59. On a Theorem of Minkowski and Its Proof of Perron.

By Zuiman YÛJÔBÔ.

Department of Mathematics, St. Paul University.

(Comm. by Z. SUETUNA, M.J.A., June 12, 1951.)

Concerning the Diophantine approximation, there is a following theorem of Minkowski:

Theorem. For arbitrary two linear forms

$$L_1(x, y) = \alpha x+\beta y-\sigma, \qquad \left(\begin{vmatrix}\alpha & \beta \\ \gamma & \delta\end{vmatrix} = \Delta \neq 0\right)$$
$$L_2(x, y) = \gamma x+\delta y-\tau$$

there exists at least a lattice point (x, y) *which satisfies*

$$|L_1(x, y)L_2(x, y)| \leqq \frac{|\Delta|}{4}.$$

I will show in this paper that this can be improved as follows from its simple proof due to Perron.[1]

Theorem. Under the same condition as above, there exist infinitely many lattice points (x_n, y_n) $(n = 1, 2, \dots)$ which satisfy $|x_n| \to \infty$, $|y_n| \to \infty$ and $|L_1(x_n, y_n)L_2(x_n, y_n)| \leqq \frac{|\Delta|}{4}$ with the inequalities $|L_1(x_n, y_n)| > K|x_n|$ and $> K|y_n|$, where K is a positive constant depending only on L_1 and L_2, if $\Delta \neq 0$, $\gamma, \delta \neq 0$ hold, γ/δ is not a rational number and $L_2(x, y) = 0$ has no lattice solution.

The particular case of this theorem, in which $L_1(x, y) = x$ and $L_2(x, y) = \theta x-y-\vartheta$ is already found by Minkowski too, and proved also by Koksma[2] by using Perron's method.

Now let us explain our proof of the above theorem which is deduced from that proof of Perron and furthermore a proof of Korkine-Zortaroff-Markoff's theorem also due to Perron.[3]

Without loss of generality we may consider the case, in which

$$L_1(x, y) = \alpha(x-\mu)+\beta(y-\nu), \qquad \left(\begin{vmatrix}\alpha & \beta \\ \gamma & \delta\end{vmatrix} = \pm 1\right)$$
$$L_2(x, y) = \gamma(x-\mu)+\delta(y-\nu).$$

---

1) O. Perron: Neuer Beweis eines Satzes von Minkowski. Math. Ann. 115 (1938).

2) J. F. Koksma: Anwendung des Perronschen Beweis eines Satzes von Minkowski. Math. Ann. 116, (1939).

3) O. Perron: Eine Abschätzung für die untere Grenze der absoluten Beträge der durch eine reelle oder imaginäre binäre quadratische Form darstellbaren Zahlen. Math. Zeits. 35 (1932).

We put

$$L_1(x, y)L_2(x, y) = a(x-\mu)^2+b(x-\mu)(y-\nu)+c(y-\nu)^2.$$

Then we have $b^2-4ac=1$. Here there is a lattice point (p, r) such that

$$|ap^2+bpr+cr^2| \leqq 1,$$

where we can suppose p and r are relatively prime, because, if not so, we can take (p', r'), such that $p=p'd$, $r=r'd$, $(p', r')=1$, which clearly also satisfies the above inequality. By the transformation

$$x = pX+qY, \qquad y = rX+sY \qquad (ps-qr=1)$$

$a(x-\mu)^2+b(x-\mu)(y-\nu)+c(y-\nu)^2$ is transformed into $A(X-M)^2 +B(X-M)(Y-N)+C(Y-N)^2$, if we determine M, N by the equations

$$\mu = pM+qN,$$
$$\nu = rM+sN.$$

Perron showed that there is a lattice point (X, Y) such that $|A(X-M)^2+B(X-M)(Y-N)+C(Y-N)^2| \leqq 1/4$ and that $|Y-N| \leqq 1/2$.

Now let us consider its improvement. When $a \neq 0$, according to Perron's proof of Korkine-Zortaroff-Markoff's theorem, if we put

$$au^2+buv+cv^2 = a(u-\rho_1 v)(u-\rho_2 v)$$

and take u, v such that

$$|u-\rho_2 v| \leqq \frac{1}{|v|}$$

and that $|v|$ is sufficiently large and $(u, v)=1$, which is possible since $\rho_2=\delta/\gamma$ is not a rational number, and further take all the integers (u_i, v_i) $(i=1, 2, \ldots)$ such that $vu_i-uv_i=1$, then there exist one or more among them which satisfy

$$|aU^2+bUV+cV^2| \leqq 1/\sqrt{5}.$$

And further he showed that such solutions become infinitely many, by taking u, v in infinitely different ways (which is possible). Then

4) loc. cit. 3). See also a remark at the end of this paper.

these solutions are relatively prime, since $(u_i, v_i) = 1$ according to $vu_i - uv_i = 1$.

For u and v we have

$$(1) \qquad |u-\rho_1 v| > |\rho_1 - \rho_2|\,|v| - \frac{1}{|v|}$$

and from $\left|\frac{u_i}{v_i} - \frac{u}{v}\right| = \frac{1}{|v v_i|}$ we have

$$(2) \qquad |u_i - \rho_1 v_i| > |\rho_1 - \rho_2|\,|v_i| - \frac{1}{|v|} - \frac{|v_i|}{|v|^2}.$$

Now let (p_1, r_1), (p_2, r_2), ... be all the solutions that are obtained by such processes, and let (M_1, N_1), (M_2, N_2), ..., and (X_1, Y_1), (X_2, Y_2), ...those corresponding to (p_1, r_1), (p_2, r_2), ... respectively in Perron's proof of Minkowski's theorem. Then we have from (1) and (2)

$$(3) \qquad |p_i - \rho_1 r_i| > \frac{|\rho_1 - \rho_2|}{2}|r_i| - 1$$

for we may take only such v that satisfies $1/|v|^2 < |\rho_1 - \rho_2|/2$.

Next let (x_1, y_1), (x_2, y_2), ... be the solutions of $|L_1(x, y)L_2(x, y)| \leqq 1/4$, corresponding respectively to (X_1, Y_1), (X_2, Y_2), ... Then $x_i = p_i X_i + q_i Y_i$, $y_i = r_i X_i + s_i Y_i$, and therefore from $p_i s_i - q_i r_i = 1$ we have $Y_i = p_i y_i - r_i x_i$. Since $N_i = p_i \nu - r_i \mu$ is similarly obtained, we have

$$(4) \qquad \frac{1}{2} \geqq |Y_i - N_i| = |p_i(y_i - \nu) - r_i(x_i - \mu)|.$$

Then we have from (3) and (4)

$$\left|\frac{x_i - \mu}{y_i - \nu} - \rho_1\right| \geqq \frac{|\rho_1 - \rho_2|}{2} - \frac{1}{|r_i|} - \frac{1}{2|y_i - \nu|\,|r_i|},$$

when $y_i - \nu \neq 0$, and so in general

$$|(x_i - \mu) - \rho_1(y_i - \nu)| \geqq \left|\frac{|\rho_1 - \bar{\rho}_2|}{2} - \frac{1}{|r_1|}\right| |y_i - \nu| - \frac{1}{2|r_i|},$$

i. e.

$$(5) \qquad |L_1(x_i, y_i)| \geqq |\alpha| \left|\frac{|\rho_1 - \rho_2|}{2} - \frac{1}{|r_i|}\right| |y_i - \nu| - \frac{|\alpha|}{2|r_i|}$$

for r_i as large as satisfies $|r_i| \geqq 2/|\rho_1 - \rho_2|$. We have however $|r_i| \to \infty$, because for the same r, there exist only a finite number of p which satisfy $|ap^2 + bpr + cr^2| \leqq 1$.

Now if there exist only a finite number of solutions for $|L_1 \cdot L_2| \leqq 1/4$, different from each other, among (x_i, y_i) $(i=1, 2, \ldots)$, there are infinitely many among (x_i, y_i) $(i=1, 2, \ldots)$ which are equal to one point (x_0, y_0). Let us denote them by (x_{n_i}, y_{n_i}) $(i=1, 2, \ldots)$. Then

$$\left| a\left(\frac{p_{n_i}}{r_{n_i}}\right)^2 + b\left(\frac{p_{n_i}}{r_{n_i}}\right) + c \right| \leqq \frac{1}{r_{ni}^2}$$

and $\left| \frac{p_{n_i}}{r_{n_i}} - \frac{x_0-\mu}{y_0-\nu} \right| \leqq \frac{1}{2|r_{n_i}(y_0-\nu)|}$, when $y_0-\nu \neq 0$; hence

$$\left| a\left(\frac{x_0-\mu}{y_0-\nu}\right)^2 + b\left(\frac{x_0-\mu}{y_0-\nu}\right) + c \right| \leqq \left| a\left(\frac{p_{n_i}}{r_{n_i}}\right)^2 + b\left(\frac{p_{n_i}}{r_{n_i}}\right) + c \right|$$

$$+ \left| b\left(\frac{p_{n_i}}{r_{n_i}} - \frac{x_0-\mu}{y_0-\nu}\right) \right| + \left| \left(\frac{p_{n_i}}{r_{n_i}} + \frac{x_0-\mu}{y_0-\nu}\right)\left(\frac{p_{n_i}}{r_{n_i}} - \frac{x_0-\mu}{y_0-\nu}\right) \right|$$

$$\leqq \frac{1}{r_{n_i}^2} + \left| \frac{b}{2r_{n_i}(y_0-\nu)} \right| + \left| a\,\frac{1}{2r_{n_i}(y_0-\nu)} \right| M,$$

where M is $\left| \frac{1}{2\,r_{n_i}(y_0-\nu)} \right| + 2\left| \frac{x_0-\mu}{y_0-\nu} \right|$.

So we must have

$$\left| a\left(\frac{x_0-\mu}{y_0-\nu}\right)^2 + b\left(\frac{x_0-\mu}{y_0-\nu}\right) + c \right| = 0,$$

since the right-hand side tends to zero in virtue of $|r_{n_i}| \to \infty$. Then from (5) $L_1(x_0, y_0) \neq 0$ and so $|L_2(x_0, y_0)| = 0$, which is impossible from the assumption of the theorem.

If $y_0-\nu = 0$, we must have $x_0-\mu = 0$ from $|r_{n_i}| \to \infty$ according to (4), but this is impossible from our hypothesis.

Next when $a=0$, thkn c must not vanish, and we can also arrive at a contradiction by exchanging x for y.

Thus we have infinitely many different ones among (x_i, y_i) $(i=1, 2, \ldots)$. Then we extract a sequence (x_{n_i}, y_{n_i}) $(i=1, 2, \ldots)$ such that $|x_{n_i}| \to \infty$ or $|y_{n_i}| \to \infty$. But when $a \neq 0$, we must have $|y_{ni}| \to \infty$, also in case $|x_{n_i}| \to \infty$, from $|a(x_{n_i}-\mu)^2 + b\,(x_{n_i}-\mu)\,(y_{n_i}-\nu) + c(y_{n_i}-\nu)^2| \leqq 1/4$. Hence there exists a positive number K such that $|L_1(x_{n_i}, y_{n_i})| > K|y_{n_i}|$ for sufficiently large i, according to (5). Then we must have clearly $L_2(x_{n_i}, y_{n_i}) \to 0$, and so $x_{n_i}/y_{n_i} \to \delta/\gamma$. Therefore we have also $|L_1(x_{n_i}, y_{n_i})| > K'|x_{n_i}|$ for a suitable positive number K' and sufficiently large i, and of course $|x_{n_i}| \to \infty$.

In case $a=0$, then c must not vanish, and so we get the same results by exchangeing x for y.

Remark to the proof of Korkine-Zortaroff-Markoff's theorem due to Perron.

In this proof, Perron assumed that ρ_1 and ρ_2 are both irrational numbers, when he gets solutions from (u, v), (u_i, v_i) $(i = 1, 2, \dots)$. But we may assume only that ρ_2 is irrational. And further we get the following theorem which includes Hurwitz's theorem:

Theorem. Given two linear forms $\alpha x + \beta y$ and $\gamma x + \delta y$, such that $\alpha\delta - \beta\gamma = \varDelta \neq 0$ and $\gamma, \delta \neq 0$, and that γ / δ is irrational, there exists a sequence of lattice points (x_n, y_n) $(n = 1, 2, \dots)$ which satisfy $|x_n| \to \infty$, $|y_n| \to \infty$ and

$$|(\alpha x_n + \beta y_n)(\gamma x_n + \delta y_n)| \leqq |\varDelta| / \sqrt{5}$$

with the inequalities $|\alpha x_n + \beta y_n| > K|x_n|$ and $> K|y_n|$, where K is a positive number depending only on α, β, γ and δ.

To prove this, we may clearly suppose that $\alpha\gamma = a$ is not zero, because we may exchange x for y, when $a = 0$. If we denote by (u, v) and (u_i, v_i) the same ones again, $|u - \rho_1 v| > |\rho_1 - \rho_2|\,|v| - 1/|v|$ and $|u_i - \rho_1 v_i| > |\rho_1 - \rho_2|\,|v_i| - \dfrac{1}{|v|} - \dfrac{|v_i|}{|v|^2}$ hold good, according to (1) and (2). On account of $|v| \to \infty$ we have $|u - \rho_1 v| > |(\rho_1 - \rho_2)/2|\,|v|$ and $|u_i - \rho_1 v_i| > |(\rho_1 - \rho_2)/2|\,|v_i|$ for sufficiently large $|v|$. So we have $|au^2 + buv + cv^2| \neq 0$ and $|au_i^2 + bu_i v_i + cv_i^2| \neq 0$. Then Perron's proof is transferred to this case without any amendment. The infinitely many solutions thus obtained are denoted by (m_1, n_1), (m_2, n_2), ... We can extract a sequence (m_{n_1}, n_{n_1}), (m_{n_2}, n_{n_2}), ... such that $|m_{n_i}| \to \infty$ or $|n_{n_i}| \to \infty$. But from $a \neq 0$ we must have $|n_{n_i}| \to \infty$, and so $|m_{n_i} - \rho_1 n_{n_i}| \to \infty$. Then we have $|m_{n_i} - \rho_2 n_{n_i}| \to 0$. So $|m_{n_i} - \rho_1 n_{n_i}| > \left|\dfrac{\rho_1 - \rho_2}{4\rho_2}\right| |n_{n_i}|$ for sufficiently large i.

Such extensions can be obtained in the same manner for similar theorems concerning Gaussian integers and integers of $K(\omega)$ which are found in the same memoir of Perron.