Uogólnienie algorytmu Euklidesa

*Adam BARAŃSKI**

* Student, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Algorytm Euklidesa najczęściej kojarzy nam się z wyznaczaniem największego wspólnego dzielnika dwóch liczb[†]. Istotnie, jest to elementarny i efektywny sposób na otrzymanie NWD dwóch liczb. Jednak czy korzystamy przy tym ze wszystkich informacji, jakie daje nam przeprowadzenie tego algorytmu? Okazuje się, że wiele jego bardzo ciekawych zastosowań... nawet nie korzysta z końcowego wyniku, jakim jest największy wspólny dzielnik. Na samym jednak początku przypomnijmy, na czym polega ów algorytm.

Weźmy dwie dowolne liczby naturalne $a > b$. Przez $\mathrm{NWD}(a,b)$ będziemy oznaczać największy wspólny dzielnik liczb a, b. Dla wygody zapisu oznaczmy $r_0 := a, r_1 := b$. Wówczas po podzieleniu z resztą otrzymujemy

$$r_0 = q_0 r_1 + r_2 \quad \text{dla pewnych naturalnych } q_0, r_2,\ 0 \leqslant r_2 < r_1.$$

Jeśli $r_2 = 0$, to kończymy algorytm, ponieważ $\mathrm{NWD}(r_0, r_1) = r_1$. W przeciwnym razie, gdy $r_2 \neq 0$, możemy powtarzać operację dzielenia z resztą aż do skutku. Jeśli przez r_{k+1} oznaczymy resztę z dzielenia r_{k-1} przez r_k, to otrzymamy ciąg nierówności

$$r_0 > r_1 > r_2 > \cdots \geqslant 0.$$

Jednak malejący ciąg nieujemnych liczb całkowitych nie może być nieskończony, więc dla pewnego n mamy $r_n > r_{n+1} = 0$. Zatem $r_{n-1} = q_{n-1} r_n$. Po obserwacji, że

$$\mathrm{NWD}(r_0, r_1) = \mathrm{NWD}(r_1, r_2) = \mathrm{NWD}(r_2, r_3) = \\ = \ldots = \mathrm{NWD}(r_{n-1}, r_n) = r_n,$$

otrzymujemy:

$$\begin{aligned} r_0 &= q_0 r_1 + r_2 & 0 &\leqslant r_2 < r_1 \\ r_1 &= q_1 r_2 + r_3 & 0 &\leqslant r_3 < r_2 \\ &\vdots & &\vdots \\ r_{n-2} &= q_{n-2} r_{n-1} + r_n & r_n &= \mathrm{NWD}(a,b). \end{aligned}$$

[†] O algorytmie Euklidesa można przeczytać w tym numerze *Delty* w Kąciku Początkującego Olimpijczyka.

Rozwiązanie zadania F 1024.
Zmiana temperatury stalowej kulki wyniesie $\Delta T = 80$°C. Dla osiągnięcia takiej zmiany należy dostarczyć energię w postaci ciepła równą

$$Q = \frac{4\pi R^3}{3} c\rho \Delta T.$$

Ciepło to będzie dostarczane przez powierzchnię kulki z szybkością

$$\frac{dQ}{dt} = 4\pi R^2 \cdot j.$$

W miarę ogrzewania wnętrza kulki strumień ciepła j wnikającego przez powierzchnię będzie się zmieniał. Dla naszego oszacowania przyjmijmy, że jego średnia (względem czasu) wartość to w (grubym) przybliżeniu

$$j \approx \lambda \frac{\Delta T}{R}.$$

Prowadzi to do oszacowania:

$$\tau \approx \frac{c\rho R^2}{3\lambda}.$$

Dla danych zadania otrzymujemy $\tau \approx 40$ s. Ściśle biorąc, ciepło właściwe stali i jej gęstość zależą od temperatury. Pominięcie tych zmian jest jednak nieistotne w porównaniu z niedokładnością naszego oszacowania średniego strumienia ciepła. Otrzymany wynik należy traktować jak oszacowanie rzędu wielkości czasu τ.

Przejdźmy więc do ciekawszej części, a mianowicie jednego z wielu zastosowań algorytmu Euklidesa. Zauważmy, że powyższe dzielenia z resztą można przepisać jako:

$$(1) \quad \frac{r_0}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}}, \quad \frac{r_1}{r_2} = q_1 + \frac{1}{\frac{r_2}{r_3}}, \quad \ldots, \quad \frac{r_{n-2}}{r_{n-1}} = q_{n-2} + \frac{1}{\frac{r_{n-1}}{r_n}}, \quad \frac{r_{n-1}}{r_n} = q_{n-1}.$$

W takim razie, podstawiając kolejno powyższe równości, otrzymujemy

$$\frac{r_0}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{r_2}{r_3}}} = \ldots = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1}}}}}.$$

Ułamki tej postaci nazywamy **ułamkami łańcuchowymi**.

Jak więc widzimy, algorytm Euklidesa pozwala nam na rozwijanie liczb wymiernych w ułamki łańcuchowe. Ponadto, skoro kończy się on po skończenie wielu krokach, to możemy dojść do następującego wniosku.

Twierdzenie 1. *Dla dowolnej liczby wymiernej algorytm Euklidesa daje skończone rozwinięcie w ułamek łańcuchowy.*

Kanoniczna wersja algorytmu Euklidesa pozwala nam rozwijać tylko liczby wymierne. Co jednak, gdybyśmy znaleźli analogiczną metodę dla wszystkich dodatnich liczb rzeczywistych? Jak się okazuje, nie jest to wcale aż tak trudne do osiągnięcia. Oznaczmy ilorazy $x_k := \frac{r_k}{r_{k+1}}$ dla $k = 0, 1, \ldots, n-1$; z równości (1) możemy odczytać

$$x_0 = q_0 + \frac{1}{x_1}, \quad x_1 = q_1 + \frac{1}{x_2}, \quad \ldots, \quad x_{n-2} = q_{n-2} + \frac{1}{x_{n-1}}, \quad x_{n-1} = q_{n-1},$$

przy czym dla każdego k zachodzi $\frac{1}{x_k} < 1$, więc q_k jest częścią całkowitą x_k. Niech $\lfloor x \rfloor$ będzie częścią całkowitą (funkcją *entier*) liczby $x \in \mathbb{R}$. Wtedy $x_k = q_k + \frac{1}{x_{k+1}} = \lfloor x_k \rfloor + \frac{1}{x_{k+1}}$, lub równoważnie

$$(2) \qquad q_k = \lfloor x_k \rfloor \quad \text{oraz} \quad x_{k+1} = \frac{1}{x_k - \lfloor x_k \rfloor} \qquad \text{dla } k = 0, 1, \ldots, n-2.$$

Wykazaliśmy więc, że x_k spełniają rekurencję (2) oraz

$$x_0 = q_0 + \cfrac{1}{\left\lfloor q_1 \right\rfloor + \cfrac{1}{\left\lfloor q_2 \right\rfloor + \cfrac{1}{\left\lfloor \cdots \right\rfloor + \cfrac{1}{\left\lfloor q_{n-1} \right\rfloor}}}}.$$

Łatwo możemy sprawdzić, że przeprowadzając operacje (2), jesteśmy w stanie rozwijać (możliwe, że „nieskończenie długo") każdą liczbę rzeczywistą w ułamek łańcuchowy. Korzystając z tego ogólnego algorytmu Euklidesa, możemy udowodnić następujący fakt.

Wniosek 1. *Liczba $\sqrt{2}$ nie należy do zbioru liczb wymiernych.*

W taki *poziomy* sposób będziemy odtąd zapisywać ułamek łańcuchowy

$$x_0 = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1}}}}}.$$

Dowód. Przyjmijmy $x_0 := \sqrt{2}$. Zauważmy, że $\lfloor\sqrt{2}\rfloor = 1$, więc $x_1 = \frac{1}{x_0 - \lfloor x_0\rfloor} = \frac{1}{\sqrt{2}-1} = = 1+\sqrt{2}$. Jednakże jeśli $x_n = 1+\sqrt{2}$, to $\lfloor x_n\rfloor = 2$, a w konsekwencji również

$$x_{n+1} = \frac{1}{x_n - \lfloor x_n\rfloor} = \frac{1}{1+\sqrt{2}-2} = \frac{1}{\sqrt{2}-1} = 1+\sqrt{2}.$$

Zatem skoro $x_1 = 1+\sqrt{2}$, to $x_n = 1+\sqrt{2}$ dla wszystkich naturalnych n. W takim razie $q_0 = 1$, $q_n = 2$ dla $n > 0$, a liczba

$$\sqrt{2} = 1 + \frac{1}{\left\lfloor 2\right\rfloor} + \frac{1}{\left\lfloor 2\right\rfloor} + \frac{1}{\left\lfloor 2\right\rfloor} + \frac{1}{\left\lfloor \cdots\right\rfloor}$$

ma nieskończone rozwinięcie w ułamek łańcuchowy, więc na mocy twierdzenia 1 nie może być wymierna. □

Przez ten nieskończony ułamek sygnalizujemy tu jedynie, że nasz algorytm się nie zatrzymuje. Przy odrobinie wysiłku można przypisać nieskończonym ułamkom łańcuchowym wartości liczbowe, ale o tym później.

Kluczową własnością algorytmu Euklidesa, z której korzystamy, jest to, że kończy się on po skończenie wielu krokach. Opiszemy teraz uogólnienie zachowujące tę cechę i dające nam możliwość szerszego zastosowania. Zauważmy, że operacja, którą wykonywaliśmy, parze (a, b) przypisywała parę (b, r), gdzie r było resztą z dzielenia a przez b. Algorytm kończył się po skończenie wielu krokach dlatego, że reszta z dzielenia była coraz mniejsza oraz ograniczona z dołu przez 0.

Podobnie możemy zdefiniować uogólnioną wersję. Dla ustalonego $m \in \mathbb{N}$ zdefiniujmy przekształcenie φ_m wzorem

$$\varphi_m(a, b) = (b \cdot m, r) \text{ dla } a \geqslant b,$$

gdzie r jest resztą z dzielenia a przez b. Zauważmy, że $b \cdot m \geqslant b > r$, a więc przy każdym przekształceniu φ_m druga współrzędna zmniejsza się i jest ograniczona z dołu przez 0. Zatem nie ma znaczenia, jakie bralibyśmy φ_{m_i} $(m_i \in \mathbb{N})$, zawsze algorytm, który w i-tym kroku przekształca parę (a, b) na $\varphi_{m_i}(a, b)$, kończy się po skończenie wielu krokach.

Zobaczmy na przykładzie, jak działa nasza uogólniona wersja algorytmu Euklidesa. Rozważmy ciąg $(m_k)_{k\in\mathbb{N}}$ taki, że $m_k = k$ dla każdego $k \in \mathbb{N}$, i zastosujmy ciąg przekształceń φ_{m_k} na liczbach 101 i 82. A więc mamy

$$(101, 82) \overset{\varphi_1}{\longmapsto} (82 \cdot 1, 19) \overset{\varphi_2}{\longmapsto} (19 \cdot 2, 6) \overset{\varphi_3}{\longmapsto} (6 \cdot 3, 2),$$

a skoro 18 jest podzielne przez 2, to kończymy algorytm. Od razu narzuca się następująca obserwacja – wynikiem naszego algorytmu nie musi być największy wspólny dzielnik liczb a i b (bowiem $\mathrm{NWD}(101, 82) = 1 \neq 2 = \mathrm{NWD}(18, 2)$). Możemy jednak w sposób analogiczny do (1) rozwinąć liczbę $\frac{101}{82}$ w uogólniony ułamek łańcuchowy, korzystając z przeprowadzonego algorytmu. Mamy:

$$\frac{101}{82} = 1 + \frac{1}{\frac{82\cdot 1}{19}}, \quad \frac{82\cdot 1}{19} = 4 + \frac{2}{\frac{19\cdot 2}{6}}, \quad \frac{19\cdot 2}{6} = 6 + \frac{3}{\frac{6\cdot 3}{2}},$$

zatem

$$\frac{101}{82} = 1 + \frac{1}{\frac{82\cdot 1}{19}} = 1 + \frac{1}{4 + \frac{2}{\frac{19\cdot 2}{6}}} = 1 + \frac{1}{4 + \frac{2}{6 + \frac{3}{\frac{6\cdot 3}{2}}}} = 1 + \frac{1}{4 + \frac{2}{6 + \frac{3}{9}}}.$$

Uogólnionymi ułamkami łańcuchowymi (*generalized continued fraction*) nazywamy wszystkie ułamki tej postaci, lub bardziej precyzyjnie, postaci:

$$a_0 + \frac{b_1}{\left\lfloor a_1\right\rfloor} + \frac{b_2}{\left\lfloor a_2\right\rfloor} + \frac{b_3}{\left\lfloor \cdots\right\rfloor} + \frac{b_n}{\left\lfloor a_n\right\rfloor}, \tag{3}$$

gdzie a_0 jest dowolną liczbą całkowitą, zaś $a_1, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ są naturalne. Ułamkiem łańcuchowym (po prostu) są wtedy ułamki postaci (3) dla $b_1 = b_2 = \ldots = b_n = 1$. Powyżej udało nam się więc rozwinąć ułamek $\frac{101}{82}$ w uogólniony ułamek łańcuchowy (3) dla $b_1 = 1$, $b_2 = 2$, $b_3 = 3$.

Zauważmy, że dla dowolnego ciągu liczb naturalnych $(m_k)_{k\in\mathbb{N}}$ możemy wyprowadzić podobne wzory, a mianowicie

$$q_k = \lfloor x_k\rfloor \quad \text{oraz} \quad x_{k+1} = \frac{m_{k+1}}{x_k - \lfloor x_k\rfloor} \qquad \text{dla } k = 0, 1, \ldots, n-2, \tag{4}$$

i wówczas

$$x_0 = q_0 + \frac{m_1}{\left\lfloor q_1\right\rfloor} + \frac{m_2}{\left\lfloor q_2\right\rfloor} + \frac{m_3}{\left\lfloor \cdots\right\rfloor} + \frac{m_{n-1}}{\left\lfloor x_{n-1}\right\rfloor}.$$

Ponieważ uogólniona wersja algorytmu Euklidesa również kończy się po skończenie wielu krokach, więc możemy sformułować odpowiednik twierdzenia 1.

Rozwiązanie zadania F 1023.
Po ogrzaniu do 100°C ciśnienie zawartego w butelce powietrza wzrośnie do $p = p_0 T/T_0$, gdzie $T = (273{,}15 + 100)$ K jest temperaturą końcową w skali Kelvina, a $T_0 = (273{,}15 + 20)$ K temperaturą początkową powietrza. Poza powietrzem w butelce będzie też para wodna. Maksymalne ciśnienie nasyconej pary wodnej w temperaturze $t_0 = 100°\mathrm{C} = = 373{,}15$ K jest równe standardowemu ciśnieniu atmosferycznemu $p_0 \approx 10^5$ Pa. Ciśnienie w butelce będzie równe sumie ciśnień powietrza i nasyconej pary wodnej. Ostatecznie:

$$p = p_0\left(1 + \frac{T}{T_0}\right).$$

Po podstawieniu danych liczbowych otrzymujemy $p \approx 2{,}34 \cdot 10^5$ Pa. Liczba moli nasyconej pary wodnej w objętości $V_0 = 10^{-3}$ m^3 i temepraturze $T = 373{,}15$ K wynosi:

$$n = \frac{p_0 V_0}{RT} \approx 0{,}041,$$

co odpowiada około 0,74 g, czyli około 0,74 cm^3 wody – jest to kropla o średnicy około 11 mm (masa 1 mola wody to 18 g, a jej gęstość w temperaturze 20°C to ok. 1 g/cm^3). Co najmniej tyle wody musi znajdować się w butelce przed rozpoczęciem ogrzewania, żeby osiągnąć obliczone wyżej ciśnienie.
W temperaturze 20°C ciśnienie pary nasyconej wynosi około 2,34 kPa. Przyjęcie, że przed ogrzewaniem poza powietrzem w butelce była także para nasycona, wprowadziłoby nieznaczną poprawkę do podanego wyniku (mniej niż 0,001 mola pary).

Rozwiązanie zadania M 1674.
Rozpatrzmy dowolny punkt X z danego zbioru i weźmy okrąg Ω o środku w punkcie X i promieniu $D + \frac{d}{2}$. Z definicji D okrąg Ω zawiera wszystkie 25 okręgów o środkach w wyjściowych punktach i promieniu $\frac{d}{2}$. Wobec tego porównując pola, dostajemy

$$\pi\left(D + \frac{d}{2}\right)^2 > 25 \cdot \pi\left(\frac{d}{2}\right)^2,$$

czyli równoważnie $D > 2d$.

Twierdzenie 2. *Dla każdego ciągu $(m_k)_{k\in\mathbb{N}}$, jeśli liczba x_0 jest wymierna, to po zastosowaniu algorytmu opisanego wzorem (4) uzyskane rozwinięcie w uogólniony ułamek łańcuchowy dla $b_i = m_{i+1}$ jest skończone.*

Warto tutaj dodać kilka słów komentarza. Rozwinięcie uzyskane przez zastosowanie algorytmu Euklidesa (bądź jego uogólnionej wersji) jest jednoznacznie wyznaczone. Nie oznacza to jednak, że rozwinięcie liczby w uogólniony ułamek łańcuchowy jest jednoznaczne – nawet po ustaleniu ciągu $(m_k)_{k\in\mathbb{N}}$ możliwe jest uzyskanie różnych rozwinięć danej liczby (jak na marginesie obok). Twierdzenie to daje nam jednak pewność, że rozwijając liczbę wymierną w szczególny sposób (dany wzorem (4)), otrzymamy rozwinięcie skończone. Zaobserwujmy jego zastosowanie na przykładzie dowodu następującego faktu.

Dla ciągu $(m_k)_{k\in\mathbb{N}} = (2, 2, \ldots)$ wszystkie poniższe rozwinięcia dają tę samą liczbę:
$\frac{2}{2}$, $\cfrac{2}{1+\frac{2}{2}}$, $\cfrac{2}{1+\cfrac{2}{1+\frac{2}{2}}}$, $\ldots$

Wniosek 2. *Liczba e jest niewymierna.*

Dowód. Dowód oprzemy na rozwinięciu e w nieskończony uogólniony ułamek łańcuchowy:

$$e = \lim_{n\to\infty} R_n, \quad \text{gdzie } R_n := 2 + \cfrac{1\rfloor}{\lceil 1} + \cfrac{1\rfloor}{\lceil 2} + \cfrac{2\rfloor}{\lceil 3} + \cfrac{3\rfloor}{\lceil \ldots} + \cfrac{n-1\rfloor}{\lceil n}.$$

Znając już rozwinięcie liczby e, łatwo uzasadnić jej niewymierność. Przyjmijmy ciąg $(m_k) = (1, 1, 2, 3, \ldots)$ i zastosujmy uogólniony algorytm Euklidesa (4) do $x_0 = e$. Dla wyznaczenia x_1 wystarczy zauważyć, że zaznaczony na marginesie kolorem ułamek $e' = 1 + \cfrac{1\rfloor}{\lceil 2} + \cfrac{2\rfloor}{\lceil 3} + \cfrac{3\rfloor}{\lceil 4} + \ldots$ jest większy od 1. W konsekwencji $\lfloor e \rfloor = 2$ i wartość $x_1 = \frac{1}{e-2}$ jest równa właśnie e'. I tak dalej, łatwo przekonać się, że uogólniony algorytm Euklidesa w kolejnych krokach po prostu *odcina* kolejne początkowe fragmenty ułamka. Skoro ułamek ten jest nieskończony, algorytm nigdy nie kończy działania, co na mocy twierdzenia 2 oznacza niewymierność e.

Można się umówić, że granicę ciągu R_n zapiszemy jako

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \ddots}}}}$$

Pozostaje uzasadnić zbieżność $R_n \to e$. W tym celu będziemy korzystać z następującej definicji liczby e:

$$\frac{1}{e} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots$$

Da się wykazać, że $R_n = \frac{P_n}{Q_n}$, gdzie P_n, Q_n zdefiniowane są rekurencyjnie, a mianowicie:

$$P_0 = 2, \quad P_1 = 3, \quad P_{n+1} = P_n(n+1) + P_{n-1}n \quad \text{dla} \quad n \geqslant 1$$
$$Q_0 = 1, \quad Q_1 = 1, \quad Q_{n+1} = Q_n(n+1) + Q_{n-1}n \quad \text{dla} \quad n \geqslant 1.$$

Dla ułamka jak w (3) rekurencję $P_{n+1} = a_{n+1}P_n + b_{n+1}P_{n-1}$ (i podobną dla Q_{n+1}) można uzasadnić przez obserwację, że zamiana a_n na $a_n + \frac{a_{n+1}}{b_{n+1}}$ daje ułamek o jedno piętro dłuższy.

Zauważmy, że $P_0 = 2 = \frac{2!}{1}$, $P_1 = 3 = \frac{3!}{2}$, $P_2 = 8 = \frac{4!}{3}$ itd. Za pomocą indukcji możemy udowodnić, że $P_n = \frac{(n+2)!}{n+1}$. Gdy znamy już wartość P_n, narzuca się podstawienie

$$\widetilde{Q}_n = \frac{Q_n}{P_n} = Q_n \frac{n+1}{(n+2)!}.$$

Wówczas $\widetilde{Q}_0 = \frac{1}{2}$, $\widetilde{Q}_1 = \frac{1}{3}$ oraz z rekurencji mamy

$$\widetilde{Q}_{n+1} \frac{(n+3)!}{n+2} = \widetilde{Q}_n (n+2)! + \widetilde{Q}_{n-1}(n+1)!$$

Dzieląc stronami przez $\frac{(n+3)!}{n+2}$, dostajemy $\widetilde{Q}_{n+1} = \widetilde{Q}_n \frac{n+2}{n+3} + \widetilde{Q}_{n-1}\frac{1}{n+3}$. Jednakże wówczas $\widetilde{Q}_{n+1} - \widetilde{Q}_n = -\frac{1}{n+3}(\widetilde{Q}_n - \widetilde{Q}_{n-1})$, co przez indukcję pozwala wyznaczyć $\widetilde{Q}_{n+1} - \widetilde{Q}_n = \frac{(-1)^{n+3}}{(n+3)!}$ i ostatecznie $\widetilde{Q}_n = \sum_{k=0}^{n+2} \frac{(-1)^k}{k!}$. Zatem

$$\lim_{n\to\infty} R_n = \lim_{n\to\infty} \frac{P_n}{Q_n} = \lim_{n\to\infty} \frac{1}{\widetilde{Q}_n} = \frac{1}{\lim\limits_{n\to\infty} \sum_{k=0}^{n+2} \frac{(-1)^k}{k!}} = \frac{1}{e^{-1}} = e.$$

Kończy to dowód zbieżności $R_n \to e$, a zatem i dowód niewymierności e. □

Liczbę π możemy zapisać jako nieskończony ułamek łańcuchowy w następujący sposób:

$$\pi = \cfrac{4}{1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \ddots}}}}}$$

W powyższym dowodzie kluczowe było przedstawienie liczby e w postaci nieskończonego ułamka łańcuchowego. Niestety, nie każde rozwinięcie ma taką własność, że przy każdym kroku algorytmu *schodzimy* o jedno piętro w dół. Taka sytuacja nie ma na przykład miejsca, gdy przeprowadzamy algorytm na przedstawionym obok rozwinięciu liczby π. Od razu więc narzuca się pytanie, czy możemy w jakiś sposób sklasyfikować te rozwinięcia, na których przeprowadzenie algorytmu *odcina* kolejne piętra? Czy jest w ogóle możliwe, aby przeprowadzenie algorytmu niekoniecznie *schodziło* o jedno, ale na przykład o kilka pięter w dół? I najważniejsze, jaki ma to wszystko związek z tytułowym algorytmem Euklidesa…?