Representing Primes by Binary Quadratic Forms

Blair K. Spearman and Kenneth S. Williams

The study of integral binary quadratic forms

$$f(x, y) = ax^2 + bxy + cy^2 \ (a, b, c \text{ integers})$$

has its origins in the work of Fermat, Euler, Lagrange, and Legendre (see for example [5, Chapter 1]). An integer n is said to be represented by f if there exist integers x and y such that $n = f(x, y)$. An important problem in the theory of binary quadratic forms is to determine the set of positive primes represented by $f(x, y)$. For this problem we restrict ourselves to those f which are (i) primitive, that is $\mathrm{GCD}(a, b, c) = 1$; (ii) irreducible, that is the discriminant $D = b^2 - 4ac$ is not a square; and (iii) positive-definite if $D < 0$. This avoids those f which represent at most one prime or for which the representation problem can be solved by factoring f. If f satisfies (i), (ii), (iii) it will be called a form for short. Dirichlet in 1840 (see [7, Vol. I, pp. 497–502]) was the first to show that a form $ax^2 + bxy + cy^2$ represents infinitely many primes for a certain class of discriminants and Weber [10] in 1882 was the first to give a proof valid for any discriminant.

In the seventeenth century Fermat characterized the set of primes represented by the form $x^2 + y^2$. He showed that this set consists of the prime 2 together with all primes $p \equiv 1 \pmod 4$. If we exclude the prime 2, which divides the discriminant -4 of the form $x^2 + y^2$, Fermat's theorem can be stated: for a prime $p \neq 2$ we have

$$p = x^2 + y^2 \ (x, y \text{ integers}) \quad \text{if and only if } p \equiv 1 \pmod 4.$$

Fermat also stated, and Euler proved, the following similar results: for a prime $p \neq 2$ we have

$$p = x^2 + 2y^2 \quad \text{if and only if } p \equiv 1, 3 \pmod 8,$$

and for a prime $p \neq 2, 3$

$$p = x^2 + 3y^2 \quad \text{if and only if } p \equiv 1 \pmod 3.$$

These and other similar results suggest a theorem of the following type: if $ax^2 + bxy + cy^2$ is a form of discriminant D then there exist positive integers $s, a_1, \ldots, a_s, m$ (depending on a, b and c) such that for an odd prime p not dividing D we have

$$p = ax^2 + bxy + cy^2 \quad \text{if and only if } p \equiv a_1, \ldots, a_s \pmod m. \tag{1}$$

However such a result does not hold for every form $ax^2 + bxy + cy^2$. This fact is often stated in number theory textbooks [1, p. 345], [2, p. 242], [4, p. 2], [5, p. 62], [6, p. 145] but when this claim is addressed [2, p. 242], [4, §1] reference is usually

made to class field theory. It seems desirable to give a more transparent justification of this assertion. We will do this by appealing to the following generalization of Weber's theorem to quadratic polynomials $ax^2 + bxy + cy^2 + dx + ey + f$ in two variables, where $a, b, \ldots, f$ are integers: the polynomial $g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$ represents infinitely many primes provided $\deg g = 2$, $\mathrm{GCD}(a, b, c, d, e, f) = 1$, $g(x, y)$ is irreducible in $Q[x, y]$, $g(x, y)$ represents arbitrarily large odd integers, and $g(x, y)$ is genuinely a function of two variables. This result follows from a theorem of Iwaniec [**9**], which can be proved without class field theory. The failure of a result of type (1) will be demonstrated for the particular form $x^2 + 14y^2$. Other forms for which (1) also fails can be treated in a similar manner. We prove

Theorem. *There do not exist positive integers* $s, a_1, \ldots, a_s, m$ *with* $\mathrm{GCD}(a_i, m) = 1$ $(i = 1, \ldots, s)$ *such that for primes* $p \neq 2, 7$

$$p = x^2 + 14y^2 \quad \text{if and only if } p \equiv a_1, \ldots, a_s \pmod{m}. \tag{2}$$

We will also need the concept of a genus (plural genera) of form classes (see for example [**3**, Chapter 4], [**5**, Chapter 1]). The theory of genera was Gauss' major contribution to the study of binary quadratic forms. Two forms $ax^2 + bxy + cy^2$ and $a'x^2 + b'xy + c'y^2$ are said to be equivalent if there exist integers r, s, t, u with $ru - st = 1$ such that

$$ax^2 + bxy + cy^2 = a'(rx + sy)^2 + b'(rx + sy)(tx + uy) + c'(tx + uy)^2.$$

Equivalent forms have the same discriminant. It is a classical result that the set of equivalence classes (called form classes) for a given discriminant is finite. It is clear that forms in the same class represent the same integers and hence represent the same primes. Gauss partitioned the set of form classes for a given discriminant into genera in such a way that the primes represented by the forms in the form classes in each genus could be characterized by means of congruences. Two form classes with representatives $f_1(x, y)$ and $f_2(x, y)$ are in the same genus if and only if $f_1(x,y)$ and $f_2(x, y)$ are equivalent modulo m for all nonzero integers m, that is, there are integers r, s, t, u (depending on f_1, f_2 and m) with $\mathrm{GCD}(ru - st, m) = 1$ such that

$$f_1(x, y) \equiv f_2(rx + sy, tx + uy) \pmod{m}$$

for all x and y. For those discriminants possessing only one form class per genus Gauss could therefore say which forms represented which primes. Euler knew of discriminants with this property. It is known that there are only finitely many such discriminants with $D < 0$. An example of such a discriminant is $D = -24$. There are 2 form classes with representatives $x^2 + 6y^2$ and $2x^2 + 3y^2$. Each form class belongs to a different genus, and by Gauss' theory of genera we can deduce: if p is a prime $\neq 2, 3$ we have

$$p = x^2 + 6y^2 \quad \text{if and only if } p \equiv 1, 7 \pmod{24}$$

and

$$p = 2x^2 + 3y^2 \quad \text{if and only if } p \equiv 5, 11 \pmod{24}.$$

In this article we are concerned with the other situation where there are at least 2 form classes in the same genus. This occurs for example when $D = -56$. Here there are 4 form classes but only 2 genera. The classes of the forms $x^2 + 14y^2$ and $2x^2 + 7y^2$ belong to the same genus, and Gauss' theory of genera tells us only that

for primes $p \neq 2, 7$ we have

$$p = x^2 + 14y^2 \text{ or } 2x^2 + 7y^2 \quad \text{if and only if } p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$

[**4**, p.2].

Proof of Theorem. If positive integers $s, a_1, \ldots, a_s, m$ exist for which (2) holds, then m may be taken to be even, since for m odd the congruence $p \equiv a_i \pmod{m}$ is equivalent to $p \equiv b_i \pmod{2m}$, where $b_i = a_i$, if a_i is odd, $b_i = a_i + m$, if a_i is even, as p is odd.

We prove the theorem by showing that any arithmetic progression $A(a, m) = \{a + km: k = 0, 1, 2, \ldots\}$, where $m \equiv 0 \pmod{2}$ and $\mathrm{GCD}(a, m) = 1$, either contains no primes of the form $x^2 + 14y^2$ or it contains primes of both forms $x^2 + 14y^2$ and $2x^2 + 7y^2$.

Suppose that $A(a, m)$ contains a prime p of the form $x^2 + 14y^2$. As the two forms $x^2 + 14y^2$ and $2x^2 + 7y^2$ are in the same genus of discriminant -56, they are equivalent modulo every positive integer and thus in particular equivalent modulo m. Hence there exist integers r, s, t, u such that

$$p = x^2 + 14y^2 \equiv 2(rx + sy)^2 + 7(tx + uy)^2 \pmod{m},$$

where $\mathrm{GCD}(ru - st, m) = 1$ [**5**, Theorem 3.21] [**8**, §12.5]. Let X and Y be integral variables and let $Q(X, Y)$ be the quadratic function

$$Q(X, Y) = 2m^2X^2 + 7m^2Y^2 + 4mAX + 14mBY + (2A^2 + 7B^2),$$

where

$$A = rx + sy, \quad B = tx + uy.$$

Clearly we have

$$\begin{aligned} Q(X, Y) &= 2(A + mX)^2 + 7(B + mY)^2 \\ &\equiv 2A^2 + 7B^2 \pmod{m} \\ &\equiv a \pmod{m}. \end{aligned}$$

It is easily checked that $Q(X, Y)$ is primitive, irreducible, represents arbitrarily large odd integers as m is even, and depends genuinely on the two variables X and Y. By Iwaniec's theorem [**9**] $Q(X, Y)$ represents infinitely many primes. Choosing X and Y so that $Q(X, Y) = q$ is prime, we see that $A(a, m)$ contains a prime of the form $2x^2 + 7y^2$. ∎

We have shown that every such arithmetic progression either contains no primes of the form $x^2 + 14y^2$ or it contains primes of both forms $x^2 + 14y^2$ and $2x^2 + 7y^2$. Thus congruences cannot be used to distinguish the representability of a prime by $x^2 + 14y^2$ from that by $2x^2 + 7y^2$.

REFERENCES

1. W. W. Adams and L. J. Goldstein, *Introduction to Number Theory*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1976.
2. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.
3. D. A. Buell, *Binary Quadratic Forms*, Springer-Verlag, New York, 1989.
4. Harvey Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag, New York, Heidelberg and Berlin, 1978.
5. David A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, New York, 1989.

6. H. Davenport, *The Higher Arithmetic*, Hutchinson University Library, London, 1962.
7. P. G. L. Dirichlet, *Werke*, Berlin, 1889–1897. (Reprint by Chelsea Publishing Co., New York, 1969.)
8. Hua Loo Keng, *Introduction to Number Theory*, Springer-Verlag, Berlin, Heidelberg, and New York, 1982.
9. H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, *Acta Arith.* 24 (1974), 435–459.
10. H. Weber, *Beweis des Satzes, daß jede eigentlich primitive quadratische Form un endliche viele Primzahlen darzustellen fähig ist*, Math. Annalen 20 (1882), 301–329.

Department of Mathematics
Okanagan College
Kelowna, B.C.

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario

Another Proof of the Fundamental Theorem of Algebra

JOSEPH BENNISH
Department of Mathematics,
California State University, Long Beach,
Long Beach, CA 90840

The fundamental theorem can be stated in the following manner: every polynomial $P(z)$ of positive degree having complex coefficients is a surjective map from $\mathbf{C}$ to $\mathbf{C}$. The proof involves examining the boundary of the image of $\mathbf{C}$ under P. First, note that the image is closed. One way this can be seen is by extending P continuously to the Riemann sphere, and noting that the continuous image of a compact set is compact. Identifying $\mathbf{C}$ with $\mathbf{R}^2$, the Jacobian of $P(z)$ is non-singular precisely when $P'(z) \neq 0$. The inverse function theorem implies that $P(z)$ is a homeomorphism in a neighborhood of z whenever $P'(z) \neq 0$. Thus, if w is in the boundary of $P(\mathbf{C})$, then $w = P(z)$ and $P'(z) = 0$ for some z in $\mathbf{C}$. However, the number of zeroes of $P'(z)$ is at most the degree of P'. This shows that $P(\mathbf{C})$ has non-empty interior, and that its boundary consists of at most finitely many points. But the boundary of a proper subset of $\mathbf{R}^2$ with non-empty interior cannot consist of only a finite set of points.