W naszych rozważaniach pominęliśmy jeden istotny aspekt: ponieważ obliczenia wykonywałem na kalkulatorze, więc również obliczane przeze mnie wartości wyrazów ciagu $x_1, x_2, x_3, \ldots$ 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 $x_1 = i, \quad x_2 = 2i$.

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