ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XLIII (2007)

Władysław Narkiewicz (Wrocław)

Teoria liczb w twórczości Eulera

1. W roku 2007 mija trzysta lat od urodzin Leonarda Eulera, jest to więc okazja, by przypomnieć jego dzieło. Zajmiemy się teorią liczb, której Euler poświęcił sporo publikacji. Wypełniają one cztery tomy jego *Opera Omnia*, objęte wspólnym tytułem *Commentationes Arithmeticae*.

Pierwszym matematykiem czasów nowożytnych, który zajął się problemami arytmetycznymi był Pierre Fermat, który sformułował wiele twierdzeń dotyczących podstawowych faktów teorii liczb, nie przedstawiając wszakże, poza jednym wyjątkiem, ich dowodów. Wielką zasługą Eulera jest znalezienie dowodów dla większości twierdzeń podanych przez Fermata, oraz dodanie do nich szeregu własnych odkryć. Ograniczymy się tu do najważniejszych rezultatów Eulera w tej dziedzinie. Zainteresowany czytelnik znajdzie więcej informacji w książce A.Weila [W], gdzie twórczości Eulera poświęconych jest 150 stron.

2. Już w swej pierwszej pracy[1] dotyczącej arytmetyki [E2], napisanej w 1732 r., nawiązuje Euler do Fermata, który twierdził, że wszystkie liczby postaci $2^{2^n}+1$, zwane dziś liczbami Fermata, są liczbami pierwszymi. Jednakże, jak pisze Euler, chociaż dla $n=1,2,3,4$ wzór ten w istocie daje liczby pierwsze, to już następna liczba, $2^{2^5}+1=4\,294\,967\,297$, dzieli się bez reszty przez 641. Nawet dzisiaj nie jest znana żadna większa liczba pierwsza Fermata. Przytacza tu też Euler twierdzenie, zwane dziś *małym twierdzeniem Fermata* (jeśli liczba p jest pierwsza i nie dzieli a, to dzieli $a^{p-1}-1$), pisząc, że jest pewny słuszności tego twierdzenia, ale nie posiada jego dowodu. Dowód ten, zresztą nieskomplikowany, oparty na prostej indukcji, znalazł Euler dopiero w roku 1736 [E5]. Później podał kilka dowodów tego twierdzenia, z których najciekawszy pojawia się w pracy [E9] z 1758 r. Jest to *de facto* dowód teorio-grupowy, gdyż rozumowanie Eulera dowodzi w istocie, że rząd podgrupy jest dzielnikiem rzędu grupy:

[1] Prace Eulera i znaczna część jego korespondencji jest dostępna na stronie internetowej www.math.dartmouth.edu˜/euler/.

Dla liczby $1 < a < p$ niech λ będzie najmniejszą liczbą spełniającą $p|a^\lambda - 1$. Jej istnienie wynika ze skończoności zbioru reszt z dzielenia przez p. Jeśli w ciągu $a, a^2, \ldots, a^\lambda$ wystąpią wszystkie takie reszty, to $\lambda = p-1$. W przeciwnym wypadku niech k będzie resztą nie pojawiającą się w tym ciągu. Wówczas reszty liczb $ak, a^2k, \ldots, a^\lambda k$ są wszystkie różne i różne od poprzednich, a więc $2\lambda \leqslant p-1$. Jeśli zachodzi tu ostra nierówność, to kontynuujemy to postępowanie, by otrzymać w końcu równość postaci $p-1 = j\lambda$. Wówczas

$$a^{p-1} - 1 = (a^\lambda)^j - 1$$

dzieli się przez $a^\lambda - 1$, a więc i przez p.

Kilka lat później ta sama metoda jest użyta do dowodu twierdzenia, zwanego dzisiaj *twierdzeniem Eulera*. Jest to dziesiąte twierdzenie pracy [E10]:

Jeśli $(a, N) = 1$*, to* $a^{\varphi(N)} - 1$ *dzieli się przez* N,

przy czym $\varphi(N)$ oznacza ilość liczb z przedziału $[1, N]$ względnie pierwszych z N.

Do funkcji φ, którą oznaczał literą π, powrócił Euler w 1780 r. [E23], podając wzór

$$\varphi\left(\prod_p p^{a_p}\right) = \prod_p p^{a_p-1}(p-1).$$

3. W parę lat później zajął się Euler tzw. *chińskim twierdzeniem o resztach*, przypisywanym, w szczególnym przypadku, chińskiemu matematykowi Sun Tsu, żyjącemu w I wieku. Głosi ono, że jeśli liczby $n_1, n_2, \ldots, n_k$ są parami względnie pierwsze, a nadto są zadane liczby $a_1, a_2, \ldots, a_k$, to istnieje liczba N dająca resztę a_j z dzielenia przez n_j dla każdego $j = 1, 2, \ldots, k$. W pracy [E4] podaje Euler sposób znajdowania takiej liczby N przy użyciu algorytmu Euklidesa.

4. Ważny postęp w badaniu struktury systemu reszt uzyskuje Euler w 1773 roku [E17], dowodząc istnienia pierwiastków pierwotnych dla liczb pierwszych. Liczba a nazywa się *pierwiastkiem pierwotnym* dla liczby N, jeśli każda reszta mod N, względnie pierwsza z N przystaje mod N do pewnej potęgi a. Nie każda liczba N ma pierwiastki pierwotne, a dowód Eulera był pierwszym krokiem do opisu takich liczb. Euler dowodzi najpierw, że kongruencja $x^n \equiv 1 \pmod{p}$ ma conajwyżej n rozwiązań, a następnie korzysta z istnienia rozkładu

$$X^n - 1 = \prod_{d|n} F_d(X),$$

gdzie $F_d(X)$ jest wielomianem stopnia $\varphi(d)$ o całkowitych współczynnikach, dowodząc tego zresztą jedynie dla liczb n mających conajwyżej 3 różne dzielniki pierwsze. Ten dowód nie jest przeprowadzony w pełni precyzyjnie, aczkolwiek nie jest trudno uczynić go ścisłym. Nie jest to jednakże dowód specjalnie prosty.

5. Kolejnym istotnym rezultatem arytmetycznym Eulera jest dowód twierdzenia o sumach 2 kwadratów, sformułowanego przez Fermata:

Na to, by nieparzysta liczba pierwsza p dała się przedstawić jako suma 2 *kwadratów, potrzeba i wystarcza, by* $p \equiv 1 \pmod 4$.

Dowód ten [E8] powstał w 1754 r., a pierwszym jego krokiem jest pokazanie tzw. *kryterium Eulera*, głoszącego, że kongruencja

$$X^2 \equiv a \pmod p$$

ma, dla a niepodzielnych przez liczbę pierwszą p, rozwiązanie wtedy i tylko wtedy, gdy

$$a^{(p-1)/2} \equiv 1 \pmod p.$$

Jest to początek teorii reszt kwadratowych. Do tej problematyki powrócił Euler w 1783 r., formułując w pracy [E19] prawo wzajemności reszt kwadratowych, udowodnione dopiero w 1801 roku przez młodego Gaussa [G]. Podjęta wcześniej przez Legendre'a [Le] próba dowodu tego prawa jest niezbyt przekonywująca, gdyż korzysta z istnienia nieskończenie wielu liczb pierwszych w postępie arytmetycznym $aX + b$ ($(a, b) = 1$). Podany w [Le] dowód tego faktu jest błędny, a pierwszy poprawny dowód podał dopiero Dirichlet [D].

Zauważmy też, że w pracy [E8] formułuje Euler twierdzenie, iż każda liczba naturalna jest sumą czterech kwadratów. Twierdzenia tego nigdy nie udało mu się dowieść, a uczynił to dopiero Lagrange [La] w 1772 roku, a w 1773 r. Euler [E16] podał inny dowód. Liczbę przedstawień tego typu znalazł dopiero w 1829 roku Jacobi [J], który pokazał, że ilość takich przedstawień liczby N jest równa pomnożonej przez 8 liczbie dzielników N, niepodzielnych przez 4. Dowód Jacobiego oparty był na teorii funkcji eliptycznych, ale obecnie znane są znacznie prostsze dowody.

6. Jeszcze przed dowodem twierdzenia o 2 kwadratach Euler zauważył [E7], że jeśli nieparzysta liczba $n > 1$ da się przedstawić jednoznacznie w postaci $x^2 + y^2$ z nieujemnymi $x < y$, a przy tym $(x, y) = 1$, to jest ona liczbą pierwszą. W dowodzie użył wcześniej udowodnionego przez siebie faktu, że każdy dzielnik sumy 2 kwadratów jest też taką sumą. Jeśli więc n nie byłaby liczbą pierwszą i $n = rs$, to mielibyśmy $r = a^2 + b^2$ i $s = c^2 + d^2$, a więc

$$n = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2,$$

i nietrudno zauważyć, że jeśli te dwa przedstawienia pokrywają się, to albo $a = b$ i $c = d$, co prowadzi do $n = (2ab)^2 + 0^2$, co jest wykluczone, albo też zachodzi jedna z równości $n = (ac)^2 + (ad)^2$, $n = (bd)^2 + (ad)^2$, co jest również niemożliwe.

Wynik ten Euler musiał znać już wcześniej, gdyż w liście do Goldbacha z 30 VI 1741 r. dowodzi złożoności liczby $F_5 = 2^{2^5} + 1$, pokazując, że ma ona dwa różne rozkłady na sumę 2 kwadratów:

$$F_5 = 65536^2 + 1 = 62264^2 + 20449^2.$$

Powyższy rezultat prowadzi do testu na pierwszość liczby $n \equiv 1 \pmod 4$, wystarczy bowiem policzyć, ile kwadratów znajduje się w ciągu $N - 1^2, N - 2^2, \ldots$ Test ten opisuje Euler w [E13] i ilustruje go na przykładzie liczby 10 091 401.

Poprzedni wynik został przez Eulera uogólniony na niektóre formy kwadratowe postaci $x^2 + Ny^2$. Euler nazywa liczbę N *liczbą wygodną* (*numerus idoneus*), jeśli z tego, że nieparzysta liczba n, względnie pierwsza z N ma jedyne przedstawienie w postaci $x^2 + Ny^2$, a przy tym $(x, y) = 1$, wynika, że n jest liczbą pierwszą. W [E20] podaje Euler następujący test:

Liczba N jest wygodna wtedy i tylko wtedy, gdy każda liczba postaci $a = N + y^2 \leqslant 4N$ przy $(y, N) = 1$ jest liczbą pierwszą, lub podwojeniem liczby pierwszej, lub kwadratem liczby pierwszej, lub też potęgą dwójki.

Euler użył tego testu do sprawdzenia wszystkich liczb mniejszych od 10 000 i znalazł 65 takich liczb, z których największą jest 1848. Pierwszy kompletny dowód tego testu podał F.Grube [Gr] w 1874 r.

W nieopublikowanej za życia Eulera pracy [E30] znajdujemy przypuszczenie, że liczb wygodnych jest jedynie skończenie wiele, a liczba 1848 jest największą z nich. Skończoność tego zbioru udowodnił S.Chowla w 1934 r. [C], a później okazało się, że może istnieć conajwyżej jedna liczba wygodna większa od 1848, a przy tym jej istnienie jest sprzeczne z Dużą Hipotezą Riemanna [CB].

7. W liście do Eulera z 28 IX 1743 r. Goldbach (patrz [F], [WJ]) stwierdził, że żaden wielomian nie może przyjmować wyłącznie wartości, które są liczbami pierwszymi. Kilka lat później (w liście z 18 XI 1752 r.) Goldbach podał poprawny dowód tego faktu w przypadku wielomianu trzeciego stopnia, a pełny dowód opublikował Euler w 1762 r. w [E11]. W pracy tej znajdziemy też stwierdzenie, że ilość liczb pierwszych w przedziale $[2, x]$ jest w przybliżeniu równa $x/\log x$. Euler przypuszczał też (w liście do Goldbacha z 28 X 1752 r.), że liczb pierwszych postaci $a^2 + 1$ jest nieskończenie wiele (teraz zazwyczaj to zagadnienie nazywa się *problemem Landau'a*), a w [E11] umieścił ich tablice aż do $1494^2 + 1 = 2\,232\,037$.

Do tego tematu powraca Euler w 1772 roku, zauważając w liście do Jana III Bernoulliego [E18], że wielomian $x^2 - x + 41$ przyjmuje w przedziale $[1, 40]$ wyłącznie wartości pierwsze. Fakt ten ma interpretację algebraiczną, odkrytą przez G.Rabinowitscha [Ra] w 1913 r. Pokazał on mianowicie, że jeśli $m > 1$, to wielomian $x^2 - x + m$ przyjmuje dla liczb $x = 0, 1, \ldots, m-1$ wyłącznie wartości pierwsze wtedy i tylko wtedy, gdy w pierścieniu liczb całkowitych ciała, generowanego przez $\sqrt{1-4m}$ zachodzi twierdzenie o jednoznaczności rozkładu na czynniki nierozkładalne. Dzisiaj wiemy, że największą liczbą m dla której to zachodzi jest $m = 41$ ([H], [S]).

W liście tym zajął się Euler także problemem pierwszości liczb Mersenne'a $M_p = 2^p - 1$ i pokazał, że liczba

$$M_{31} = 2\,147\,483\,647$$

jest pierwsza. Najpierw zauważa, iż z małego twierdzenia Fermata wynika, że każdy dzielnik pierwszy p liczby M_{31} spełnia $p \equiv 1 \pmod{62}$, a nadto z uwagi na $p|2(2^{31}-1) = x^2 - 2$ z x całkowitym, otrzymuje $p \equiv \pm 1 \pmod 8$. Tu wykorzystuje Euler fakt, że liczba 2 jest resztą kwadratową tylko dla liczb pierwszych przystających do $\pm 1 \pmod 8$, a zatem p musi przystawać do 1 lub 63 mod 248. Pozostaje jedynie sprawdzić, czy M_{31} dzieli się przez takie liczby $p \leqslant 46339$, a ponieważ jest ich tylko 84, nie sprawiło mu to wielkiego kłopotu.

8. W pracy [E25], przedstawionej w Akademii Petersburskiej 5 grudnia 1735 r., ale opublikowanej dopiero w 1740 r., pojawia się funkcja, zwana później funkcją *zeta Riemanna*, zdefiniowana dla $x > 1$ wzorem

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}.$$

Euler znajduje w tej pracy wzór dla wartości tej funkcji w punktach parzystych, a mianowicie

$$\zeta(2m) = (-1)^{m-1} \frac{B_{2m}}{2(2m)!} (2\pi)^{2m},$$

aczkolwiek jego dowód jest daleki od poprawności. Występujące tu liczby Bernoulliego B_n są określone przez

$$\sum_{n=0}^{\infty} \frac{B_n}{n} x^n = \frac{x}{e^x - 1}.$$

Pierwszy poprawny dowód tego wzoru znajdujemy dopiero w pracy [E27], napisanej w 1740 r.

Bardzo ważną równość

$$\zeta(x) = \prod_p \left(1 - \frac{1}{p^x}\right)^{-1}, \quad x > 1$$

udowodnił Euler w [E26] (tw. 8) a następnie zastosował ją do pokazania rozbieżności szeregu odwrotności liczb pierwszych. Jest to pierwszy z tzw. *iloczynów eulerowskich*, które odegrały później dużą rolę w analitycznej teorii liczb.

Później (w pracy [E28]) rozpatrywał Euler szereg

$$\Phi(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^x},$$

zbieżny dla dodatnich wartości x. Wiąże się on z funkcją $\zeta(x)$, jak nietrudno sprawdzić, wzorem

$$\Phi(x) = (1 - 2^{1-x})\zeta(x).$$

Euler przypuszczał, że $\Phi(x)$ spełnia równanie funkcyjne

$$\frac{\Phi(1-x)}{\Phi(x)} = -\Gamma(x)\frac{2^x - 1}{2^{x-1} - 1}\pi^{-x}\cos\left(\frac{\pi x}{2}\right)$$

w każdym punkcie, w którym funkcja Γ nie ma bieguna i próbował, zresztą bezskutecznie, znaleźć dowód, rozpatrując przypadek całkowitego x. Wówczas szereg $\Phi(1-x)$ jest co prawda rozbieżny, ale nie było to przeszkodą dla Eulera, który na różne sposoby nadawał wartość sumy szeregom rozbieżnym, głównie metodą sumowania abelowego. Dziś wiemy, że równanie funkcyjne zaproponowane przez Eulera jest w istocie inną formą równania funkcyjnego dla funkcji zeta, znalezionego przez Riemanna [R] w 1860 r.

9. Wiele prac Eulera dotyczy równań diofantycznych. Pierwsza jego praca na ten temat [E3] została napisana w 1732 roku. Sprowadza w niej Euler rozwiązanie równania

$$ax^2 + bx + c = y^2$$

do równania Pella $X^2 - dY^2 = 1$. Do tego równania powróci jeszcze w 1765 r., gdy w pracy [E12] poda algorytm jego rozwiązywania przy użyciu ułamków łańcuchowych, bez kompletnego dowodu, a tymczasem w 1738 roku przedstawia w Akademii Petersburskiej dużą pracę [E6], opublikowaną dopiero po dziewięciu latach, której głównym wynikiem jest dowód Wielkiego Twierdzenia Fermata dla wykładnika 4, niewiele zresztą różniący się od dowodu podanego przez Fermata. Znajdujemy w niej także twierdzenia o wielu innych równaniach diofantycznych. I tak np. Euler pokazuje, że różnica czwartych potęg liczb naturalnych nie może być kwadratem (tw. 2), a także (tw. 7), że liczba trójkątna większa od jedności nie może być czwartą potęgą, co wcześniej sformułował Fermat. Pojawia się tu też wynik, który obecnie należy do teorii krzywych eliptycznych: Euler dowodzi mianowicie (tw. 10), że jeśli x, y są liczbami wymiernymi, spełniającymi $y^2 = x^3 + 1$, to $x = 2, y = \pm 3$.

W wydanym w 1770 roku podręczniku algebry [E1] znajdujemy dowód Wielkiego Twierdzenia Fermata dla wykładnika 3. Przez długi czas uważano

dowód ten za niekompletny, gdyż korzystał z pewnego nieudowodnionego faktu, aż w 1966 roku Bergmann [Be] zauważył, że poprawny dowód tego faktu można bez trudu wyprowadzić z rezultatów jednej z wcześniejszych prac Eulera.

W 1783 roku zajął się Euler [E22] zagadnieniem, pochodzącym od Diofantesa, który znalazł cztery dodatnie liczby wymierne $x_1, \ldots, x_4$ o tej własności, że dla $i \neq j$ liczba $x_i x_j + 1$ jest kwadratem liczby wymiernej. Fermat znalazł cztery liczby całkowite o tej własności, mianowicie $1, 3, 8, 120$, zaś Euler pokazał, że jeśli przyjmiemy $x_5 = 777480/8288641$, to warunek $x_i x_j + 1 = \square$ będzie spełniony dla $1 \leqslant i < j \leqslant 5$. Obecnie wiadomo, że istnieją szóstki liczb wymiernych o tej własności [Gi], ale, jak pokazał Dujella [Du] w 2004 r., nie ma takiej szóstki liczb naturalnych. W tej samej pracy Dujella udowodnił także, że może istnieć conajwyżej skończenie wiele takich piątek liczb naturalnych. Nadal nie wiadomo, czy istnieje chociaż jedna taka piątka.

10. W 1772 r. sformułował Euler [E15] przypuszczenie, związane z zagadnieniem Fermata:

Dla każdego $n \geqslant 3$ równanie

$$x_1^n + \cdots + x_n^n = y^n$$

ma rozwiązanie w liczbach naturalnych, zaś równanie

$$x_1^n + \cdots + x_{n-1}^n = y^n$$

takich rozwiązań nie ma.

W przypadku $n = 3$ jest to twierdzenie Fermata dla wykładnika 3. Niestety, w 1967 r. Lander i Parkin [LP] znaleźli kontrprzykład

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

dla $n = 5$, a w 1988 r. Elkies [El] znalazł, używając teorii krzywych eliptycznych, kontrprzykład także i dla $n = 4$, mianowicie

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Później Frye znalazł kilka innych kontrprzykładów dla tego wykładnika, w tym najmniejszy:

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

11. W liście z 7 VI 1742 r. Goldbach napisał do Eulera, iż wydaje mu się, że każda liczba większa od 2 jest sumą trzech liczb pierwszych (pamiętajmy, że w owym czasie liczba 1 była uważana za pierwszą). Euler odpisał 30 czerwca, że uważa za pewne, że każda liczba parzysta jest sumą 2 liczb pierwszych, ale nie potrafi tego udowodnić. Obecnie te przypuszczenia

nazywa się *hipotezą Goldbacha*, przy czym formułuje się ją w następujący sposób:

Każda liczba parzysta $\geqslant 6$ *jest sumą* 2 *liczb pierwszych nieparzystych, a każda liczba nieparzysta* $\geqslant 9$ *jest sumą* 3 *liczb pierwszych nieparzystych.*

Problem ten jest dotąd otwarty, aczkolwiek wiemy już bardzo wiele na ten temat. W 1937 roku Winogradow [Wi] pokazał, że każda dostatecznie duża liczba nieparzysta jest sumą trzech liczb pierwszych, pozostaje więc sprawdzenie skończenie wielu przypadków. Niestety, ich jest bardzo wiele, gdyż obecnie wiemy jedynie, że teza twierdzenia Winogradowa zachodzi dla liczb nieparzystych większych od e^{114}, co pokazali Wang i Chen [WC] w 1993 roku. Tego problemu nie ma, jeśli prawdziwa jest duża hipoteza Riemanna, gdyż wówczas twierdzenie Winogradowa zachodzi dla liczb większych od 10^{20}, co pokazał Zinowiew [Z] w 1997 roku, a rozwój komputerów pozwolił na sprawdzenie, że każda liczba nieparzysta przedziału $[9, 10^{20})$ jest sumą trzech liczb pierwszych [DERZ].

W przypadku liczb parzystych wiemy mniej. Od 1937 roku wiadomo [Co], że prawie wszystkie liczby parzyste są sumami 2 liczb pierwszych, tzn. dla liczby $N_2(x)$ liczb parzystych $n \leqslant x$, nie będących takimi sumami mamy

$$\lim_{x\to\infty} \frac{N_2(x)}{x} = 0,$$

a dokładniej

$$N_2(x) \leqslant cx^{0.95}$$

zachodzi z pewną stałą c [Ch2]. Wiemy też (twierdzenie Chena, [Ch1]), że każda dostatecznie duża liczba parzysta da się zapisać w postaci $p+a$, gdzie p jest liczbą pierwszą, zaś a jest bądź liczbą pierwszą, bądź też iloczynem 2 liczb pierwszych.

12. We wrześniu 1740 r. otrzymał Euler list od Filipa Naudé, w którym pytał on o ilość rozkładów liczby naturalnych na sumę zadanej ilości liczb dodatnich, a także o ilość takich rozkładów z nie powtarzającymi się składnikami. Już 23 września 1740 Euler przesłał mu swe rozwiązanie:

Połóżmy

$$P(x,z) = \prod_{j=1}^{\infty}(1+x^j z) = \sum_{m=0}^{\infty} A_m(x) z^m = \sum_{m,n\geqslant 0} N_{m,n} x^m z^n.$$

Wówczas współczynnik $N_{m,n}$ będzie równy ilości przedstawień liczby n, jako sumy m różnych liczb dodatnich, gdyż

$$P(x,z) = \sum_{j_i \text{ różne}} x^{j_1+\cdots+j_s} z^s.$$

Z uwagi na

$$P(x,z) = (1+xz)P(x,xz)$$

otrzymujemy przez indukcję

$$A_m(x) = \frac{x^{m(m+1)/2}}{(1-x)(1-x^2)\cdots(1-x^m)},$$

co pozwala na wyliczenie $N_{m,n}$.

Podobnie, rozpatrując funkcję

$$Q(x,z) = \prod_{i=1}^{\infty} \frac{1}{1+x^i z}$$

znajduje Euler odpowiedź na pierwsze pytanie Naudé.

Pojawiająca się tutaj metoda funkcji tworzących znalazła później wiele zastosowań. Sam Euler w swym podręczniku analizy [E24] podaje kilka. I tak np. dla ilości rozkładów $p(n)$ (tzw. *partycji*) liczby n na sumy liczb dodatnich, o co jeszcze w 1659 pytał Leibniz w liście do Jana Bernoulliego (patrz [DHTN], t. II, str. 101) pokazuje Euler, że funkcja tworząca dla partycji ma prostą postać, a mianowicie

$$1 + \sum_{n=1}^{\infty} p(n)x^n = \frac{1}{\prod_{n=1}^{\infty}(1-x^n)}.$$

Innym typem partycji zajął się Euler w pracy [E14], gdzie pojawia się szereg

$$\sum_{n=1}^{\infty} c_n x^n = \prod_{j=1}^{t}(x + x^2 + \cdots + x^{m_j}),$$

którego n-ty współczynnik jest równy ilości sposobów uzyskania liczby n przy rzucaniu t kostkami mającymi $m_1, m_2, \ldots, m_t$ boków.

Warto tu też przypomnieć znalezioną przez Eulera tożsamość, związaną z tzw. *liczbami pięciokątnymi*, tj. liczbami postaci $(3n^2 \pm n)/2$. W [E21] Euler dowodzi, że jeśli $a_1 = 0, a_2 = 1, \ldots$ jest rosnącym ciągiem wszystkich liczb pięciokątnych, to

$$\prod_{j=1}^{\infty}(1-x^j) = \sum_{j=1}^{\infty}(-1)^{n_j} x^{a_j},$$

przy czym n_j jest określone z równości

$$a_j = \frac{3n^2 \pm n}{2}.$$

13. Euler nigdy nie wydał podręcznika teorii liczb, aczkolwiek w jego notatkach znaleziono dość obszerny tekst [E29] wprowadzający do tej teorii.

Został on opublikowany dopiero w roku 1849. Znajdujemy w nim pełny wykład teorii kongruencji (aczkolwiek bez symbolu "≡", wprowadzonego dopiero przez Gaussa w [G]), a także elementy teorii reszt kwadratowych oraz reszt trzeciego i czwartego stopnia.

Bibliografia[1]

[Be] Bergmann, G., *Über Eulers Beweis des grossen Fermatschen Satzes für den Exponenten* 3, Math. Ann., **164**, 1966, 159–175.

[Ch1] Chen, J.R., *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica, **16**, 1973, 157–176.

[Che2] —, *The exceptional set of Goldbach numbers*, III, Chinese Quart. J. Math., **4**, 1989, 1–15.

[C] Chowla, S., *An extension of Heilbronn's class-number theorem*, Quart. J. Math., Oxford ser., **5**, 1934, 304–307.

[CB] Chowla, S., Briggs, W.E., *On discriminants of binary quadratic forms with a single class in each genus*, Canad. J. Math., **6**, 1954, 463–470.

[Co] Corput, J.G. van der, *Sur l'hypothése de Goldbach pour presque tous les nombres pairs*, å, **2**, 1937, 266–290.

[DERZ] Deshouillers, J.-M., Effinger, G., te Riele, H., Zinoviev, D., *A complete Vinogradov* 3*–primes theorem under the Riemann hypothesis*, Electron. Res. Announc. Amer. Math. Soc., **3**, 1997, 99–104.

[DHTN] Dickson, L.E., *History of Number Theory*, Washington, 1919–1923; reprinty: Stechert 1934, Chelsea 1952.

[D] Dirichlet, P.G.L., *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*. Abh. Kgl. Preuß. Akad. Wiss. Berlin, 1837, 45–81; *Werke*, **I**, 313—-342, Berlin 1889.

[Du] Dujella, A., *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math., **566**, 2004, 183–214.

[El] Elkies, N.D., *On* $A^4 + B^4 + C^4 = D^4$, Math. Comp., **51**, 1988, 825–835.

[E1] Euler, L., *Vollständige Einleitung in die Algebra*, St. Petersburg 1770; *Opera omnia*, $\mathbf{I}_1$.

[E2] —, *Observationis de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*, Comment. Acad. Sci. Petropol., **6**, 1738, 103–107; *Opera Omnia*, $\mathbf{I}_2$, 1–5.

[E3] —, *De solutione problematum diophanteorum per numeros integros*, Comment. Acad. Sci. Petropol., **6**, 1738, 175–188; *Opera Omnia*, $\mathbf{I}_2$, 6–17.

[E4] —, *Solutio problematis arithmetici de inveniendo numero, qui per datos numeros divisus relinquat data residua*, Comment. Acad. Sci. Petropol., **7**, 1740, 46–66; *Opera Omnia*, $\mathbf{I}_2$, 18–32.

[E5] —, *Theorematum quorundam ad numeros primos spectantium demonstratio*, Comment. Acad. Sci. Petropol., **8**, 1741, 141–146; *Opera Omnia*, $\mathbf{I}_2$, 33–37.

[E6] —, *Theorematum quorundam arithmeticorum demonstrationes*, Comment. Acad. Sci. Petropol., **10**, 1747, 125–146; *Opera omnia* , $\mathbf{I}_2$, 38–58.

[1] Przy pracach Eulera podana jest rzeczywista, a nie nominalna, data publikacji.

[E7] —, *De numeris, qui sunt aggregata duorum quadratorum*, Novi Comment. Acad. Sci. Petropol., **4**, 1758, 3–40; *Opera Omnia*, $\mathbf{I}_2$, 295–327.

[E8] —, *Demonstratio theorematis Fermatiani omnem numerorum primum formae* $4n+1$ *esse summum duorum quadratum*, Novi Comment. Acad. Sci. Petropol., **5**, 1760, 3–13; *Opera Omnia*, $\mathbf{I}_2$, 328–337.

[E9] —, *Theoremata circa residua ex divisione potestatum relicta*, Novi Comment. Acad. Sci. Petropol., **7** , 1761, 49–82 ; *Opera Omnia*, $\mathbf{I}_2$, 493–518.

[E10] —, *Theoremata arithmetica nova methodo demonstrata*, Novi Comment. Acad. Sci. Petropol., **8**, 1763, 74–104; *Opera Omnia*, $\mathbf{I}_2$, 531–555.

[E11] —, *De numeris primis valde magnis*, Novi Comment. Acad. Sci. Petropol., **9**, 1764, 99–153, *Opera Omnia*, $\mathbf{I}_3$, 1–45.

[E12] —, *De usu novi algorithmi in problemato Pelliano solvendo*, Novi Comment. Acad. Sci. Petropol., **11**, 1767, 29–66; *Opera Omnia*, I_3, 73—111.

[E13] —, *Quomodo numeri praemagni sint explorandi utrum sint primi necne*, Novi Comment. Acad. Sci. Petropol., **13**, 1769, 67–88; *Opera Omnia*, $\mathbf{I}_3$, 112–130.

[E14] —, *De partitione numerorum in partes tam numero quam species datas*, Novi Comment. Acad. Sci. Petropol., **14**, 1770, 168–187; *Opera omnia*, $\mathbf{I}_3$, 131–147.

[E15] —, *Observationes circa bina biquadrata quorum summam in duam alia biquadrata resolvere liceat*, Novi Comment. Acad. Sci. Petropol., **17**, 1773, 64–69; *Opera omnia*, $\mathbf{I}_3$, 211–217.

[E16] —, *Novae demonstrationes circa resolutionem numerorum in quadrata*, Nova Acta Eruditorum 1773, 193–211; *Opera omnia*, $\mathbf{I}_3$, 218–239.

[E17] —, *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, Novi Comment. Acad. Sci. Petropol., **18**, 1774, 85–135, *Opera Omnia*, $\mathbf{I}_3$, 240–281.

[E18] —, *Extrait d'une lettre de M.Euler le pére à M.Bernoulli concernant la mémoire imprimé parmi ceux de 1771 p.318*, Nouv. Mém. Acad. Berlin, 1772/1774, 35–36; *Opera Omnia*, $\mathbf{I}_3$, 335–337.

[E19] —, *Observationes circa divisionem quadratorum per numeros primos*, Opuscula varii argumenti, **1**, 1783, 64–84; *Opera Omnia*, $\mathbf{I}_3$, 497–512.

[E20] —, *Extrait d'une lettre de M. Euler à M. Beguelin*, Nouv. Mém. Acad. Sci. Berlin, 1776–1779, 337–339; *Opera omnia* , $\mathbf{I}_3$, 418–420.

[E21] —, *Evolutio producti infiniti* $(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)$ *in seriem simplicem*, Acta Acad. Sci. Petropol., 1780/1783, 47–55; *Opera omnia*, $\mathbf{I}_3$, 472–479.

[E22] —, *Miscellanea analytica*, Opuscula analytica, **1**, 1783, 329–344; *Opera Omnia*, $\mathbf{I}_4$, 91–104.

[E23] —, *Speculationes circa quasdam insignes proprietates numerorum*, Acta Acad. Sci. Petropol., **4**, 1784, 18–30; *Opera Omnia*, $\mathbf{I}_4$, 105–115.

[E24] —, *Introductio in analysin infinitorum*, Petropoli 1748; *Opera Omnia*, $\mathbf{I}_8$, $\mathbf{I}_9$.

[E25] —, *De summis serierum reciprocarum*, Comment. Acad. Sci. Petropol., **7**, 1740, 123–134; *Opera Omnia*, $\mathbf{I}_{14}$, 73–86.

[E26] — *Variae observationes circa series infinitas*, Comment. Acad. Sci. Petropol., **9**, 1744, 160–188; *Opera Omnia*, $\mathbf{I}_{14}$, 216–244.

[E27] —, *De seriebus quibusdam considerationes*, Comment. Acad. Sci. Petropol., **12**, 53–96, 1750; *Opera omnia*, $\mathbf{I}_{14}$, 407–462.

[E28] —, *Remarques sur un beau rapport entre les series des puissances tant directes que reciproques*, Mémoires Acad. Sci. Berlin, **17**, 1768, 83–106; *Opera omnia*, $\mathbf{I}_{15}$, 70–90.

[E29] —, *Tractatus de numerorum doctrina capita sedecim, quae supersunt*, Commentationes arithmeticae, **2**, 1849, 503–575, *Opera omnia*, $\mathbf{I}_5$, 182–283.

[E30] —, *Illustratio paradoxi circa progressionem numerorum idoneorum sive congruorum*, Novi Acta Acad. Sci. Petropol., **15**, 1806, 29–32; *Opera omnia*, $\mathbf{I}_4$, 395–398.

[F] Fuss, P.-H., *Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIéme siécle*, St.Pétersbourg 1843; reprint: Johnson 1968.

[G] Gauss, C.F., *Disquisitiones arithmeticae*, Gottingae 1801.

[Gi] Gibbs, P., *Some rational Diophantine sextuples*, Glasnik mat., **41**, 2006, 195–203.

[Gr] Grube, F., *Ueber einige Euler'sche Sätze aus der Theorie der quadratischen Formen*, Zeitschr. Math. Phys., (5) **19**, 1874, 492–519.

[H] Heegner, H., *Diophantische Analysis und Modulfunktionen*, Math. Z., **56**, 1952, 227–253.

[J] Jacobi, C.G.J., *Fundamenta nova theoriae functionum ellipticarum*, Regiomontani 1829; *Gesammelte Werke*, **1**, 49–239, Berlin 1881; reprint: Chelsea 1969.

[La] Lagrange, J.L., *Démonstration d'un théorème d'arithmétique*, Oeuvres, **3**, 189–201, Paris 1869.

[Le] Legendre, A.M., *Essai sur la théorie des nombres*, Paris 1798; 2 wyd. 1808, 3 wyd. (pod tytułem *Théorie des Nombres*), 1830.

[LP] Lander, L.J., Parkin, T.R., *Counterexample to Euler's conjecture on sums of like powers*, Bull. Amer. Math. Soc., **72**, 1966, str. 1079.

[Ra] Rabinowitsch, G., *Eindeutigkeit der Zerlegung in Primfaktoren in quadratischen Zahlkörpern*, J. Reine Angew. Math., **142**, 1913, 153–164.

[Rie] Riemann, B., *Ueber die Anzahl der Primzahlen unter einer gegebener Größe*, Monatsber. Kgl. Preuß. Akad. Wiss. Berlin, 1860, 671–680.

[S] Stark, H.M., *A complete determination of the complex quadratic fields of class-number one*, Michigan J. Math., **14**, 1967, 1–27.

[W] Weil, A., *Number Theory, An approach through history*, Birkhäuser 1983.

[WC] Wang, T., Chen, J.-R., *On odd Goldbach problem under general Riemann hypothesis*, Science in China, A, **36**, 1993, 682–691.

[Wi] Winogradow, I.M., *Представление нечетного числа в теории чисел*, Dokl. Akad. Nauk SSSR, **15**, 1937, 291–294.

[WJ] Winters, E., Juškevič, A.P., (wydawcy), *Leonhard Euler und Christian Goldbach: Briefwechsel 1729-1764*, Akademie-Verlag, 1965.

[Z] Zinoview, D., *On Vinogradov's constant in Goldbach's ternary problem*, J. Number Theory, **65**, 1997, 334–358.

Władysław Narkiewicz

Instytut Matematyczny
Uniwersytet Wrocławski
e-mail: narkiew@math.uni.wroc.pl