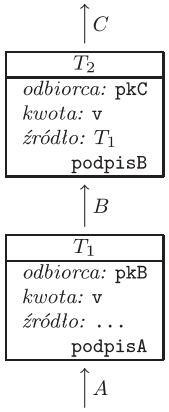
Jedyne dane powiązane z użytkownikiem Bitcoina to jego identyfikator – losowo wyglądający ciąg 34 liter i cyfr. Dlatego często mówi się o anonimowości Bitcoina, choć lepszym określeniem byłaby *pseudonimowość* – użytkownicy występują pod pseudonimami, nikt nie zna ich prawdziwych danych osobowych, jednak ich zachowanie jest w pełni jawne.



publiczny, który jednocześnie pełni rolę identyfikatora użytkownika. Są to klucze systemu cyfrowego podpisu ECDSA, który jest wykorzystywany do podpisywania i weryfikowania transakcji. I tak oto w miejsce odbiorcy mamy *klucz publiczny* odbiorcy `pkB`, a zamiast nadawcy mamy *źródło* wskazujące na inną transakcję, z której pochodzą środki nadawcy. Dodatkowo każda transakcja jest podpisana przez nadawcę (`podpisA`) przy użyciu jego klucza prywatnego.

Aby to sobie zobrazować, o Bitcoinie należy myśleć jak o sieci, w której transakcje stanowią węzły, a użytkownicy to połączenia pomiędzy nimi, nie na odwrót. Aby użytkownik B mógł zapłacić użytkownikowi C kwotę v, w sieci musi istnieć (niewydana) transakcja T_1 o kwocie v zaadresowana do B. Jeśli tylko taka transakcja istnieje, B może ją *wydać*, tworząc transakcję T_2, wpisując `pkC` (klucz publiczny użytkownika C) w pole odbiorcy i podpisując ją swoim podpisem. Taka transakcja jest następnie wysyłana do górników, którzy ją weryfikują, sprawdzając, czy `podpisB` na transakcji T_2 odpowiada kluczowi publicznemu `pkB` na transakcji T_1. Bezpieczeństwo algorytmu ECDSA gwarantuje nam, że transakcja zaadresowana do B nie zostanie wydana przez nikogo innego niż on sam.

Oczywiście, gdyby przedstawiony przeze mnie powyżej uproszczony opis był w pełni zgodny z rzeczywistością, Bitcoin byłby niesłychanie niepraktyczny – wszystkie transakcje musiałyby mieć tę samą wartość (jaką?). W rzeczywistości bitcoiny można w prosty sposób rozmieniać – każda transakcja może mieć kilku odbiorców i dzielić swoją wartość w dowolny sposób pomiędzy nich. Zatem chcąc wysłać użytkownikowi C tylko część kwoty v, użytkownik B może podać samego siebie jako drugiego odbiorcę transakcji T_2 i w ten sposób wziąć sobie *resztę*. Kwoty z mniejszych transakcji można też łączyć w większe, używając transakcji z kilkoma źródłami i w ten sposób wydać naraz kilka spośród swoich transakcji. Użytkownicy mogą więc tworzyć transakcje o dowolnej wartości, a majętność użytkownika określona jest przez sumę niewydanych i zaadresowanych do niego transakcji w sieci.

Z powyższego opisu można by wywnioskować, że Bitcoin służy jedynie do przelewania pieniędzy z jednego konta na drugie. Tymczasem jego możliwości są o wiele większe! Zamiast odbiorcy każda transakcja może mieć w sobie warunek (napisany w specjalnym języku programowania), który musi być spełniony, aby transakcja była poprawna. Można np. opublikować transakcję, którą może wydać pierwszy użytkownik, który poda rozkład na czynniki pierwsze jakiejś dużej liczby i w ten sposób stworzyć konkurs, który sam się rozstrzyga i sam wręcza nagrody. Można też o wiele więcej, ale to już temat na osobny artykuł.

Rozwiązanie zadania M 1496.
Zauważmy, że każda z liczb $1, \ldots, 2016$ jest wielokrotnością co najwyżej jednej z liczb $a_1, \ldots, a_n$. Jednocześnie wśród liczb $1, \ldots, 2016$ dokładnie $\left\lfloor \frac{2016}{a_i} \right\rfloor$ jest wielokrotnością liczby a_i. Stąd otrzymujemy

$$\left\lfloor \frac{2016}{a_1} \right\rfloor + \ldots + \left\lfloor \frac{2016}{a_n} \right\rfloor \leqslant 2016.$$

Ponieważ dla dowolnej liczby x prawdziwa jest nierówność $x - 1 < \lfloor x \rfloor$, więc

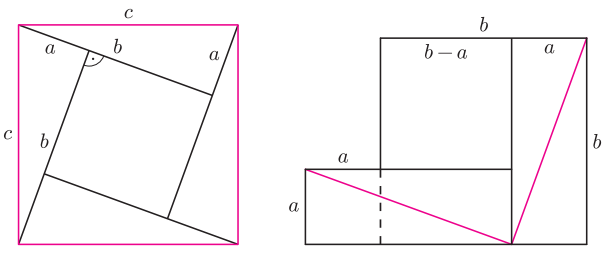
$$\left(\frac{2016}{a_1} - 1\right) + \ldots + \left(\frac{2016}{a_n} - 1\right) < 2016.$$

Dzieląc obie strony nierówności przez 2016 i przenosząc część wyrazów na prawą stronę, otrzymujemy tezę.

Kwadraty

*Jarosław GÓRNICKI**

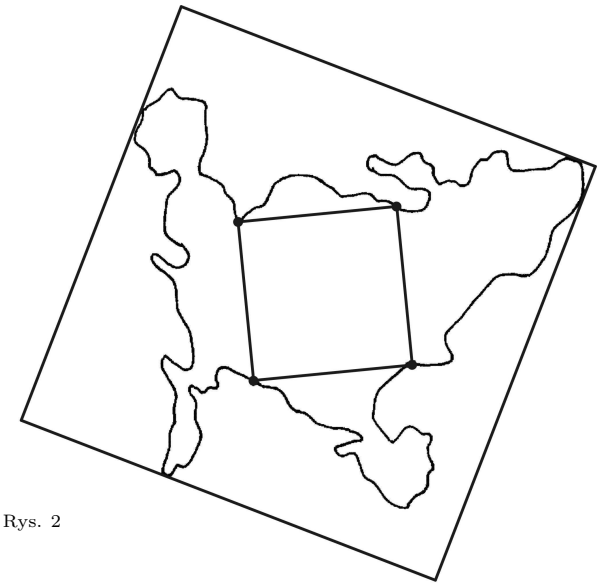
Euklides w *Elementach* pisał: „... kwadrat jest tym, co równoboczne i prostokątne...". Oto kilka niebanalnych obserwacji, w których kwadrat jest jednym z bohaterów.



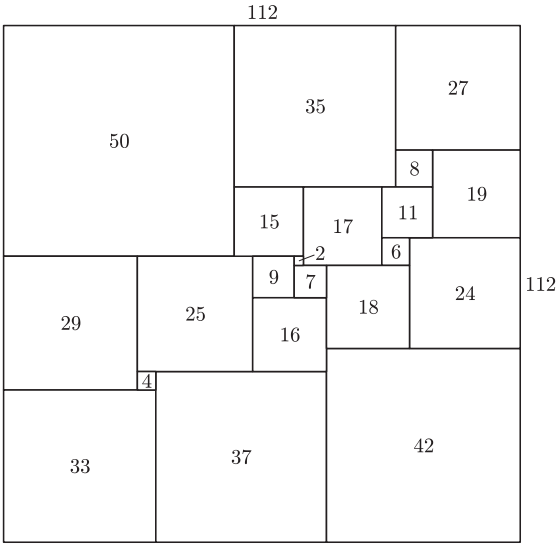
Rys. 1

(1) Badanie związków miarowych w kwadracie doprowadziło Pitagorejczyków (między innymi Hippasusa z Metapontu, V w. p.n.e.) do odkrycia, że $\sqrt{2}$, czyli długość przekątnej kwadratu jednostkowego nie jest ułamkiem zwykłym, a w konsekwencji do wyróżnienia liczb niewymiernych.
(2) Indyjski matematyk Bhāskara II (XII w.) w traktacie *Siddhānta Shiromani* (*Korona nauki*) podał dowód twierdzenia Pitagorasa w postaci rysunku 1 z napisem: Patrz!
(3) Kwadrat jest ciągłym obrazem odcinka (G. Peano, 1890).

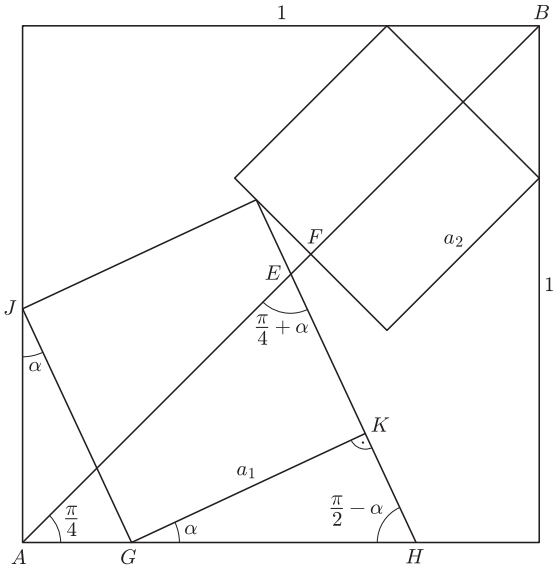
*Katedra Matematyki, Politechnika Rzeszowska



Rys. 2



Rys. 3



Rys. 4

(4) Wokół każdej figury (niekoniecznie wypukłej) można opisać kwadrat (rys. 2).
(5) Na każdej płaskiej krzywej zamkniętej istnieją cztery punkty, które są wierzchołkami kwadratu (L. Sznirelman, 1929, rys. 2).
(6) Rysunek 3 przedstawia jedyny podział kwadratu na najmniejszą możliwą (21) liczbę różnych kwadratów (A.J.W. Duijvestijn, 1978).

Z kwadratem związanych jest wiele pytań, na które nie znamy odpowiedzi. Prezentację kilku z nich poprzedzimy wykazaniem następującej obserwacji.

(7) *Jeżeli kwadraty o rozłącznych wnętrzach oraz bokach długości a_1, a_2 zawarte są w kwadracie jednostkowym, to $a_1 + a_2 \leqslant 1$.*

Dowód. Przy oznaczeniach z rysunku 4 pokażemy, że $|AE| \geqslant a_1\sqrt{2}$. Z twierdzenia sinusów zastosowanego do trójkąta AEH,

$$\frac{|AE|}{\sin\left(\frac{\pi}{2}-\alpha\right)} = \frac{|AH|}{\sin\left(\frac{\pi}{4}+\alpha\right)},$$

gdzie

$$|AG| = a_1 \sin\alpha \quad (\text{z } \triangle AGJ),$$
$$|GH| = \frac{a_1}{\cos\alpha} \quad (\text{z } \triangle KGH),$$
$$|AH| = |AG| + |GH| = a_1\left(\sin\alpha + \frac{1}{\cos\alpha}\right).$$

Zatem

$$|AE| = a_1 \frac{\left(\sin\alpha + \frac{1}{\cos\alpha}\right)\sin\left(\frac{\pi}{2}-\alpha\right)}{\sin\left(\frac{\pi}{4}+\alpha\right)} =$$
$$= a_1\sqrt{2}\,\frac{\sin\alpha\cos\alpha + 1}{\sin\alpha + \cos\alpha} \geqslant a_1\sqrt{2},$$

gdyż dla $\alpha \in \left[0, \frac{\pi}{2}\right)$,

$$\sin\alpha\cos\alpha + 1 - \sin\alpha - \cos\alpha =$$
$$= (1-\cos\alpha)(1-\sin\alpha) \geqslant 0.$$

Oznacza to, że

$$a_1 + a_2 \leqslant \frac{|AE|}{\sqrt{2}} + \frac{|BF|}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|AE| + |BF|) \leqslant$$
$$\leqslant \frac{1}{\sqrt{2}}\sqrt{2} = 1.$$

Ponadto istnieje wiele realizacji równości $a_1 + a_2 = 1$.

Rozważmy kwadrat jednostkowy, a w nim $n \geqslant 2$ kwadratów o rozłącznych wnętrzach i bokach długości $a_1, a_2, \ldots, a_n$.

Problem. *Jaka jest wartość funkcji $f(n) = \max \sum_{i=1}^{n} a_i$ dla poszczególnych wartości $n = 2, 3, \ldots$?*

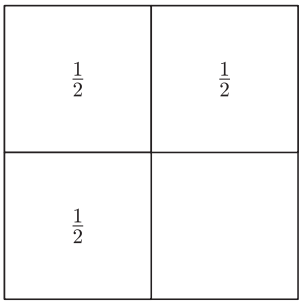
Poza wybranymi przypadkami odpowiedzi na to pytanie nie znamy! Z przeprowadzonego rozumowania wiemy już, że $f(2) = 1$.

Obliczmy wartość $f(3)$. Niech a_1, a_2, a_3 będą długościami boków trzech kwadratów o rozłącznych wnętrzach zawartymi w kwadracie jednostkowym. Skoro

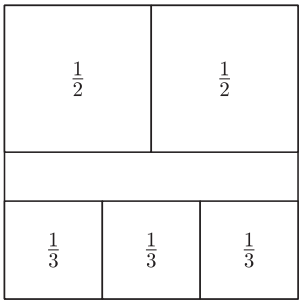
$$a_1 + a_2 \leqslant 1 \quad \text{i} \quad a_1 + a_3 \leqslant 1 \quad \text{i} \quad a_2 + a_3 \leqslant 1,$$

więc

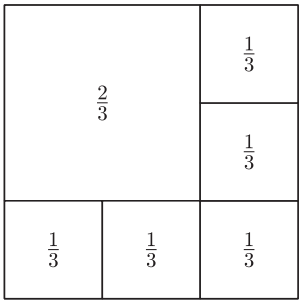
$$a_1 + a_2 + a_3 \leqslant \frac{3}{2}.$$



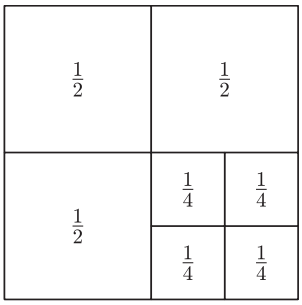
Rys. 5



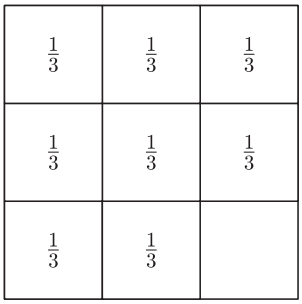
Rys. 6



Rys. 7



Rys. 8



Rys. 9

Ponieważ kwadraty z rysunku 5 realizują równość $a_1 + a_2 + a_3 = \frac{3}{2}$, więc $f(3) = \frac{3}{2}$.

Obliczając wartość $f(2^2)$, pokażemy rozumowanie ogólniejsze. Z nierówności Cauchy'ego:

$$\Big(\sum_{i=1}^{n} a_i b_i\Big)^2 \leqslant \Big(\sum_{i=1}^{n} a_i^2\Big)\Big(\sum_{i=1}^{n} b_i^2\Big),$$

przy $b_1 = b_2 = \ldots = b_n = 1$ mamy oszacowanie $\sum_{i=1}^{n} a_i \leqslant \sqrt{n}$, czyli

$$(*) \qquad f(n) \leqslant \sqrt{n}.$$

Wynik ten w połączeniu z podziałem kwadratu jednostkowego na $n = k^2$ przystających kwadratów zapewnia, że $f(k^2) = k$. Zatem,

$$f(2^2) = 2, \quad f(3^2) = 3, \quad f(4^2) = 4, \quad \text{itd.}$$

Pokażemy teraz oszacowanie funkcji $f(n)$ od dołu,

$$(**) \qquad \lfloor\sqrt{n}\rfloor \leqslant f(n),$$

gdzie symbol $\lfloor x\rfloor$ oznacza największą liczbę całkowitą nie większą niż x.

Dowód. Zauważmy, że funkcja $f(n)$ jest niemalejąca. Oznacza to, że nierówność $n \geqslant \lfloor\sqrt{n}\rfloor^2$ implikuje nierówność

$$f(n) \geqslant f(\lfloor\sqrt{n}\rfloor^2).$$

Gdy podzielimy kwadrat jednostkowy na $\lfloor\sqrt{n}\rfloor^2$ przystających kwadratów, każdy o boku długości $\frac{1}{\lfloor\sqrt{n}\rfloor}$ i obliczymy sumę długości ich boków $\frac{1}{\lfloor\sqrt{n}\rfloor} \cdot \lfloor\sqrt{n}\rfloor^2 = \lfloor\sqrt{n}\rfloor$, to otrzymamy nierówność

$$f(\lfloor\sqrt{n}\rfloor^2) \geqslant \lfloor\sqrt{n}\rfloor,$$

która w połączeniu z poprzednią nierównością daje oczekiwane oszacowanie.

W 1932 roku Pál Erdős (jako 19-letni student matematyki na Uniwersytecie w Budapeszcie) wyraził przypuszczenie, które do dziś nie zostało rozstrzygnięte.

Hipoteza Erdősa. *Dla każdej liczby naturalnej k, $f(k^2 + 1) = k$.*

W 1995 roku (po ponad sześćdziesięciu latach) Pál Erdős i Alexander Soifer uzyskali następujący rezultat.

Twierdzenie. *Dla każdej liczby naturalnej n postaci $n = k^2 + m$, gdzie $0 \leqslant m \leqslant 2k$ prawdziwe są oszacowania*:

(a) *jeżeli $m = 2t + 1$, gdzie $0 \leqslant t < k$, to $f(n) \geqslant k + \frac{t}{k}$,*
(b) *jeżeli $m = 2t$, gdzie $0 \leqslant t \leqslant k$, to $f(n) \geqslant k + \frac{t}{k+1}$.*

Dla małych n jest to konsekwencją elementarnych ilustracji. Niech $n = 5$. Wtedy oszacowanie $f(5) \geqslant 2$ wynika z rozmieszczenia kwadratów na rysunku 6. Dla $n = 6$ oszacowanie $f(6) \geqslant \frac{7}{3}$ jest konsekwencją sumy długości boków kwadratów przedstawionych na rysunku 7. Oszacowanie dla $n = 7$ w postaci $f(7) \geqslant \frac{5}{2}$ ilustrują kwadraty z rysunku 8. Sytuację dla $n = 8$ i oszacowanie $f(8) \geqslant \frac{8}{3}$ przedstawia rysunek 9.

Pozostaje wykazać, że $f(5) = 2$, $f(6) = \frac{7}{3}$, $f(7) = \frac{5}{2}$, $f(8) = \frac{8}{3}$, itd., lub wskazać przykłady, że wartości funkcji f mogą być większe, ale dotychczas nikt nie napisał, jak to zrobić. Można również badać ogólniejszy problem: dla jakich n zachodzi $f(n + 1) = f(n)$?