ON THE DISTRIBUTION OF INTEGER SOLUTIONS OF $f(x, y) = z^2$ FOR A DEFINITE BINARY QUADRATIC FORM f

Nobuo Nobusawa

Let f be a positive definite binary quadratic form with rational coefficients. We shall call a point (x, y) in E^2 with integers x and y a Pythagorean point of f when $f(x, y) = z^2$ is satisfied with some integer z, and shall prove the following theorem.

THEOREM. Inside a region in E^2 bounded by two parallel lines one of which passes through the origin and a Pythagorean point of f, there are at most a finite number of Pythagorean points.

First of all, we shall reduce the general form to a simple one. It is well known that by a linear transformation $x' = a_{11}x + a_{12}y$ and $y' = a_{21}x + a_{22}y$ a form $f(x, y)$ can be changed to a form $F(x', y') = rx'^2 + sy'^2$ with positive rational numbers r and s. Here we may assume that all a_{ij} are integers. Then a Pythagorean point of f is changed to a Pythagorean point of F. We also note that the region stated in Theorem is changed to a region of the same type. Here r and s are not necessarily integers. In that case, we multiply F by t^2 where t is a suitable integer such that t^2F has integer coefficients. A Pythagorean point of F is naturally a Pythagorean point of t^2F. Thus, it is sufficient to prove the theorem under the assumption $f(x, y) = rx^2 + sy^2$ where r and s are positive integers. Then consider a linear transformation $X = r^{1/2}x$ and $Y = s^{1/2}y$. $f(x, y)$ is changed to a form $X^2 + Y^2$. A Pythagorean point (x, y) of f is changed to a point $(r^{1/2}x, s^{1/2}y)$ in the X-Y plane, the distance from which to the origin is an integer. So, we consider such points.

https://doi.org/10.4153/CMB-1967-082-0 Published online by Cambridge University Press

LEMMA. Let a, b, c and d be real numbers and put $\ell = (a^2 + b^2)^{1/2}$, $m = (c^2 + d^2)^{1/2}$, $A = ac + bd$ and $B = ad - bc$. If ℓ, m and A are integers and $B \neq 0$, then $B^2 \geq 2\ell m - 1$.

Proof. From $(\ell m)^2 = A^2 + B^2$ and $B \neq 0$, it follows that $A^2 < (\ell m)^2$. Now suppose $B^2 < 2\ell m - 1$. Then $A^2 = (\ell m)^2 - B^2 > (\ell m - 1)^2$, which is impossible since A is an integer.

PROPOSITION. Let (a, b) and (c, d) be two points such that all assumptions in Lemma are satisfied. Denote by D the distance from (c, d) to a line passing through the origin and (a, b). Then $D^2 \geq 2m/\ell - 1/\ell^2$.

Proof. Clearly $D = |B|/\ell$. Hence, by Lemma, we have the result immediately.

The proof of Theorem is now almost clear. We take $(r^{1/2}x_1, s^{1/2}y_1)$ and $(r^{1/2}x_2, s^{1/2}y_2)$ for (a, b) and (c, d) where (x_1, y_1) and (x_2, y_2) are two Pythagorean points not lying on the same line passing through the origin. Then by Proposition $m \leq \ell(D^2 + 1/\ell^2)/2$, which implies m cannot be big if we restrict the distance D and fix ℓ. This proves Theorem.

Lastly, there are some questions arising from what we have discussed. In Theorem, we assumed that a line passes through a Pythagorean point. What can we say if we drop this condition? We also assumed f is definite. Can we discuss the problem without this condition? Is it possible to generalize the result to a case of a quadratic form with more than two variables?

University of Calgary and
University of Rhode Island