A RESULT CONCERNING INTEGRAL BINARY QUADRATIC FORMS

WILLIAM EDWARD CHRISTILLES

This paper contains an extension of an earlier work by Dickson ([1], p. 95), in which the following theorem was proven:

THEOREM 1. (Dickson's Theorem). *If a number is represented properly by a form* $[a, b, c]$ *of discriminant* $D = 4ac - b^2$, *then any divisor of that number is represented by some form of the same discriminant* D.

DEFINITION. ([1], p. 68). A positive form $[a, b, c]$ is called reduced if $-a < b \leqq a$, $c \geqq a$, with $b \geqq 0$ if $c = a$.

As a consequence of the above definition it follows that $4a^2 \leqq 4ac = D + b^2 \leqq D + a^2$, $3a^2 \leqq D$, and finally $a \leqq \sqrt{(1/3)\,D}$

THEOREM 2. *Let* M *be properly represented by the integral positve definite quadratic form* $a\alpha^2 + b\alpha\gamma + c\gamma^2$ *of discriminant* $D = 4ac - b^2$. *If* $M \leqq 3D/16$ *and* $(D, M) = 1$, *then in every factorization of* M *one of the factors is* a_i, *one of the minimal values of a primitive quadratic form of discriminant* D. *In other words,* $M = M_1M_2$ *where* M_1 *is a unit or a prime and* M_2 *is the product of no more than two* a_i.

Proof. According to the remark following the definition $a_i \leqq \sqrt{D/3}$, where equality for a primitive reduced form is possible only if $a_i = b_i = c_i = 1$ and hence $D = 3$ so that the inequality $0 < M \leqq 3D/16$ cannot be satisfied. Thus $a_i < \sqrt{D/3}$.

Now assume $M = r_1r_2$. Then according to Theorm 1 it follows that

$$r_1 = a_i\alpha_i^2 + b_i\alpha_i\gamma_i + c_i\gamma_i^2\,, \quad r_2 = a_j\alpha_j^2 + b_j\alpha_j\gamma_j + c_j\gamma_j^2$$

where the two quadratic forms are primitive reduced forms of discriminant D. Hence

$$\begin{aligned}(4a_ir_1)(4a_jr_2) &= [(2a_i\alpha_i + b_i\gamma_i)^2 + D\gamma_i^2]\,[(2a_j\alpha_j + b_j\gamma_j)^2 + D\gamma_j^2] \\ &= (\beta_i^2 + D\gamma_i^2)(\beta_j^2 + D\gamma_j^2) = 16a_ia_jM \\ &< 16(D/3)M \leqq (16D/3)(3D/16) = D^2\,,\end{aligned}$$

where $\beta_i = (2a_i\alpha_i + b_i\gamma_i)$ and $\beta_j = (2a_j\alpha_j + b_j\gamma_j)$. This implies that $\gamma_i\gamma_j = 0$, say $\gamma_i = 0$, and therefore $r_1 = a_i$.

To prove the final statement of the theorem, assume $M \neq a_i$ and

Received November 21, 1963. The author is indebted to the referee for the suggested revision of both the statement and the proof of Theorem 2.

let r_2 be a minimal factor of M so that $r_2 \neq a_j$. If M_1 is any prime factor of r_2, then $M = M_1 M_2$ where $M_2 = (M/r_2)(r_2/M_1) = a_i a_j$.

Reference

1. L. E. Dickson, *Introduction to the Theory of Numbers*, Dover Publications, Inc., New York, 1929.

St. Mary's University, San Antonio, Texas