Section 3.4

2. 
1|a because there exists integer n, namely n = a, s.t. a = n * 1.

a|0 because there exists integer n, namely n = 0, s.t. 0 = n * a.

6. By assumptions that a|c and b|d, there exist integers n₁, n₂ s.t. c = n₁a and d = n₂b. Therefore cd = (n₁n₂)ab, i.e. there exists integer n, namely n = n₁n₂, s.t. cd = n(ab), and therefore ab|cd.

8. This is not true. For example 8|4 * 2 but it’s not true that either 8|4 or 8|2.

12. Note that we showed the opposite direction in class! This direction appears a bit more complicated. Let’s show this by arguing the counterpositive, i.e. that if (a mod n) ≠ (b mod n) then a ≡ b (mod n).

By the division algorithm theorem there exist unique remainders r₁ and r₂ in ℤₙ s.t. n|(a - r₁) and n|(b - r₂). (The theorem also says that the quotients are unique, but we don’t need it here.) Let q₁, q₂ be integers s.t. nq₁ = a - r₁ and nq₂ = b - r₂. Therefore n(q₁ - q₂) = (a - b) + (r₂ - r₁). Therefore we have

n | (a - b) + (r₂ - r₁) (1)

Now assume that the following holds:

n | (b - a) (2)

If that was the case then by part (i) of theorem 1, page 202, from (1) and (2) we would have that n|(r₂ - r₁). But since r₁, r₂ ∈ ℤₙ, integer (r₂ - r₁) is smaller than n and larger than -n, therefore n can divide (r₂ - r₁) only if r₂ = r₁. However, if (a mod n) ≠ (b mod n) then r₁ ≠ r₂, so we have a contradiction. Therefore we can conclude that the assumption (2) was wrong. Since (2) is equivalent with the statement that a ≡ b (mod n), we conclude that a ≢ b (mod n).

18. Any integer of the form 12 * n + 4 for some other integer n.

Section 3.5

10. 1, 5, 7, 11

12. (a) yes: 21 = 3 * 7, 34 = 2 * 17, 55 = 5 * 11, so no two of these have a common factor.
(b) no: 17|85
(c) yes: 25, 49, 64 are squares of 5, 7, 8 = 2³, respectively, while 41 is prime, so no two of these have a common factor.
(d) yes: 17, 19, 23 are prime, and 18 = 2 * 3², so no common factors again.

20. You should use the method of example 13, page 216, to find these gcd’s.

22. To compute the lcm, you should use the formula below definition 5, page 217, as in example 15. You can also use the gcd found in exercise (20) above and then use theorem 5, page 217.