Chapter 9

Quadratic equations

9.1. Sums of two squares

Exercise 9.1.1. Prove that any odd integer n that can be written as the sum of two squares must be $\equiv 1 \pmod 4$. Deduce Proposition 9.1.1.

Exercise 9.1.2. Prove that if prime p divides $a^2 + b^2$, then either $p = 2$ or p divides (a, b) or $p \equiv 1 \pmod 4$.

Exercise 9.1.3. Find four distinct representations of $1105 = 5 \times 13 \times 17$ as a sum of two squares.

Exercise 9.1.4. Prove that if $n = n_1 \cdots n_k$ where $n_1, \ldots, n_k$ are each the sum of two squares, then n is the sum of two squares.

Exercise 9.1.5. Prove that if n is squarefree and is the sum of two squares, then every positive divisor of n is also the sum of two squares.

Exercise 9.1.6. Deduce that positive integer n can be written as the sum of two squares of *rationals* if and only if n can be written as the sum of two squares of integers.

Exercise 9.1.7.† Suppose that prime $p = a^2 + b^2$.

(a) Prove that $|a|, |b| < \sqrt{p}$.

(b) Prove that if $r^2 \equiv -1 \pmod p$, then either $r \equiv a/b \pmod p$ or $r \equiv b/a \pmod p$.

(c) If prime p divides $c^2 + d^2$ but $p \nmid cd$, show that p divides either $ac - bd$ or $ad - bc$, and deduce that p divides both terms on the right-hand side of either (9.1.1) or (9.1.2), respectively.

(d) Suppose that $p = a^2 + b^2 = c^2 + d^2$ where $a, b, c, d > 0$. Show that $\{a, b\} = \{c, d\}$.

In other words, we have proved that each prime $\equiv 1 \pmod 4$ has a unique representation as the sum of two squares, unique up to changing the order of the squares, or their signs.

Exercise 9.1.8.† Prove, using the method of Theorem 9.1, that a squarefree integer n can be written as the sum of two squares if and only if -1 is a square mod n.

9.2. The values of $x^2 + dy^2$

Exercise 9.2.1. Fix integer $d \geq 1$. Give an identity showing that the product of two integers of the form $a^2 + db^2$ is also of this form.

Exercise 9.2.2. Which primes are of the form $a^2 + 3b^2$? Which integers?

Exercise 9.2.3. Which primes are of the form a^2+5b^2? Try listing what primes are represented and compare the list with the set of primes p for which $(-5/p)=1$.

9.3. Is there a solution to a given quadratic equation?

Exercise 9.3.1. Given one integer solution to $ax_0^2+by_0^2+cz_0^2=0$, show that all other integer solutions to $ax^2+by^2+cz^2=0$ are given by the parametrization

$$x:y:z \;=\; (ar^2-bs^2)x_0+2brsy_0 \;:\; 2arsx_0-(ar^2-bs^2)y_0 \;:\; (ar^2+bs^2)z_0\ .$$

9.4. Representation of integers by ax^2+by^2 with x, y rational, and beyond

9.5. *The failure of the local-global principle for quadratic equations in integers*

9.6. Primes represented by x^2+5y^2

Additional exercises

Exercise 9.7.1. Let $f(n)$ be the arithmetic function for which $f(n)=1$ if n can be written as the sum of two squares, and $f(n)=0$ otherwise. Prove that $f(n)$ is a multiplicative function.

Exercise 9.7.2. Let p be a prime $\equiv 1 \pmod 4$. This exercise yields another proof that p is the sum of two squares.

(a) Use Theorem 8.3 to prove that there exist integers a and b such that a^2+b^2 is a positive multiple of p.

(b) Let rp be the smallest such multiple of p. Prove that $r \le p/2$.

(c)† Prove that if $r>1$, then there exists a positive integer $s \le r/2$ such that $rs=c^2+d^2$ for some integers c and d, selected so that $ad-bc$ is divisible by r.

(d) Use (9.1.2) to deduce that if $r>1$, then sp is a sum of two squares.

This contradicts the minimality of r unless $r=1$; that is, p is the sum of two squares.

Exercise 9.7.3. Let p be an odd prime.

(a)† Suppose that $b \pmod p$ is given and that $R, S \ge 1$ such that $RS=p$. Prove that there exist integers r, s with $|r| \le R, 0 < s \le S$ such that $b \equiv r/s \pmod p$.

(b) Prove that there exists an integer m with $|m| < \sqrt{p}$ for which $\left(\frac{m}{p}\right)=-1$.

(c) Deduce that if $p \equiv 1 \pmod 4$, then there exists an integer n in the range $1 < n < \sqrt{p}$ for which $\left(\frac{n}{p}\right)=-1$.

Exercise 9.7.4. Show that x and y are integers in (9.1.3) if and only if r^2+s^2 divides $2(ar+bs)$, and show that this can only happen if r^2+s^2 divides $2n$.

Exercise 9.7.5. What values of r and s yield the point $(-a,-b)$ in Proposition 9.1.2?

Exercise 9.7.6. Reprove exercise 9.1.8 using Theorem 9.1 and (9.1.1).

Exercise 9.7.7.† $33^2+56^2=65^2$ and $16^2+63^2=65^2$ are examples of the side lengths of different primitive Pythagorean triangles with the same hypotenuse. Classify those integers that appear as the hypotenuse of at least two different primitive Pythagorean triangles.

Exercise 9.7.8. Prove that for every integer m there exists an integer n which is the length of the hypoteneuse of at least m different primitive Pythagorean triples. (You may use Theorem 7.4 which implies that there are infinitely many primes $\equiv 1 \pmod 4$.)

Exercise 9.7.9.† Prove that an integer of the form a^2+4b^2 with $(a,2b)=1$ cannot be divisible by any integer of the form m^2-2 with $m>1$, or m^2+2. Conversely prove that an integer of the form m^2-2n^2 or m^2+2n^2 with $(m,2n)=1$ cannot be divisible by any integer of the form a^2+4.

Exercise 9.7.10.‡ (Zagier's proof that every prime $\equiv 1 \pmod 4$ is the sum of two squares) Let

$$S := \{(x,y,z) \in \mathbb{N}^3 : \ p = x^2+4yz\}.$$

Define the map $\phi : S \to S$ by

$$\phi : (x,y,z) \to \begin{cases} (x+2z, z, y-x-z) & \text{if } x < y-z, \\ (2y-x, y, x-y+z) & \text{if } y-z < x < 2y, \\ (x-2y, x-y+z, y) & \text{if } x > 2y. \end{cases}$$

(a) Show that ϕ is an *involution*, that is, $\phi^2 = 1$, and verify that each $\phi(S)$ belongs to S.
(b) Prove that if $\phi(v) = v$, then $v = (1, 1, \frac{p-1}{4})$.
(c) Deduce that there are an odd number of elements of S (in particular, S is non-empty). Let $\psi : S \to S$ be the involution $\psi(x,y,z) = (x,z,y)$.
(d) Prove that ψ has a fixed point (x,y,y) so that $z = y$.
(e) Deduce that $p = x^2 + (2y)^2$ for some integers x, y.

Appendix 9A. Proof of the local-global principle for quadratic equations

9.8. Lattices and quotients

Exercise 9.8.1. (a) Show that there exist integers U, V, W, coprime with abc, for which $U \equiv u \pmod{bc}$, $V \equiv v \pmod{ac}$, $W \equiv w \pmod{ab}$, so that $aU^2+bV^2+cW^2 \equiv 0 \pmod{|abc|}$.
(b) Let U^{-1} be an integer $\equiv 1/U \pmod{abc}$ and W^{-1} be an integer $\equiv 1/W \pmod{abc}$. Show that Λ is generated by the vectors $(1, VU^{-1}, WU^{-1})$, $(0, c, -bVW^{-1})$, and $(0,0,ab)$.)
(c) Deduce that $\det(\Lambda) = |abc|$.

9.9. A better proof of the local-global principle

Exercise 9.9.1. (a) Prove that if $(x,y,z) \in \Lambda$, then $ax^2+by^2+cz^2 \equiv 0 \pmod{4|abc|}$.
(b) Prove that $\det(\Lambda) = 4|abc|$.

Exercise 9.9.2. Give infinitely many examples in which $\max\{|a\ell^2|, \ |bm^2|, \ |cn^2|\} = |abc|$ in the smallest non-trivial solution of $a\ell^2+bm^2+cn^2 = 0$.

Appendix 9B. Reformulation of the local-global principle

9.10. The Hilbert symbol

9.11. The Hasse-Minkowski principle

Exercise 9.11.1. Suppose we are given a quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$ with each $a_i \in \mathbb{Z}$.

(a) By changing variables and multiplying through by a suitable constant, show that we may assume each a_i is squarefree.

(b) Prove that if the a_i do not all have the same sign, then there is a non-trivial real solution to $a_1x_1^2 + \cdots + a_nx_n^2 = 0$.

Let p be a given prime.

(c) By possibly multiplying through by p and changing variables, show that we may assume that for every prime p, no more than $n/2$ of the a_i are divisible by p.

(d) Deduce that if $n \geq 5$, then there exist integers $m_1, \ldots, m_n$ for which $a_1m_1^2 + \cdots + a_nm_n^2 \equiv 0 \pmod{p}$, such that there exists some j for which $a_jm_j \not\equiv 0 \pmod{p}$.

(e) Prove Theorem 9.7 using the Hasse-Minkowski principle.

Appendix 9C. The number of representations

9.12. Distinct representations as sums of two squares

Exercise 9.12.1. Give another proof of exercise 9.7.1 using exercise 4.3.2.

Exercise 9.12.2. Prove that $R(n)/4$ equals the number of divisors of n that are $\equiv 1 \pmod 4$ minus the number of divisors of n that are $\equiv 3 \pmod 4$.

Appendix 9D. Descent and the quadratics

9.13. Further solutions through linear algebra

Exercise 9.13.1. Fix integer $k \geq 1$. Let $x_0 = 0$, $x_1 = 1$, and $x_n = kx_{n-1} - x_{n-2}$ for all $n \geq 2$. Prove that all solutions to $a^2 + b^2 = k(ab+1)$ in non-negative integers a, b with $k = m^2$ are given by $a = mx_n,\ b = mx_{n-1}$ for some integer $n \geq 1$.

Exercise 9.13.2. Prove that if A is any 2-by-2 matrix and the vector $u_n = A^n u_0$ for some given matrix u_0, then u_n satisfies a second-order linear recurrence.

9.14. The Markov equation

Exercise 9.14.1.† Determine what solutions are obtained from (1,1,1) by using the maps $(x, y) \to (3y - x, y)$ and $(x, y) \to (x, 3x - y)$.

9.15. Apollonian circle packing

Exercise 9.15.1. Suppose that you are given three mutually tangent circles A, B, and C_0 of curvatures a, b, and x_0 in an Apollonian circle packing. For each $n \geq 0$ let C_{n+1} be the circle tangent to the circles A, B, and C_n that lies in the crescent between these three circles, and let x_{n+1} be its curvature. Prove that

$$x_n = (a + b)(n^2 - n) + (x_1 - x_0)n + x_0 \text{ for all } n \geq 0.$$