \qquad \begin{array}{rcl} \gcd(435, 377) & = & \gcd(377, 58) \\ & = & \gcd(58, 29) \\ & = & 29 \end{array}$$

The repeated divisions show that $\gcd(435, 377) = 29$, since the remainder in the last equation is 0. To write 29 as a linear combination of 435 and 377 we need to use the same equations, but we need to solve them for the remainders.

$$\begin{aligned} 58 &= 435 - 1 \cdot 377 \\ 29 &= 377 - 6 \cdot 58 \end{aligned}$$

Now take the equation involving the remainder 29, and substitute for 58, the remainder in the previous equation.

$$\begin{aligned} 29 &= 377 - 6 \cdot 58 \\ &= 377 - 6 \cdot (435 - 1 \cdot 377) \\ &= 7 \cdot 377 - 6 \cdot 435 \end{aligned}$$

This gives the linear combination we need, $29 = (7)(377) - (6)(435)$.

23. Find $\gcd(3553, 527)$, and express it as a linear combination of 3553 and 527.

Solution: Just as in Problem 22, the first step is to divide the smaller number into the larger. We get $3553 = 6 \cdot 527 + 391$, so this tells us to multiply the bottom row of the matrix $\begin{bmatrix} 1 & 0 & 3553 \\ 0 & 1 & 527 \end{bmatrix}$ by 6 and subtract from the first row. The rest of the steps in reducing the matrix to the form we want should be clear. We have

$$\begin{aligned} \begin{bmatrix} 1 & 0 & 3553 \\ 0 & 1 & 527 \end{bmatrix} &\rightsquigarrow \begin{bmatrix} 1 & -6 & 391 \\ 0 & 1 & 527 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -6 & 391 \\ -1 & 7 & 136 \end{bmatrix} \rightsquigarrow \\ \begin{bmatrix} 3 & -20 & 119 \\ -1 & 7 & 136 \end{bmatrix} &\rightsquigarrow \begin{bmatrix} 3 & -20 & 119 \\ -4 & 27 & 17 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 31 & -209 & 0 \\ -4 & 27 & 17 \end{bmatrix}. \end{aligned}$$

Therefore $\gcd(3553, 527) = 17$, and $17 = (-4)(3553) + (27)(527)$.

24. Which of the integers $0, 1, \dots, 10$ can be expressed in the form $12m + 20n$, where m, n are integers?

Solution: Theorem 1.1.6 provides the answer. An integer k is a linear combination of 12 and 20 if and only if it is a multiple of their greatest common divisor, which is 4. Therefore we can express 0, 4, and 8 in the required form, but we can't do it for the rest.

25. If n is a positive integer, find the possible values of $\gcd(n, n + 10)$.

Solution: Let $d = \gcd(n, n + 10)$. Then $d|n$ and $d|(n + 10)$, so we must have $d|10$, and therefore d is limited to one of 1, 2, 5, or 10. Can each of these occur for some n ?

Yes: $\gcd(3, 13) = 1$; $\gcd(2, 12) = 2$; $\gcd(5, 15) = 5$; $\gcd(10, 20) = 10$.

26. Prove that if a and b are nonzero integers for which $a|b$ and $b|a$, then $b = \pm a$.

Solution: Since $a|b$, there is an integer m with $b = ma$. Since $b|a$, there is an integer k with $a = kb$. Substituting $a = kb$ in the equation $b = ma$ we get $b = m(kb)$, so since b is nonzero we can cancel it to get $1 = mk$. Since both m and k are integers, and $|1| = |m||k|$, we must have $|m| = 1$ and $|k| = 1$, so either $b = a$ or $b = -a$.

27. Prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8.

Solution: First, we need to use the given information about m and n . Since they are odd, we can write them in the form $m = 2k + 1$ and $n = 2q + 1$, for some integers k and q . We can factor $m^2 - n^2$ to get $(m + n)(m - n)$, so substituting for m and n we get

$$m^2 - n^2 = (2k + 1 + 2q + 1)(2k + 1 - 2q - 1) = (2)(k + q + 1)(2)(k - q) .$$

Now we need to take two cases. If $k - q$ is even, then $k - q$ has 2 as a factor, say $k - q = 2p$, for some integer p . Substituting for $k - q$ gives us

$$m^2 - n^2 = (2)(k + q + 1)(2)(2)(p) = (8)(k + q + 1)(p) .$$

If $k - q$ is odd, then $k + q = (k - q) + (2q)$ is the sum of an odd integer and an even integer, so it must also be odd. That means that $k + q + 1$ is even, so it has 2 as a factor. Now we can suppose that $k + q + 1 = 2t$, for some integer t . In this case, substituting for $k + q + 1$ gives us

$$m^2 - n^2 = (2)(2)(t)(2)(k - q) = (8)(t)(k - q) .$$

Showing that we can factor 8 out of $m^2 - n^2$ gives exactly what we were to prove: if m and n are odd, then $m^2 - n^2$ is divisible by 8.

28. Prove that if n is an integer with $n > 1$, then $\gcd(n-1, n^2+n+1) = 1$ or $\gcd(n-1, n^2+n+1) = 3$.

Solution: Problem 25 gives a hint. In that problem, since the gcd was a divisor of n and $n+10$, it had to be a divisor of 10. To use the same approach, we would have to write n^2+n+1 as $n-1$ plus something. That doesn't work, but we are very close. Dividing n^2+n+1 by $n-1$ (using long division of polynomials) we get a quotient of $n+2$ and a remainder of 3, so $n^2+n+1 = (n+2)(n-1) + 3$. Now we can see that any common divisor of $n-1$ and n^2+n+1 must be a divisor of 3, so the answer has to be 1 or 3.

29. Prove that if n is a positive integer, then
$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

if and only if $4|n$.

Solution: We begin by computing A^2 , $A^3 = A \cdot A^2$, $A^4 = A \cdot A^3$, etc.

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^4 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Now we can see that if $4|n$, say $n = 4q$, then $A^n = A^{4q} = (A^4)^q = I^q = I$.

Conversely, if $A^n = I$, we can use the division algorithm to write $n = 4q + r$, with $0 \leq r < 4$. Then $A^r = A^{n-4q} = A^n(A^{-4})^q = I \cdot I^q = I$, so $r = 0$ since A , A^2 , and A^3 are not equal to I . We conclude that $4|n$.

30. Give a proof by induction to show that each number in the sequence 12, 102, 1002, 10002, ..., is divisible by 6.

Solution: To give a proof by induction, we need a statement that depends on an integer n . We can write the numbers in the given sequence in the form $10^n + 2$, for $n = 1, 2, \dots$, so we can prove the following statement: for each positive integer n , the integer $10^n + 2$ is divisible by 6.

The first step is to check that the statement is true for $n = 1$. (This "anchors" the induction argument.) Clearly 12 is divisible by 6.

The next step is to prove that if we assume that the statement is true for $n = k$, then we can show that the statement must also be true for $n = k + 1$. Let's start by assuming that $10^k + 2$ is divisible by 6, say $10^k + 2 = 6q$, for

some $q \in \mathbf{Z}$, and then look at the expression when $n = k + 1$. We can easily factor a 10 out of 10^{k+1} , to get $10^{k+1} + 2 = (10)(10^k) + 2$, but we need to involve the expression $10^k + 2$ in some way. Adding and subtracting 20 makes it possible to get this term, and then it turns out that we can factor out 6.

$$\begin{aligned} 10^{k+1} + 2 &= (10)(10^k) + 20 - 20 + 2 = (10)(10^k + 2) - 18 \\ &= (10)(6q) - (6)(3) = (6)(10q - 3) \end{aligned}$$

We have now shown that if $10^k + 2$ is divisible by 6, then $10^{k+1} + 2$ is divisible by 6. This completes the induction.