Hints for exercises in chapter 3

Exercise 3.0.1. The only divisors of p are 1 and p. Therefore $\gcd(p,a) = 1$ or p, and so $\gcd(p,a) = p$ if and only if p divides a. This implies that $\gcd(p,a) = 1$ if and only if p does not divide a.

Exercise 3.1.1. Use induction and the fact that every integer > 1 has a prime divisor, as proved in the "prerequisites" section. (The proof will appear as part of the proof of Theorem 3.2.)

Exercise 3.1.2(a). Apply Theorem 3.1 with $a = a_1 \cdots a_{k-1}$ and $b = a_k$, and if p divides a, then proceed by induction.

(b) p divides some q_j by (a), and as q_j only has divisors 1 and q_j, and as $p > 1$, we deduce that $p = q_j$.

Exercise 3.1.3(b). Write $n = 2^k m$ with m odd. Then n has an odd prime factor if and only if $m > 1$. Therefore if n has no odd prime factor, then $n = 2^k$.

Exercise 3.2.1. We have $[a,b] = ab$ by Corollary 3.2.2. The result follows from Lemma 1.4.1.

Exercise 3.3.1. Look at this first in the case that m and n are both powers of p, say, $m = p^a$ and $n = p^b$. If d divides m and n, then $d = p^c$, say, with $c \le a$ and $c \le b$. The maximum c that satisfies both of these inequalities is $\min\{a,b\}$. Similarly if m and n divide $L = p^e$, then $a \le e$ and $b \le e$ and so the minimum e that satisfies both of these inequalities is $\max\{a,b\}$. Now use this idea when m and n are arbitrary integers.

Exercise 3.3.5. Use exercise 3.3.3(d).

Exercise 3.3.7(c). Use exercise 3.3.3(c).

Exercise 3.5.1(a). Show that the $aj + b$ are distinct mod m.

Exercise 3.5.2. Prove that the $r_j \pmod m$ are all reduced residues, and then that they are distinct.

Exercise 3.5.3. If $ar \equiv c \pmod b$, then b divides $ar - c$. Therefore $\gcd(a,b)$ divides $ar - c$ and so c. In the other direction, we write $g = \gcd(a,b)$ and so $a = gA, b = gB, c = gC$, and we are looking for solutions to $Ar \equiv C \pmod B$. Then use exercise 3.5.1(b).

Exercise 3.5.5. Use the second proof of Corollary 3.5.2.

Exercise 3.6.4. If $am + bn = c$, then $am + bn \equiv c \pmod b$ (or indeed mod any integer $r \ge 1$). On the other hand if $au + bv \equiv c \pmod b$ and m is any integer $\equiv u \pmod b$, then $am \equiv au + bv \equiv c \pmod b$ and so there exists an integer n for which $am + bn = c$.

Exercise 3.7.2(a) We proceed by induction on the number of moduli using exercise 3.2.1.

(b) Replace m in (a) by $m - n$.

Exercise 3.7.8(a). Work with the prime power divisors of m and use the Chinese Remainder Theorem.

Exercise 3.8.3. Calculate the product mod p^e, for every prime power $p^e \| m$.

Exercise 3.9.1. Use exercise 1.7.20(a).

Exercise 3.9.3(a). If $2k+1 = n/m$, take $u = \alpha^m$ and $v = \beta^m$ in

$$\frac{u^{2k+1} + v^{2k+1}}{u+v} = (-uv)^k + \sum_{j=1}^{k} (-uv)^{k-j}(u^{2j} + v^{2j}),$$

so that y_n/y_m is a linear polynomial in the y_{2jm} with coefficients that are $\pm$ powers of b.

Exercise 3.9.6. Use exercise 3.3.7(c), and factor $gA^2 - gB^2$.

Exercise 3.9.7(a). Write $\frac{z^p - y^p}{z-y}$ as a polynomial in y and z.

Exercise 3.9.10(a). $\sqrt{2} + \sqrt{3}$ is a root of $x^4 - 10x^2 + 1$. Use Theorem 3.4.

(b) $\sqrt{a} + \sqrt{b}$ is a root of $x^4 - 2(a+b)x^2 + (a-b)^2$. Therefore the rational root $m = \sqrt{a} + \sqrt{b}$ must be an integer, and then m divides $a - b$. Writing $a = b + mk$ we have $k = \sqrt{a} - \sqrt{b}$ so that $b = (\frac{m-k}{2})^2$ and $a = (\frac{m+k}{2})^2$.

Exercise 3.9.11(b). Prove that $(\sqrt{d} + m)(\sqrt{d} - m)$ is an integer

Exercise 3.9.15(b). Use Corollary 2.3.1.

Exercise 3.9.17(b). Write $m = gM$ and $n = gN$ where $g = \gcd(m, n)$ so that $(M, N) = 1$, and then use exercise 3.7.7 (or exercise 3.9.16(b), for a less complete solution).

Exercise 3.10.2. Write the trinomial coefficient as the product of binomial coefficients.

Exercise 3.11.1. Prove this by induction on $n \geq 1$, using the observation in the paragraph immediately above.

Exercise 3.15.2. Let $G = \mathbb{Z}/4\mathbb{Z}$ and H be the subgroup of order two. Determine the maximal order of an element of $H \oplus G/H$, as well as of G.

Exercise 3.19.1. Use exercise 0.14.6.

Exercise 3.19.2. R is a Euclidean domain if there exists $w : R \to \mathbb{Z}_{\geq 0}$ such that for any $a, b \in R$ with $b \neq 0$, there exists $q \in R$ such that if $r = a - qb$, then $w(r) < w(b)$. Given any ideal I of R, let $b \in I$, $b \neq 0$, with $w(b)$ minimal. For any $a \in I$ let $r = a - qb \in I$ so that $w(r) < w(b)$ which contradicts the minimality of $w(b)$.

Exercise 3.22.1. Use Proposition 2.10.1 and adapt the proof of Euclid's Lemma.

Exercise 3.24.1(c). $f(x) = 3x + 1$ has the rational root $-\frac{1}{3}$ yet $f(n) \equiv 1 \pmod 3$, for all integers n.