Fukcja Eulera incognito

Arkadiusz Męcel

Seminarium monograficzne: popularyzacja matematyki
16 marca 2009r.

Jedną z najważniejszych funkcji rozważanych w teorii liczb jest funkcja Eulera $\phi : \mathbb{N}_+ \to \mathbb{N}_+$ określona wzorem:

$$\phi(n) = |\{k \in \mathbb{N} : 1 \leqslant k < n \wedge (k, n) = 1\}|.$$

Fundamentalny fakt związany z tym obiektem pochodzi od człowieka, nazwisko którego funkcja ta nosi. W 1760 roku Leonhard Euler udowodnił następujący fakt:

Twierdzenie 1 (Euler, 1760) *Jeżeli $m \in \mathbb{Z}_+$, $a \in \mathbb{Z}$ przy czym $(a, m) = 1$, to:*

$$m \mid a^{\phi(m)} - 1.$$

Aby wyrobić sobie przekonanie o przydatności tego faktu wystarczy zauważyć, że jeśli m jest liczbą pierwszą, wówczas $\phi(m) = m - 1$, sam zaś fakt przybiera postać dobrze nam znanego Małego Twierdzenia Fermata. Warto poświecić chwilę na przytoczenie krótkiej historii tych zagadnień. Sam Fermat, jak wiadomo udowodnił wiele twierdzeń, a jeszcze więcej udowodnił być może – przynajmniej sam tak twierdził nie dając zarazem nikomu możliwości potwierdzenia faktycznego stanu rzeczy. Historycznie rzecz biorąc, fakt znany dziś pod nazwą Małego Twierdzenia sformułował Fermat po raz pierwszy (bez dowodu) w 1640r. przy okazji korespodencji z Marinem Mersenne'm. Aż do 1736r. nie opublikowano żadnego dowódu tego faktu. Na podstawie notatek Leibniza uważa się jednak, że dowód takowy pojawił się już w XVII wieku. Skąd u Eulera zainteresowanie tą tematyką? Zaczęło się od pozornie znacznie bardziej skomplikowanego problemu. Fermat był za życia przekonany, że wszystkie liczby postaci $2^{2^n} + 1$ są pierwsze. Stawiał ten problem jako wyzwanie przed swoimi korespondentami. Żaden nie umiał zaprezentować uzasadnienia. Po kilkudziesięciu latach Christian Goldbach, podówczas Sekretarz Cesarkiej Akademii Nauk w Petersburgu, wspomina o tym problemie jednemu z nowo zatrudnionych pracowników Wydziału Matematycznego – Eulerowi właśnie. Ten w krótkim artykule obala tezę Fermata przedstawiając kontrprzykład dla $n = 5$, dołączając jednocześnie w odpowiedzi zestaw sześciu hipotez, z którymi sam nie potrafi sobie w tamtym momencie poradzić. Jedną z nich jest MTF. Ostatecznie Euler prezentuje dowód siedem lat później. Później wprowadza pojęcie funkcji ϕ, a twierdzenie cytowane wyżej dowodzi dopiero w roku 1760.
Zanim pozwolimy funkcji ϕ przejść do tytułowego 'incognito', poznajmy odrobinę lepiej jej podstawowe własności. Wiemy już, że dla każdej liczby pierwszej p wartość $\phi(p) = p - 1$. Następującą serię faktów proponujemy jako proste ćwiczenia:

Zadanie 1 *Dla dowolnej liczby naturalnej $n \geqslant 2$ wartość $\phi(n)$ jest liczbą parzystą.*

Zadanie 2 *Dla dowolnej liczby naturalnej $n > 0$ zachodzi: $\phi(p^n) = p^n - p^{n-1}$.*

Zadanie 3 *Dla dowolnych dwóch różnych liczb pierwszych p, q mamy: $\phi(pq) = \phi(p) \cdot \phi(q)$.*

Zadanie 4 *Dla dowolnych dwóch względnie pierwszych liczb a, b mamy: $\phi(ab) = \phi(a) \cdot \phi(b)$.*

Twierdzenie 2 *Jeśli $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gdzie p_i są dla $i = 1, 2, \ldots, k$ parami różnymi liczbami pierwszymi, oraz α_i są dla $i = 1, 2, \ldots, k$ całkowite dodatnie, to:*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Dowód tego twierdzenia można uzyskać bezpośrednio przez indukcję, korzystając z poprzednich zadań. Istnieje też kombinatoryczny dowód korzystający z zasady włączeń i wyłączeń. My zaprezentujemy tu jeszcze inne, ale ładne, bo probabilistyczne podejście: załóżmy, że x jest wybraną losową liczbą ze zbioru $X = \{1, 2, \ldots, n\}$, przy czym prawdopodobieństwo wyciągnięcia dowolnej ustalonej liczby z tego zbioru wynosi w każdym przypadku $\frac{1}{n}$. Prawdopodobieństwo, że wyciągniemy liczbę względnie pierwszą z n jest na mocy definicji klasycznej równe $\frac{\phi(n)}{n}$. Możemy to prawdopodobieństwo policzyć jeszcze inaczej. Rozważmy zdarzenia: $A_1, A_2, \ldots, A_k$ postaci:

$$A_k = \{x \in X : p_i \,|\, x\}.$$

Innymi słowy zdarzenie A_i to wyciągnięcie liczby podzielnej przez p_i. Zauważmy, że liczb podzielnych jednocześnie przez pewne q różnych liczb pierwszych jest dokładnie tyle, ile wielokrotności iloczynu tych liczb jest w n. Formalnie, dla dowolnych $i_1, i_2, \ldots, i_q$, gdzie $q \leqslant k$ mamy:

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_q}| = \frac{n}{p_{i_1} p_{i_2} \ldots p_{i_q}}.$$

To dowodzi, że zdarzenia $A_1, A_2, \ldots, A_k$ są niezależne. Wyciągnięcie liczby względnie pierwszej z n to NIE WYCIĄGNIĘCIE liczby podzielnej przez dowolną z $p_1, p_2, \ldots, p_k$. Jest to więc:

$$P\left(\bigcap_{i=1}^{k} A_i^c\right) = \prod_{i=1}^{k} P(A_i^c) = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Wiemy już niemal wszystko. Dla utrwalenia wiadomości i oswojenia się z zaprezentowanym twierdzeniem proponujemy następujące trzy zadania:

Zadanie 5 *Dla każdej liczby naturalnej $n \geqslant 6$ mamy: $n > \phi(n) \geqslant \sqrt{n}$.*

Zadanie 6 *Rozwiąż w liczbach naturalnych równania: $\phi(x) = 6, \quad \phi(x) = 14$.*

Ostatnie równanie jest jedną z manifestacji faktu udowodnionego w pełnej ogólności przez Andrzeja Schinzla: funkcja ϕ nie przyjmuje wartości postaci $2 \cdot 7^k$ dla k całkowitych dodatnich. Z funkcją tą związanych jest wiele interesujących równości, nierówności, hipotez i ciekawostek. Dla porządku podamy jedną z nich, bynajmniej nie dowodzącą się łatwo.

Policzmy $\phi(30)$. Łatwe? Jasne, to oczywiście 8. A wypiszmy zbiór, którego to 8 jest mocą:

$$\{1, 7, 11, 13, 17, 19, 23, 29\}$$

Poza jedynką zbiór ten składa się z samych liczb pierwszych! Okazuje się, że 30 jest największą liczbą o tej własności! Choć nie jedyną.

A jakaś prosta hipoteza otwarta? Liczbę x nazwiemy liczbą Phibonacciego, jeśli $\phi(x) = \phi(x-1) + \phi(x-2)$. Jedną z takich liczb jest 3, inną 5. A czy istnieje jakaś złożona? Tak, najmniejsza to 1037. A czy istnieje parzysta? Tego nie wiadomo...

Skoro jednak chcemy zająć się odnajdywaniem jej w nieoczekiwanych miejscach, przejdźmy do rzeczy.

1. Zacznijmy od teorii liczb. Jeden z najprostszych dowodów na to, że liczb pierwszych jest nieskończenie wiele pochodzi od Kummera. Korzystamy z funkcji ϕ. Załóżmy, że liczb pierwszych jest skończenie wiele i są to: $p_1 < p_2 < \ldots < p_k$. Niech $n = p_1 p_2 \ldots p_k$. Wtedy zgodnie ze wzorem powyżej:

   $$\phi(n) = (p_1 - 1)(p_2 - 1)\ldots(p_n - 1).$$

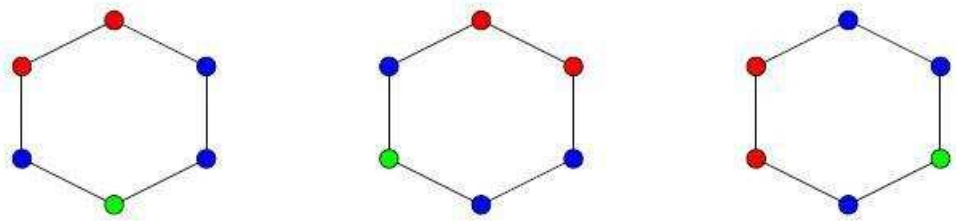
   Ale to jest sprzeczność, bo jeśli istnieje liczba k mniejsza od n, że $(n, k) = 1$, to oznacza, że żadna z liczb p_i nie jest dzielnikiem n, a przecież każda liczba naturalna jest iloczynem liczb pierwszych.

2. Przypomnijmy sobie zagadnienie gwiazdek, które rozważaliśmy na jednym z poprzednich seminariów. Przyda nam się ono do geometrycznego dowodu twierdzenia Eulera, uzyskanego przez Poinsota w 1845 roku. Szukaliśmy wtedy wszystkich gwiazdek o n wierzchołkach pochodzących od wielokąta foremnego, o równych krawędziach. Okazało się, że jest ich $\phi(n)/2-1$. Teraz spróbujemy tak: weźmy a względnie pierwsze z n, różne od 1. Rozważmy dowolny wierzchołek n – kąta foremnego i budujmy gwiazdkę idąc co a wierzchołków. Nazwijmy tę gwiazdkę G_1. W drugim kroku idąc co a wierzchołków gwiazdki G_1 tworzymy wierzchołki gwiazdki G_2 (innymi słowy od wyjściowego n kąta foremnego idziemy co a^2 modulo n wierzchołków). Tak dostajemy kolejne G_i aż w końcu dla pewnego n mamy G_k – wyjściowy wielokąt foremny. Istotnie, ilość możliwych długości krawędzi jest skończona, a więc dla pewnych $k_1 < k_2$ mamy $a^{k_1} = a^{k_2}$(mod n). Skoro $(a, n) = 1$, to $a^{k_2-k_1} = 1$(mod n). Istotnie więc dostajemy wielokąt foremny. Na przykład dla ośmiokąta foremnego i $a = 3$ procedura ta jest osiągnięta już w dwóch krokach. Kluczowym punktem dowodu, którego tu nie prezentujemy, jest pokazanie, że uzyskane k jest dzielnikiem $\phi(n)$. Widać, że w tym miejscu przypomina to nam już twierdzenie Lagrange'a znane z teorii grup. Dalej jest już łatwo. Skoro $a^k = 1$ modulo n, to także $a^{\phi(n)} = 1$ modulo n.

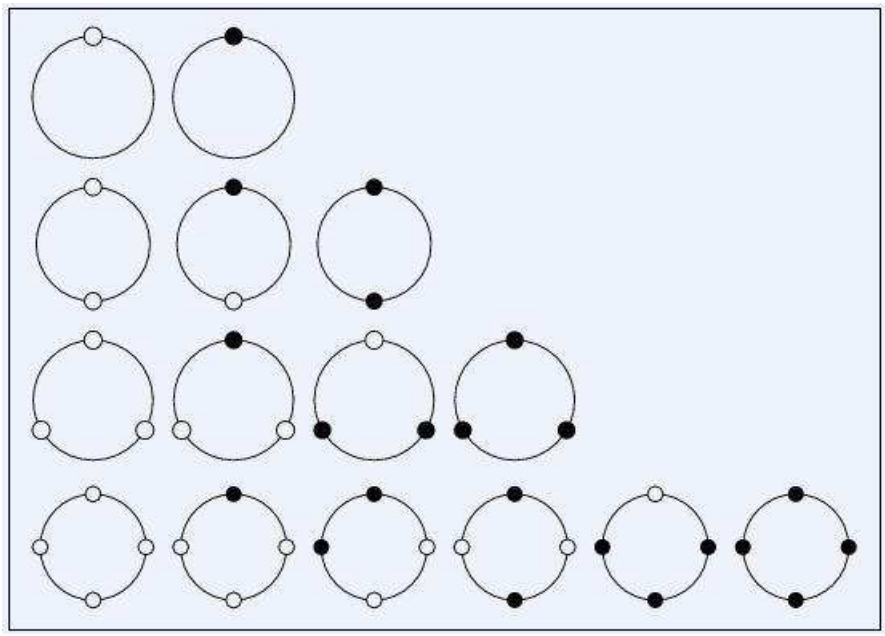
   Co ciekawe, o problemie tym można też myśleć nieco inaczej. Wyobraźmy sobie, że rozważamy zupełnie inny problem. Mamy stół do bilarda o kształcie koła. Bila jest jednorodna, toczy się bez poślizgu i spełniona jest zasada zachowania kąta odbicia. Wtedy wielokąty gwiaździste tworzą wraz z wielokątem foremnym zestaw tzw. orbit periodycznych. Oznacza to, że bila umiejscowiona w punkcie należącym do jednej z tych figur uderzona w kierunku jednego z boków będzie podróżowała po okresowej orbicie. Także trójkąt równoboczny, wpisany w koło tworzy taką periodyczną orbitę. Steinhaus zauważył, że w dowolnym stole bilardowym, którego brzeg jest gładki i bez samoprzecięć, istnieje trójkątna orbita periodyczna. Tworzy ją ten z trójkątów wpisanych w ten stół, który ma największy obwód. Postawił też hipotezę, że istnieje jeszcze inny, nieprzystający trójkąt periodyczny. Po latach udowodniono, że tak jest. Co więcej, wykazano, że w każdym takim stole jest przynajmniej $\phi(k)$ orbit periodycznych tworzonych przez k - kąty. Można też szukać orbit na wielokątnych stołach, coś już ciekawego na ten temat wiadomo, ale to materiał na osobny referat...

3. Przejdźmy wreszcie do zagadnienia, które omówimy tutaj najszerzej – do naszyjników. Czym jest naszyjnik, to każdy wie. Mamy sznurek o kształcie okręgu i nawleczone na niego koraliki różnych kolorów. Dla przykładu:

$$rbbgbr \equiv rrbbgb \equiv bbgbrr$$



Na rysunku widać także jakie naszyjniki uznajemy za równoważne – takie dokładnie, które możemy uznać za obrót innych. Widać, że naszyjniki długości n mające koraliki w co najwyżej k kolorach można opisać matematycznie jako klasy równoważności słów długości n nad pewnym alfabetem długości k, względem obrotów. Podstawowe zagadnienie to ile jest takich (n, k) – naszyjników? Oznaczymy tę liczbę przez $m(n, k)$ Spróbujmy wykonać tę pracę 'ręcznie' mając do dyspozycji 2 kolory i naszyjniki długości co najwyżej 4. Oto rezultaty:



Podamy najpierw wzór na liczbę tych orbit, a potem krótko opowiemy o pięknej drodze, na której fakt ten można dowodzić. Otóż:

$$m(n,k) = \frac{1}{n}\sum_{d\,|\,n} \phi(d)k^{n/d}.$$

Zauważmy na boku, że gdy mamy tylko 1 kolor, wówczas $m(n, 1) = 1$. Stąd dostajemy znany fakt mówiący, że liczba jest równa sumie wartości funkcji ϕ na swoich dzielnikach właściwych:

$$\sum_{d\,|\,n} \phi(d) = n.$$

Pełen dowód tego faktu nie wydaje się być odpowiednim na seminarium z popularyzacji matematyki. Korzysta on z pewnych ważnych, choć prostych, faktów z teorii grup. Zauważmy, że w języku tej teorii (n, k) – naszyjnik, to orbita przy działaniu n – elementowej grupy cyklicznej na zbiór słów długości n nad k – elementowym alfabetem. Działanie polega oczywiście na obracaniu tych słów. Skoro naszyjniki to orbity działania grup, to trzeba szukać teoriogrupowych rezultatów dotyczących zliczania orbit. Dla grup skończonych służy tu tzw. **Lemat, który nie jest Burnside'a**. Mówi on tyle, że liczba orbit działania skończonej grupy G na zbiór X równa jest sumie ilości elementów X, które są zachowywane przez kolejne elementy G, podzielonej przez ilość elementów G. Chcąc zapisać to wzorem, mamy:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Dlaczego nie jest on Burnside'a? Otóż matematyk ten, który notabene bardzo przysłużył się algebrze jako takiej, sformułował i udowodnił ten fakt w swojej książce o teorii grup wydanej w 1897 roku, nazywając go twierdzeniem Frobeniusa z 1887 roku. Wiadomo jednak, że już w 1845 roku formuła ta była znana Cauchy'emu. Generalnie, fakt ten był uznawany pod koniec XIX wieku za tak elementarny, iż nie przejmowano się jego dokładnym pochodzeniem.

Lemat ten jest sam w sobie bardzo ciekawy i pozwala na rozstrzygnięcie wielu pięknych kombinatorycznych zagadnień. Na przykład: wyznaczyć ilość możliwych układów prowadzących do rozwiązania zagadnienia kostki Rubika, albo ilość różnych kolorowań ścian wielościanów (przy odpowiednich założeniach), można za jego pomocą dowodzić małe twierdzenie Fermata czy twierdzenie Wilsona z teorii liczb. Doskonały materiał na osobny referat.

Jak może on nam pomóc w dowodzie? Elementy grupy cyklicznej n – elementowej traktować musimy jako podgrupę permutacji zbioru n – elementowego. Grupa ta jest generowana przez element postaci $g = (1\,2\,3\,\ldots\,n)$. Następnie są jego potęgi tak, że $g^n = e$. Kluczem jest tu rozkład permutacji na cykle. Okazuje się, że jeśli permutacja g ma c – cykli, wówczas dokładnie k^c słów długości n nad alfabetem wielkości k permutacja g trzyma w miejscu. Dla przykładu – permutacja $(1\,2\,3\,\ldots\,n)$ nie zmienia jedynie k słów: tych dokładnie, których wszystkie litery są w jednym (spośród k) ustalonym kolorze. To powinno obrazować skąd bierze się ogólny fakt. Dalej przypominamy sobie kolejne proste fakty z teorii permutacji: i – ta potęga permutacji $(1\,2\,3\,\ldots\,n)$ ma dokładnie (n, i) cykli w swoim rozkładzie. Stąd zgodnie z lematem Burnside'a:

$$m(n, k) = \frac{1}{n} \sum_{i=1}^{n} k^{(n,i)}.$$

W każdej grupie cyklicznej rzędu n mamy dokładnie $\phi(d)$ elementów rzędu d, gdzie d – zgodnie z twierdzeniem Lagrange'a dzieli n. Stąd już nasza formuła:

$$m(n, k) = \frac{1}{n} \sum_{d \mid n} \phi(d) k^{n/d}.$$

Istnieje jeszcze inny dowód, korzystający z fascynującego twierdzenia Polyi o numerowaniu. To jednak znowu materiał na osobną opowieść... W tym, jak i w wielu innych zastosowaniach, korzysta się oczywiście z pewnych faktów dotyczących pierścienia reszt z dzielenia przez n, z którym wprost z definicji, funkcja ϕ jest nierozerwalnie związana. Nie skupialiśmy się na tych faktach, głównie z

powodu braku czasu i chęci zwrócenia uwagi na możliwie szerokie spektrum zagadnień. Na pewno dałoby się powiedzieć znacznie więcej, ale zatrzymamy się już w tym miejscu.

Literatura

[1] CROFT H.T, FALCONER K.J., GUY R.K., *Unsolved Problems in Geometry*, Springer, (1991).

[2] CRTICI B., MITRINOVIC D., SANDOR J., *Handbook of Number Theory II*, Springer (2004).

[3] PALKA Z., RUCIŃSKI A., *Wykłady z kombinatoryki*, WNT (2004).

[4] ROYLE G., *Polya Counting I*, The University of Western Australia (2004), dostępny online: http://undergraduate.csse.uwa.edu.au/units/CITS7209/polya.pdf.

[5] SANDIFER E., *How Euler did it? Fermat's Little Theorem*, Mathematical Assiociation of America (2007), dostępny online: http://www.maa.org/editorial/euler/How%20Euler%20Did%20It%2001%20Fermats%20little%20theorem.pdf

[6] WEISSTEIN E.W., *Necklace*, From MathWorld – A Wolfram Web Resource, dostępny online: http://mathworld.wolfram.com/Necklace.html

[7] WIKIPEDIA, *Burnside's lemma*, *Euler's Theorem*, dostępne online: http://www.wikipedia.com.