ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria I: PRACE MATEMATYCZNE IX (1965)

J. Wójcik (Warszawa)

O przedstawieniach liczb pierwszych przez formy kwadratowe

A. Cunningham ([1]) dowiódł, że jeśli zachodzi równość

$$(Dx^2-a^2)(Dy^2-a^2) = Dz^2-a^2$$

i oba czynniki iloczynu są liczbami pierwszymi, to czynniki te są równe, a w przypadku $D = 2$, $a = 1$ zachodzi równość $x^2 = y^2 = 4$. Można to sformułować inaczej: dla dowolnych liczb naturalnych D, y i a takich, że Dy^2-a^2 jest liczbą pierwszą, istnieje co najwyżej jedna liczba pierwsza p mająca przedstawienie postaci:

$$p = Dx^2-a^2 = \frac{Dz^2-a^2}{Dy^2-a^2},$$

mianowicie liczba $p = Dy^2-a^2$; jeśli $D = 2$, $a = 1$, $y \neq 2$, to takich liczb p w ogóle nie ma.

Celem niniejszej pracy jest dowiedzenie twierdzenia, które chociaż mniej precyzyjne od wyniku Cunninghama, jest jednak znacznie ogólniejsze.

Twierdzenie. *Dla dowolnych liczb całkowitych a, b, c, ξ, η, m, n, spełniających warunek: $amn(n\xi^2-m\eta^2) \neq 0$, ilość liczb pierwszych p mających przedstawienie postaci:*

$$(1) \qquad p = \frac{ax^2+b\xi x+c\xi^2}{m} = \frac{ay^2+b\eta y+c\eta^2}{n}$$

jest skończona.

Lemat. *Dla dowolnych liczb całkowitych D, ξ, η, m, n spełniających warunek $mn(n\xi^2-m\eta^2) \neq 0$, ilość liczb pierwszych p mających przedstawienie postaci:*

$$(2) \qquad p = \frac{x^2-D\xi^2}{m} = \frac{y^2-D\eta^2}{n}$$

jest skończona.

Dowód lematu. Przypuśćmy, że liczb pierwszych mających przedstawienie (2) jest nieskończenie wiele. Ustawiając te liczby w ciąg rosnący otrzymujemy:

$$p_k = \frac{x_k^2 - D\xi^2}{m} = \frac{y_k^2 - D\eta^2}{n}, \tag{3}$$

gdzie liczby x_k, y_k są wyznaczone z dokładnością do znaku. Pokażemy, że można tak dobrać znaki liczb x_k, y_k by liczby

$$m\frac{\eta x_k + \xi y_k}{x_k^2 - D\xi^2} \qquad (k = 1, 2, \ldots)$$

były całkowite.

W tym celu zauważmy, że (3) pociąga za sobą równość:

$$(n\xi^2 - m\eta^2)p_k = \xi^2(y_k^2 - D\eta^2) - \eta^2(x_k^2 - D\xi^2) =$$

$$= \xi^2 y_k^2 - \eta^2 x_k^2 = (\xi y_k - \eta x_k)(\xi y_k + \eta x_k);$$

zatem

$$p_k \mid (\xi y_k - \eta x_k)(\xi y_k + \eta x_k),$$

a stąd

$$p_k \mid \xi y_k - \eta x_k \quad \text{lub} \quad p_k \mid \xi y_k + \eta x_k,$$

gdyż p_k jest liczbą pierwszą. Przez odpowiedni dobór znaku można więc sprawić, aby liczba

$$\frac{\eta x_k + \xi y_k}{p_k} = m\frac{\eta x_k + \xi y_k}{x_k^2 - D\xi^2}$$

była całkowita.

Z drugiej strony, dla dostatecznie dużych k, $y_k \neq 0$ i z (3) otrzymujemy:

$$\left(\frac{x_k}{y_k}\right)^2 = \frac{m}{n} + \frac{D}{y_k^2}\left(\xi^2 - \frac{m}{n}\eta^2\right),$$

ponieważ $\lim\limits_{k=\infty} y_k^2 = \infty$, więc

$$\lim_{k=\infty}\left(\frac{x_k}{y_k}\right)^2 = \frac{m}{n}.$$

Mamy zatem

$$\lim_{k=\infty}\left|\frac{x_k}{y_k}\right| = \sqrt{\frac{m}{n}}, \qquad \lim_{k=\infty}\left| m\frac{\eta x_k + \xi y_k}{x_k^2 - D\xi^2}\right| \leqslant |m| \lim_{k=\infty} \frac{\dfrac{1}{|y_k|}\left(|\xi| + |\eta|\left|\dfrac{x_k}{y_k}\right|\right)}{\left|\left(\dfrac{x_k}{y_k}\right)^2 - D\left(\dfrac{\xi}{y_k}\right)^2\right|} = 0,$$

skąd

$$\lim_{k=\infty}\left| m\frac{\eta x_k + \xi y_k}{x_k^2 - D\xi^2}\right| = 0.$$

Ponieważ liczby

$$m\frac{\eta x_k+\xi y_k}{x_k^2-D\xi^2}$$

są całkowite, dla dostatecznie dużych k muszą być równe 0, zatem $\eta x_k+\xi y_k=0$ i wobec (3) $n\xi^2-m\eta^2=0$ wbrew założeniu. Otrzymana sprzeczność kończy dowód.

Dowód twierdzenia. Mamy tożsamość

$$ax^2+bx\xi+c\xi^2=\frac{1}{4a}[(2ax+b\xi)^2-D\xi^2],$$

gdzie $D=b^2-4ac$.

Gdyby istniało nieskończenie wiele liczb pierwszych mających przedstawienie (1), to istniałoby też, wobec powyższej tożsamości, nieskończenie wiele liczb pierwszych mających przedstawienie

$$p=\frac{u^2-D\xi^2}{4am}=\frac{v^2-D\eta^2}{4an}.$$

Ponieważ

$$(4am)(4an)(4an\xi^2-4am\eta^2)=64a^3mn(n\xi^2-m\eta^2)\neq 0,$$

co jest sprzeczne z lematem, a więc niemożliwe, c.b.d.o.

Metoda dowodu twierdzenia przenosi się na przypadek, gdy liczby a, b, c, ξ, η, m, n należą do ustalonego ciała kwadratowego o wyróżniku <0, x, y przebiega liczby całkowite tego ciała, a (p) jest ideałem pierwszym.

Prace cytowane

[1] A. Cunningham, Sphin-Oedipe 7 (1912), str. 77-79.

J. Wójcik (Warszawa)

ON THE REPRESENTATION OF PRIMES BY QUADRATIC FORMS

SUMMARY

The following theorem is proved:

For arbitrary integers a, b, c, ξ, η, m, n satisfying the condition $amn(n\xi^2-m\eta^2)\neq 0$, there exist only finitely many primes p representable in the form

$$p=\frac{ax^2+b\xi x+c\xi^2}{m}=\frac{ay^2+b\eta y+c\eta^2}{n}$$

where x and y are integers.
