ON INDEFINITE BINARY QUADRATIC FORMS

BY

A. OPPENHEIM

University of Malaya, Singapore, Malaya

1. If

$$Q(x, y) = a x^2 + b x y + c y^2 = [a, b, c] \tag{1}$$

is an indefinite binary quadratic form with real coefficients in integral variables x, y, not both zero, it is well known that M, the lower bound of $|Q(x, y)|$ (usually called the minimum) satisfies the inequality

$$M \leq D/5^{\frac{1}{2}} \tag{2}$$

where D^2 is the discriminant of Q,

$$D^2 = b^2 - 4 a c > 0, \quad D > 0. \tag{3}$$

If equality holds in (2) then Q must be equivalent to a multiple of the form $[1, 1, -1]$.

This is part of a famous theorem due to Markoff [4], a considerably simplified proof of which has lately been given by Cassels [2].

Put briefly, Markoff's theorem states that

$$\overline{\lim}\ M/D = \tfrac{1}{3} \tag{4}$$

if we consider all classes of forms with discriminant D^2, and that any form Q with $3M(Q) > D$ is equivalent to a multiple of one of a denumerable set of forms, the Markoff forms, of which the first is $[1, 1, -1]$, the second $[1, 2, -1]$, the third $[5, 11, -5]$.

Recently Barnes [1] has discussed the problem of obtaining corresponding bounds for the product

$$Q(x, y)\, Q(u, v) \tag{5}$$

over integers x, y, u, v such that

$$x v - y u = \pm 1 \tag{6}$$

and gave complete results, both for asymmetric and for one-sided inequalities, which are analogous to those of Markoff.

To illustrate I quote the following theorem on non-zero forms.

Theorem (Barnes). (i) *If Q is not equivalent to a multiple of any of the forms h_1 or f_n $(n = 1, 3, 5, \ldots)$, then there exist integers x, y, u, v satisfying* (6) *for which*

$$-\frac{D^2}{2\sqrt{5}+2} \leq Q(x, y)\, Q(u, v) < 0. \tag{7}$$

(iii) *For any $\varepsilon > 0$ there exists a set of forms Q, none of which is equivalent to a multiple of any other, for which every negative value of the product $Q(x, y)\, Q(u, v)$ satisfies*

$$Q(x, y)\, Q(u, v) < -D^2\left(\frac{1}{2\sqrt{5}+2} - \varepsilon\right), \tag{8}$$

and this set has the cardinal number of the continuum.

(I use D^2 where Barnes uses D. I have omitted (ii).)

It is curious that in a paper [5] of which Barnes was unaware, (i), (ii) and part of (iii) (but not the other theorems obtained by Barnes) had been anticipated. In some respect even more was proved. Thus *if we exclude multiples of the forms h_1, f_n $(n = 1, 3, 5, \ldots)$* my results implied that *integers x, y, u, v exist satisfying* (6) *and such that simultaneously we have both* (7) *and*

$$D\left|\frac{1}{Q(x, y)} - \frac{1}{Q(u, v)}\right| > 3 + \sqrt{5} \tag{9}$$

and a third inequality, which it is easier to express in terms of continued fractions or in terms of the coefficients of reduced forms.

The indefinite binary quadratic form

$$\Phi(x, y) = \alpha x^2 + \beta x y + \gamma y^2 \tag{10}$$

is said to be reduced if

$$\alpha\gamma < 0, \quad \beta > |\alpha + \gamma|. \tag{11}$$

It is well known that Q is equivalent to any member of a chain of such reduced forms. Barnes's theorem amounts to this: *exclude multiples of the forms h_1, f_n, then there is a reduced form $\Phi \sim Q$ and such that*

$$0<|\alpha\gamma|<\frac{D^2}{2\sqrt{5}+2}. \tag{12}$$

My results showed that *the inequalities*

$$\frac{1}{|\alpha|}+\frac{1}{|\gamma|}>\frac{3+\sqrt{5}}{D} \tag{13}$$

and

$$D-\beta<(2\sqrt{5}-4)(|\alpha|+|\gamma|) \tag{14}$$

can also be satisfied at the same time as (12).

2. In this note I consider a problem of apparently the same order of difficulty. Let

$$L=\min\{\max(|Q(x, y)|,\ |Q(u, v)|)\} \tag{15}$$

for integers subject to (6), or, what is the same thing, let

$$L=\min\{\max(|a|,\ |c|)\} \tag{16}$$

for all forms $[a, b, c]$ equivalent, properly or improperly, to Q. What are the results for L which correspond to those for $\min|a|$ and for $\min|ac|$?

It is surprising to find that the results for L contrast sharply with those for M or for $\min|ac|$ in that there is but one minimum and that not isolated. In addition the proof is very simple.

My results are contained in the theorems which follow.

Theorem 1. *If $Q(x, y)$ is a zero form then*

$$L\leq\tfrac{1}{2}D \tag{17}$$

with equality if and only if

$$Q\sim\tfrac{1}{2}D(2xy+y^2)\sim\tfrac{1}{2}D(x^2-y^2). \tag{18}$$

Theorem 2. (i) *If Q is not a zero form then necessarily*

$$L<\tfrac{1}{2}D. \tag{19}$$

(ii) *For every $\varepsilon>0$ there exists a form which is a multiple of an integral form such that*

$$\tfrac{1}{2}D-\varepsilon<L<\tfrac{1}{2}\mathrm{D}. \tag{20}$$

In place of Theorem 2 (ii) it can be shown that *the set of non-equivalent forms of discriminant D^2 such that* (20) *holds has the cardinal number of the continuum.*

3. *Proof of Theorem 1.* If $Q(p, q) = 0$ for coprime integers p and q, the unimodular transformation

$$x = p X + r Y, \quad y = q X + s Y$$

where $p s - q r = \pm 1$ carries Q into an equivalent form

$$\beta X Y + \gamma Y^2 \sim D(x y + \theta y^2)$$

where $0 \leq |\theta| \leq \frac{1}{2}$. For this form it is plain that

$$L(Q) \leq |\theta| D \leq \tfrac{1}{2} D$$

and that equality implies $\theta = \pm \frac{1}{2}$.

For the form $2 x y \pm y^2 \sim x^2 - y^2$ it is clear that

$$L = 1, \ D = 2.$$

Theorem 1 is proved.

4. *Proof of Theorem 2.* We use a simple Lemma on reduced forms which do not represent zero.

Lemma 1. *Suppose that*

$$\Phi = [\alpha, \beta, -\gamma], \quad \beta^2 + 4 \alpha \gamma = D^2,$$

is reduced with

$$\alpha > 0, \quad \gamma > 0, \quad \beta > |\gamma - \alpha|. \tag{21}$$

Then

$$\min(\gamma, \alpha + \beta - \gamma) < \tfrac{1}{2} D, \tag{22}$$

$$\min(\alpha, \gamma + \beta - \alpha) < \tfrac{1}{2} D. \tag{23}$$

Note that

$$(\alpha - \gamma)^2 + 4 \alpha \gamma < \beta^2 + 4 \alpha \gamma = D^2, \quad \alpha + \gamma < D.$$

If

$$\gamma \geq \tfrac{1}{2} D, \quad \alpha + \beta - \gamma \geq \tfrac{1}{2} D,$$

then

$$\beta \geq \tfrac{1}{2} D + \gamma - \alpha \geq D - \alpha > 0,$$

$$D^2 - 2 D \alpha \geq D^2 - 4 \alpha \gamma = \beta^2 \geq (D - \alpha)^2, \quad 0 \geq \alpha^2,$$

a contradiction.

This proves (22). And (23) follows by applying (22) to the reduced form

$$[\gamma, \beta, -\alpha] \sim -\Phi.$$

Now by (21) we have

$$\min(\alpha, \gamma) < \tfrac{1}{2} D. \quad \beta \pm \gamma \mp \alpha > 0. \tag{24}$$

It follows therefore that one at least of the three forms

$$\begin{gathered} \Phi(x, y) = [\alpha, \beta, \gamma], \quad \Phi(x+y, y) = [\alpha, 2\alpha+\beta, \alpha+\beta-\gamma], \\ \Phi(x, -x+y) = [\alpha-\beta-\gamma, \beta+2\gamma, -\gamma] \end{gathered} \tag{25}$$

is such that each of its extreme coefficients is numerically less than $\frac{1}{2} D$. Hence for *infinitely many integers* x, y, u, v such that $xv - yu = \pm 1$ we have

$$\max(|Q(x, y)|, \quad |Q(u, v)|) < \tfrac{1}{2} D \tag{26}$$

since Q is equivalent to infinitely many reduced forms.

It can also be shown that if $[a, b, c]$ is such that $|a| < \frac{1}{2} D$, $|c| < \frac{1}{2} D$, then $[a, b, c]$ is either a reduced form or derivable from a reduced form in the manner indicated above.

5. *Proof of Theorem 2* (ii). Let $g \geq 1$ be any positive integer and consider the chain of reduced indefinite binary quadratic forms with period

$$\begin{gathered} \Phi = \Phi_0 = [2, 2g, -g-1], \quad \Phi_1 = [-g-1, 2, g+1], \quad \Phi_2 = [g+1, 2g, -2], \\ \Phi_3 = [-2, 2g, g+1], \quad \Phi_4 = [g+1, 2, -g-1], \quad \Phi_5 = [-g-1, 2g, 2] \end{gathered} \tag{27}$$

and discriminant

$$D^2 = 4(h^2+1), \quad h = g+1. \tag{28}$$

Lemma 2. *For this class of integral forms we have*

$$L = g+1 = h, \quad 2L/D = h/(h^2+1)^{\frac{1}{2}}.$$

By a theorem of Lagrange (see Dickson [3]), any number a properly represented by Φ and such that $|a| \leq \frac{1}{2} D$ must be the leading coefficient of some form in the chain determined by Φ.

Now $[\frac{1}{2} D] = h$ and Φ is an integral form. It follows by inspection of the period for Φ that the only integers numerically less than or equal to h which are properly represented by Φ must be 2 and h. It follows therefore that

$$L = 2 \quad \text{or} \quad L = h.$$

If however $L = 2$ then necessarily

$$\Phi \sim 2x^2 + 2bxy \pm 2y^2$$

where the integer b is such that

$$b^2 \mp 4 = h^2 + 1,$$

$$b^2 - h^2 = 5, \quad b = \pm 3, \ h = 2,$$

$$h^2 - b^2 = 3, \quad b = \pm 1, \ h = 2.$$

In all cases therefore $L = h \geq 2$. The second part of Theorem 1 follows from Lemma 2.

6. The proof in the last section can be modified to show that the set of non-equivalent forms of discriminant D^2 such that

$$\tfrac{1}{2} D (1 - \varepsilon) < L < \tfrac{1}{2} D \tag{29}$$

has the cardinal number of the continuum, ε being any assigned positive number.

For this purpose I constructed a chain of equivalent reduced forms

$$\Phi_i = [(-1)^i \alpha_i, \beta_i, (-1)^{i+1} \alpha_{i+1}] \qquad (-\infty < i < \infty) \tag{30}$$

such that each form fell into one of two categories.

Dr. Barnes however has pointed out to me that one of these categories can be avoided and I use therefore Dr. Barnes's simpler example.

Each form Φ_i is assumed to have the property **A**:

A

$$0 < \min (\alpha_i, \alpha_{i+1}) < \varepsilon D,$$

$$\tfrac{1}{2} D (1 - \varepsilon) < \max (\alpha_i, \alpha_{i+1}) < \tfrac{1}{2} D (1 + \varepsilon),$$

and, in consequence,

$$D (1 - \varepsilon') < \beta_i < D.$$

Herein ε is an assigned small enough positive number and ε' is a small positive number which depends on ε.

Lemma 3. *A class of forms whose reduced forms satisfy* **A** *must be such that*

$$\tfrac{1}{2} D (1 - \varepsilon) \leq L < \tfrac{1}{2} D.$$

If this is not the case then there exists a form in the class

$$Q = [a, b, c] \tag{31}$$

such that

$$|a| < \tfrac{1}{2} D (1 - \varepsilon), \quad |c| < \tfrac{1}{2} D (1 - \varepsilon). \tag{32}$$

Now by the theorem of Lagrange already quoted, if Q represents a number t such that $|t| \leq \frac{1}{2} D$, there must be a reduced form in the chain determined by Q which has t for its leading coefficient. Since the reduced forms all satisfy **A**, it follows that (32) can be replaced by the stronger inequality

$$|a| < \varepsilon D, \quad |c| < \varepsilon D. \tag{33}$$

Now we saw that one of the forms

$$Q_1 = Q(x, y), \quad Q_2 = Q(x \pm y, y), \quad Q_3 = Q(x, \pm x + y)$$

must be reduced since Q_1 is such that $|a| < \frac{1}{2} D$, $|c| < \frac{1}{2} D$. But Q_1 plainly does not satisfy **A**: Q_2 is such that the coefficient of y^2 is numerically at least

$$|b| - |a| - |c| > (D^2 - 4\varepsilon^2 D^2)^{\frac{1}{2}} - 2\varepsilon D > D(1 - 3\varepsilon)$$

if ε is small enough, so that Q_2 does not satisfy **A**. So too for Q_3.

The contradiction proves Lemma 3.

7. It remains to construct a chain (Φ_i) with the properties stated. Take a sequence of positive integers

$$(g_i) \qquad (-\infty < i < \infty) \tag{34}$$

such that

$$g_i = 2 \ (i \text{ even}), \quad g_i \geq N \ (i \text{ odd}) \tag{35}$$

where N is an appropriately chosen large positive integer.

Let

$$F_i = [g_i, g_{i+1}, \ldots], \quad H_i = [g_{i-1}, g_{i-2}, \ldots]. \tag{36}$$

Then the forms Φ_i defined by

$$\frac{\alpha_i}{F_i} = \frac{\beta_i}{F_i H_i - 1} = \frac{\alpha_{i+1}}{H_i} = \frac{D}{F_i H_i + 1} \tag{37}$$

constitute a chain of reduced forms with discriminant D^2.

Now, for i even,

$$2 < F_i < 2 + \frac{1}{N}, \quad H_i > N, \tag{38}$$

so that

$$0 < \alpha_i < \frac{D}{N}, \quad \tfrac{1}{2}\left(1 - \frac{1}{N}\right) D < \alpha_{i+1} < \tfrac{1}{2} D. \tag{39}$$

4 – 533807. *Acta Mathematica*. 91. Imprimé le 15 mai 1954.

It follows that the chain (Φ_i) satisfies **A** if

$$N > \frac{1}{\varepsilon}. \tag{40}$$

Since the set of sequences (g_i) so constructed has the cardinal number of the continuum and since each sequence gives rise to at most two classes of forms, the result stated at the beginning of this section is proved.

In place of the sequence (35) given me by Dr. Barnes, we can use the sequence

$$g_i = 1 \ (i \equiv 1, 2), \quad g_i \geq N \ (i \equiv 0),$$

the congruences being modulo 3. But the details are not so simple.

References

[1]. E. S. Barnes, The minimum of the product of two values of a quadratic form, I, II, II, *Proc. London Math. Soc.*, (3), 1 (1951), 257–283, 385–414, 415–434.

[2]. J. W. S. Cassels, The Markoff Chain, *Annals of Math.*, (2), 50 (1949), 676–685.

[3]. L. E. Dickson, Introduction to the Theory of Numbers, Chicago (1929).

[4]. A. Markoff, Sur les formes quadratiques binaires indéfinies, *Math. Annalen.* 15 (1879), 381–400; 17 (1880), 379–399.

[5]. A. Oppenheim, The continued fractions associated with chains of quadratic forms, *Proc. London Math., Soc.*, (2), 44 (1938), 323–335.