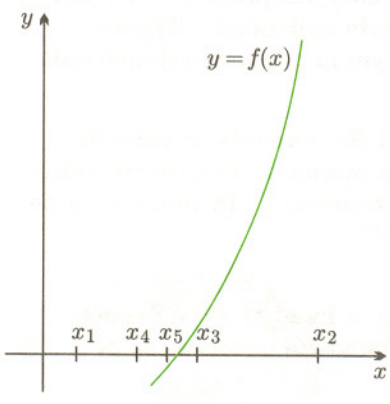
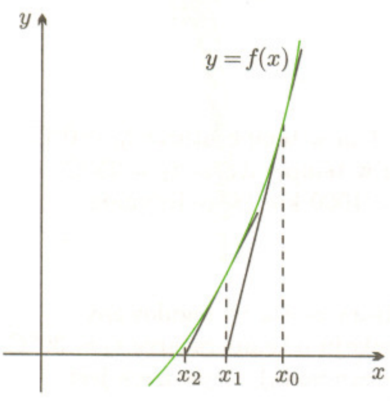
Zabawy z kalkulatorem (II)

Piotr HAJŁASZ

Oto metoda z poprzedniego artykułu: Niech funkcja $y = f(x)$ ma wykres mniej więcej taki jak na rysunku 1. Załóżmy, że x_1 leży na lewo od rozwiązania, a x_2 na prawo. Zakładamy, że oba punkty x_1 i x_2 leżą dostatecznie blisko miejsca zerowego funkcji f, tak że pomiędzy x_1 i x_2 równanie $f(x) = 0$ ma tylko jeden pierwiastek. Kolejny punkt wybieramy na środku $x_3 = \frac{1}{2}(x_1 + x_2)$. Znak liczby $f(x_3)$ pokazuje, czy punkt x_3 leży na lewo czy na prawo od rozwiazania. Załóżmy, że na prawo. Wówczas, jako kolejne przybliżenie bierzemy $x_4 = \frac{1}{2}(x_1 + x_3)$. Analogicznie określamy $x_5, x_6, x_7, \ldots$ Za każdym razem dzielimy przedział, do którego należy rozwiązanie, na pół. Skracająca się długość przedziału świadczy o polepszającej się dokładności przybliżenia. Ponieważ po trzech podziałach długość przedziału skraca się 8 razy, a po czterech 16 razy, więc uzyskamy kolejną dokładną cyfrę rozwinięcia dziesiętnego po wyliczeniu 3–4 nowych przybliżeń x_n, a dokładniej mniej więcej co 3,3 nowych przybliżeń, bo $10^{-1} \approx 2^{-3,3}$. W efekcie, jak widzieliśmy w poprzednim artykule, stosując tę metodę do równania $x^2 - 2 = 0$, uzyskaliśmy przybliżoną wartość $\sqrt{2} = 1{,}414\,213\,5$ dopiero po obliczeniu x_{26}. To naprawdę mozolne rachunki.



Rys. 1



Rys. 2

W poprzednim artykule (*Delta* 1/2001) opisaliśmy bardzo prostą metodę pozwalającą na znajdowanie przybliżonego rozwiązania równania $f(x) = 0$. Szczególnie dużo uwagi poświęciliśmy znajdowaniu przybliżonej wartości $\sqrt{2}$, czyli rozwiązania równania $x^2 - 2 = 0$. Metoda była jednak mało skuteczna z racji tego, że wymagała wykonania wielu obliczeń (jej ideę przypominamy na marginesie).

W niniejszym artykule opiszemy zupełnie inną metodę zwaną *metodą stycznych Newtona*. Jak zobaczymy, w odróżnieniu od metody poprzedniej pozwala ona na nieomal błykawiczne uzyskanie oczekiwanego wyniku.

Rozwiązanie równania $f(x) = 0$ to punkt przecięcia wykresu funkcji $y = f(x)$ z osią x-ów. Załóżmy, że wykres funkcji $y = f(x)$ wygląda mniej więcej tak jak na rysunku 2.

Weźmy jakiś punkt x_0 leżący na prawo od punktu przecięcia. Narysujmy styczną do wykresu w punkcie $(x_0, f(x_0))$. Przecina ona oś x-ów w jakimś punkcie x_1. Teraz rysujemy styczną do wykresu w punkcie $(x_1, f(x_1))$. Przecina ona oś x-ów w punkcie x_2 itd. W efekcie otrzymujemy ciąg x_n zbieżny do rozwiązania równania $f(x) = 0$. Zobaczmy, czy ciąg ten można opisać za pomocą jakiegoś konkretnego wzoru. Z rysunku 3. widać, że $f(x_n) = \operatorname{tg} \alpha_n (x_n - x_{n+1}) = f'(x_n)(x_n - x_{n+1})$. Stąd otrzymujemy wzór rekurencyjny

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}. \tag{1}$$

A więc punkt x_0 wybieramy w sposób dowolny (ma to być jednak punkt położony niezbyt daleko od rozwiązania), kolejne zaś punkty obliczamy za pomocą wzoru (1).

Oczywiście $\sqrt{2}$ jest rozwiązaniem równania $f(x) = 0$ dla $f(x) = x^2 - 2$. Ponieważ $f'(x) = 2x$, więc wzór (1) przyjmuje postać

$$x_{n+1} = x_n - \frac{x_n^2 - 2}{2x_n} = \frac{x_n^2 + 2}{2x_n}.$$

Otrzymaliśmy interesujący wzór opisujący ciąg zbieżny do $\sqrt{2}$. Przyjmijmy $x_0 = 2$ i zobaczmy, jak szybko ten ciąg przybliża się do $\sqrt{2}$. Obliczenia wykonałem na moim kalkulatorze: $x_0 = 2$, $x_1 = 1{,}5$, $x_2 = 1{,}416\,666\,6$, $x_3 = 1{,}414\,215\,6$, $x_4 = 1{,}414\,213\,5$. I to wszystko. To jest najlepsze przybliżenie, jakie mogę uzyskać na moim kalkulatorze.

Zobaczmy, jak niebywale lepsza jest to metoda od poprzednio opisanej! Długie i mozolne rachunki zostały zastąpione przez wciśnięcie kilku klawiszy na kalkulatorze. Nie byłoby jednak tej metody, gdyby nie znajomość pochodnych!

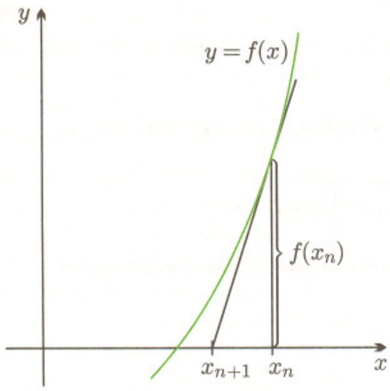
Dla jakich równań daje się zastosować tę metodę? Pamiętajmy, że w sposób istotny korzystaliśmy z tego, że wykres wygląda tak jak na rysunku 2. Co to znaczy? Jak to precyzyjnie opisać? Czy da się wytłumaczyć, dlaczego metoda Newtona jest wielekroć lepsza od poprzednio opisanej? Czy można oszacować, jak szybko ciąg x_n dąży do rozwiązania równania?

Aby odpowiedzieć na te pytania, musimy sięgnąć nieco głębiej do matematyki, wyjaśnienie bowiem niebywałej skuteczności metody Newtona ukryte jest w twierdzeniu Taylora.

Załóżmy, że funkcja $y = f(x)$ ma drugą pochodną ciągłą oraz że $f(\alpha) = 0$. Naszym zadaniem jest znalezienie przybliżonej wartości α.

Załóżmy, że $f'(\alpha) \neq 0$, co oznacza, że wykres funkcji $y = f(x)$ przecina oś x-ów w punkcie α pod kątem różnym od zera, czyli odrzucamy sytuację, w której wykres jest styczny do osi x-ów w punkcie α.

Przy badaniu metody Newtona skorzystamy z *Twierdzenia Taylora* (zwanego też wzorem Taylora), które mówi, że *jeżeli funkcja f jest dwukrotnie różniczkowalna,* Istnieje wersja wzoru Taylora, w której występują pochodne funkcji f rzędów wyższych niż 2. Wówczas twierdzenie Taylora mówi o tym, z jak dużą dokładnością możemy przybliżać funkcję f wielomianami.



Rys. 3

Metoda Newtona to jedna z metod numerycznego rozwiązywania równań. Metody numeryczne tworzą bardzo rozbudowany dział matematyki stosowanej. Odgrywają one fundamentalną rolę w fizyce, technice, informatyce. Dużo mówi się o zastosowaniach komputerów, między innymi, do prognozowania pogody, projektowania samolotów i rozwiązywania wielu innych praktycznych problemów. Podstawowa metoda polega na tym, że najpierw matematycy razem z fizykami i inżynierami przeformułowują problem na język równań. Są to na ogół bardzo skomplikowane równania *różniczkowe*, tak skomplikowane, że zazwyczaj ich zrozumienie wymaga wieloletnich studiów matematycznych. Następnie do ich przybliżonego rozwiązania wykorzystuje się komputery. Na ogół wymaga to wielu godzin pracy najszybszych komputerów. Dlatego też istotne jest, aby stosowana przez nas metoda przybliżonego rozwiązywania równania jak najszybciej prowadziła do celu. Z tego też względu metoda Newtona jest znacznie lepsza do zastosowań w komputerach niż metoda omawiana w poprzednim artykule. Trzeba również umieć oszacować błąd przybliżenia, które otrzymujemy. To wszystko są bardzo skomplikowane zagadnienia, wymagające doskonałej znajomości abstrakcyjnej matematyki. Drogi Czytelniku, jeżeli ta tematyka wzbudziła Twoje zainteresowanie, polecam Ci dwie książki: G. Dahlquist, Å. Björk, *Metody numeryczne*, PWN 1983, oraz A. Palczewski, *Równania różniczkowe zwyczajne (teoria i metody numeryczne z wykorzystaniem komputerowego systemu obliczeń symbolicznych)*, WNT 1999. W książce Palczewskiego znajdziesz konkretne przykłady zastosowań w fizyce, elektronice, mechanice, ekonomii, biologii i medycynie. Niestety, obie książki wymagają dość dobrego przygotowania matematycznego w zakresie pierwszych trzech semestrów studiów matematycznych. Obejrzyj je, może zachęcą Cię do studiowania matematyki?

to dla dowolnych liczb c i x istnieje taka liczba ξ, leżąca pomiędzy c i x, że spełniona jest równość

$$f(x) = f(c) + f'(c)(x-c) + \frac{1}{2}f''(\xi)(x-c)^2 .$$

Spróbujmy wyjaśnić znaczenie tego twierdzenia. Potraktujmy x jako zmienną, c zaś jako ustalony parametr. Zauważmy, że pierwsze dwa składniki po prawej stronie to funkcja liniowa zmiennej x. Jeśli zaś odległość x od c (czyli $|x-c|$) jest mała, to $(x-c)^2$ ma bardzo małą wartość i w efekcie trzeci składnik sumy po prawej stronie ma bardzo małą wartość. Dlatego też twierdzenie Taylora należy rozumieć jako twierdzenie mówiące o tym, z jak dużą dokładnością możemy przybliżyć funkcję $f(x)$ funkcją liniową. Mianowicie, funkcja $f(x)$ różni się od funkcji liniowej $f(c)+f'(c)(x-c)$ o bardzo niewielką wartość $\frac{1}{2}f''(\xi)(x-c)^2$.

Twierdzenie Taylora jest dość abstrakcyjne, zobaczymy jednak, jak niesłychanie skutecznym narzędziem jest ono przy badaniu metody Newtona.

Niech x_n będzie ciągiem uzyskanym metodą Newtona, dla równania $f(x)=0$, przy założeniach powyżej opisanych. Oznaczmy $\varepsilon_n = x_n - \alpha$. Liczba ε_n mówi, z jaką dokładnością x_n przybliża rzeczywistą wartość α.

Ponieważ założyliśmy, że funkcja f ma drugą pochodną ciągłą, więc możemy zastosować twierdzenie Taylora. Podstawiając $x=\alpha$ i $c=x_n$, otrzymujemy

$$0 = f(\alpha) = f(x_n) + f'(x_n)(\alpha - x_n) + \frac{1}{2}f''(\xi)(\alpha - x_n)^2 ,$$

gdzie ξ jest pewną liczbą leżącą pomiędzy α i x_n. Dzieląc przez $f'(x_n)$, dostajemy

$$-\frac{f(x_n)}{f'(x_n)} - (\alpha - x_n) = \frac{1}{2}\frac{f''(\xi)(\alpha - x_n)^2}{f'(x_n)} .$$

Zauważmy, że na mocy wzoru rekurencyjnego (1) lewa strona to nic innego, jak tylko $x_{n+1} - \alpha = \varepsilon_{n+1}$. Stąd zaś otrzymujemy

$$\varepsilon_{n+1} = \frac{1}{2}\frac{f''(\xi)}{f'(x_n)}\varepsilon_n^2 . \tag{2}$$

Wzór ten mówi, jak szybko zmienia się błąd przybliżenia. Wartości x_n szybko zbliżają się do α, jeżeli ε_n szybko dąży do zera. No właśnie, jak odczytać ze wzoru (2) szybkość, z jaką ε_n dąży do zera?

Załóżmy, że α leży pomiędzy liczbami a i b, czyli $\alpha \in (a,b)$. Załóżmy, że funkcja f ma tę własność, iż iloraz

$$\frac{1}{2}\left|\frac{f''(y)}{f'(x)}\right|$$

jest ograniczony z góry przez pewną stałą m dla dowolnych liczb x i y leżących pomiędzy a i b (czyli $x, y \in (a,b)$).

Załóżmy, wreszcie, że przedział (a,b) jest na tyle szeroki, iż wszystkie wyrazy ciągu x_n należą do tego przedziału. Wówczas ze wzoru (2) wynika, że $|\varepsilon_{n+1}| \le m\varepsilon_n^2$. To zaś oznacza, że jeżeli, na przykład, ε_1 i m są małe, to ciąg ε_n bardzo szybko dąży do 0. Istotnie, załóżmy dla przykładu, że $m \le 1$ oraz że $\varepsilon_1 < 0{,}1$. Wówczas $\varepsilon_2 < 0{,}01$, $\varepsilon_3 < 0{,}000\,1$, $\varepsilon_4 < 0{,}000\,000\,01, \ldots, \varepsilon_n < 10^{-2^{n-1}}$. A więc obliczenie kolejnego wyrazu podwaja liczbę dokładnych cyfr po przecinku!

Przyjrzyjmy się omawianemu już przykładowi ciągu zbieżnego do $\sqrt{2}$. Funkcja $f(x) = x^2 - 2$ spełnia warunek

$$\frac{1}{2}\left|\frac{f''(y)}{f'(x)}\right| = \frac{1}{2x} < 1 = m ,$$

dla dowolnych $x, y \ge 1$. Biorąc $x_0 = 2$, otrzymujemy $x_1 = 1{,}5$, skąd $\varepsilon_1 < 0{,}1$. Mamy więc sytuację dokładnie taką samą, jak opisana przed chwilą. A więc $\varepsilon_4 < 0{,}000\,000\,01$, lepszej dokładności na moim kalkulatorze (na którym wyświetla się 8 cyfr) już nie osiągnę. I rzeczywiście, jak już wcześniej zauważyliśmy, lepszego przybliżenia niż x_4 na tym kalkulatorze nie uzyskam.

W naszych rozważaniach pominęliśmy jeden istotny aspekt: ponieważ obliczenia wykonywałem na kalkulatorze, więc również obliczane przeze mnie wartości wyrazów ciągu $x_1, x_2, x_3, \ldots$ były obarczone pewnym błędem przybliżenia. Kolejne wyrazy ciągu obliczałem, korzystając z przybliżonej wartości wyrazów poprzednich. Czy błędy te przypadkiem nie kumulowały się?

W metodzie omawianej w *Delcie* 1/2001 musieliśmy obliczyć x_{26}, żeby uzyskać 7 dokładnych cyfr po przecinku. Przy metodzie Newtona dla x_{26} otrzymalibyśmy co najmniej $2^{25} = 33\,554\,432$ dokładnych cyfr!.

Zadanie 1. Udowodnić nierówność

$$|\varepsilon_n| \leq \frac{1}{m}(m\varepsilon_0)^{2^n}$$

i wyciągnąć stąd wniosek, że gdy $|m\varepsilon_0| < 1$, to $x_n \to \alpha$. Zastanowić się nad stwierdzeniem, że x_n bardzo szybko dąży do α.

Zadanie 2. Ze wzorów na pierwiastki równań stopnia trzeciego wynika, że pierwiastkiem równania $x^3 = x + 4$ jest

$$\alpha = \sqrt[3]{2 + \frac{1}{9}\sqrt{321}} + \sqrt[3]{2 - \frac{1}{9}\sqrt{321}}\,.$$

Wykorzystać metodę Newtona w celu wyznaczenia przybliżonej wartości α.

„Zespolone" kongruencje kwadratowe

Kwadrat liczby całkowitej przy dzieleniu przez 3 nie daje reszty 2. Zatem kongruencja $x^2 \equiv 2 \pmod 3$ nie ma rozwiązania w liczbach całkowitych. Idąc wytyczonym szlakiem teorii liczb zespolonych (patrz *Delta* 10/2000; można też zajrzeć do *Delty* 4/1999), spróbujmy poszukać rozwiązania na innym gruncie.

Załóżmy, że p jest taką liczbą pierwszą, dla której równanie $x^2 \equiv p - 1 \pmod p$ nie ma rozwiązania w liczbach całkowitych. Określamy zbiór par liczb całkowitych ze zbioru $Z_p = \{0, 1, 2, \ldots, p-1\}$ z działaniami

$$(a, b) + (c, d) = (a + c,\ b + d),$$
$$(a, b) \cdot (c, d) = (ac - bd,\ ad + bc),$$

gdzie działania w nawiasach należy rozumieć jako dodawanie, odejmowanie i mnożenie modulo p. Można sprawdzić, że zdefiniowane działania mają porządne własności, co fachowo wyraża się, mówiąc, iż zbiór $Z_p \times Z_p$ z tak określonymi działaniami tworzy ciało. Para postaci $(a, 0)$ to zwykła liczba całkowita ze zbioru Z_p. Jednostką urojoną jest, oczywiście, $i = (0, 1)$. Mamy bowiem $i^2 = (0, 1) \cdot (0, 1) = (p - 1, 0)$ (pamiętamy, że działania są określone w zbiorze Z_p, a więc liczbę -1, która pojawiła się w wyniku formalnego mnożenia, zastąpiliśmy liczbą $p - 1$).

Przykład. Rozwiązać równanie $x^2 + x + 3 \equiv 0 \pmod 7$ (milcząco założyliśmy, że kongruencja $t^2 \equiv 6 \pmod 7$ nie ma rozwiązania – łatwo to sprawdzić). Zastosujemy znane wzory. Mamy

$$\Delta = 1^2 - 4 \cdot 1 \cdot 3 = -11 \equiv 3 \pmod 7.$$

Należy wyznaczyć $\sqrt{\Delta}$. Ponieważ kwadrat liczby całkowitej przy dzieleniu przez 7 może dawać tylko reszty 0, 1, 2, 4, więc liczba $\sqrt{\Delta}$ jest „zespolona". Niech $\sqrt{\Delta} = (a, b)$, czyli $3 = (a, b) \cdot (a, b)$. Inaczej: $(3, 0) = (a^2 - b^2,\ 2ab)$. Wynika stąd, że $a^2 - b^2 = 3$ i $2ab = 0$. Zatem $a = 0$ lub $b = 0$. Równość $b = 0$ prowadzi do sprzeczności, bo wtedy $a^2 \equiv 3 \pmod 7$, co jest niemożliwe. Jeśli $a = 0$, to $-b^2 \equiv 3 \pmod 7$, co daje $b = 2$ lub $b = 5$. Zatem $\sqrt{\Delta} = (0, 2)$ lub $\sqrt{\Delta} = (0, 5)$, czyli $\sqrt{\Delta} = 2i$ lub $\sqrt{\Delta} = 5i$.

Wobec tego

$$x_1 = \frac{-1 + 2i}{2} = -\frac{1}{2} + i \quad \text{lub} \quad x_2 = \frac{-1 + 5i}{2} = -\frac{1}{2} + \frac{5}{2}i.$$

Co z ułamkami? Przecież szukamy rozwiązań całkowitych. Pamiętajmy jednak, że działania są modulo, a zatem i dzielenie jest modulo: $\frac{1}{2}$ to 4, bo $4 \cdot 2 \equiv 1 \pmod 7$. Ostatecznie

$$x_1 \equiv -4 + i \equiv 3 + i, \qquad x_2 \equiv -4 + 20i \equiv 3 + 6i \pmod 7.$$

Jeszcze prościej otrzymujemy rozwiązania wspomnianej kongruencji $x^2 \equiv 2 \pmod 3$. Mamy tu $x_1 = i$, $x_2 = 2i$.

Nasuwają się następujące pytania:

(1) Dla jakich liczb pierwszych p kongruencja $x^2 \equiv p - 1 \pmod p$ nie zachodzi dla żadnego całkowitego x?

(2) Czy dla dowolnej pary $(a, 0)$ istnieje taka para (x, y), że $(x, y) \cdot (x, y) = (a, 0)$, to znaczy czy każdą liczbę z Z_p można pierwiastkować w sensie „zespolonym"?

(3) Czy zachodzi Zasadnicze Twierdzenie Algebry w tak określonym ciele $Z_p \times Z_p$, to znaczy, czy każdy wielomian o współczynnikach całkowitych ma „zespolone" miejsca zerowe (w sensie kongruencji)?

Ad (1). Postulowany warunek spełniają liczby pierwsze p postaci $4k + 3$ i tylko takie (np. W. Sierpiński, *Arytmetyka teoretyczna*, PWN, Warszawa 1969, str. 158).

Ad (2). Odpowiedź jest pozytywna (j.w.).

Ad (3). Odpowiedź jest negatywna. Na przykład kongruencja $x^3 - x + 1 \equiv 0 \pmod 3$ nie ma rozwiązania w $Z_3 \times Z_3$. Przypuśćmy bowiem, że $x = a + bi$ jest takim rozwiązaniem. Wówczas

$$(a + bi)^3 - (a + bi) + 1 \equiv 0 \pmod 3.$$

Stąd po przekształceniach otrzymujemy

$$(a^3 - 3ab^2 - a + 1) + (3a^2b - b^3 - b)i \equiv 0 \pmod 3,$$

czyli

$$a^3 - a + 1 \equiv 0 \pmod 3 \quad \text{i} \quad -b^3 - b \equiv 0 \pmod 3.$$

Ponieważ $a^3 - a = a(a - 1)(a + 1)$, więc $a^3 - a \equiv 0 \pmod 3$, bo spośród trzech kolejnych liczb całkowitych jedna zawsze jest podzielna przez 3. Stąd $a^3 - a + 1 \equiv 1 \pmod 3$. Proste uogólnienie tego rozumowania wskazuje, że w żadnym ciele skończonym nie zachodzi Zasadnicze Twierdzenie Algebry. Szkoda!

Witold BEDNAREK