A NEW PROOF OF MINKOWSKI'S THEOREM ON THE PRODUCT OF TWO LINEAR FORMS

BY R. Q. SEALE

Remak,* Mordell,† Landau,‡ and Blichfeldt§ have all proved the theorem, first proved by Minkowski‖ (1901):

If $\alpha, \beta, \gamma, \delta, \xi_0, \eta_0$ *are real and* $\alpha\delta - \beta\gamma = 1$, *integers* x, y *always exist such that*

$$\left| (\alpha x + \beta y - \xi_0)(\gamma x + \delta y - \eta_0) \right| \leqq \frac{1}{4}.$$

This theorem includes as a special case, the classical theorem of Tchebychef¶ (1866):

If a *is irrational and* b *is real, an infinite number of pairs of integers* x, y $(y > 0)$ *always exist such that* $\left|(x - ay - b)\right|$ *can be made arbitrarily small, and at the same time*

$$\left| x - ay - b \right| < \frac{2}{y}.$$

In what follows, by making use of no principles more advanced than the elementary properties of convergents, I have proved three theorems, the first one being the Tchebychef theorem stated above. The second is Minkowski's theorem on the product of two homogeneous forms, while the third is the Minkowski theorem stated above. I feel that, although Tchebychef's theorem is a special case of Minkowski's theorem, its

---

* Bachmann, *Die Arithmetik der Quadratischen Formen*, Zweite Abteilung, p. 66; or Remak, Journal für die reine und angewandte Mathematik, vol. 142, p. 278.

† Mordell, Journal of the London Mathematical Society, vol. 3 (1928), p. 19.

‡ Landau, Journal für die reine und angewandte Mathematik, vol. 165 (1931), p. 1.

§ Published in a syllabus which Professor Blichfeldt distributed to a class in geometry of numbers at Stanford University, winter and spring quarters, 1932.

‖ Minkowski, *Diophantische Approximationen*, pp. 42–45.

¶ Œuvres de Tchebychef, vol. 1, p. 637.

proof should be included in this paper because it so completely illustrates the simplicity of the methods I have used.

Professor Blichfeldt, in his proof, shows that if the ratio α/β is irrational, the form $|(\alpha x+\beta y-\xi_0)|$ can be made arbitrarily small at the same time that Minkowski's theorem is satisfied. This is not shown in any of the other proofs I have read, although it follows from the method Minkowski used in his proof.

THEOREM 1. *Integers x, y $(y\neq 0)$ always exist such that $|x-\theta y-\omega|$ can be made arbitrarily small, and at the same time*

$$|x-\theta y-\omega|<\frac{1}{4|y|}, \tag{1}$$

where θ is irrational and ω is not an integer.

PROOF. We use the following lemmas.

LEMMA A. *If m and n are relatively prime integers, $nx-my=N$ has a solution in integers x_0, y_0, such that $|y_0|\leqq n/2$.*

LEMMA B. *If $e_1^2=e_2^2=e_3^2=1$, and $a\leqq 1$, $b\leqq 1$, $c\leqq 1$, at least one of the inequalities*

$$|a(e_1e_3ab-e_2c)|\leqq 1, \tag{a}$$

and

$$|(2-a)[e_1e_3(2-a)b+e_2c]|\leqq 1, \tag{b}$$

is true.

To prove this lemma, assume that

$$a(ab+c)>1. \tag{c}$$

This assumption is permissible, since (a) is surely true if (e_1e_3) and e_2 agree in algebraic sign.

Then if (b) is false we must have either

$$(2-a)[c-(2-a)b]>1, \tag{d}$$

or

$$(2-a)[c-(2-a)b]<-1. \tag{e}$$

From (c) we obtain $1\geqq b>(1-ac)/a^2$. If, however, we re-

place b by $(1-ac)/a^2$ in (d), the inequality is certainly not weakened. That is,

$$(2-a)\left[c-(2-a)\frac{1-ac}{a^2}\right]$$
$$=(2-a)\left(\frac{a^2c-2+2ac+a-a^2c}{a^2}\right)$$
$$=(2-a)\left(\frac{-2+2ac+a}{a^2}\right)>1$$

is true. But this reduces to

$$c[(a-1)^2-1]+1+(a-1)^2<0,$$

which is impossible. Hence, (c) and (d) are not both possible.

From (c) we obtain $1\geqq c>(1-a^2b)/a$, and if we replace c by the right-hand side of this inequality, (e) is not weakened. That is,

$$(2-a)\left[\frac{1-a^2b}{a}-(2-a)b\right]=(2-a)\left(\frac{1-a^2b-2ab+a^2b}{a}\right)$$
$$=(2-a)\left(\frac{1-2ab}{a}\right)<-1$$

is true. But this reduces to

$$1-2ab+a^2b=1+[(1-a)^2-1]b<0,$$

which is impossible. The lemma is therefore true.

Now let us define P by means of the equation

$$P=x-\theta y-\omega, \tag{2}$$

then express θ as a continued fraction, and let m/n be *any* convergent to θ. If we write

$$\frac{m}{n}-\theta=\frac{e_1b}{n^2}, \tag{3}$$

we have $b<1$ and $e_1^2=1$.

Define N and k by the equation

$$n\omega=N+k, \tag{4}$$

where N is an integer and $|k| \leqq 1/2$. Say that

$$k = \frac{e_2 c}{2}. \tag{5}$$

Then $e_2^2 = 1$, and $c \leqq 1$.

We can now write

$$\begin{aligned} P &= \frac{nx - my - N}{n} + \left(\frac{m}{n} - \theta\right) y - \frac{k}{n} \\ &= \frac{nx - my - N}{n} + Q. \end{aligned} \tag{6}$$

From (3), (5), and (6), we obtain

$$Q = y\left(\frac{m}{n} - \theta\right) - \frac{k}{n} = \frac{e_1 b y}{n^2} - \frac{e_2 c}{2n}. \tag{7}$$

By Lemma A, $nx - my - N = 0$ has a solution (x_0, y_0), both integers, with $|y_0| \leqq n/2$. Since ω is not an integer, $y_0 \neq 0$. Say that

$$y_0 = \frac{e_3 a n}{2}, \tag{8}$$

where $0 < a \leqq 1$, and $e_3^2 = 1$.

A second solution of $nx - my - N = 0$ will be $x_1 = x_0 - e_3 m$, $y_1 = y_0 - e_3 n$. Then

$$y_1 = y_0 - e_3 n = -\frac{e_3 n}{2}(2 - a). \tag{9}$$

When $x = x_0$, $y = y_0$, $Q = Q_0$, that is, from (7) and (8),

$$\begin{aligned} Q_0 &= y_0\left(\frac{m}{n} - \theta\right) - \frac{k}{n} = \frac{e_3 a n}{2} \cdot \frac{b e_1}{n^2} - \frac{e_2 c}{2n} \\ &= \frac{1}{2n}(e_1 e_3 a b - e_2 c). \end{aligned} \tag{10}$$

Similarly, for $x_1 = x_0 - e_3 m$, $y_1 = y_0 - e_3 n$, we obtain

$$Q_1 = (y_0 - e_3 n)\left(\frac{m}{n} - \theta\right) - \frac{k}{n} = -\frac{e_3 n}{2}(2 - a)\frac{e_1 b}{n^2} - \frac{e_2 c}{2n}$$

(11)

$$= -\frac{1}{2n}[e_1 e_3(2 - a)b + e_2 c].$$

Both (10) and (11) can be made arbitrarily small, numerically, for large enough n, and therefore $|x_0 - \theta y_0 - \omega|$ and $|x_1 - \theta y_1 - \omega|$ can both be made arbitrarily small for large enough n.

The corresponding values of $4y_0Q_0$ and $4y_1Q_1$ are

$$4y_0Q_0 = 4\frac{e_3 an}{2}\cdot\frac{1}{2n}(e_1 e_3 ab - e_2 c) = e_3 a(e_1 e_3 ab - e_2 c), \tag{12}$$

$$4y_1Q_1 = -4\frac{e_3 n}{2}(2 - a)\cdot\frac{-1}{2n}[e_1 e_3(2 - a)b + e_2 c] \tag{13}$$

$$= e_3(2 - a)[e_1 e_3(2 - a)b + e_2 c].$$

By Lemma B at least one of (12) and (13) is less than or equal 1, numerically. But θ is irrational; hence b in (3) is neither 0 nor 1. Therefore (a) or (b) of Lemma B must be less than 1, and the theorem is completely proved.

THEOREM 2. *There exist two relatively prime integers m, n such that*

$$|(\alpha m + \beta n)(\gamma m + \delta n)| < 1, \tag{14}$$

if $\alpha\delta - \beta\gamma = 1$. If α/β is irrational, infinitely many such pairs exist and $|\alpha m + \beta n|$ can be made arbitrarily small and at the same time $|\gamma m + \delta n|$ can be made arbitrarily large.

PROOF. We consider two cases.

CASE 1. α/β is rational. Then $\beta/\alpha = -(m/n)$, where m and n are relatively prime integers. Hence

$$\alpha m + \beta n = 0, \tag{15}$$

and the theorem is true.

CASE 2. α/β is irrational. We write

$$(\alpha x + \beta y) = \alpha\left(x + \frac{\beta}{\alpha}y\right) = \alpha(x - \theta y), \tag{16}$$

where θ is irrational. Let m/n be a convergent to θ. Then, from (3),

$$\frac{m}{n} - \theta = e_1 \frac{b}{n^2}. \tag{17}$$

Hence

$$m - \theta n = \frac{e_1 b}{n}. \tag{18}$$

Equation (18) shows that $|\alpha m + \beta n|$ can be made as small as we please for large enough n.

Since $\beta/\alpha = -\theta$, we obtain

$$\frac{m}{n} + \frac{\beta}{\alpha} = \frac{e_1 b}{n^2}, \tag{19}$$

which, solved for m, gives

$$m = -\frac{\beta}{\alpha} n + \frac{e_1 b}{n}. \tag{20}$$

Therefore

$$\begin{aligned} |\gamma m + \delta n| &= \left|\gamma\left(-\frac{\beta}{\alpha} n + \frac{e_1 b}{n}\right) + \delta n\right| \\ &= \left|\left(\delta - \frac{\beta}{\alpha}\gamma\right) n + \frac{e_1 b \gamma}{n}\right| = \left|\frac{n}{\alpha}\left(1 + \frac{e_1 b \alpha \gamma}{n^2}\right)\right|. \end{aligned} \tag{21}$$

The right-hand side of (21) can be made arbitrarily large for large enough n. If we choose m/n in (17) so that $(e_1 b\alpha\gamma)/n < 0$, (16), (18), and (21) give

$$|(\alpha m + \beta n)(\gamma m + \delta n)| < \frac{\alpha}{n} \cdot \frac{n}{\alpha} = 1. \tag{22}$$

Hence, since there are infinitely many convergents to θ, the theorem is completely proved.

THEOREM 3. *If $\xi = \alpha x + \beta y$ and $\eta = \gamma x + \delta y$ are two linear forms, and if $\alpha\delta - \beta\gamma = 1$, and if ξ_0 and η_0 are any two real numbers, integers x_1, y_1 can always be found such that*

$$|(\xi - \xi_0)(\eta - \eta_0)| \leqq \frac{1}{4}. \tag{23}$$

If α/β is irrational $|(\xi-\xi_0)|$ can be made arbitrarily small at the same time that (23) *is satisfied.*

PROOF. We write

$$\xi = \alpha x + \beta y, \qquad \eta = \gamma x + \delta y, \qquad \alpha\delta - \beta\gamma = 1. \tag{24}$$

By Theorem 2, two relatively prime integers m, n exist such that

$$\alpha m + \beta n = \lambda, \qquad \gamma m + \delta n = \mu, \qquad |\lambda\mu| < 1. \tag{25}$$

Without loss of generality we can assume that $\mu > 0$. Then we have

$$\lambda\mu = e_1 b, \tag{26}$$

where $e_1^2 = 1$, and $b < 1$. We define N and k by means of the equation

$$\mu\xi_0 - \lambda\eta_0 = N + k, \tag{27}$$

where N is an integer and $|k| \leqq 1/2$. Say that

$$k = \frac{e_2 c}{2}, \tag{28}$$

where $e_2^2 = 1$, and $c \leqq 1$. We can now write

$$\begin{aligned} \mu\xi - \lambda\eta = N &= (\gamma m + \delta n)(\alpha x + \beta y) - (\alpha m + \beta n)(\gamma x + \delta y) \\ &= nx - my. \end{aligned} \tag{29}$$

By Lemma A, $nx - my = N$ has a solution in integers x_0, y_0. Then all solutions of $nx - my = N$ are represented by

$$x_i = x_0 - im, \qquad y_i = y_0 - in, \tag{30}$$

where i assumes all integral values. Hence, since

$$\gamma x_i + \delta y_i = \gamma(x_0 - im) + \delta(y_0 - in) = (\gamma x_0 + \delta y_0) - i\mu, \tag{31}$$

it follows that i, an integer, can always be determined so that

$$\gamma x_i + \delta y_i - \eta_0 = \frac{e_3 a\mu}{2}, \tag{32}$$

where $e_3^2 = 1$, and $a \leqq 1$. Supposing i so determined and denoting $\alpha x_i + \beta y_i$ and $\gamma x_i + \delta y_i$ by ξ_1 and η_1, respectively, we get

$$\eta_1 - \eta_0 = \frac{e_3 a \mu}{2}. \tag{33}$$

Substituting ξ_1 for ξ and η_1 for η in (29), then subtracting (27) and using (28) and (33), we obtain

$$\mu(\xi_1 - \xi_0) = \lambda\eta_1 + N - \lambda\eta_0 - N - k = \lambda(\eta_1 - \eta_0) - \frac{e_2 c}{2}. \tag{34}$$

Therefore

$$(\xi_1 - \xi_0) = \frac{\lambda}{\mu} \cdot \frac{e_3 a}{2} \mu - \frac{e_2 c}{2\mu} = \frac{1}{2\mu}(e_1 e_3 a b - e_2 c). \tag{35}$$

Similarly, for $\eta_2 = \eta_1 - e_3\mu$, and $\xi_2 = \xi_1 - e_3\lambda$, we get

$$\eta_2 - \eta_0 = -\frac{e_3\mu}{2}(2 - a), \tag{36}$$

and

$$\xi_2 - \xi_0 = -\frac{1}{2\mu}[e_1 e_3(2 - a)b + e_2 c]. \tag{37}$$

For the product of (33) and (35) we have

$$4(\xi_1 - \xi_0)(\eta_1 - \eta_0) = e_3 a(e_1 e_3 a b - e_2 c), \tag{38}$$

while the result of multiplying (36) and (37) is

$$4(\xi_2 - \xi_0)(\eta_2 - \eta_0) = e_3(2 - a)[e_1 e_3(2 - a)b + e_2 c]. \tag{39}$$

If α/β is rational, we see from (26) and the proof of Case 1, Theorem 2, that $b = 0$ in (38); (38) is therefore less than or equal to 1, numerically, and therefore (23) is true. If α/β is irrational, by Lemma B at least one of (38) and (39) is less than or equal 1 numerically, while both (35) and (37) can be made arbitrarily small. Hence the theorem is completely proved.

STANFORD UNIVERSITY