Hints for exercises in chapter 1

Exercise 1.1.1(a). Write $a = db$ for some integer d. Show that if $d \neq 0$, then $|d| \geq 1$. (b) Prove that if u and v are integers for which $uv = 1$, then either $u = v = 1$ or $u = v = -1$. (c) Write $b = ma$ and $c = na$ and show that $bx + cy = max + nay$ is divisible by a.

Exercise 1.1.2. Use Lemma 1.1.1 and induction on a for fixed b.

Exercise 1.2.1(a). By exercise 1.1.1(c) we know that d divides $au + bv$ for any integers u and v. Now use Theorem 1.1. (d) First note that a divides b if and only if $-a$ divides b. If $|a| = \gcd(a, b)$, then $|a|$ divides both a and b, and so a divides b. On the other hand if a divides b, then $|a| \leq \gcd(a, b) \leq |a|$ by (c).

Exercise 1.2.4(b). Let $g = \gcd(a, b)$ and write $a = gA, b = gB$ for some integers A and B. What is the value of $Au + Bv$? Now apply (a).

Exercise 1.2.5(a). Use Theorem 1.1.

Exercise 1.4.2. Use Lemma 1.4.1.

Exercise 1.7.5(e). Write $r = m + \delta$ where $0 < \delta < 1$, so that $[r] = m$ and $a - r = a - m - \delta$ so that $[a - r] =?$.

Exercise 1.7.10. Given any solution, determine u using Lemma 1.1.1.

Exercise 1.7.11. One might apply Corollary 1.2.2.

Exercise 1.7.14(d). Use exercise 1.7.10.

Exercise 1.7.22. For each given $m \geq 1$, prove that $x_m | x_{mr}$ for all $r \geq 1$, by induction on r, using exercise 0.4.10(a) with $k = rm$.

Exercise 1.7.23(a). Prove that $\gcd(x_n, b) = \gcd(ax_{n-1}, b)$ for all $n \geq 2$, and then use induction on $n \geq 1$, together with Corollary 1.2.2. (b) Prove that $\gcd(x_n, x_{n-1}) = \gcd(bx_{n-2}, x_{n-1})$ for all $n \geq 2$, and then use induction on $n \geq 1$, together with Corollary 1.2.2. (c) Use exercise 0.4.10(a) with $k = n - m$ and then (b). (d) Follow the steps of the Euclidean algorithm using (c).

Exercise 1.9.1. Use the matrix transformation for $(u_j, u_{j+1}) \to (u_{j+1}, u_{j+2})$.

Exercise 1.14.1(c). If n is odd, take $a = b = c = 1, d = -1$. Show that if n is even, then a, b, c, d are odd so that $ad - bc$ is even.

Exercise 1.17.1. Divide the representation of $2/n$ above by an appropriate power of 2. Be careful when b is a power of 2.