

1.2 SOLUTIONS

23. (a) Use the Euclidean algorithm to find
- $\gcd(1776, 1492)$
- .

Solution: We have $1776 = 1492 \cdot 1 + 284$; $1492 = 284 \cdot 5 + 72$;

$284 = 72 \cdot 3 + 68$; $72 = 68 \cdot 1 + 4$; $68 = 4 \cdot 17$. Thus $\gcd(1776, 1492) = 4$.

- (b) Use the prime factorizations of 1492 and 1776 to find
- $\gcd(1776, 1492)$
- .

Solution: Since $1776 = 2^4 \cdot 3 \cdot 37$ and $1492 = 2^2 \cdot 373$, Proposition 1.2.9 shows that $\gcd(1776, 1492) = 2^2$.

24. (a) Use the Euclidean algorithm to find
- $\gcd(1274, 1089)$
- .

Solution: We have $1274 = 1089 \cdot 1 + 185$; $1089 = 185 \cdot 5 + 164$;

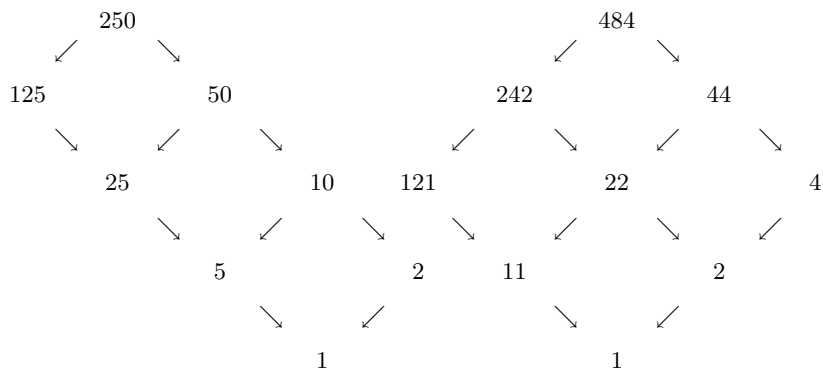
$185 = 164 \cdot 1 + 21$; $164 = 21 \cdot 7 + 17$; $21 = 17 \cdot 1 + 4$; $17 = 4 \cdot 4 + 1$. Thus $\gcd(1274, 1089) = 1$.

- (b) Use the prime factorizations of 1274 and 1089 to find
- $\gcd(1274, 1089)$
- .

Solution: Since $1274 = 2 \cdot 7^2 \cdot 13$ and $1089 = 3^2 \cdot 11^2$, we see that 1274 and 1089 are relatively prime.

25. Give the lattice diagram of all divisors of 250. Do the same for 484.

Solution: The prime factorizations are $250 = 2 \cdot 5^3$ and $484 = 2^2 \cdot 11^2$. In each diagram, we need to use one axis for each prime. Then we can just divide (successively) by the prime, to give the factors along the corresponding axis. For example, dividing 250 by 5 produces 50, 10, and 2, in succession. These numbers go along one axis of the rectangular diagram.



26. Find all integer solutions of the equation
- $xy + 2y - 3x = 25$
- .

Solution: If we had a product, we could use the prime factorization theorem. That motivates one possible method of solution.

$$xy + 2y - 3x = 25$$

$$\begin{aligned}
 (x+2)y - 3x &= 25 \\
 (x+2)y - 3x - 6 &= 25 - 6 \\
 (x+2)y - 3(x+2) &= 19 \\
 (x+2)(y-3) &= 19
 \end{aligned}$$

Now since 19 is prime, the only way it can be factored is to have $1 \cdot 19 = 19$ or $(-1) \cdot (-19) = 19$. Therefore we have 4 possibilities: $x+2 = 1$, $x+2 = -1$, $x+2 = 19$, or $x+2 = -19$. For each of these values there is a corresponding value for y , since the complementary factor must be equal to $y-3$. Listing the solutions as ordered pairs (x, y) , we have the four solutions $(-1, 22)$, $(-3, -16)$, $(17, 4)$, and $(-21, 2)$.

27. For positive integers a, b , prove that $\gcd(a, b) = 1$ if and only if $\gcd(a^2, b^2) = 1$.

Solution: Proposition 1.2.3 (d) states that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Using $c = b$ gives $\gcd(a, b^2) = 1$ if and only if $\gcd(a, b) = 1$. Then a similar argument yields $\gcd(a^2, b^2) = 1$ if and only if $\gcd(a, b^2) = 1$.

28. Prove that $n-1$ and $2n-1$ are relatively prime, for all integers $n > 1$. Is the same true for $2n-1$ and $3n-1$?

Solution: We can write $(1)(2n-1) + (-2)(n-1) = 1$, which proves that $\gcd(2n-1, n-1) = 1$. Similarly, $(2)(3n-1) + (-3)(2n-1) = 1$, and so $\gcd(3n-1, 2n-1) = 1$.

Comment: Is this really a proof? Yes—producing the necessary linear combinations is enough; you don't have to explain how you found them.

29. Let m and n be positive integers. Prove that $\gcd(2^m - 1, 2^n - 1) = 1$ if and only if $\gcd(m, n) = 1$.

Comment: We need to do the proof in two parts. First, we will prove that if $\gcd(m, n) = 1$, then $\gcd(2^m - 1, 2^n - 1) = 1$. Then we will prove the converse, which states that if $\gcd(2^m - 1, 2^n - 1) = 1$, then $\gcd(m, n) = 1$. To prove the converse, we will use a proof by contradiction, assuming that $\gcd(m, n) \neq 1$ and showing that this forces $\gcd(2^m - 1, 2^n - 1) \neq 1$.

Before beginning the proof, we recall that the following identity holds for all values of x : $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$.

Solution: If $\gcd(m, n) = 1$, then there exist $a, b \in \mathbf{Z}$ with $am + bn = 1$. Substituting $x = 2^m$ and $k = a$ in the identity given above shows that $2^m - 1$ is a factor of $2^{am} - 1$, say $2^{am} - 1 = (2^m - 1)(s)$, for some $s \in \mathbf{Z}$. The same argument shows that we can write $2^{bn} - 1 = (2^n - 1)(t)$, for some $t \in \mathbf{Z}$. The proof now involves what may look like a trick (but it is a useful one). We have

$$\begin{aligned}
 1 &= 2^1 - 1 \\
 &= 2^{am+bn} - 2^{bn} + 2^{bn} - 1
 \end{aligned}$$

$$\begin{aligned}
&= 2^{bn}(2^{am} - 1) + 2^{bn} - 1 \\
&= 2^{bn}(s)(2^m - 1) + (t)(2^n - 1)
\end{aligned}$$

and so we have found a linear combination of $2^m - 1$ and $2^n - 1$ that equals 1, which proves that $\gcd(2^m - 1, 2^n - 1) = 1$.

If $\gcd(m, n) \neq 1$, say $\gcd(m, n) = d$, then there exist $p, q \in \mathbf{Z}$ with $m = dq$ and $n = dp$. But then an argument similar to the one given for the first part shows that $2^d - 1$ is a common divisor of $2^{dq} - 1$ and $2^{dp} - 1$. Therefore $\gcd(2^m - 1, 2^n - 1) \neq 1$, and this completes the proof.

30. Prove that $\gcd(2n^2 + 4n - 3, 2n^2 + 6n - 4) = 1$, for all integers $n > 1$.

Solution: We can use the Euclidean algorithm. Long division of polynomials shows that dividing $2n^2 + 6n - 4$ by $2n^2 + 4n - 3$ gives a quotient of 1 and a remainder of $2n - 1$. The next step is to divide $2n^2 + 4n - 3$ by $2n - 1$, and this gives a quotient of $n + 2$ and a remainder of $n - 1$. We have shown that

$$\gcd(2n^2 + 6n - 4, 2n^2 + 4n - 3) = \gcd(2n^2 + 4n - 3, 2n - 1) = \gcd(2n - 1, n - 1)$$

and so we can use Problem 28 to conclude that $2n^2 + 4n - 3$ and $2n^2 + 6n - 4$ are relatively prime since $2n - 1$ and $n - 1$ are relatively prime.

(Of course, you could also continue with the Euclidean algorithm, getting $\gcd(2n - 1, n - 1) = \gcd(n - 2, 1) = 1$.)