ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE VII (1964)

wmptm 1897

A. Schinzel i W. Sierpiński (Warszawa)

O równaniu $x^2-2y^2=k$

Ministerstwo Nauki i Szkolnictwa Wyższego

W niniejszym artykule zajmiemy się wyznaczeniem wszystkich liczb całkowitych k, dla których równanie

$$x^2-2y^2=k \tag{1}$$

jest rozwiązalne w liczbach naturalnych x i y.

Zagadnienie to nie jest nowe, a wyniki, które tu podamy, są znane. Sądzimy jednak, że zebranie ich i przedstawienie w sposób elementarny będzie rzeczą pożyteczną, zwłaszcza z uwagi na zauważone w ostatnich latach powiązania równania (1) z innymi równaniami diofantycznymi, o czym też tu będzie mowa.

Dla $k=0$ równanie (1) oczywiście nie ma rozwiązań w liczbach naturalnych x, y. Z tożsamości zaś

$$(x+2y)^2-2(x+y)^2=2y^2-x^2$$

wynika natychmiast, że jeżeli równanie (1) ma rozwiązanie w liczbach naturalnych x i y, to mamy

$$(x+2y)^2-2(x+y)^2=-k.$$

Wystarczy więc rozpatrzyć równanie (1) w przypadku, gdy k jest liczbą naturalną. Udowodnimy tu

Twierdzenie 1. *Na to, żeby równanie* (1), *gdzie k jest daną liczbą naturalną, było rozwiązalne w liczbach naturalnych x, y, potrzeba i wystarcza, żeby iloraz z dzielenia liczby k przez największy kwadrat, dzielący k, nie był podzielny przez żadną liczbę pierwszą postaci $8t\pm3$.*

Dowód. Niech m oznacza największą liczbę naturalną, której kwadrat jest dzielnikiem liczby k i niech $k=m^2l$, gdzie l jest liczbą naturalną, niepodzielną przez żaden kwadrat liczby naturalnej większej od 1, i przypuśćmy, że liczby naturalne x i y spełniają równanie

$$x^2-2y^2=m^2l. \tag{2}$$

Niech $(x,y)=d$; mamy więc $x=dx_1$, $y=dy_1$, gdzie x_1 i y_1 są liczbami naturalnymi względnie pierwszymi. Wobec równania (2) mamy więc

$d^2 \mid m^2 l$, skąd $d \mid m$ oraz $m = dm_1$, gdzie m_1 jest liczbą naturalną, zatem wobec równania (2) jest

$$x_1^2 - 2y_1^2 = m_1^2 l. \tag{3}$$

Przypuśćmy, że liczba l jest podzielna przez liczbę pierwszą p postaci $8t \pm 3$. Prawa strona wzoru (3) jest więc podzielna przez p, a ponieważ liczby x_1 i y_1 są względnie pierwsze, więc żadna z nich nie jest podzielna przez p, a wobec wzoru (3), mamy

$$x_1^2 \equiv 2y_1^2 (\mathrm{mod}\, p),$$

skąd, podnosząc obie strony do potęgi o wykładniku $(p-1)/2$, w myśl twierdzenia Fermata, znajdujemy

$$1 \equiv 2^{(p-1)/2} (\mathrm{mod}\, p), \quad \text{skąd} \quad 2^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p),$$

co dowodzi, że 2 jest resztą kwadratową dla modułu p, wbrew temu, że $p = 8t \pm 3$.

Dowiedliśmy więc, że warunek naszego twierdzenia jest konieczny.

Aby dowieść, że jest on dostateczny, oprzemy się na następującym twierdzeniu T [1]:

T. *Na to, żeby liczba pierwsza nieparzysta p była postaci $x^2 - 2y^2$, gdzie x i y są liczbami naturalnymi, potrzeba i wystarcza, żeby p było liczbą postaci $8t \pm 1$.*

Mamy

$$2^2 - 2 \cdot 1^2 = 2 \quad \text{oraz} \quad (3m)^2 - 2(2m)^2 = m^2 \quad \text{dla} \quad m = 1, 2, \ldots$$

Przypuśćmy teraz, że dla liczb naturalnych k_1 i k_2 istnieją liczby naturalne x_1, y_1 i x_2, y_2 takie, że

$$x_1^2 - 2y_1^2 = k_1, \quad x_2^2 - 2y_2^2 = k_2.$$

Wynika stąd, jak łatwo sprawdzić, że

$$(x_1 x_2 + 2y_1 y_2)^2 - 2(x_1 y_2 + x_2 y_1)^2 = k_1 k_2.$$

Zatem z twierdzenia T i z uwagi, że liczba l, w myśl warunku twierdzenia 1, może mieć tylko czynniki pierwsze 2 lub postaci $8t \pm 1$, wnosimy, że liczba $k = m^2 l$ jest postaci (1). Warunek twierdzenia 1 jest więc dostateczny.

Twierdzenie 1 zostało zatem udowodnione.

---

[1] Dowód elementarny tego twierdzenia znajduje się w książce: W. Sierpiński, *Teoria Liczb*, część II, Warszawa 1959, str. 338, twierdzenie 3.

I. A. H. Hunter wypowiedział następujące

TWIERDZENIE 2. *Jeżeli równanie* (1), *gdzie* k *jest liczbą całkowitą, jest rozwiązalne w liczbach naturalnych, to równanie*

$$(x^2-k)(z^2-k)=(y^2-k)^2 \tag{4}$$

ma nieskończenie wiele rozwiązań w różnych liczbach naturalnych x, y, z [2].

Dowód I. A. H. Huntera jego twierdzenia (podanego przez niego w formie zadania) nie jest nam znany, ale można je udowodnić na przykład w następujący sposób. Przypuśćmy, że a i b są liczbami naturalnymi, spełniającymi równanie

$$a^2-2b^2=k. \tag{5}$$

Wynika stąd, jak łatwo sprawdzić, że

$$(3a+4b)^2-2(2a+3b)^2=k, \tag{6}$$

skąd łatwy wniosek, że jeżeli dla danej liczby całkowitej k równanie (1) jest rozwiązalne w liczbach naturalnych x, y, to ma ono nieskończenie wiele takich rozwiązań.

Łatwo też sprawdzić, że z wzoru (5) wynika wzór

$$2b(2a+3b)=(a+2b)^2-k. \tag{7}$$

Niech

$$x=a, \quad z=3a+4b, \quad y=a+2b, \tag{8}$$

mamy więc $z-x=2y$ i z wzorów (5), (6) i (7) wynika natychmiast, że liczby naturalne x, y, z (które są różne) spełniają równanie (4). Równanie to ma więc nieskończenie wiele rozwiązań w różnych liczbach naturalnych x, y, z, co dowodzi twierdzenia 2.

W przypadku $k=1$, jeżeli liczby naturalne a i b spełniają równanie $a^2-2b^2=1$, to a jest liczbą nieparzystą i przeto liczby (8) są wszystkie trzy nieparzyste. Stąd

WNIOSEK. *Równanie*

$$(x^2-1)(z^2-1)=(y^2-1)^2 \tag{9}$$

ma nieskończenie wiele rozwiązań w różnych liczbach naturalnych nieparzystych x, y, z.

Mamy na przykład rozwiązania

$$(x, y, z)=(3, 7, 17), (17, 41, 99), (99, 239, 577).$$

---

[2] Porównaj The American Mathematical Monthly 69 (1962), str. 316, zadanie 5020.

Nie wiemy, czy równanie (9) ma rozwiązanie w różnych liczbach parzystych x, y, z.

Jeżeli liczby naturalne nieparzyste x, y, z spełniają równanie (9), to mamy, co łatwo sprawdzić,

$$t_{(x-1)/2}t_{(z-1)/2} = t_{(y-1)/2},$$

gdzie $t_n = n(n+1)/2$ oznacza n-tą liczbę trójkątną. Wniosek nasz jest więc równoważny twierdzeniu, że *istnieje nieskończenie wiele postępów geometrycznych, utworzonych z trzech różnych liczb trójkątnych* [3].

Nie wiemy, czy istnieją cztery różne liczby trójkątne tworzące postęp geometryczny.

Określmy ciąg nieskończony u_n $(n = 1, 2, \ldots)$ warunkami

$$u_1 = 3, \quad u_2 = 7, \quad u_{n+2} = u_n + 2u_{n+1} \quad \text{dla} \quad n = 1, 2, \ldots$$

Można dowieść, że liczby

$$x = u_{2n-1}, \quad y = u_{2n}, \quad z = u_{2n+1} \quad \text{dla} \quad n = 1, 2, \ldots$$

spełniają równanie (9). Łatwo też dowieść, że

$$u_n = \frac{(1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}}{2} \quad \text{dla} \quad n = 1, 2, \ldots$$

Nie wiemy, czy równanie (9) ma inne rozwiązanie w liczbach naturalnych x, y, z, gdzie $x < y < z$.

W związku z twierdzeniem 2 zauważymy, że, jak to zaznaczył I. A. H. Hunter, równanie (4) może dla pewnych liczb całkowitych k mieć rozwiązania w różnych liczbach naturalnych x, y, z, pomimo że równanie (1) nie ma rozwiązań w liczbach naturalnych; tak jest na przykład dla $k = -6$, gdzie równanie (4) ma rozwiązanie $x = 2$, $y = 8$, $z = 22$. Nie znamy odpowiedzi na pytanie postawione przez I. A. H. Huntera, dla jakich całkowitych k równanie (4) ma nieskończenie wiele rozwiązań w różnych liczbach naturalnych x, y, z.

---

[3] Twierdzenie to udowodnił na innej drodze Kazimierz Szymiczek w pracy znajdującej się w druku w wydawnictwie Publikacje Elektrotechn. Fakulteta Universiteta w Beogradu.