Chapter 12

Binary quadratic forms

12.1. Representation of integers by binary quadratic forms

An integer N is *represented* by f if there exist integers m, n for which $N = f(m, n)$, and N is *properly represented* if $(m, n) = 1$ (see exercise 3.9.13 for the same question for linear forms).

Exercise 12.1.1. Prove that if N is squarefree, then all representations of N are proper.

Exercise 12.1.2. (a) Suppose that d is a fundamental discriminant. Prove that the character $(d/\cdot)$ has conductor dividing d.
(b) Prove that for any non-zero integer d, the character $(d/\cdot)$ has conductor that divides $4d$.

The *conductor* of $f(\cdot)$ is the minimum $p > 0$ such that $f(n + p) = f(n)$ for all integers n.

Exercise 12.1.3. Suppose that $d \equiv 0$ or $1 \pmod 4$. Show that every binary quadratic form of discriminant d is primitive if and only if d is a fundamental discriminant.

Exercise 12.1.4. (a) Show that if $d < 0$, then $am^2 + bmn + cn^2$ has the same sign as a, no matter what the choices of integers m and n.
(b) Show that if $ax^2 + bxy + cy^2$ is positive definite, then $a, c > 0$.
(c) Show that if $d > 0$, then $am^2 + bmn + cn^2$ can take both positive and negative values, by making explicit choices of integers m, n.

Exercise 12.1.5. Use (12.1.3) to show that two equivalent binary quadratic forms have the same discriminant.

Exercise 12.1.6. Show that the principal form is equivalent to every binary quadratic form $x^2 + bxy + cy^2$ with leading coefficient 1, up to equivalence.

Exercise 12.1.7. In each part, determine whether the two binary quadratic forms are equivalent. If so, make the equivalence explicit; if not, explain why not.
(a) $y^2 + xy + 4x^2$ and $x^2 - 5xy + 10y^2$.
(b) $x^2 + 3xy + 5y^2$ and $3x^2 - 4xy + 11y^2$.

12.2. Equivalence classes of binary quadratic forms

12.3. Congruence restrictions on the values of a binary quadratic form

Exercise 12.3.1.† Prove that if $f \sim g$, then $\sigma_f(p) = \sigma_g(p)$ for all odd primes p dividing d.

Exercise 12.3.2. Prove that if $p_1, \dots, p_k$ are distinct primes that are each represented by some form of discriminant d, then $p_1 \cdots p_k$ is also represented by some form of discriminant d.

12.4. Class numbers

Exercise 12.4.1. Determine all of the reduced binary quadratic forms of discriminant d for $-20 \le d \le -1$ as well as for $d = -28, -43, -67, -167$, and -171.

Exercise 12.4.2. Determine all of the reduced binary quadratic forms of discriminant d for $d = -3, -15, -23, -39, -47, -87, -71$, and -95.

Exercise 12.4.3. Determine all of the reduced binary quadratic forms of discriminant d for $d = -4, -20, -56$, and -104.

Exercise 12.4.4. Prove that if $ax^2 + bxy + cy^2$ is a reduced binary quadratic of discriminant $d < 0$, then $|c| \ge \sqrt{|d|}/2$.

12.5. Class number one

Exercise 12.5.1. (a) Determine the two reduced binary quadratic forms of discriminant -15.
(b) Determine which reduced residue classes can be represented by some form of discriminant -15?
(c) Distinguish which primes are represented by which form (with proof).

Exercise 12.5.2.† Prove that if $n^2 + n + A$ is prime for all integers n in the range $0 \le n \le B$, where $1 \le B < (A-1)/2$, then $\left(\frac{1-4A}{p}\right) = -1$ for all primes $p \le 2B + 1$.

Exercise 12.5.3. Let q be a prime $\equiv -1 \pmod 4$. Prove that $\left(\frac{p}{q}\right) = -1$ for all primes $p < \frac{q+1}{4}$ if and only if $h(-q) = 1$. This result suggests that finding a small prime p with $\left(\frac{p}{q}\right) = 1$ can be a deep problem (see appendix 8B for a discussion of small quadratic residues).

Additional exercises

Exercise 12.6.1. Suppose that $f(x, y) = ax^2 + bxy + cy^2$ is a reduced binary quadratic form.
(a) Show that if $am^2 + bmn + cn^2 \le a - |b| + c$ with $(m, n) = 1$, then $|m|, |n| \le 1$.
(b) Prove that the least values properly represented by f are $a \le c \le a - |b| + c$, the first two properly represented twice, the last twice unless $b = 0$, in which case it is properly represented four times.

Exercise 12.6.2. We now use the results of exercise 12.6.1 to understand equivalences between primitive reduced binary quadratic forms. The idea is to recognize a reduced binary quadratic form by the smallest values it properly represents.

(a) Prove that:
- If $0 < |b| < a < c$, then $[a, b, c]$ properly represents a, c, and $a - |b| + c$ in exactly 2, 2, and 2 different ways, respectively.
- If $0 < |b| = a < c$, then $[a, b, c]$ properly represents a, and $c = a - |b| + c$ in exactly 2, and 4 different ways, respectively.
- If $0 < |b| < a = c$, then $[a, b, c]$ properly represents $a = c$, and $a - |b| + c$ in exactly 4, and 2 different ways, respectively.
- If $0 = |b| < a < c$, then $[a, b, c]$ properly represents a, c, and $a - |b| + c$ in exactly 2, 2, and 4 different ways, respectively.
- $[1, 1, 1]$ properly represents 1 in exactly six different ways.
- $[1, 0, 1]$ properly represents both 1 and 2 in exactly four different ways.

(b) Deduce that if $[a, b, c]$, and $[A, B, C]$ are equivalent primitive reduced binary quadratic forms, then $A = a$, $C = c$, and $B = b$ or $-b$.

(c) Use exercise 12.6.1(a) to show that the entries of a matrix representing such an equivalence must each be -1, 0, or 1.

(d) Prove that distinct primitive reduced binary quadratic forms are all inequivalent. Together with Theorem 12.1 this implies that every positive definite binary quadratic form is properly equivalent to a unique reduced form.

(e) Suppose that $M \in \mathrm{SL}(2, \mathbb{Z})$ transforms a primitive reduced binary quadratic form to itself (this is an *automorphism*). Show that $M = \pm I$, except in the following two cases:
- $[1, 1, 1]$ has automorphisms given by $\pm I$, $\pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, and $\pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.
- $[1, 0, 1]$ has automorphisms given by $\pm I$ and $\pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Exercise 12.6.3. (a) Show that if $[A, B, C] \sim [a, b, c]$, then $[A, -B, C] \sim [a, -b, c]$.

(b) Use exercise 12.6.2(d) to show that if $[a, b, c]$ is reduced, then $[a, b, c] \sim [a, -b, c]$ if and only if $b = 0$, $b = a$, or $a = c$.

(c) Deduce that $[A, B, C] \sim [A, -B, C]$ if and only if they are equivalent to a quadratic form $[a, 0, c]$, $[a, a, c]$, or $[a, b, a]$.

(d) Prove that $[a, a, c] \sim [c, 2c - a, c]$.

(e) If $d < 0$ is odd, then show that the primitive reduced forms are given by taking each factorization $-d = rs$ with $0 < r \le s$ and $(r, s) = 1$,

$$\begin{cases} [a, a, c] & \text{if } s \ge 3r \text{ where } a = r \text{ and } c = (r + s)/4, \\ [a, b, a] & \text{if } s < 3r \text{ where } a = (r + s)/4 \text{ and } b = (s - r)/2. \end{cases}$$

(f) If $d < 0$ is even, then show that the primitive reduced forms are given by taking each factorization $-d/4 = rs$ with $0 < r \le s$ and $(r, s) = 1$,

$$\begin{cases} [a, 0, c] & \text{with } a = r \text{ and } c = s, \\ [a, a, c] & \text{if } s > 3r \text{ where } a = 2r \text{ and } c = (r + s)/2, \\ [a, b, a] & \text{if } s < 3r \text{ where } a = (r + s)/2 \text{ and } b = s - r. \end{cases}$$

Note that the last two cases hold only if $d/4$ is odd.

(g) Show that each binary quadratic form either represents both r and s, or both $2r$ and $2s$. (In (d), take $f(1, -2) = s$ in the first case; $f(1, 1) = s$, $f(1, -1) = r$ in the second case.)

(h) Deduce that if $d < 0$ is a fundamental discriminant, then there are exactly 2^{t-1} reduced binary quadratic forms for which $[a, b, c] \sim [a, -b, c]$, where t is the number of odd prime divisors of $|d|$, unless $4 \| d$ in which case there are 2^t.

Exercise 12.6.4.† (a) Prove that x^2+6y^2 and $2x^2+3y^2$ are the only binary quadratic forms, up to equivalence, of discriminant -24.
(b) Prove that prime p can be written in the form a^2+6b^2 if and only if $p \equiv 1$ or $7 \pmod{24}$.
(c) Prove that prime p can be written in the form $2u^2+3v^2$ if and only if $p = 2$ or 3, or $p \equiv 5$ or $11 \pmod{24}$.
We can refine this further:
(d) Prove that prime p can be written in the form a^2+24B^2 if and only if $p \equiv 1 \pmod{24}$.
(e) Prove that prime p can be written in the form $8U^2+3v^2$ if and only if $p = 3$, or $p \equiv 11 \pmod{24}$.

Automorphisms of binary quadratic forms.

Exercise 12.6.5. Suppose that $f \sim g$ via the transformation M and that G is the group of automorphisms of f.
(a) Prove that $M^{-1}GM$ is the group of automorphisms of g.
(b) Prove that MG is the set of transformations yielding g from f.
(c) Deduce that there are $\omega(d)$ automorphisms of every primitive quadratic form of discriminant d, where $\omega(-3) = 6, \omega(-4) = 4$, and $\omega(d) = 2$ for all other discriminants $d < 0$.

Exercise 12.6.6. (a) If $N = f(a,b)$, then $N = f(-a,-b)$. If $N = a^2+b^2$, then $N = b^2+(-a)^2 = (-a)^2+(-b)^2 = (-b)^2+a^2$. If $N = a^2+ab+b^2$, then find five other representations of N by the quadratic form x^2+xy+y^2.
(b) Explain how these representations correspond to the automorphisms of the quadratic form.
(c) Why did we not include $N = (-a)^2+b^2$ in the representations in part (a)?

Exercise 12.6.7. (a) Let $\alpha, \beta, \gamma, \delta$ be given integers for which $\alpha\delta - \beta\gamma = 1$. Prove that β', δ' are integers for which $\alpha\delta' - \beta'\gamma = 1$ if and only if there exists an integer k such that

$$\begin{pmatrix} \alpha & \beta' \\ \gamma & \delta' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.$$

(b) If $A = f(\alpha,\gamma)$ with $(\alpha,\gamma) = 1$, then prove that there exists a unique pair of integers β, δ such that $f \sim [A,B,C]$ using the matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ for some integer B in the range $-A < B \le A$.
(c) Deduce that the proper representations of the integer A by reduced binary quadratic forms of discriminant d are in $\omega(d)$-to-1 correspondence with the solutions to $B^2 \equiv d \pmod{4A}$ with $-A < B \le A$.

Exercise 12.6.8. Let $f_1, \dots, f_h$ be the $h = h(d)$ distinct reduced binary quadratic forms of discriminant d, where $d \equiv 0$ or $1 \pmod 4$. Let $r_j(A)$ denote the number of proper representations of A by f_j. Prove that

$$r_1(A) + \cdots + r_h(A) = \frac{1}{2}\omega(d) \cdot \#\{B \pmod{4A} : B^2 \equiv d \pmod{4A}\}$$

and that this equals $\omega(d) \cdot \prod_{p|A} \left(1 + \left(\frac{d}{p}\right)\right)$ unless perhaps $4|(A,d)$.

Exercise 12.6.9. Suppose that p is an odd prime for which $(d/p) = 1$. Prove that p is properly represented either by only the principal form of discriminant d, or by only two non-principal, reduced, binary quadratic forms of discriminant d, one, say, $ax^2+bxy+cy^2$, the other $ax^2-bxy+cy^2$.

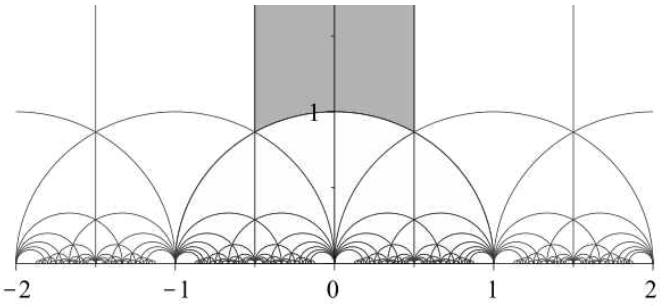
Transformations of the upper half-plane.

Exercise 12.6.10. Prove that S represents the transformation $z \to z+1$ and that T represents the transformation $z \to -1/z$.

Exercise 12.6.11.† Prove that the binary quadratic form $ax^2+bxy+cy^2$ with discriminant $d < 0$ is reduced if and only if $\frac{-b+\sqrt{d}}{2a} \in \mathcal{F}$.

Exercise 12.6.12.† Prove that for every $z \in \mathbb{C}$ there exists $M \in \mathrm{SL}(2,\mathbb{Z})$ such that $Mz \in \mathcal{F}$. Prove that M is unique.

Exercise 12.6.13.‡ Show that $\{M\mathcal{F} : M \in \mathrm{SL}(2,\mathbb{Z})\}$ is a partition of $\mathcal{H}$ into disjoint sets.



The shaded region is $\mathcal{F}$. Each enclosed region is a domain $M\mathcal{F}$ for some $M \in \mathrm{SL}(2,\mathbb{Z})$.

Appendix 12A. Composition rules: Gauss, Dirichlet, and Bhargava

12.7. Composition and Gauss

Exercise 12.7.1. (a) Prove that if n is represented by $ax^2+bxy+cy^2$, then an is represented by the principal form of the same discriminant.
(b) Suppose that $d<0$. Deduce that if d is a square mod $4n$, then there is a multiple an of n which is represented by the principal form of discriminant d, with $1 \le a \le \sqrt{|d|/3}$.
(c) We obtained the bound $1 \le a \le \sqrt{|d|}$ when d is even in section 9.6. Use that method to find a bound in the case that d is odd.

Exercise 12.7.2. Suppose that a is a prime and $d=b^2-4ac$ is even. Let $D=-d/4$.
(a) Show that if a divides r^2+Ds^2, then a divides either $r+(b/2)s$ or $r-(b/2)s$.
(b) Prove that if $r^2+Ds^2=an$, then there exist integers X,Y for which $n=aX^2+bXY+cY^2$.

If n is prime, then this result is true whether or not a is prime, but we will not prove that here. Assume though that is so.
(c) Suppose that $(d/p)=1$ and that ap is the smallest multiple of p that is represented by the principal form. Prove that a here must take the same value as in exercise 12.6.9.
(d) Prove that $1 \le a \le \sqrt{|d|/3}$ and then use exercises 12.4.4 and 12.6.1(b) to prove that if $p<\sqrt{|d|}/2$, then $a=p$.

Exercise 12.7.3. Given non-zero integers a,b,c,d prove that there exist integers m,n such that the set of integers that can be represented by $(ar+bs)(cu+dv)$ as r,s,u,v run over the integers is the same as the set of integers that can be represented by $mx+ny$ as x,y run over the integers.

Exercise 12.7.4. Show that the above congruences for b_3 can be solved.

12.8. Dirichlet composition

Exercise 12.8.1. Given any primitive binary quadratic form $f(x,y) \in \mathbb{Z}[x,y]$ and non-zero integer A, prove that there exist integers r and s such that $f(r,s)$ is coprime to A. Deduce that there exists a binary quadratic form g, for which $f \sim g$, with $(g(1,0),A)=1$.

Exercise 12.8.2. Suppose that $f(x,y), F(X,Y)$ are two binary quadratic forms, with $\operatorname{disc}(f) \equiv \operatorname{disc}(F) \pmod 2$, for which $f(1,0) = a$ is coprime to $F(1,0) = A$. Prove that there exist quadratic forms $g = ax^2 + bxy + cy^2$ and $G = AX^2 + bXY + CY^2$ with the same middle coefficient, such that $f \sim g$ and $F \sim G$.

12.9. Bhargava composition

Appendix 12B. The class group

12.10. A dictionary between binary quadratic forms and ideals

Exercise 12.10.1. (a) Show that if a and b are represented by f of discriminant d, then ab is represented by the principal quadratic form of discriminant d.
(b) Show that if a is represented by f of discriminant d, and b is represented by the principal quadratic form of discriminant d, then ab is represented by f.
(c) Prove that if $f(x,y)$ represents integers a, b, and c, then it represents abc.

12.11. Elements of order two in the class group

Exercise 12.11.1. Use Corollary 9.4.1 and quadratic reciprocity to prove that $\prod_{p|d} \sigma_f(p) = 1$.

Exercise 12.11.2. Prove that if $f \sim g$, then $\sigma_f(2) = \sigma_g(2)$ when d is even.

Exercise 12.11.3. Suppose that $f = [a,b,c]$ and $F = [A,B,C]$ are reduced, primitive binary quadratic forms of fundamental discriminant $d < 0$ for which $\sigma_f(p) = \sigma_F(p)$ for all primes p dividing d. Prove that f and F are equivalent over the rationals. (In other words, there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ with $\alpha\delta - \beta\gamma = 1$ for which $F = f(\alpha x + \beta y, \gamma x + \delta y)$.)

Appendix 12C. Binary quadratic forms of positive discriminant

12.12. Binary quadratic forms with positive discriminant, and continued fractions

Exercise 12.12.1. Prove that every reduced form of positive discriminant has a unique reduced neighboring form to the left and a unique reduced neighboring form to the right.

12.13. The set of automorphisms

Appendix 12D. Sums of three squares

12.14. Connection between sums of 3 squares and $h(d)$

Exercise 12.14.1.‡ If p is a prime and $p = 8n \pm 1$ or ± 5, then there are exactly n solutions to $p^2 = a^2 + b^2 + c^2$ with $1 \le a \le b \le c$. (I do not know how to prove it using only elementary methods.)

12.15. Dirichlet's class number formula

Exercise 12.15.1. (a) Prove that $J_p = 0$ if $p \equiv 1 \pmod 4$.
(b) Prove that J_p is divisible by p if p is a prime > 3.

For $p \equiv 3 \pmod 4$ and $p > 3$ we find that the values of $j_p := J_p/p$ are

$$j_7 = -1,\ j_{11} = -1,\ j_{19} = -1,\ j_{23} = -3,\ j_{31} = -3,\ j_{43} = -1,\ j_{47} = -5,\ j_{59} = -3, \ldots.$$

Can you see any patterns and perhaps guess at the value? Write a program to get more data. At this point Jacobi did something unexpected: He computed the class number $h(-p)$ for primes $p \equiv 3 \pmod 4$ (see, e.g., section 12.4) and compared. Do you see a pattern now?

Exercise 12.15.2. Let $S := \sum_{n=1}^{(p-1)/2} \left(\frac{n}{p}\right)$ and $T := \sum_{n=1}^{(p-1)/2} \left(\frac{n}{p}\right) n$.
(a) Show that $S = 0$ when $p \equiv 1 \pmod 4$. Henceforth assume that $p \equiv 3 \pmod 4$ with $p > 3$.
(b) Note that $\left(\frac{p-n}{p}\right)(p-n) = \left(\frac{n}{p}\right)(n-p)$. Use this to evaluate the sum $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) n$ in terms of S and T by pairing up the nth and $(p-n)$th term, for $n = 1, 2, \ldots, \frac{p-1}{2}$.
(c) Do this taking $n = 2m$, $m = 1, 2, \ldots, \frac{p-1}{2}$ to deduce from (12.15.1) that

$$h(-p) \;=\; \frac{1}{2 - \left(\frac{2}{p}\right)} \sum_{n=1}^{(p-1)/2} \left(\frac{n}{p}\right).$$

Exercise 12.15.3. Let p be an odd prime and $x \equiv \frac{p-1}{2}! \pmod p$. In exercise 7.4.3 we showed that $x^2 \equiv -\left(\frac{-1}{p}\right) \pmod p$.
(a) Prove that $x^{\frac{p-1}{2}} \equiv (-1)^N \pmod p$ where $N \equiv \frac{1}{2}\sum_{n=1}^{(p-1)/2} \left(1 - \left(\frac{n}{p}\right)\right) \pmod 2$.
(b) Show that if $p \equiv 3 \pmod 4$, then $h(-p)$ is odd and $N \equiv \frac{1}{2}(h(-p)+1) \pmod 2$ using exercise 12.15.2(c).
(c) Deduce that if $p \equiv 3 \pmod 4$, then $\frac{p-1}{2}! \equiv (-1)^{\frac{h(-p)+1}{2}} \pmod p$.

Appendix 12E. Sums of four squares

12.16. Sums of four squares

Exercise 12.16.1. Prove that we may take $|a|, |b|, |c|, |d| < p/2$, so that $m < p$.

Exercise 12.16.2. Show that if m is even, then we can reorder a, b, c, d so that $a - b$ and $c - d$ are both even. Using the identity

$$\left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 = \frac{1}{2}(a^2+b^2+c^2+d^2),$$

prove that m must be odd.

Exercise 12.16.3. Prove that $A \equiv B \equiv C \equiv D \equiv 0 \pmod m$.

Exercise 12.16.4. Prove that no integer of the form 2^{2k+1} is the sum of three or four positive squares, and the only such representation of 2^{2k} is $(2^{k-1})^2 + (2^{k-1})^2 + (2^{k-1})^2 + (2^{k-1})^2$.

12.17. Quaternions

12.18. The number of representations

Exercise 12.18.1. Prove that this can rewritten as follows:

$$\sum_{N\geq 0} r_4(N)x^N := \left(\sum_{n\in\mathbb{Z}} x^{n^2}\right)^4 = 8\sum_{\substack{d\geq 1\\ 4\nmid d}} \frac{dx^d}{1-x^d} = 1+8\left(\sum_{n\geq 1}\frac{x^n}{(1-x^n)^2} - \sum_{m\geq 1}\frac{4x^{4m}}{(1-x^{4m})^2}\right).$$

Exercise 12.18.2. (a) Show that if $8|N$ and $N = a^2+b^2+c^2+d^2$, then a, b, c, d are all even; and so deduce that $r_4(2^k m) = r_4(2^{k-2}m)$ if $k \geq 3$.

(b)† Prove that if m is odd, then $r_4(2^k m) = 3r_4(m)$ for all $k \geq 1$.

Exercise 12.18.3. (a) Verify the identity

$$4(a^2+b^2+c^2+d^2) = (a+b+c+d)^2+(a+b-c-d)^2+(a-b+c-d)^2+(a-b-c+d)^2.$$

(b)† Suppose that $m \equiv n \pmod 2$. Prove that there exist integers a, b, c, d for which $n = a^2+b^2+c^2+d^2$ with $m = a+b+c+d$ if and only if $4n-m^2$ can be written as the sum of three squares.

Henceforth let n be odd.

(c) Deduce that for every odd integer m with $|m| < 2\sqrt{n}$ there exist integers a, b, c, d for which $n = a^2+b^2+c^2+d^2$ and $m = a+b+c+d$.

(d) Show that there is a 1-to-1 correspondence between solutions to $4n-m^2 = u^2+v^2+w^2$ with $u \equiv v \equiv w \equiv m \pmod 4$ and solutions to $n = a^2+b^2+c^2+d^2,\ m = a+b+c+d$ with $a \not\equiv b \equiv c \equiv d \pmod 2$.

(e) Deduce that there is a 2-to-1 correspondence between solutions to $4n-m^2 = u^2+v^2+w^2$ and solutions to $n = a^2+b^2+c^2+d^2,\ m = a+b+c+d$.

(f) Using Gauss's result mentioned at the end of section 12.14 of appendix 12D, deduce that if n is odd, then there are $12h(m^2-4n)$ solutions to $n = a^2+b^2+c^2+d^2,\ m = a+b+c+d$.

Appendix 12F. Universality

12.19. Universality of quadratic forms

Appendix 12G. Integers represented in Apollonian circle packings

12.20. Combining these linear transformations

Exercise 12.20.1. Suppose that we are given four mutually tangent circles with integer radii, and create an Apollonian circle packing from them. Prove that there is an infinite chain of distinct circles in the packing with *prime* curvatures $p_1 < p_2 < \cdots$ where the circles of curvatures p_m and p_{m+1} are mutually tangent, for every $m \geq 1$.