Hints for exercises in chapter 8

Exercise 8.1.2(b). Use Lemma 8.1.1.

Exercise 8.1.3(a). Use that $\left(\frac{b^2}{p}\right) = \left(\frac{b}{p}\right)^2 = (\pm 1)^2 = 1$.

Exercise 8.1.6(a). The residues $1, g^2, g^4, \dots, g^{p-3} \pmod p$ are evidently distinct and non-zero squares. As there are $\frac{p-1}{2}$ of them, they are all of the quadratic residues by Lemma 8.1.1.

(b) We see above that $g = g^1$ is not one of the quadratic residues.

Exercise 8.2.1. There are two solutions to $r^2 \equiv a \pmod p$, say, r and $-r \pmod p$, whose product is $r \cdot (-r) \equiv -a \pmod p$. Note also that $|S| = \frac{p-3}{2}$.

Exercise 8.4.1. r is the largest integer with $2r - 1 \le \frac{q-1}{2}$; that is, $r \le \frac{q+1}{4}$.

Exercise 8.4.5. Look at $(2/p)$.

Exercise 8.7.2(a). Use the Chinese Remainder Theorem and exercise 8.1.2(b).

Exercise 8.7.5. If a is odd, then $a = 1 + 2 \cdot \frac{a-1}{2}$, and so

$$1+2\cdot\frac{ab-1}{2} = ab = \left(1+2\cdot\frac{a-1}{2}\right)\left(1+2\cdot\frac{b-1}{2}\right) \equiv 1+2\cdot\left(\frac{a-1}{2}+\frac{b-1}{2}\right) \pmod 4.$$

Exercise 8.7.6. Select $a^2 \equiv -2 \pmod p$ with a odd and minimal, so that $1 \le a \le p-1$. Write $a^2 + 2 = pr$. Evidently $pr \equiv a^2 + 2 \equiv 3 \pmod 8$ and so $r \equiv 3p \equiv 5$ or $7 \pmod 8$. But then $a^2 \equiv -2 \pmod r$ and so $\left(\frac{-2}{r}\right) = 1$ with $r = \frac{a^2+2}{p} < p$. This contradicts the induction hypothesis, and so $\left(\frac{-2}{p}\right) = -1$.

Exercise 8.8.1. Suppose that $k > \ell \ge 1$. If r is a quadratic residue mod p^k, then r is a quadratic residue mod p^ℓ, trivially. On the other hand if r is a quadratic residue mod p^ℓ, then it is a quadratic residue mod $p^{\ell+1}$ by Proposition 8.8.1, then mod $p^{\ell+2}$ by Proposition 8.8.1, etc., up to mod p^k. We take $\ell = 1$ if p is odd, and $\ell = 3$ if $p = 2$ and note that if r is a quadratic residue mod 8, then $r \equiv 1 \pmod 8$.

Exercise 8.9.5(a). Write $n = 3^a m$ where $3 \nmid m$.

Exercise 8.9.9(a). Consider the size of the set of residues $\{a^2 \pmod p\}$ and of the set of residues $\{m - b^2 \pmod p\}$, as a and b vary.

(b) Take $m = -1$.

(c) Prove there is a solution u, v to $au^2 + bv^2 \equiv -c \pmod p$ and then multiply through by any $z \pmod p$.

Exercise 8.9.10(e). Apply Gauss's trick as in the proof of Corollary 7.5.2.

Exercise 8.9.12. For each solution to $y^2 \equiv b \pmod p$, consider whether there are solutions to $x^2 \equiv y \pmod p$.

Exercise 8.9.14. Let $b^2 \equiv -1 \pmod p$ and study $(1 + b)^2 \pmod p$.

Exercise 8.9.15. Show that if a has order $m \pmod p$, then $\sigma_{a,p}$ consists of $\frac{p-1}{m}$ cycles of length m.

Exercise 8.9.16(a). Use exercise 1.7.20(c). (b) Use exercise 1.7.20(b).

Exercise 8.9.17. Select integer m with $(m/n) = -1$. Consider the prime divisors of integers of the form $kn + m$ for well-chosen values of k.

Exercise 8.9.18(a). Modify the ideas in Euclid's proof that there are infinitely many primes. (b) $n = -3$. (c) Look at $4m^2 + 3$ with m odd. (d) $n = 3$. Note $(m^2 - 3)/2 \equiv 2 \pmod 3$. (e) $n = -4$. Note $m^2 + 4 \equiv 5 \pmod 8$. (f) $n = 2$. Note $m^2 - 2 \equiv 7 \pmod 8$. (g) $n = -2$. Note $m^2 + 2 \equiv 3 \pmod 8$. (h) $n = -4$ with $(m, 6) = 1$.

Exercise 8.9.24. Therefore $\left(\frac{2}{n}\right) = \left(\frac{2}{n-2}\right)$ if $n \equiv 1 \pmod 4$, and $\left(\frac{2}{n}\right) = -\left(\frac{2}{n-2}\right)$ if $n \equiv 3 \pmod 4$, and so the result follows by the induction hypothesis.

Exercise 8.10.2. If $N = pq+m$ where $0 \le m \le p-1$, then $N-p[N/p] = N-pq = m$. If $r \ge 0$, then $m = r$; and if $r < 0$, then $m = p + r$.

Exercise 8.16.3(f). Prove this first when n is a prime power; and then note that if $m \not\equiv 1 \pmod n$, then $m \not\equiv 1 \pmod{p^k}$ for some prime power $p^k \| n$.

Exercise 8.17.2(a). Use the law of quadratic reciprocity. (c) Look back at exercise 8.9.5.

Exercise 8.18.1. Calculate $F_{p-1} \pmod p$ using F_p and F_{p+1}, and then proceed by induction.

Exercise 8.18.2. Prove that $F_{n+p+1} \equiv -F_n \pmod p$ by induction.

Exercise 8.18.3. Proceed analogously to as in the two previous exercises.

Exercise 8.18.6(a). Let $m = kr$ in exercise 0.4.10, and use the congruence in exercise 2.5.19(c) with $r = 1$ and 2. (b) When does $F_{kr}, F_{kr+1} \equiv 0, 1 \pmod{p^2}$?