Hints for exercises in chapter 9

Exercise 9.1.2. If p does not divide a, then $(b/a)^2 \equiv -1 \pmod{p}$. Therefore $p = 2$ or $p \equiv 1 \pmod{4}$. We get the same conclusion if p does not divide b and, otherwise, p divides (a, b).

Exercise 9.1.4. By induction on $k \geq 1$: It is trivial for $k = 1$ and otherwise let $n_k = a^2 + b^2$ and $n_1 \cdots n_{k-1} = c^2 + d^2$ (by the induction hypothesis), and then the result follows from (9.1.1).

Exercise 9.1.7(d). Use (a) to prove that $|ac - bd|, |ad - bc| < p$.

Exercise 9.3.1. Proceed as in the geometric proof of (6.1.1), or as in the proof of Proposition 9.1.2.

Exercise 9.7.2(b). Replace a and b by their absolutely least residues mod p.

Exercise 9.7.3(b). Select any b with $\left(\frac{b}{p}\right) = -1$ in (a), and let $m = r$ or s.

Exercise 9.7.7. We know that n is the length of the hypotenuse of a primitive Pythagorean triple iff there exist coprime integers r, s of different parity with $n = r^2 + s^2$. Hence all of n's prime factors are $\equiv 1 \pmod{4}$, and we know we get at least two representations of n if it has at least two distinct prime factors.

Exercise 9.7.9. Since $m^2 \pm 2$ are odd they must be $\equiv 3 \pmod{4}$, and so must be divisible by a prime $\equiv 3 \pmod{4}$.

Exercise 9.7.10(a). In what domains do each of the ranges of ϕ lie? (b) We must be in the middle case (as $y, z \neq 0$) so that $x = y$ in which case $x(x + 4z) = p$. Since p can only be factored in one way into positive integers, we have $x = 1, z = \frac{p-1}{4}$; that is, $v = (1, 1, \frac{p-1}{4})$. (c) Pair up the elements of S using ϕ.

Exercise 9.9.2. Try $a = b = n = 1$.

Exercise 9.11.1(d). Use exercise 8.9.9(c).

Exercise 9.12.2. Use (9.12.1).

Exercise 9.13.2. Use the characteristic polynomial for A, which is the polynomial $x^2 - tx + d$ satisfied by A, where t is the trace of A and d is the determinant.