O niektórych twierdzeniach Eulera

Wykład dla nauczycieli z okazji finału II Olimpiady Matematycznej Gimnazjalistów 2007

Wojciech GUZICKI, Warszawa

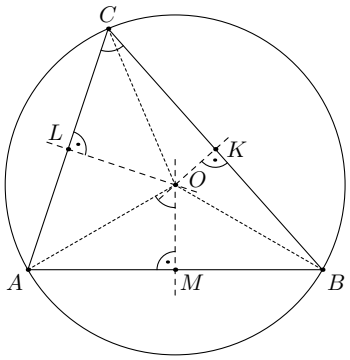
W tym roku obchodzimy 300-ną rocznicę urodzin wielkiego XVIII-wiecznego matematyka Leonharda Eulera (ur. 15.4.1707 w Bazylei, zm. 18.9.1783 w Petersburgu). Z tej okazji pokażę kilka twierdzeń i dowodów pochodzących od Eulera i możliwych do zaprezentowania uczniom. Twierdzenia te pochodzą z kilku działów matematyki: geometrii, teorii liczb i kombinatoryki.

Część I: geometria.

Pokażemy dwa twierdzenia pochodzące od Eulera oraz dowód Eulera wzoru Herona na pole trójkąta. Zaczniemy od twierdzeń dotyczących położenia tzw. punktów szczególnych trójkąta.

Punkty szczególne trójkąta.

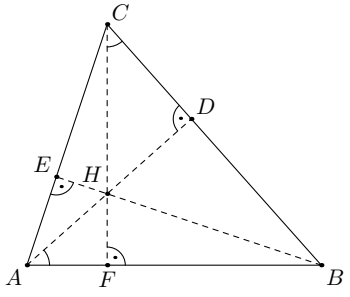
W każdym trójkącie pewne trzy proste przecinają się w jednym punkcie; takie punkty przecięcia nazywamy **punktami szczególnymi** trójkąta. Przypomnijmy teraz cztery podstawowe punkty szczególne. Pierwszym z nich jest **środek okręgu opisanego**, będący punktem przecięcia symetralnych boków trójkąta:



Proste KO, LO i MO są symetralnymi boków trójkąta ABC. Z własności symetralnych wynika, że odcinki AO, BO i CO są równej długości; są to promienie okręgu opisanego. Jeśli trójkąt ABC jest ostrokątny, to środek okręgu opisanego leży wewnątrz trójkąta (tak jak na powyższym rysunku). Z twierdzenia o kącie wpisanym i środkowym wynika wtedy na przykład, że $\measuredangle AOB = 2 \cdot \measuredangle ACB$. Ponieważ trójkąt ABO jest równoramienny, więc

$$\measuredangle AOM = \frac{1}{2} \cdot \measuredangle AOB = \measuredangle ACB.$$

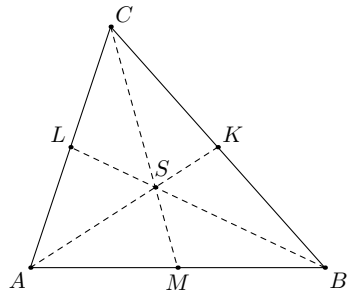
Drugim punktem szczególnym trójkąta jest punkt przecięcia wysokości (dokładniej: prostych zawierających wysokości). Ten punkt nazywamy **ortocentrum** trójkąta.



Odcinki AD, BE i CF są wysokościami trójkąta ABC. Jeśli trójkąt jest ostrokątny, to jego ortocentrum (na powyższym rysunku punkt H) leży wewnątrz trójkąta. Nietrudno dostrzec na tym rysunku pewne pary kątów równych. Na przykład

$$\measuredangle BAD = 90^\circ - \measuredangle ABD = 90^\circ - \measuredangle EBC = \measuredangle ECB.$$

Trzecim punktem szczególnym trójkąta jest punkt przecięcia środkowych. Ten punkt nazywamy **środkiem ciężkości** trójkąta.

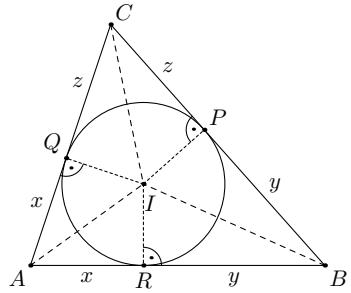


Ważną własnością środka ciężkości jest to, że dzieli on każdą środkową w stosunku $2:1$:

$$\frac{AS}{SK} = \frac{BS}{SL} = \frac{CS}{SM} = 2.$$

Ponieważ istnieje tylko jeden punkt dzielący odcinek w danym stosunku, więc do udowodnienia, że dany punkt S jest środkiem ciężkości, wystarcza pokazać, że na przykład $CS : SM = 2 : 1$.

Ostatnim z rozważanych punktów szczególnych jest punkt przecięcia dwusiecznych kątów trójkąta. Ten punkt nazywamy **środkiem okręgu wpisanego** w trójkąt.



Półproste AI, BI i CI są dwusiecznymi kątów trójkąta. Punkty P, Q i R są punktami styczności okręgu wpisanego z bokami trójkąta. Z twierdzenia o odcinkach stycznych do okręgu wynika, że

$$AQ = AR = x, \quad BP = BR = y \quad \text{oraz} \quad CP = CQ = z.$$

Przyjmijmy oznaczenia:

$$a = BC, \quad b = AC, \quad c = AB, \quad p = \frac{a+b+c}{2}$$

$$\text{oraz} \quad r = AI = BI = CI.$$

Zatem obwód trójkąta ABC jest równy $2p$. Zauważmy, że $p = x + y + z$. Stąd wynika, że

$$x = (x+y+z) - (y+z) = p - a,$$
$$y = (x+y+z) - (x+z) = p - b,$$
$$z = (x+y+z) - (x+y) = p - c.$$

Wreszcie zauważmy, że pole trójkąta ABC jest sumą pól trzech trójkątów: BCI, CAI oraz ABI. Zatem

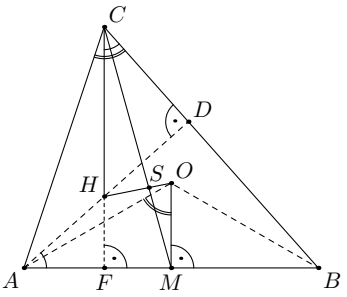
$$P_{ABC} = \frac{ar}{2} + \frac{br}{2} + \frac{cr}{2} = pr.$$

Prosta Eulera.

Udowodnimy teraz twierdzenie Eulera dotyczące położenia pierwszych trzech punktów szczególnych trójkąta:

Twierdzenie 1. Ortocentrum H, środek ciężkości S i środek O okręgu opisanego na trójkącie leżą na jednej prostej (nazywanej dziś **prostą Eulera**), przy czym punkt S dzieli odcinek HO w stosunku $2:1$, tzn. $HS = 2 \cdot OS$.

Dowód. Dla ustalenia uwagi przyjmiemy, że trójkąt ABC jest ostrokątny i skorzystamy z zauważonych wyżej równości kątów. Niewielką modyfikację dowodu dla innych trójkątów pozostawimy jako ćwiczenie. Niech punkt H będzie ortocentrum trójkąta ABC, punkt O środkiem okręgu opisanego na tym trójkącie i punkt S punktem przecięcia odcinków HO i CM. Wykażemy, że punkt S jest środkiem ciężkości trójkąta ABC.



Po pierwsze, mamy równość $\measuredangle HCD = \measuredangle ECB = \measuredangle BAD$. Wynika z niej, że trójkąty CDH i ADB są podobne (oba są prostokątne i mają parę równych kątów ostrych). Zatem

$$\frac{CD}{CH} = \frac{AD}{AB}, \quad \text{czyli} \quad CH = \frac{AB \cdot CD}{AD}.$$

Po drugie, mamy równość $\measuredangle ACD = \measuredangle ACB = \measuredangle AOM$. Wynika z niej, podobnie jak wyżej, że trójkąty ACD i AOM są podobne. Mamy stąd równość

$$\frac{CD}{AD} = \frac{OM}{AM},$$

czyli

$$OM = \frac{AM \cdot CD}{AD} = \frac{\frac{1}{2}AB \cdot CD}{AD} = \frac{1}{2} \cdot CH.$$

Wreszcie, odcinki CH i OM są równoległe, skąd wynika, że trójkąty CHS i MOS są podobne (mają parę równych kątów wierzchołkowych i dwie pary równych kątów naprzemianległych). Stąd dostajemy proporcję

$$\frac{CS}{CH} = \frac{MS}{OM},$$

z której wynika, że

$$CS = MS \cdot \frac{CH}{OM} = 2 \cdot MS.$$

Punkt S dzieli zatem odcinek CM w stosunku $2:1$, a więc rzeczywiście jest środkiem ciężkości trójkąta ABC, c. b. d. o.

Nierówność Eulera.

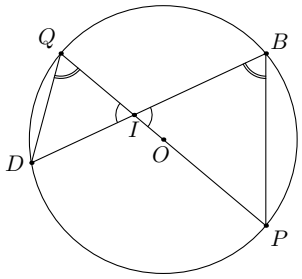
Zajmiemy się teraz położeniem środków obu okręgów: opisanego i wpisanego. Wnioskiem z przeprowadzonych rozważań będzie tzw. **nierówność Eulera** między promieniami tych okręgów.

Twierdzenie 2. Dany jest trójkąt ABC. Punkt O jest środkiem okręgu opisanego o promieniu R, punkt I jest środkiem okręgu wpisanego o promieniu r. Niech d będzie długością odcinka OI. Wtedy $d^2 = R^2 - 2Rr$ oraz $R \geq 2r$.

Przed przystąpieniem do dowodu udowodnimy następujący lemat.

Lemat. Dany jest okrąg o środku O i promieniu R oraz punkt I leżący wewnątrz tego okręgu, w odległości d od środka. Niech BD będzie dowolną cięciwą tego okręgu przechodzącą przez punkt I. Wtedy $BI \cdot DI = R^2 - d^2$.

Dowód. Poprowadźmy średnicę PQ przechodzącą przez punkt I.



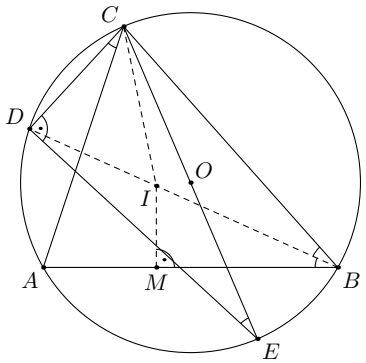
Trójkąty IBP oraz IQD są podobne: $\measuredangle DIQ = \measuredangle PIB$ (kąty wierzchołkowe) oraz $\measuredangle DQI = \measuredangle PBI$ (kąty wpisane). Zatem

$$\frac{BI}{PI} = \frac{QI}{DI},$$

skąd wynika, że

$$BI \cdot DI = PI \cdot QI = (R+d) \cdot (R-d) = R^2 - d^2.$$

Dowód twierdzenia. Niech D będzie punktem przecięcia dwusiecznej BI z okręgiem opisanym na trójkącie ABC i niech CE będzie średnicą tego okręgu opisanego. Niech wreszcie punkt M będzie rzutem punktu I na bok AB.



Punkt M jest oczywiście punktem styczności okręgu wpisanego z bokiem AB, a więc $MI = r$. Ponieważ odcinek CE jest średnicą okręgu opisanego na trójkącie ABC, więc $\measuredangle EDC = 90^\circ$ oraz $CE = 2R$. Zauważmy

następnie, że z twierdzenia o kątach wpisanych wynika, że

$$\measuredangle DCA = \measuredangle DBA = \measuredangle DBC = \measuredangle DEC.$$

Stąd i z twierdzenia o kącie zewnętrznym trójkąta dostajemy równość

$$\measuredangle DCI = \measuredangle DCA + \measuredangle ACI = \measuredangle DBC + \measuredangle BCI = \\ = \measuredangle CBI + \measuredangle BCI = \measuredangle DIC.$$

Trójkąt ICD jest zatem równoramienny: $DC = DI$. Teraz zauważamy, że trójkąty BMI oraz EDC są podobne: oba są prostokątne i $\measuredangle DEC = \measuredangle MBI$. Zatem

$$\frac{DC}{CE} = \frac{MI}{BI},$$

czyli

$$\frac{DI}{CE} = \frac{MI}{BI}.$$

Stąd wynika, że

$$BI \cdot DI = CE \cdot MI.$$

Z lematu otrzymujemy równość

$$R^2 - d^2 = 2R \cdot r,$$

czyli $d^2 = R^2 - 2Rr$. Ponieważ $d^2 \geq 0$, więc $R^2 \geq 2Rr$, czyli $R \geq 2r$, c. b. d. o.

Wzór Herona.

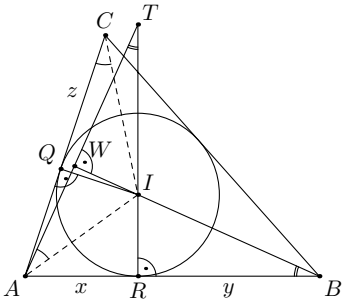
W I wieku Heron z Aleksandrii udowodnił następujące twierdzenie:

Twierdzenie 3. Pole trójkąta o bokach długości a, b i c wyraża się wzorem

$$P = \sqrt{p(p-a)(p-b)(p-c)},$$

gdzie $2p = a + b + c$.

Dowód Herona był dość skomplikowany i Euler podał dowód znacznie prostszy. Podamy teraz szkic dowodu Eulera. Niech punkt W będzie rzutem punktu A na dwusieczną BI. Punkty Q i R są punktami styczności okręgu wpisanego z bokami AC i AB trójkąta ABC.



Jak pamiętamy,

$$AR = x = p - a, \quad BR = y = p = b \\ \text{oraz} \quad CQ = z = p - c.$$

Nietrudno zauważyć, że $\measuredangle WAI = \measuredangle ICQ$ oraz $\measuredangle ATR = \measuredangle ABW$. Wynika stąd, że

$$\triangle IAW \sim \triangle ICQ, \quad \triangle TIW \sim \triangle BAW \\ \text{oraz} \quad \triangle ATR \sim \triangle BIR.$$

Mamy zatem

$$\frac{AW}{WI} = \frac{CQ}{QI} = \frac{z}{r} \quad \text{oraz} \quad \frac{WI}{TI} = \frac{AW}{AB},$$

czyli

$$\frac{z}{r} = \frac{AW}{WI} = \frac{AB}{TI} = \frac{x+y}{TR-r}.$$

Stąd wynika, że $z \cdot (TR - r) = r \cdot (x + y)$, czyli $z \cdot TR = rx + ry + rz = pr$. Z podobieństwa trójkątów ATR i BIR otrzymujemy równość

$$\frac{TR}{AR} = \frac{BR}{IR},$$

czyli

$$TR = \frac{xy}{r}.$$

Zatem

$$\frac{xyz}{r} = pr,$$

czyli $xyz = pr^2$. Mnożąc obie strony tej równości przez p, otrzymujemy

$$(P_{ABC})^2 = (pr)^2 = pxyz = p(p-a)(p-b)(p-c),$$

czyli

$$P_{ABC} = \sqrt{p(p-a)(p-b)(p-c)},$$

c. b. d. o.

Część II: teoria liczb.

Zanim zajmiemy się osiągnięciami Eulera w teorii liczb, wyprowadzimy ważny wzór, z którego kilkakrotnie skorzystamy. Niech a będzie dowolną liczbą rzeczywistą różną od jedności ($a \neq 1$). Wówczas dla dowolnej liczby naturalnej n mamy równość

$$1 + a + a^2 + a^3 + \ldots + a^{n-1} + a^n = \frac{a^{n+1} - 1}{a - 1}.$$

Oznaczmy bowiem sumę po lewej stronie literą S. Mamy wówczas

$$S = 1 + a + a^2 + a^3 + \ldots + a^{n-1} + a^n = \\ = 1 + a(1 + a + 2^2 + \ldots + a^{n-2} + a^{n-1}) = \\ = 1 + a(S - a^n).$$

Otrzymaliśmy zatem równanie $S = 1 + a(S - a^n)$, czyli

$$S = 1 + aS - a^{n+1}, \\ a^{n+1} - 1 = aS - S, \\ (a-1)S = a^{n+1} - 1, \\ S = \frac{a^{n+1} - 1}{a - 1}.$$

Z otrzymanego wzoru wyprowadzimy dwa ważne wnioski. Po pierwsze, dla $a = 2$ otrzymujemy równość

$$1 + 2 + 4 + 8 + \ldots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$

Po drugie, jeśli liczba a jest całkowita, to suma S też jest liczbą całkowitą. Wynika stąd, że liczba $a - 1$ jest dzielnikiem liczby $a^{n+1} - 1$ dla dowolnej liczby naturalnej n. W szczególności, jeśli liczba d jest dzielnikiem $a - 1$ to dla każdego n jest też dzielnikiem $a^n - 1$. Po trzecie, dla $n = 2m$ otrzymujemy

$$1 - a + a^2 - a^3 + a^4 - \ldots + a^{2m-2} - a^{2m-1} + a^{2m} = \\ = \frac{a^{2m+1} + 1}{a + 1}.$$

Mianowicie, jeśli sumę po lewej stronie oznaczymy literą S, to otrzymamy:

$$\begin{aligned} S &= 1-a+a^2-a^3+a^4-\ldots+a^{2m-2}-a^{2m-1}+a^{2m} = \\ &= 1+(-a)+(-a)^2+(-a)^3+\ldots+ \\ &\quad +(-a)^{2m-2}+(-a)^{2m-1}+(-a)^{2m} = \\ &= \frac{(-a)^{2m+1}-1}{(-a)-1} = \frac{-a^{2m+1}-1}{-a-1} = \\ &= \frac{a^{2m+1}+1}{a+1}. \end{aligned}$$

W szczególności, jeśli liczba a jest całkowita, to suma S jest też liczbą całkowitą i stąd wynika, że liczba $a^{2m+1}+1$ dzieli się bez reszty przez liczbę $a+1$. Stąd z kolei wynika, że jeśli liczba $a+1$ dzieli się przez liczbę n, to liczba $a^{2m+1}+1$ też dzieli się przez n.

Małe twierdzenie Fermata.

w liście datowanym 18 października 1640 roku (adresatem był Bernard Frénicle de Bessy) Fermat napisał, że udowodnił następujące twierdzenie, nazywane **małym twierdzeniem Fermata**:

Twierdzenie 4. Jeśli p jest liczbą pierwszą oraz a jest liczbą całkowitą niepodzielną przez p, to p jest dzielnikiem liczby $a^{p-1}-1$.

Szczególne przypadki małego twierdzenia Fermata (dla małych liczb pierwszych) można łatwo udowodnić. Na przykład:

1) Jeśli liczba a nie jest podzielna przez 3, to liczba a^2-1 jest podzielna przez 3. Wystarczy bowiem zauważyć, że wśród trzech kolejnych liczb: $a-1$, a oraz $a+1$ jedna jest podzielna przez 3. Ale liczba a nie jest podzielna przez 3, więc jedna z liczb $a-1$ oraz $a+1$ jest podzielna przez 3. Stąd wynika, że liczba $a^2-1=(a-1)(a+1)$ jest podzielna przez 3.

2) Jeśli liczba a nie jest podzielna przez 5, to liczba a^4-1 jest podzielna przez 5. Tym razem zauważamy, że wśród pięciu kolejnych liczb: $a-2$, $a-1$, a, $a+1$ oraz $a+2$ jedna jest podziedlna przez 5. Znów liczba a nie jest podzielna przez 5. Zatem jedna z pozostałych czterech liczb jest podzielna przez 5. Stąd wynika, że iloczyn

$$\begin{aligned} (a-2)(a-1)(a+1)(a+2) &= (a^2-4)(a^2-1) = \\ &= a^4-5a^2+4 \end{aligned}$$

jest podzielny przez 5. A więc liczba

$$a^4-1=(a-2)(a-1)(a+1)(a+2)+5a^2-5$$

też jest podzielna przez 5.

3) Jeśli liczba a nie jest podzielna przez 7, to liczba a^6-1 jest podzielna przez 7. Postępujemy podobnie i tym razem skorzystamy z nietrudnej do sprawdzenia tożsamości:

$$\begin{aligned} a^6-1 = (a-3)(a-2)(a-1)(a+1)(a+2)(a+3)+ \\ +14a^4-49a^2+35. \end{aligned}$$

Z łatwością zauważamy, że liczba po prawej stronie jest podzielna przez 7.

Nie znamy oryginalnego dowodu Fermata. We wspomnianym liście napisał on bowiem, że nie chciałby on niepotrzebnie tego listu wydłużać, więc dowód pominie. Pierwszy dowód małego twierdzenia Fermata opublikował Euler, choć wiemy, że to twierdzenie umiał udowodnić Leibniz przed rokiem 1683 (dowód znajduje się w nieopublikowanym rękopisie).

Dowód tego twierdzenia pominiemy, natomiast zobaczymy, jak to twierdzenie zostało użyte do rozwiązania innego problemu postawionego przez Fermata.

Liczby Fermata.

Fermat przypuszczał, że wszystkie liczby F_n dane wzorem

$$F_n = 2^{2^n}+1$$

są liczbami pierwszymi (takie liczby nazywamy dziś **liczbami Fermata**). Tak jest w istocie dla $n \le 4$:

$$\begin{aligned} n=0: &\quad F_n = 2^{2^0}+1 = 2^1+1 = 3, \\ n=1: &\quad F_n = 2^{2^1}+1 = 2^2+1 = 5, \\ n=2: &\quad F_n = 2^{2^2}+1 = 2^4+1 = 17, \\ n=3: &\quad F_n = 2^{2^3}+1 = 2^8+1 = 257, \\ n=4: &\quad F_n = 2^{2^4}+1 = 2^{16}+1 = 65537. \end{aligned}$$

Nietrudno sprawdzić, że liczby 3, 5, 17, 257 i 65537 są liczbami pierwszymi. Jednak sprawdzenie tego dla $n=5$ przekraczało już cierpliwość Fermata, gdyż

$$F_5 = 2^{2^5}+1 = 2^{32}+1 = 4\,294\,967\,297.$$

W 1732 roku Euler znalazł dzielnik pierwszy tej dużej liczby:

$$4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Czyżby Euler miał więcej cierpliwości, dłużej szukał dzielnika liczby F_5 i wreszcie znalazł go? Było inaczej. Otóż Euler udowodnił twierdzenie o postaci dzielników pierwszych liczb Fermata. Popatrzmy teraz, jak takie twierdzenie może wyglądać.

Lemat 1. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a+1$, to p jest liczbą nieparzystą, czyli jest postaci $p=2k+1$ dla pewnej liczby całkowitej k.

Dowód. Ponieważ a jest liczbą parzystą, więc $a+1$ jest liczbą nieparzystą, a więc nie dzieli się przez 2. Zatem $p \neq 2$, czyli p jest liczbą nieparzystą.

Lemat 2. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem a^2+1, to p jest postaci $p=4k+1$ dla pewnej liczby całkowitej k.

Dowód. Liczba a^2 jest parzysta oraz p jest dzielnikiem a^2+1. Z lematu 1 wynika zatem, że p jest liczbą nieparzystą: $p=2\ell+1$ dla pewnej liczby całkowitej ℓ. Jeśli $\ell=2k$ dla pewnej liczby k, to $p=4k+1$ i dowód lematu będzie zakończony. Jeśli zaś $\ell=2k+1$, to $p=4k+3$. Wykażemy, że ta druga możliwość nie może mieć miejsca.

Przypuśćmy więc, że $p=4k+3$. Ponieważ p jest dzielnikiem a^2+1, więc nie jest dzielnikiem a. Z małego

twierdzenia Fermata wynika zatem, że p jest dzielnikiem liczby $a^{p-1}-1$. Zauważmy teraz, że

$$a^{p-1}-1 = a^{4k+2}-1.$$

Ponieważ p jest dzielnikiem a^2+1, więc jest też dzielnikiem $(a^2)^{2k+1}+1$. Ale

$$(a^2)^{2k+1}+1 = a^{2(2k+1)}+1 = a^{4k+2}+1,$$

więc p jest dzielnikiem liczby $a^{4k+2}+1$. Zatem p jest dzielnikiem różnicy

$$\left(a^{4k+2}+1\right)-\left(a^{4k+2}-1\right)=2.$$

Stąd wynika, że $p=2$, co jest niemożliwe.

Pokazaliśmy zatem, że niemożliwe jest, by $p=4k+3$; pozostaje więc tylko możliwość pierwsza: $p=4k+1$ dla pewnej liczby całkowitej k.

Lemat 3. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem a^4+1, to p jest postaci $p=8k+1$ dla pewnej liczby całkowitej k.

Dowód. Ponieważ $a^4=(a^2)^2$ oraz p jest dzielnikiem a^4+1, więc z lematu 1 wynika, że p jest liczbą postaci $p=4\ell+1$ dla pewnej liczby całkowitej ℓ. Jeśli $\ell=2k$ dla pewnej liczby k, to $p=8k+1$ i dowód lematu będzie zakończony. Jeśli zaś $\ell=2k+1$, to $p=8k+5$. Wykażemy, że ta druga możliwość nie może mieć miejsca.

Przypuśćmy więc, że $p=8k+5$. Ponieważ p jest dzielnikiem a^4+1, więc nie jest dzielnikiem a. Z małego twierdzenia Fermata wynika zatem, że p jest dzielnikiem liczby $a^{p-1}-1$. Zauważmy teraz, że

$$a^{p-1}-1 = a^{8k+4}-1.$$

Zatem p jest dzielnikiem liczby $a^{8k+4}-1$.

Ponieważ p jest dzielnikiem a^4+1, więc jest też dzielnikiem $(a^4)^{2k+1}+1$. Ale

$$(a^4)^{2k+1}+1 = a^{4(2k+1)}+1 = a^{8k+4}+1,$$

więc p jest dzielnikiem liczby $a^{8k+4}+1$. Zatem p jest dzielnikiem różnicy

$$\left(a^{8k+4}+1\right)-\left(a^{8k+4}-1\right)=2.$$

Stąd wynika, że $p=2$, co jest niemożliwe.

Pokazaliśmy zatem, że niemożliwe jest, by $p=8k+5$; pozostaje więc tylko możliwość pierwsza: $p=8k+1$ dla pewnej liczby całkowitej k.

W podobny sposób można udowodnić kolejne lematy (szczegóły dowodów pozostawimy Czytelnikowi):

Lemat 4. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem a^8+1, to p jest postaci $p=16k+1$ dla pewnej liczby całkowitej k.

Lemat 5. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a^{16}+1$, to p jest postaci $p=32k+1$ dla pewnej liczby całkowitej k.

Lemat 6. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a^{32}+1$, to p jest postaci $p=64k+1$ dla pewnej liczby całkowitej k.

Czytelnik znający zasadę indukcji udowodni bez trudu twierdzenie ogólne:

Twierdzenie 5. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a^{2^n}+1$, gdzie n jest liczbą naturalną, to p jest postaci $p=2^{n+1}k+1$ dla pewnej liczby całkowitej k.

Teraz poszukiwanie dzielnika pierwszego liczby F_5 jest znacznie łatwiejsze. Popatrzmy na kolejne liczby k:

k=1: p=64k+1=65=5·13 nie jest liczbą pierwszą,

k=2: p=64k+1=129=3·43 nie jest liczbą pierwszą,

k=3: p=64k+1=193 jest liczbą pierwszą, ale nie jest dzielnikiem F_5,

k=4: p=64k+1=257 jest liczbą pierwszą, ale nie jest dzielnikiem F_5,

k=5: p=64k+1=321=3·107 nie jest liczbą pierwszą,

k=6: p=64k+1=385=5·77 nie jest liczbą pierwszą,

k=7: p=64k+1=449 jest liczbą pierwszą, ale nie jest dzielnikiem F_5,

k=8: p=64k+1=513=3·171 nie jest liczbą pierwszą,

k=9: p=64k+1=577 jest liczbą pierwszą, ale nie jest dzielnikiem F_5.

Wreszcie dla $k=10$ otrzymujemy dzielnik pierwszy $p=64k+1=641$ liczby F_5. Zauważmy, że znaleziony dzielnik 641 jest piątą z kolei liczbą pierwszą, przez którą musieliśmy dzielić liczbę F_5. Euler w istocie udowodnił nieco mocniejsze twierdzenie (którego dowód jest znacznie trudniejszy):

Twierdzenie 6. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a^{2^n}+1$, gdzie n jest liczbą naturalną, to p jest postaci $p=2^{n+2}k+1$ dla pewnej liczby całkowitej k.

Zauważmy, że z tego twierdzenia wynika, że dzielniki pierwsze liczby F_5 mają postać $p=128k+1$ i okazuje się, że liczba 641 była drugą z kolei liczbą pierwszą, przez którą Euler musiał dzielić liczbę F_5. Widzimy więc, że znalezienie tego dzielnika nie było wyłącznie wynikiem wielkiej cierpliwości, której zabrakło Fermatowi, ale było rezultatem przenikliwego rozumowania, które znacznie skróciło czas potrzebny na wykonanie obliczeń.

Przypuszczenie Fermata okazało się nieprawdziwe: liczba F_5 jest złożona. A jakie są pozostałe liczby Fermata? W 1880 roku F. Landry podał rozkład na czynniki pierwsze liczby F_6:

$$F_6 = 2^{64}+1 = 18\,446\,744\,073\,709\,551\,617 = \\ = 274\,177\cdot 67\,280\,421\,310\,721$$

(ten rozkład znał już wcześniej T. Clausen i napisał go w liście do Gaussa z 1 stycznia 1856 r.). Na rozkład następnej liczby Fermata też trzeba było czekać: w 1970 roku Brillhart i Morrison za pomocą obliczeń komputerowych i bardzo wyrafinowanego algorytmu pokazali, że

$$F_7 = 2^{128}+1 = \\ = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457 = \\ = 59\,649\,589\,127\,497\,217\cdot 5\,704\,689\,200\,685\,129\,054\,721.$$

O obu tych liczbach już wcześniej wiedziano, że są złożone, gdyż w 1877 roku T. Pepin znalazł test pozwalający stwierdzić, czy liczba Fermata jest pierwsza, bez konieczności znajdowania jej dzielników. Dziś znamy wiele liczb złożonych Fermata, znamy rozkłady niektórych z nich na iloczyn liczb pierwszych, ale nie znaleźliśmy żadnej innej liczby pierwszej oprócz pięciu podanych na początku. Zdumiewający związek liczb pierwszych Fermata z konstrukcjami geometrycznymi wielokątów foremnych odkrył Gauss, ale to już powinien być temat innego wykładu.

Liczby doskonałe.

Starożytni Grecy ze szczególną uwagą traktowali **liczby doskonałe**. Liczbą doskonałą nazywamy liczbę, która jest sumą swoich dzielników (oprócz największego – jej samej). Przykładami takich liczb są:

$$\begin{aligned} 6 &= 1+2+3,\\ 28 &= 1+2+4+7+14,\\ 496 &= 1+2+4+8+16+31+62+124+248,\\ 8128 &= 1+2+4+8+16+32+64+127+245+\\ &\quad +508+1016+2032+4064. \end{aligned}$$

Te cztery liczby doskonałe były znane już w starożytności. Euklides udowodnił bardzo ważne twierdzenie pokazujące, w jaki sposób można konstruować takie liczby. Zanim udowodnimy to twierdzenie, przyjmiemy wygodne oznaczenie. Mianowicie symbolem $\sigma(n)$ będziemy oznaczać sumę wszystkich dzielników dodatnich liczby n (wraz z nią samą). Zatem liczba n jest doskonała wtedy i tylko wtedy, gdy $\sigma(n) = 2n$. A oto twierdzenie Euklidesa:

Twierdzenie 7. Jeśli liczba $2^p - 1$ jest pierwsza, to liczba $n = 2^{p-1}(2^p - 1)$ jest doskonała.

Dowód. Ponieważ liczba $q = 2^p - 1$ jest pierwsza, więc jedynymi dzielnikami liczby $n = 2^{p-1}q$ są liczby

$$\begin{array}{cccccccc} 1, & 2, & 4, & 8, & \ldots & 2^{p-2}, & 2^{p-1},\\ q, & 2q, & 4q, & 8q, & \ldots & 2^{p-2}q, & 2^{p-1}q. \end{array}$$

Mamy zatem

$$\begin{aligned} \sigma(n) &= (1+2+4+\ldots+2^{p-1}) +\\ &\quad + q(1+2+4+\ldots+2^{p-1}) =\\ &= (q+1)(1+2+4+\ldots+2^{p-1}) = 2^p(2^p-1) =\\ &= 2\cdot 2^{p-1}(2^p-1) =\\ &= 2n, \end{aligned}$$

c. b. d. o.

Twierdzenie Euklidesa skłania nas do zadania dwóch pytań:

1) Które liczby postaci $2^p - 1$ są liczbami pierwszymi?

2) Czy każda liczba doskonała jest postaci takiej jak w twierdzeniu Euklidesa?

Na pierwsze pytanie możemy łatwo dać odpowiedź częściową. Okazuje się, że jeśli liczba $2^p - 1$ jest pierwsza, to liczba p też jest pierwsza. Gdyby bowiem liczba p była złożona: $p = k\ell$ (gdzie $1 < k < p$), to liczba $2^k - 1$ byłaby dzielnikiem liczby

$$(2^k)^\ell - 1 = 2^{k\ell} - 1 = 2^p - 1.$$

Popatrzmy zatem jeszcze raz na nasze cztery przykłady liczb doskonałych:

1) Dla $p = 2$ otrzymujemy liczbę pierwszą $2^p - 1 = 3$. Zatem liczba $2^1(2^2 - 1) = 2 \cdot 3 = 6$ jest doskonała.

2) Dla $p = 3$ otrzymujemy liczbę pierwszą $2^p - 1 = 7$. Zatem liczba $2^2(2^3 - 1) = 4 \cdot 7 = 28$ jest doskonała.

3) Dla $p = 5$ otrzymujemy liczbę pierwszą $2^p - 1 = 31$. Zatem liczba $2^4(2^5 - 1) = 16 \cdot 31 = 496$ jest doskonała.

4) Dla $p = 7$ otrzymujemy liczbę pierwszą $2^7 - 1 = 127$. Zatem liczba $2^6(2^7 - 1) = 64 \cdot 127 = 8128$ jest doskonała.

Następną liczbę doskonałą otrzymamy dopiero dla $p = 13$. Mamy wtedy $2^{13} - 1 = 8191$ oraz $2^{12}(2^{13} - 1) = 4096 \cdot 8191 = 33\,550\,336$. W XVII wieku rozpoczęto intensywne poszukiwania liczb pierwszych postaci $2^p - 1$. Wiele czasu tym poszukiwaniom poświęcił franciszkański mnich żyjący w Paryżu, Marin Mersenne; stąd też takie liczby pierwsze nazywamy dzisiaj **liczbami Mersenne'a** i oznaczamy symbolem $M_p = 2^p - 1$.

Mersenne stwierdził bez dowodu, że liczby M_p dla

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

są pierwsze oraz że są to jedyne liczby pierwsze postaci M_p dla $p \le 257$. W ciągu następnych 300 lat stwierdzono, że Mersenne popełnił 5 błędów: liczby M_{67} i M_{257} są złożone oraz liczby M_{61}, M_{89} i M_{107} są pierwsze. Od lat poszukiwano też coraz większych liczb pierwszych. Największe odkrywane liczby pierwsze były z reguły liczbami Mersenne'a. Największą znaną liczbą Mersenne'a jest liczba $2^{32582657} - 1$ mająca 9808358 cyfr (odkryto ją 6 września 2006 roku w ramach międzynarodowego programu poszukiwania takich liczb – The Great Internet Mersenne Prime Search, GIMPS). Nie wiemy jednak, czy istnieje nieskończenie wiele takich liczb.

Przejdźmy teraz do drugiego pytania. Częściowej odpowiedzi udzielił Euler. Udowodnił on mianowicie następujące twierdzenie:

Twierdzenie 8. Jeśli n jest parzystą liczbą doskonałą, to istnieje liczba pierwsza p taka, że $n = 2^{p-1}(2^p - 1)$ oraz liczba $2^p - 1$ jest liczbą pierwszą Mersenne'a.

Dowód. Liczba n jest parzysta, więc jest postaci $n = 2^{p-1}q$, gdzie $p > 1$ oraz q jest liczbą nieparzystą. Ponieważ n jest liczbą doskonałą, więc $\sigma(n) = 2n = 2^p q$. Popatrzmy teraz, jak wyglądają dzielniki liczby n. Są to mianowicie liczby

$$\begin{array}{ccccccccc} 1\cdot d_1, & 2\cdot d_1, & 4\cdot d_1, & 8\cdot d_1, & \ldots & 2^{p-2}\cdot d_1, & 2^{p-1}\cdot d_1,\\ 1\cdot d_2, & 2\cdot d_2, & 4\cdot d_2, & 8\cdot d_2, & \ldots & 2^{p-2}\cdot d_2, & 2^{p-1}\cdot d_2,\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 1\cdot d_m, & 2\cdot d_m, & 4\cdot d_m, & 8\cdot d_m, & \ldots & 2^{p-2}\cdot d_m, & 2^{p-1}\cdot d_m, \end{array}$$

gdzie $d_1, d_2, \ldots, d_m$ są wszystkimi dzielnikami liczby q. Zatem

$$\begin{aligned} \sigma(n) &= (1+2+4+8+\ldots+2^{p-1})\cdot(d_1+d_2+\ldots+d_m) =\\ &= (2^p-1)\cdot\sigma(q). \end{aligned}$$

Otrzymujemy więc równość $2^p \cdot q = (2^p - 1) \cdot \sigma(q)$, czyli

$$\frac{2^p - 1}{2^p} = \frac{q}{\sigma(q)}.$$

Ułamek po lewej stronie jest nieskracalny, gdyż licznik i mianownik różnią się o 1. Nie wiemy jednak, czy ułamek po prawej stronie też jest nieskracalny. Możemy jedynie powiedzieć, że istnieje taka liczba c, że

$$q = c \cdot (2^p - 1) \quad \text{oraz} \quad \sigma(q) = c \cdot 2^p.$$

Chcemy pokazać, że $c = 1$. Przypuśćmy zatem, że $c > 1$. Widzimy, że liczby 1, c, $2^p - 1$ oraz q są dzielnikami liczby q. Pokażemy, że są one różne.

1) Przypuśćmy, że $q = 1$. Wówczas $n = 2^{p-1}$ i wtedy

$$\sigma(n) = 1 + 2 + 4 + \ldots + 2^{p-1} = 2^p - 1 \neq 2^p = 2n,$$

wbrew założeniu, że liczba n jest doskonała.

2) $c \neq 1$ z przyjętego założenia.

3) Przypuśćmy, że $2^p - 1 = 1$. Wtedy $p = 1$, czyli $n = q$, wbrew założeniu, że liczba n jest parzysta.

4) Przypuśćmy, że $q = c$. Wtedy, $2^p - 1 = 1$, a tę możliwość wyeliminowaliśmy wyżej.

5) Przypuśćmy, że $q = 2^p - 1$. Wtedy $c = 1$, co też już wykluczyliśmy.

6) Przypuśćmy, że $c = 2^p - 1$. Wtedy $q = c^2$, a więc liczba q ma co najmniej trzy różne dzielniki: 1, c i c^2. Zatem

$$\sigma(q) \geq 1 + c + c^2.$$

Z drugiej strony,

$$\sigma(q) = c \cdot 2^p = c \cdot (2^p - 1 + 1) = c(c + 1) =$$
$$= c^2 + c < 1 + c + c^2 \leq \sigma(q),$$

co jest niemożliwe.

Pokazaliśmy więc, że rzeczywiście liczby 1, c, $2^p - 1$ oraz q są czterema różnymi dzielnikami liczby q. Zatem

$$\sigma(q) \geq 1 + c + (2^p - 1) + q = q + c + 2^p =$$
$$= c(2^p - 1) + c + 2^p = c \cdot 2^p + 2^p > c \cdot 2^p = \sigma(q),$$

co jest niemożliwe. Otrzymana sprzeczność dowodzi, że $c = 1$.

Zatem $q = 2^p - 1$ oraz

$$\sigma(q) = 2^p = q + 1.$$

Stąd wynika, że liczba q ma tylko dwa dzielniki: 1 oraz q, a więc jest pierwsza. Zatem $n = 2^{p-1}(2^p - 1)$, gdzie liczba $2^p - 1$ jest liczbą pierwszą Mersenne'a, c. b. d. o.

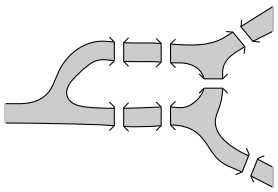
Wiemy zatem, jak wyglądają parzyste liczby doskonałe. Nie wiemy natomiast, czy istnieją nieparzyste liczby doskonałe. Udowodniono jednak, że jeśli istnieje nieparzysta liczba doskonała, to musi ona mieć co najmniej 8 dzielników pierwszych, te dzielniki muszą być większe od 7, drugi pod względem wielkości musi być większy od 1000, a sama ta liczba musi być większa od 10^{300}. Ponadto udowodniono, że w pewnym sensie takich liczb jest mało.

Część III: kombinatoryka i teoria grafów.

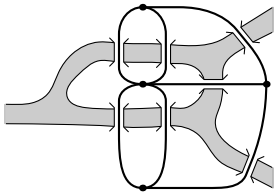
Spośród licznych osiągnięć Eulera w kombinatoryce i teorii grafów wspomnimy o trzech twierdzeniach. Twierdzeń tych nie będziemy dowodzić, a jedynie zilustrujemy je przykładami.

Problem mostów królewieckich.

Pytanie, które postawił sobie Euler, brzmiało: czy możliwy jest taki spacer po Królewcu, by przejść się po każdym z siedmiu mostów dokładnie jeden raz i wrócić do punktu wyjścia. A oto schematyczny plan Królewca z czasów Eulera z zaznaczonymi mostami na Pregole:



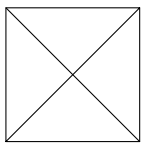
Sformułujmy ten problem w języku teorii grafów. Mamy do czynienia z grafem o czterech wierzchołkach: każdy wierzchołek odpowiada jednej części miasta (oba brzegi rzeki Pregoły i dwie wyspy), każda krawędź odpowiada drodze z jednej części do drugiej przez któryś z mostów. Ten graf zaznaczony jest na planie Królewca grubszą linią.



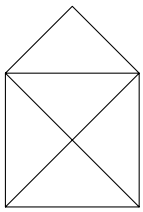
Pytanie zatem brzmi: czy w danym grafie istnieje droga przechodząca przez każdą krawędź dokładnie jeden raz i kończąca się w punkcie wyjścia. Taką drogę nazywamy **cyklem Eulera**. Jeśli zrezygnujemy z warunku mówiącego o tym, że koniec drogi ma się pokrywać z jej początkiem, to otrzymamy tzw. **drogę Eulera**. Pytamy zatem o to, w jakich grafach istnieją cykle lub drogi Eulera. Od razu widzimy, że konieczny jest warunek, by graf składał się z jednego kawałka, czyli, by każde dwa wierzchołki grafu można było połączyć jakąś drogą. Takie grafy nazywamy **grafami spójnymi**. Euler udowodnił następujące twierdzenie:

Twierdzenie 9. W grafie spójnym istnieje cykl Eulera wtedy i tylko wtedy, gdy w każdym wierzchołku schodzi się parzysta liczba krawędzi. Droga Eulera istnieje natomiast wtedy i tylko wtedy, gdy istnieją dokładnie dwa wierzchołki, w których schodzi się nieparzysta liczba krawędzi. Każda droga Eulera zaczyna się wtedy w jednym z tych wierzchołków i kończy w drugim.

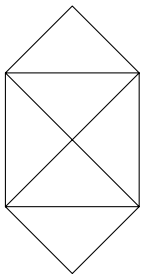
Z twierdzenia Eulera wynika w szczególności, że niemożliwe jest narysowanie kwadratu z przekątnymi jednym pociągnięciem ołówka, bez odrywania go od papieru:



Rozważany graf ma bowiem cztery wierzchołki, w których schodzą się po trzy krawędzie. Narysowanie koperty:



jest możliwe, ale nakreślona linia musi mieć początek w jednym z dwóch dolnych wierzchołków i koniec w drugim; są to bowiem jedyne wierzchołki, w których schodzi się nieparzysta liczba krawędzi. Wreszcie narysowanie podwójnej koperty:

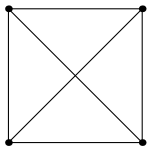


jest możliwe i rysowanie linii możemy zakończyć w punkcie wyjścia; w każdym wierzchołku schodzą się bowiem dwie lub cztery krawędzie.

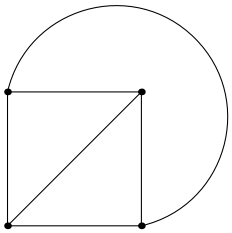
Powszechnie uważa się, że powyższe twierdzenie jest pierwszym twierdzeniem teorii grafów; Eulera uważamy zatem za twórcę tej teorii.

Wzór Eulera.

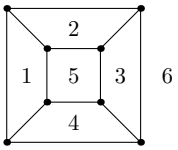
Mówimy, że dany graf narysowany na płaszczyźnie jest **grafem płaskim**, jeśli jego krawędzie nie przecinają się poza wierzchołkami. Na przykład graf



nie jest grafem płaskim (wierzchołkami są tylko punkty zaznaczone grubą kropką), a graf



jest grafem płaskim. Graf płaski dzieli płaszczyznę na obszary ograniczone liniami tworzącymi krawędzie. Każdy taki obszar nazywamy **ścianą** grafu płaskiego (łącznie z obszarem nieograniczonym). Na przykład, następujący graf ma 6 ścian:



Euler udowodnił następujące twierdzenie.

Twierdzenie 10. Niech w oznacza liczbę wierzchołków grafu płaskiego i spójnego, k liczbę krawędzi tego grafu, a s liczbę jego ścian. Wtedy $w - k + s = 2$.

Na przykład, powyższy graf ma 8 wierzchołków, 12 krawędzi oraz 6 ścian i rzeczywiście $8 - 12 + 6 = 2$. Zauważmy, że terminologia stosowana w teorii grafów została zaczerpnięta z geometrii. Mówimy przecież o wierzchołkach, krawędziach i ścianach wielościanów. Nie jest to przypadek. Okazuje się, że jeśli dany jest wielościan wypukły, to można przypisać mu taki graf płaski i spójny, który ma tyle samo wierzchołoków, krawędzi i ścian (a nawet są one w pewnym sensie tak samo położone względem siebie). Twierdzenie Eulera można wypowiedzieć zatem w następującej postaci:

Twierdzenie 11. Jeśli wielościan wypukły ma w wierzchołków, k krawędzi i s ścian, to $w - k + s = 2$.

Podziały liczb.

Podziałem liczby n nazywamy przedstawienie jej w postaci sumy liczb naturalnych. Na przykład, liczba 6 ma 11 podziałów (zauważmy, że kolejność składników nie jest istotna):

$$6,\ 5+1,\ 4+2,\ 4+1+1,\ 3+3,\ 3+2+1,$$
$$3+1+1+1,\ 2+2+2, 2+2+1+1,$$
$$2+1+1+1+1,\ 1+1+1+1+1+1.$$

Zauważmy, że wśród tych 11 podziałów istnieją cztery podziały na liczby nieparzyste

$$5+1,\ 3+3,\ 3+1+1+1,\ 1+1+1+1+1+1$$

i cztery podziały na liczby niepowtarzające się:

$$6,\ 5+1,\ 4+2,\ 3+2+1.$$

Euler zauważył, że nie jest to przypadek i udowodnił następujące twierdzenie:

Twierdzenie 12. Dla każdej liczby naturalnej liczba podziałów na składniki nieparzyste jest równa liczbie podziałów na składniki parami różne (niepowtarzające się).

Mianowicie każdemu podziałowi liczby n na liczby nieparzyste

$$n = k_1 + k_2 + \ldots + k_m$$

przyporządkujemy podział na liczby parami różne. Przypuśćmy, że liczba k_1 występuje w tym podziale l_1 razy. Liczbę l_1 zapiszemy w postaci sumy różnych potęg dwójki (czyli w systemie dwójkowym): $l_1 = 2^{p_1} + 2^{p_2} + \ldots$. Następnie zamiast l_1 składników k_1 zapiszemy składniki $k_1 \cdot 2^{p_1}, k_1 \cdot 2^{p_2}, \ldots$. W podobny sposób potraktujemy pozostałe składniki nieparzyste podziału liczby n. Popatrzmy na przykład:

$$69 = 7+7+7+5+5+5+5+5+5+$$
$$+3+3+3+3+3+1+1+1.$$

Ten podział zapisujemy w postaci

$$\begin{aligned}69 &= 7\cdot 3+5\cdot 6+3\cdot 5+1\cdot 3=\\ &= 7\cdot(2^1+2^0)+5(2^2+2^1)+3\cdot(2^2+2^0)+\\ &\quad +1\cdot(2^1+2^0)=\\ &= 7\cdot 2+7\cdot 1+5\cdot 4+5\cdot 2+3\cdot 4+3\cdot 1+\\ &\quad +1\cdot 2+1\cdot 1=\\ &= 14+7+20+10+12+3+2+1=\\ &= 20+14+12+10+7+3+2+1.\end{aligned}$$

Nietrudno udowodnić, że w ten sposób otrzymujemy wszystkie podziały na liczby parami różne oraz różnym podziałom na liczby nieparzyste odpowiadają różne podziały na liczby niepowtarzające się. Wynika to stąd, że każdą liczbę naturalną $m \geq 1$ można w jednoznaczny sposób przedstawić w postaci $m = 2^p \cdot q$, gdzie liczba q jest nieparzysta.

Dodatek.

Pokażemy teraz pominięty w wykładzie dowód indukcyjny twierdzenia 6.

Twierdzenie 6. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a^{2^n}+1$, to p jest postaci $p = 2^{n+1}k+1$ dla pewnej liczby całkowitej k.

Dowód. Dla $n \leq 2$ twierdzenie zostało już udowodnione (lematy 1, 2 i 3). Przeprowadzimy teraz krok indukcyjny.

Założenie indukcyjne. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a^{2^n}+1$, to p jest postaci $p = 2^{n+1}\ell+1$ dla pewnej liczby całkowitej ℓ.

Teza indukcyjna. Jeśli a jest liczbą parzystą, p jest liczbą pierwszą oraz p jest dzielnikiem $a^{2^{n+1}}+1$, to p jest postaci $p = 2^{n+2}k+1$ dla pewnej liczby całkowitej k.

Dowód tezy indukcyjnej. Ponieważ $a^{2^{n+1}} = (a^{2^n})^2$ oraz p jest dzielnikiem $a^{2^{n+1}}+1$, więc z założenia indukcyjnego wynika, że p jest liczbą postaci $p = 2^{n+1}\ell+1$ dla pewnej liczby całkowitej ℓ. Jeśli $\ell = 2k$ dla pewnej liczby k, to $p = 2^{n+2}k+1$ i dowód twierdzenia będzie zakończony. Jeśli zaś $\ell = 2k+1$, to $p = 2^{n+2}k+2^{n+1}+1$. Wykażemy, że ta druga możliwość nie może mieć miejsca.

Przypuśćmy więc, że $p = 2^{n+2}k+2^{n+1}+1$. Ponieważ p jest dzielnikiem $a^{2^{n+1}}+1$, więc nie jest dzielnikiem a. Z małego twierdzenia Fermata wynika zatem, że p jest dzielnikiem liczby $a^{p-1}-1$. Zauważmy teraz, że

$$a^{p-1}-1 = a^{2^{n+2}k+2^{n+1}}-1.$$

Zatem p jest dzielnikiem liczby $a^{2^{n+2}k+2^{n+1}}-1$.

Ponieważ p jest dzielnikiem $a^{2^{n+1}}+1$, więc jest też dzielnikiem $\left(a^{2^{n+1}}\right)^{2k+1}+1$. Ale

$$\left(a^{2^{n+1}}\right)^{2k+1}+1 = a^{2^{n+1}\cdot(2k+1)}+1 = a^{2^{n+2}k+2^{n+1}}+1,$$

więc p jest dzielnikiem liczby $a^{2^{n+2}k+2^{n+1}}+1$. Zatem p jest dzielnikiem różnicy

$$\left(a^{2^{n+2}k+2^{n+1}}+1\right)-\left(a^{2^{n+2}k+2^{n+1}}-1\right)=2.$$

Stąd wynika, że $p = 2$, co jest niemożliwe. Ta sprzeczność kończy dowód twierdzenia.

Bibliografia

[1] Dunham, William, *Euler. The Master of Us All*, The Dolciani Mathematical Expositions, The Mathematical Association of America, 1999.

[2] Dunham, William, *Journey Through Genius*, Wiley Science Editions, 1990.

[3] Lipski, Witold, Marek, Wiktor, *Analiza kombinatoryczna*, PWN Warszawa, 1986.

[4] Ribenboim, Paulo, *Mała księga wielkich liczb pierwszych*, WNT Warszawa, 1997.

[5] Sierpiński, Wacław, *Wstęp do teorii liczb*, WSiP Warszawa, 1987 (wyd. III poprawione).

[6] Wilson, Robin J., *Wprowadzenie do teorii grafów*, PWN Warszawa, 2004.

[7] Yiu, Paul, *Notes on Euclidean Geometry*, 1998, Notatki zamieszczone na stronie internetowej `http://www.math.fau.edu/yiu/EuclideanGeometryNotes.pdf`