Chapter 5
Binary Quadratic Forms and the Löschian Diophantine Equation

One proof of Gauss's Law of Reciprocity, using contemporary techniques was linked to at the end of the previous chapter. There are also numerous classical proofs, some of which rest on the Chinese Remainder Theorem (link to one of them). Because such proofs often assume that the reader already knows the Chinese Remainder Theorem, and because it has been our experience that readers often do not know this theorem, we present it here in detail.

The Chinese Remainder Theorem

At the time the greatest common divisor was defined, it would have been possible to define a related number, the least common multiple.

Definition 5.1. Suppose a and b are two positive integers. The least common multiple $[a, b]$ is the smallest positive integer which is a multiple of both a and b. The relationship between them is illustrated in the following lemma.

Lemma 5.2. Let a and b be two positive integers. Then

a) $(a, b)\ [a, b] = ab$
b) If $d \mid a$ and $d \mid b$, then $d \mid (a, b)$
c) If $a \mid m$ and $b \mid m$, then $ab \mid m$.

Proof:

a) Consider the prime factorizations of a, b. Let

$$a = p_1^{a1} p_2^{a2} \ldots p_k^{ak}$$
$$b = p_1^{b1} p_2^{b2} \ldots p_k^{bk}$$

(in this case, some exponents may be 0; a prime is included in the list if it is a divisor of either a or b).

Then

$$(a, b) = p_1^{c1} \ldots p_k^{ck} \text{ where } c_i = \min \{a_i, b_i)$$
$$[a, b] = p_1^{d1} \ldots p_k^{dk} \text{ where } d_i = \max (a_i, b_i)$$

Since $a_i + b_i = c_i + d_i$ for each i, $(a, b)\ [a, b] = ab$.

b) There are integers s, t such that $(a, b) = as + bt$. If $a = dx$, $b = dy$, $(a, b) = d(xs) + d(yt) = d(xs + yt)$. So $d \mid (a, b)$.

c) Let $m = [a, b]q + r$, $0 \leq r < [a, b]$. As in b), since $a \mid m$ and a $\mid [a, b]$, $a \mid r$. Similarly $b \mid r$. Since $r < [a, b]$, this contradicts the fact that $[a, b]$ is the LEAST common multiple of a and b. So $r = 0$. If $(a, b) = 1$, $[a, b] = ab$ by part a), so $ab \mid m$.

The least common multiple is used in arithmetic to add fractions, where it is called the least common denominator. For example, since [15, 21] = 15(21)/(15,21) = 15(21)/3 = 105

$$4/15 + 5/21 = (4/15)((21/3)/(21/3)) + (5/21)((21/3)/(21/3)) = (4(7) + 5(5))/105 = 53/105.$$

The least common multiple arises when it is desired to solve several congruences (with different moduli) simultaneously. The process below appears to have been known in first century China. Hence it has come to be known as the Chinese Remainder Theorem.

Theorem 5.3. The Chinese Remainder Theorem
Let m_1, m_2, ..., m_r be positive integers such that $(m_i, m_j) = 1$ if $i \neq j$. Let a_1, ..., a_r be any integers. Then the system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$....$$
$$x \equiv a_r \pmod{m_r}$$

has a common solution of x, and if x, y are two such solutions $x \equiv y (\text{mod } m=m_1m_2...m_r)$.

Proof:
For each j, let $k_j = m / m_j$. Thus $(k_j, m_j) = 1$, since m_j has no factors in common with any m_i if $i \neq j$. Thus there is an integer b_j with $k_jb_j \equiv 1 (\text{mod } m_j)$. Also, if $i \neq j$ $k_jb_j \equiv 0(\text{mod } m_i)$. Let $x = Sk_jb_ja_j$ $1 \leq j \leq r$. Then, for each i, $x \equiv k_ib_ia_i \equiv a_i (\text{mod } m_i)$. Further, if x and y are two solutions $x \equiv y(\text{mod } m_i)$. Thus $m_i \mid (x - y)$ for each i. By Lemma 5.2c) $m \mid (x - y)$. So $x \equiv y(\text{mod } m)$.

Here is a classic example. A man has a basket of eggs. He doesn't know how many eggs there are, but when he counts them by twos, there is one left over. Similarly, when he counts by threes or fives, there is one remaining. When he counts by sevens, there are two left over. What is the least number of eggs he could have in his basket? If x is the number of eggs, the system of congruences is

$$x \equiv 1 (\text{mod } 2)$$
$$x \equiv 1 (\text{mod } 3)$$
$$x \equiv 1 (\text{mod } 5)$$
$$x \equiv 2 (\text{mod } 7)$$

So $m=210$, $k_1=105$, $k_2=70$, $k_3=42$, $k=30$. To find b_1, b_2, b_3, b_4 solve

$$105b_1 \equiv 1(\text{mod } 2) \text{ or } b_1 \equiv 1(\text{mod } 2)$$
$$70b_2 \equiv 1(\text{mod } 3) \text{ or } b_2 \equiv 1(\text{mod } 3)$$
$$42b_3 \equiv 1(\text{mod } 5) \text{ or } 2b_3 \equiv 1(\text{mod } 5)$$
$$30b_4 \equiv 1(\text{mod } 7) \text{ or } 2b_4 \equiv 1(\text{mod } 7)$$

One set of solution is $b_1=1$, $b_2=1$, $b_3=3$, $b_4=4$. Thus $x=105(1)(1)+70(1)(1)+42(3)(1)+30(4)(1)=541$. The smallest positive integer congruent to 541(mod 210) is 121. Thus the least number of eggs the man has is 121.

While computations such as those of the above example are fascinating, the theoretical consequences are more important.

Theorem 5.4. Suppose $(m_1, m_2) = 1$. Then the equation $f(x) \equiv 0(\text{mod } m=m_1m_2)$ has a solution if and only if both $f(x) \equiv 0(\text{mod } m_1)$, and $f(x) \equiv 0(\text{mod } m_2)$ have solutions (here $f(x)$ is a polynomial with integer coefficients).

Remark: In fact if $f(x) \equiv 0(\text{mod } m_1)$ has n_1 solutions and $f(x) \equiv 0(\text{mod } m_2)$ has n_2 solutions, then $f(x) \equiv 0(\text{mod } m)$ has n_1n_2 solutions. See Niven, Zuckerman, and Montgomery, Theorem 2.20, for a proof. In the book, the theorem will be used to see if $x^2 \equiv a$ has solutions for certain composite moduli.

Proof: If $f(x) \equiv 0 \pmod{m}$, then for some integer k, $f(x) \equiv km = km_1m_2$. Thus $f(x) \equiv 0 \pmod{m_1}$ and $f(x) \equiv 0 \pmod{m_2}$. On the other hand, suppose $f(x) \equiv 0 \pmod{m_1}$ and $f(x) \equiv 0 \pmod{m_2}$ both have solutions. Suppose $f(a_1) \equiv 0 \pmod{m_1}$ and $f(a_2) \equiv \pmod{m_2}$. By the Chinese Remainder Theorem, there is an integer $x \pmod{m}$, $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$. Then $f(x) \equiv f(a_1) \equiv 0 \pmod{m_1}$ and $f(x) \equiv f(a_2) \equiv 0 \pmod{m_2}$. Thus $m_1 \mid f(x)$, $m_2 \mid f(x)$. Thus since $(m_1, m_2) \equiv 1$, by Lemma 5.2 $m = m_1m_2 \mid f(x)$, so $f(x) \equiv 0 \pmod{m}$.

The Chinese Remainder Theorem can also be used to help calculate the value of Euler's ϕ-function.

Theorem 5.5.

a) If p is a prime, $\phi(p^n) = p^n - p^{n-1}$
b) If $(m_1, m_2) = 1$, $\phi(m_1, m_2) = \phi(m_1)\phi(m_2)$.

Proof:

a) Suppose p is a prime. Then, consider the complete residue system 1, 2, ..., p^n. The only integers in this list NOT relatively prime to p are p_1, $2p$, ..., $(p^{n-1})p$. Thus $\phi(p^n) = p^n - p^{n-1}$.
b) The goal is to establish a one-to-one correspondence between integers a in the set {1, 2, ..., m} which are relatively prime to m and pairs of integers (a_1, a_2), where

a_1 is in {1, 2, ..., m_1}, relatively prime to m_1
a_2 is in {1, 2, ..., m_2}, relatively prime to m_2.

First, suppose $(a, m) = 1$. Then $(a, m_1) = 1$ and $(a, m_2) = 1$. Let a_i be the remainder when a is divided by m_i, $_i$ = 1, 2. Second, suppose a_1, a_2 are as above. Then the Chinese Remainder Theorem assures there is a unique a in {1, 2, ..., m} with $a \equiv a_1 \pmod{m_1}$ and $a \equiv a_2 \pmod{m_2}$. Since $(a, m_1) = 1$ and $(a, m_2) = 1$, it follows that $(a, m_1m_2) = 1$. Thus, since this one-to-one correspondence exists, $f(m) = f(m_1)\, f(m_2)$.

For example, since $\phi(4) = 4 - 2 = 2$ and $\phi(5) = 4$, $\phi(20) = 8$. Since $\phi(8) = 8 - 4 = 4$ and $\phi(9) = 9 - 3 = 6$, $\phi(72) = 4(6) = 24$. One of the pairings of part b) of the theorem is of (1, 2), where (1, 8) = 1 and (2, 9) = 1 with 65, a number relatively prime to 72 with $65 \equiv 1 \pmod{8}$ and $65 \equiv 2 \pmod{9}$. This is the solution of the system

$x \equiv 1 \pmod{8}$
$x \equiv 2 \pmod{9}$

determined by the Chinese Remainder Theorem ($k_1=9$, $k_2=8$; $b_1=1$, $b_2=8$) since $x \equiv 9(1)(1) + 8(8)(2) = 137 \equiv 65 \pmod{72}$.

Binary Quadratic Forms

In order to find which integers are of the form $x^2 + xy + y^2$ for integers x, y (as desired by Loeb and Dacey), it is first necessary to study binary quadratic forms in general.

Definition 5.6.

a) A function $f(x, y) = ax^2 + bxy + cy^2$ is called a binary quadratic form. If $n = f(x_0, y_0)$ for some integers x_0, y_0, then the form f represents n properly if $(x_0, y_0) = 1$, improperly if $(x_0, y_0) \neq 1$.
b) The points (x, y) where x, y are integers are called lattice points.
c) The discriminant d of a quadratic form is $d = b^2 - 4ac$.
d) A form is called

positive definite if it takes on only positive values when $(x, y) \neq (0, 0)$.
negative definite if it takes on only negative values when $(x, y) \neq (0, 0)$.
semidefinite if it takes on only non-negative values or non-positive values.

Theorem 5.7.

a) $d \equiv 0$ or 1 (mod 4)
b) A form with $d = 0$ is semidefinite but not definite. A form with positive discriminant is indefinite. A form with negative discriminant is definite (positive if $a>0$, negative if $a<0$)

Theorem 5.8. Let $M = [m_{11}m_{12}; m_{21}, m_{22}]$. Let $[u; v] = M[x; y]$, that is $u = m_{11}x + m_{12}y$, $v = m_{21}x + m_{12}y$. Then this transformation is a permutation of the lattice points in the plane if and only if det M = +/- 1.

Definition 5.9. Two quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are said to be equivalent if there is a matrix M of determinant 1, $M = [m_{11}, m_{12}; m_{21}, m_{22}]$, such that $g(x, y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$.

Theorem 5.8 suggests that matrices of determinant -1 could have been allowed in Definition 5.9. Indeed, some number theory texts allow this. Still others use the term "properly equivalent" if det M = 1, "improperly equivalent" if det M = -1. Niven, Zuckerman, and Montgomery use the approach of Definition 5.9.

Theorem 5.9.

a) Equivalence of forms partitions the set of quadratic forms into sets of forms all of which are equivalent to each other.
b) Equivalent forms represent the same integers n, and represent the same integers properly.
c) Equivalent forms have the same discriminant.

Definition 5.10. Let f be a binary quadratic form whose discriminant is not a perfect square; f is called reduced if $-|a| < b \leq |a| < |c|$ or if $0 \leq b \leq |a| = |c|$.

Theorem 5.11. If d is not a perfect square, each equivalence class of binary quadratic forms of discriminant d contains at least one reduced form.

Theorem 5.12. Suppose f is a reduced positive definite quadratic form of discriminant d. The $0 < a \leq (-d/3)^{0.5}$.

Corollary 5.13. There is only one reduced form with discriminant -3.

Proof: By Theorem 5.12 $a = 1$; $b = 0$ is impossible since $d \equiv b^2$ (mod 4). Therefore, Definition 5.10 assures $b = 1$, $c = 1$.

Theorem 5.14. Let n and d be given integers with $n \neq 0$. There is a binary quadratic form of discriminant d which represents n properly if and only if $x^2 \equiv d$(mod $4|n|$) has a solution.

Corollary 5.15. Suppose $d \equiv 0$ or 1 (mod 4). If p is an odd prime, there is a binary quadratic form of discriminant which represents p if and only if $(d/p) = 1$.

Application to Löschian Numbers

Definition 5.16. A positive integer n is called Löschian if there are integers x and y such that $n = x^2 + xy + y^2$.

Since there is only one reduced form of discriminant -3, namely $x^2 + xy + y^2$, and since if n is representable by a form of discriminant -3 if and only if it is representable by an equivalent reduced form, Theorem 5.14 assures that n is properly representable by $x^2 + xy + y^2$ if and only if $x^2 \equiv -3$ (mod $4n$) or $x^2 + 3 \equiv 0$(mod $4n$) has a solution.

By Theorem 5.4, $x^2 + 3 \equiv 0$ (mod $4n$) has a solution if and only if $x^2 + 3 \equiv 0$ (mod $p_i^{a_i}$) has a solution for every i.

1) If $p \mid n$ and $p \equiv 1$ (mod 3), then by quadratic reciprocity $(-3/p) = (p/3) = 1$ and also $(-3/p^n) = (p^n/3) = (p/3)^n$

= 1, so $x^2 + 3 \equiv 0 \pmod{p^n}$ has a solution for every n.
2) However suppose $p \equiv 2 \pmod 3$. Then $(-3/p) = 1$, and so $x^2 + 3 \equiv 0 \pmod p$ has no solution. But $x^2 + 3 \equiv 0 \pmod{p^n}$ implies $p^n \mid (x^2 + 3)$ which in turn implies that $p \mid (x^2 + 3)$, which is impossible.
3) Of course $x^2 + 3 \equiv 0 \pmod 3$ has a solution (x = 0) but $x^2 + 3 \equiv 0 \pmod{3^n}$ has no solution for $n > 1$ since $9 \mid (x^2 + 3)$ implies $3 \mid x^2$ implies $3 \mid x$, say $x = 3a$; but then $x^2 + 3 = 3(3a^2 + 1) \equiv 3 \pmod 9$, a contradiction.

Thus N is properly representable by $x^2 + xy + y^2$ if and only if $N = 3^{\mathrm{a}}\mathrm{p}p^{\mathrm{b}}$, where every $p \equiv 1 \pmod 3$ and a =0 or 1. Of course if $N = x^2 + xy + y^2$, $c^2N = (cx)^2 + (cx)(cy) + (cy)^2$ so the square of any properly representable integer is improperly representable. Thus an integer N is Löschian if and only if $N = 3^{\mathrm{a}}\mathrm{p}p^{\mathrm{b}}\mathrm{p}q^{2\mathrm{g}}$ where every $p \equiv 1 \pmod 3$, every $q \equiv 2 \pmod 3$. Of course, sometimes, it is not necessary to find the prime factorization of N to see if it is Löschian. Since always $x^2 + xy + y^2 \equiv 0$ or $1 \pmod 3$ [try the nine cases $x \equiv a$, $y \equiv b \pmod 3$; if $a = b$, $x^2 + xy + y^2 \equiv 0 \pmod 3$; otherwise $x^2 + xy + y^2 \equiv 1 \pmod 3$].

So if $N \equiv 2 \pmod 3$, N is non-Löschian.

For example, N=32759 is non-Löschian (it is not immediately obvious that N = 17(41)(47).

Similarly, suppose $N = p^nM$, where $(M, p) = 1$, $p \equiv 0, 1 \pmod p$. If $M \equiv 2 \pmod 3$, N is non-Löschian, since the sum of the exponents of the primes $\equiv 2 \pmod 3$ in the prime factorization of M must be odd.

For example, $N = 8073 = 3^3(299)$, and $299 \equiv 2 \pmod 3$. So 8073 is non-Löschian. In fact, $8073 = 3^3(13)(23)$.

In summary,
Theorem 5.17. Let N be a positive integer. Then

a) N is properly representable as $x^2 + xy + y^2$ for integers x, y if and only if $N = 3^{\mathrm{a}}M$, where a = 0,1 and every prime factor of M is $\equiv 1 \pmod 3$.
b) N is Löschian if $N = 3^{\mathrm{a}}MT^2$, where every prime factor of M is $\equiv 1 \pmod 3$ and every prime factor of T is $\equiv 2 \pmod 3$.
c) N is non-Löschian if $N \equiv 2 \pmod 3$
d) N is non-Löschian if $N = p^nM$, $(M, p) = 1$, $M \equiv 2 \pmod 3$.

Löschian numbers: examples of Theorem usage

In this chapter, we have proved a theorem that lets anyone determine exactly which numbers are Löschian and which numbers are not Löschian. The formal mechanics of proof drew on a variety of earlier theorems and on facts from number theory. The creative effort involved the recasting of Marshall's earlier work in a form that would lead to the desired conclusion of a sufficient condition. Readers wishing to examine the history of this development are referred to articles published by Marshall (1975), S. Arlinghaus (1985), and S. Arlinghaus and W. Arlinghaus (1989). So that one might see how the results of Theorem 5.17 can be implemented, we offer several examples below.

- K = 175 is Löschian, since K = 52 x 7.
- $K = 125 = 5^3$ is not Löschian
- K = 245 = 5 x 72 is not Löschian
- K = 85 is not Löschian, even though 85 is congruent to 1(mod 3), since K = 5 x 17, and both 5 and 17 are congruent to 2(mod 3)
- K = 49 is Löschian as 49 may be generated using the Diophantine equation on either the ordered pair (0, 7) or on (3, 5): representation is not unique.

Theorem 5.17 offers an easy way to check whether a given number is Löschian. It does not give the geometric characterization of the associated hierarchy. For that characterization, the reader then needs to return to the material in Chapter 4 and the Fundamental Theorem offered there.

Spatial Synthesis: Centrality and Hierarchy, Volume I, Book 1.

Sandra Lach Arlinghaus and William Charles Arlinghaus