Journal of Number Theory 129 (2009) 464–468

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Five peculiar theorems on simultaneous representation of primes by quadratic forms

David Brink

Institut for Matematiske Fag, Københavns Universitet, DK-2100, Denmark

ARTICLE INFO

Article history:
Received 17 January 2008
Available online 12 August 2008
Communicated by M. Pohst

Keywords:
Prime representation
Quadratic form
Ring class field
Genus field
Ambiguous class
Rédei–Reichardt theorem
Convenient number

ABSTRACT

Text. It is a theorem of Kaplansky that a prime $p \equiv 1 \pmod{16}$ is representable by both or none of $x^2 + 32y^2$ and $x^2 + 64y^2$, whereas a prime $p \equiv 9 \pmod{16}$ is representable by exactly one of these binary quadratic forms. In this paper five similar theorems are proved. As an example, one theorem states that a prime $p \equiv 1 \pmod{20}$ is representable by both or none of $x^2 + 20y^2$ and $x^2 + 100y^2$, whereas a prime $p \equiv 9 \pmod{20}$ is representable by exactly one of these forms. A heuristic argument is given why there are no other results of the same kind. This argument relies on the (plausible) conjecture that there are exactly 485 negative discriminants Δ such that the class group $\mathscr{C}(\Delta)$ has exponent 4.

Video. For a video summary of this paper, please visit http://www.youtube.com/watch?v=l_yRq0oqKx4.

Consider a negative integer $\Delta \equiv 0, 1 \pmod 4$ and recall that the principal (binary, quadratic) form $F(x, y)$ of discriminant Δ is $x^2 - \frac{\Delta}{4}y^2$ or $x^2 + xy - \frac{\Delta-1}{4}y^2$ according to Δ's parity. It is well known that the prime numbers representable by $F(x, y)$ are describable by congruence conditions if and only if each genus of forms of discriminant Δ consists of a single class, or—equivalently—the class group $\mathscr{C}(\Delta)$ is either trivial or has exponent 2 (see e.g. [2, p. 62]).

The determination of the negative discriminants with one class per genus is a famous problem in number theory. Gauss, who considered only forms of type $ax^2 + 2bxy + cy^2$, found 65 such discriminants $-4n$ and showed that they correspond to Euler's *idoneal* or *convenient* numbers n. Dickson [3] compiled a similar list containing in addition 36 odd discriminants, and it is highly plausible that this list of 101 discriminants is complete. It is a strange coincidence that the number of fundamental discriminants on Dickson's list is also 65.

E-mail address: brink@math.ku.dk.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.04.007

As an example, the primes represented by $x^2 + 2^n y^2$ are describable by congruence conditions for $n = 0, 1, 2, 3, 4$ (by classical results of Fermat), but not for any $n > 4$. In light of this, the following theorem of Kaplansky [7] is surprising:

Theorem 0. *A prime $p \equiv 1 \pmod{16}$ is representable by both or none of $x^2 + 32y^2$ and $x^2 + 64y^2$, whereas a prime $p \equiv 9 \pmod{16}$ is representable by exactly one of these forms.*

In this paper we show that Kaplansky's theorem is only one member of a small family of results on congruence conditions for the simultaneous representation of primes by two principal forms:

Theorem 1. *A prime $p \equiv 1 \pmod{20}$ is representable by both or none of $x^2 + 20y^2$ and $x^2 + 100y^2$, whereas a prime $p \equiv 9 \pmod{20}$ is representable by exactly one of these forms.*

Theorem 2. *A prime $p \equiv 1, 16, 22 \pmod{39}$ is representable by both or none of $x^2 + xy + 10y^2$ and $x^2 + xy + 127y^2$, whereas a prime $p \equiv 4, 10, 25 \pmod{39}$ is representable by exactly one of these forms.*

Theorem 3. *A prime $p \equiv 1, 16, 26, 31, 36 \pmod{55}$ is representable by both or none of $x^2 + xy + 14y^2$ and $x^2 + xy + 69y^2$, whereas a prime $p \equiv 4, 9, 14, 34, 49 \pmod{55}$ is representable by exactly one of these forms.*

Theorem 4. *A prime $p \equiv 1, 65, 81 \pmod{112}$ is representable by both or none of $x^2 + 14y^2$ and $x^2 + 448y^2$, whereas a prime $p \equiv 9, 25, 57 \pmod{112}$ is representable by exactly one of these forms.*

Theorem 5. *A prime $p \equiv 1, 169 \pmod{240}$ is representable by both or none of $x^2 + 150y^2$ and $x^2 + 960y^2$, whereas a prime $p \equiv 49, 121 \pmod{240}$ is representable by exactly one of these forms.*

After the proofs we give a heuristic argument why these six theorems are the only results of their kind. For example, we prove that there are no similar relations between the primes represented by $x^2 + 128y^2$ and $x^2 + 256y^2$.

It should be noted that none of the forms appearing in the above theorems have discriminants with one class per genus. Nevertheless, there are simple criteria characterising the primes represented by three of these forms individually: $p = x^2 + 32y^2$ if and only if -4 is an 8th power modulo p (Barrucand and Cohn [1]), $p = x^2 + 64y^2$ if and only if 2 is a 4th power modulo p (Gauss, see e.g. [2]), and $p = x^2 + 100y^2$ if and only if 5 is a 4th power modulo p (Hasse [6, p. 69]).

Proof of the theorems. We start by reviewing some general facts about quadratic forms and ring class fields and refer once and for all the reader to [2]. Consider a negative discriminant Δ with class group $\mathscr{C}$. Write $\Delta = d_K f^2$ where d_K is fundamental and let K be the imaginary quadratic field of discriminant d_K. The ring class field N of discriminant Δ is a field extension of K with Galois group $\mathrm{Gal}(N/K)$ canonically isomorphic to $\mathscr{C}$ via the Artin symbol. Moreover, N is (generalised) dihedral over $\mathbb{Q}$:

$$\mathrm{Gal}(N/\mathbb{Q}) \cong \mathscr{C} \rtimes \mathbb{Z}/2,$$

meaning that the non-trivial element in $\mathbb{Z}/2$ acts on $\mathscr{C}$ by inversion. For a prime p with $p \nmid \Delta$, it is a fundamental result that p is representable by the principal form of discriminant Δ if and only if p splits in N [2, p. 181].

The genus field Γ of discriminant Δ is the subextension of N/K corresponding to the subgroup of squares in $\mathscr{C}$ via Galois theory and Artin symbol. It is the maximal elementary abelian 2-extension of K (or $\mathbb{Q}$) contained in N. Γ is obtained by adjoining to $\mathbb{Q}$ the square roots of what one could call the *assigned discriminants* of Δ. These are the prime discriminants q_i such that the *assigned characters* of Δ are the Kronecker symbols $(q_i/\ )$. Their number is conventionally denoted μ, and the degree of Γ thus equals 2^μ.