1.1 Divisors

Before working through the solved problems for this section, you need to make sure that you are familiar with all of the definitions and theorems in the section. In many cases, the proofs of the theorems contain important techniques that you need to copy in solving the exercises in the text. Here are several useful approaches you should be able to use.

—When working on questions involving divisibility you may find it useful to go back to Definition 1.1.1. If you expand the expression $b|a$ by writing "$a = bq$ for some $q \in \mathbf{Z}$", then you have an equation to work with. This equation involves ordinary integers, and so you can use all of the things you already know (from high school algebra) about working with equations.

—To show that $b|a$, try to write down an expression for a and expand, simplify, or substitute for terms in the expression until you can show how to factor out b.

—Another approach to proving that $b|a$ is to use the division algorithm (see Theorem 1.1.3) to write $a = bq + r$, where $0 \leq r < b$. Then to prove that $b|a$ you only need to find some way to check that $r = 0$.

—Theorem 1.1.6 states that any two nonzero integers a and b have a greatest common divisor, which can be expressed as the smallest positive linear combination of a and b. An integer is a linear combination of a and b if and only if it is a multiple of their greatest common divisor. This is really useful in working on questions involving greatest common divisors.

SOLVED PROBLEMS: §1.1

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

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

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

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

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

27. Prove that if m and n are odd integers, 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 $\gcd(n - 1, n^2 + n + 1) = 3$.

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 $4|n$.

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