Równania czy nie równania?

Piotr WOJCIECHOWSKI

Autor w momencie złożenia artykułu w Redakcji był uczniem Szkoły Podstawowej nr 65 w Warszawie. Obecnie uczęszcza do Liceum im. Gottwalda.

Wszystkie zapisane tu liczby niech będą całkowite. Jeżeli mamy trzy liczby: a, b, m, spełniające warunek: $a-b$ jest podzielne przez m, to piszemy wówczas $a \equiv b \pmod m$. Ten ostatni zapis czytamy: a przystaje do b według modułu m. W ten sposób określona relacja nosi nazwę relacji *kongruencji*. Przykłady: $5 \equiv 1 \pmod 4$, bo $5-1 = 4$ jest podzielne przez 4; $-1 \equiv 5 \pmod 3$, bo $-1-5 = -6$ jest podzielne przez 3. Oczywistą jest rzeczą, że m nie może być 0. Zapis kongruencji nie został wybrany przypadkowo (mam tu na myśli podobieństwo do zapisu równości liczb). Okazało się, że kongruencje mają wiele cech wspólnych z równościami. Np. każda liczba przystaje do siebie według dowolnego modułu; jeżeli jedna liczba przystaje do drugiej według jakiegoś modułu, to ta druga przystaje do pierwszej według tegoż modułu; i trzecia własność — przechodniości: jeżeli jedna liczba przystaje do drugiej według danego modułu, a druga do trzeciej według tegoż modułu, to i pierwsza przystaje do trzeciej według tegoż modułu. Ponadto kongruencje o tym samym module można mnożyć i dodawać stronami, np. z kongruencji $5 \equiv 1 \pmod 4$ i $6 \equiv 2 \pmod 4$ tworzymy prawdziwe kongruencje $30 \equiv 2 \pmod 4$ i $11 \equiv 3 \pmod 4$. Kongruencję $a \equiv b \pmod m$ można stronami dzielić przez liczbę $p \neq 0$ pod warunkiem, że a i b są podzielne przez p oraz że m i p są względnie pierwsze; np. z $20 \equiv 2 \pmod 9$ wynika $10 \equiv 1 \pmod 9$, bo dzieliliśmy tu przez 2, a 2 jest pierwsze względem 9. Daną kongruencję możemy także pomnożyć przez każdą, różną od 0 liczbę, mnożąc i liczby przystające, i moduł; np. $5 \equiv 1 \pmod 4$ jest równoważne $35 \equiv 7 \pmod{28}$. Widzimy, że kongruencje zbliżone są pod względem własności do równości.

W teorii liczb znane jest określenie „rozwiązywanie kongruencji". Tutaj pod terminem „kongruencja" rozumiane jest wyrażenie $F(x) \equiv 0 \pmod m$, gdzie $F(x)$ jest funkcją zmiennej x. „Rozwiązać" znaczy podać zbiór liczb, które podstawione pod x uczynią powyższy zapis zdaniem prawdziwym. My przez „kongruencję" rozumiemy relację — odpowiednik równości, a tu mamy do czynienia z odpowiednikiem równania. Uniknijmy przeto powstałej dwuznaczności wprowadzając pojęcie „kongruencjonału", które zastąpi „kongruencję" w tym drugim znaczeniu. Kongruencjonałem nazywamy kongruencję, w której występują wyrażenia niewiadome. Czytelnik zwróci uwagę na analogię z definicją równania. Oto przykłady kongruencjonałów z jedną niewiadomą: $2x+3 \equiv 0 \pmod 7$, $x^2+x-2 \equiv 0 \pmod 3$. Umówmy się, że funkcja $F(x)$ jest wielomianem. Jeżeli w kongruencjonale podstawimy jakąś liczbę x_0 i w ten sposób powstanie kongruencja prawdziwa, to mówimy, że liczba x_0 spełnia dany kongruencjonał. Np. wspomniany kongruencjonał $2x+3 \equiv 0 \pmod 7$ spełniają liczby $\ldots, -7, 2, 13, \ldots$. Nietrudno zorientować się, że liczby spełniające ten kongruencjonał przystają do 2 według modułu 7. Mówimy tu, że kongruencja $x_1 \equiv 2 \pmod 7$ jest pierwiastkiem naszego kongruencjonału. Kongruencjonał $x^2+x-2 \equiv 0 \pmod 3$ spełniają liczby $\ldots, -1, 1, 2, 4, 5, 7, \ldots$. Zbiór ten, jak łatwo sprawdzić, da się podzielić na takie dwie części, mianowicie na zbiory $\{\ldots, -1, 2, 5, \ldots\}$ oraz $\{\ldots, 1, 4, 7, \ldots\}$, że każda liczba z pierwszego zbioru przystaje do -1 według modułu 3 i każda liczba z drugiego zbioru przystaje do 1 według modułu 3. Mówimy tu, że dany kongruencjonał posiada dwa pierwiastki $x_1 \equiv -1 \pmod 3$ i $x_2 \equiv 1 \pmod 3$. Należy podkreślić, że liczba spełniająca kongruencjonał, a jego pierwiastek — to dwa różne pojęcia. Rozwiązać kongruencjonał znaczy podać wszystkie jego pierwiastki.

Nazwa „kongruencjonał" jest pomysłem autora. Nie jest rzeczą oczywistą, że to pojęcie w ogóle zasłużyło sobie na oddzielną nazwę. W artykule jest to jednak wygodny skrót zwrotu definiującego.

Poznane na początku twierdzenia, dotyczące kongruencji, wykorzystałem do udowodnienia bardzo ważnych twierdzeń, które pozwolą rozwiązywać kongruencjonały. Twierdzenia te orzekają, że: 1°, jeżeli do kongruencjonału dodamy stronami tożsamość (tożsamością nazywamy kongruencję prawdziwą dla każdej liczby podstawionej w miejsce występującej tam niewiadomej, np. $2xm \equiv 0 \pmod m$), to otrzymamy kongruencjonał równoważny danemu (tzn. będzie posiadał to samo rozwiązanie); 2°, jeżeli kongruencjonał dany pomnożymy stronami przez stałą pierwszą względem modułu, to otrzymany kongruencjonał pozostanie równoważny danemu; 3°, jeżeli kongruencjonał dany pomnożymy przez dowolną różną od 0 stałą, mnożąc i liczby przystające, i moduł, to otrzymany kongruencjonał pozostanie równoważny danemu.

Podamy po jednym przykładzie na każde twierdzenie. 1°. Kongruencjonał $5x+1 \equiv 0 \pmod 3$ jest równoważny kongruencjałowi $2x+1 \equiv 0 \pmod 3$. Dodaliśmy tu stronami kongruencjonał dany do tożsamości $-3x \equiv 0 \pmod 3$. 2°. Dany wyżej kongruencjonał równoważny jest następującemu: $10x+2 \equiv 0 \pmod 3$, bowiem stronami pomnożyliśmy go przez 2, a 2 jest pierwsze względem 3. 3°. Dany kongruencjonał jest równoważny $15x+3 \equiv 0 \pmod 9$. Można powiedzieć, że twierdzenia 1°—3° ustalają przekształcenia równoważne, jakie wolno stosować do kongruencjonałów. Opierając się na tych twierdzeniach chciałbym zaproponować sposób rozwiązywania kongruencjonałów. Zacznijmy od kongruencjonałów najprostszych, tj. liniowych ($ax+b \equiv 0 \pmod m$, gdzie $a \neq 0$). Postarajmy się rozwiązać kongruencjonał $4x+1 \equiv 0 \pmod 3$. Nasze postępowanie kierujemy w stronę jak najprostszego zapisania owego kongruencjonału. W tym celu zauważmy, że tożsamością jest $-3x \equiv 0 \pmod 3$. Wolno nam na podstawie twierdzenia 1° dodać do danego kongruencjonału tożsamość. A więc dodajmy. Otrzymamy $x+1 \equiv 0 \pmod 3$, a więc $x \equiv -1 \pmod 3$. Zatem pierwiastkiem (i rozwiązaniem) naszego

Rozwiązanie zadania M36:
Zauważmy najpierw, że na liście jest najwyżej jedno zdanie prawdziwe, gdyż koniunkcja dwóch różnych zdań jest fałszywa. Gdyby wszystkie zdania były fałszywe, to zdanie o numerze 1975 byłoby prawdziwe wbrew przypuszczeniu.
Na liście musi więc być co najmniej jedno zdanie prawdziwe, a ponieważ nie może być ich więcej niż jedno, więc dokładnie jedno zdanie jest prawdziwe, pozostałe 1974 są fałszywe. Prawdziwe jest więc tylko zdanie o numerze 1974.

kongruencjonału jest $x_1 \equiv -1 \pmod 3$. Czytelnik łatwo to sprawdzi podstawiając pod x_1 odpowiednie liczby i stwierdzając, że żadna inna liczba nie spełnia naszego kongruencjonału. Inny przykład niech stanowi wspomniany wcześniej kongruencjonał $2x+3 \equiv 0 \pmod 7$. Postępujemy w sposób następujący: mnożymy nasz kongruencjonał stronami przez -3. Dostajemy $-6x-9 \equiv 0 \pmod 7$. Korzystając z tego, że $7x \equiv 0 \pmod 7$ jest tożsamością, dodajemy ją stronami do ostatniego kongruencjonału i w ten sposób mamy $x-9 \equiv 0 \pmod 7$, czyli $x \equiv 9 \pmod 7$. Ponieważ $9 \equiv 2 \pmod 7$, a relacja kongruencji jest przechodnia, więc ostatecznym („najprostszym") zapisem pierwiastka jest $x_1 \equiv 2 \pmod 7$. Pokażę jeszcze, kiedy należy stosować twierdzenie 3°. Weźmy np. kongruencjonał $10x+2 \equiv 0 \pmod 4$. Dzielimy liczby przystające i moduł przez 2. Otrzymujemy $5x+1 \equiv 0 \pmod 2$. Czytelnik łatwo, w sposób analogiczny do poprzednich przykładów, dojdzie do rozwiązania $x_1 \equiv 1 \pmod 2$, a więc do faktu, że każda liczba nieparzysta spełnia ów kongruencjonał. Jak widać, kongruencjonały liniowe, posiadające rozwiązanie, mają dokładnie jeden pierwiastek. Widoczna jest tu analogia do równań. Są też różnice: nie wszystkie kongruencjonały liniowe posiadają rozwiązania, np. kongruencjonał $2x+1 \equiv 0 \pmod 4$ rozwiązania nie posiada; tak samo $12x+5 \equiv 0 \pmod 6$. Ogólnie, kongruencjonały liniowe nie posiadają rozwiązania, gdy współczynnik przy niewiadomej i moduł mają wspólny podzielnik większy od 1, natomiast wyraz wolny już nie dzieli się przez ową liczbę.

Przejdziemy teraz do omawiania niektórych kongruencjonałów stopnia wyższego niż 1. Można dowieść, że gdy moduł jest liczbą pierwszą, to aby rozwiązać taki kongruencjonał, potrzeba i wystarcza rozłożyć występujący wielomian $F(x)$ na czynniki i rozwiązać kongruencjonały, których lewymi stronami są kolejne czynniki, prawą 0, a modułem — moduł wyjściowego kongruencjonału. Otrzymane pierwiastki są pierwiastkami danego kongruencjonału. Podamy przykłady.

Kongruencjonał kwadratowy $x^2+x-2 \equiv 0 \pmod 5$ ma pierwiastki $x_1 \equiv 1 \pmod 5$ i $x_2 \equiv -2 \pmod 5$, bowiem $x^2+x-2 = (x-1)(x+2)$, a kongruencjonały $x-1 \equiv 0 \pmod 5$ i $x+2 \equiv 0 \pmod 5$ dają wymienione pierwiastki. Weźmy teraz kongruencjonał $6x^2+5x+1 \equiv 0 \pmod{11}$. Rozkładamy trójmian na czynniki i otrzymujemy

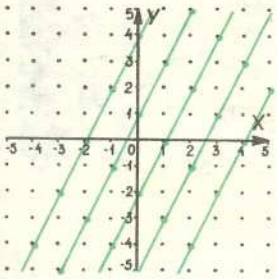
$$6\left(x+\frac{1}{2}\right)\left(x+\frac{1}{3}\right) \equiv 0 \pmod{11}.$$

Pozbywamy się ułamków w czynnikach przedstawiając 6 w postaci iloczynu $2 \cdot 3$, a więc $(2x+1)(3x+1) \equiv 0 \pmod{11}$. Pozostały teraz do rozwiązania kongruencjonały liniowe $2x+1 \equiv 0 \pmod{11}$ i $3x+1 \equiv 0 \pmod{11}$. Czytelnik sprawdzi, że ich pierwiastkami są odpowiednio $x_1 \equiv 6 \pmod{11}$ i $x_2 \equiv -4 \pmod{11}$. Kongruencje te stanowią rozwiązanie kongruencjonału wyjściowego.

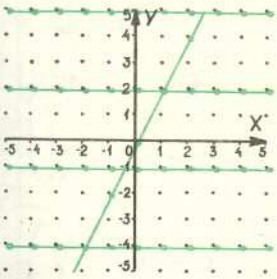
Rozwiążmy jeszcze kongruencjonał trzeciego stopnia $x^3-1 \equiv 0 \pmod 3$. Rozkładamy wyrażenie stojące po lewej stronie znaku przystawania na następujące czynniki: $(x-1)(x^2+x+1)$. Rozwiązujemy kongruencjonał liniowy $x-1 \equiv 0 \pmod 3$ i otrzymujemy $x_1 \equiv 1 \pmod 3$. Rozwiążmy jeszcze kongruencjonał kwadratowy $x^2+x+1 \equiv 0 \pmod 3$. Występujący tu wielomian sam nie rozłoży się na czynniki, ale kongruencjonał jest równoważny $x^2+x-2 \equiv 0 \pmod 3$, bo $2 \equiv -1 \pmod 3$. Kongruencjonał ten ma pierwiastki $x_2 \equiv 1 \pmod 3$ i $x_3 \equiv -2 \pmod 3$. Ale $x_2 \equiv x_3 \equiv 1 \pmod 3$, również $x_1 \equiv x_2 \equiv x_3 \equiv 1 \pmod 3$. Otrzymaliśmy zatem potrójny pierwiastek kongruencjonału. Płynie stąd prawdziwy dla wszystkich dających się rozwiązać kongruencjonałów o module pierwszym wniosek: liczba pierwiastków jest taka, jaki jest stopień tego kongruencjonału.

Wiadomo, że równania można zilustrować graficznie w układzie współrzędnych. Nasunęło mi to pomysł zilustrowania w sposób analogiczny kongruencjonałów. W tym celu obieramy układ współrzędnych na płaszczyźnie kratowej, tzn. zbudowanej z punktów o współrzędnych całkowitych. Nietrudno pokazać, że wykresem wyrażenia $y \equiv F(x) \pmod m$ jest rodzina „linii" równoległych do „linii" $y = F(x)$ i przecinających oś rzędnych w punktach odległych kolejno o m. Np. wykresem wyrażenia liniowego $y \equiv 2x+1 \pmod 3$ jest rodzina „prostych" (rys. 1). Za pomocą ilustracji graficznej kongruencjonały można rozwiązywać podobnie jak równania. W tym celu wykonujemy wykres wyrażenia $y = F(x) \pmod m$, a następnie kładziemy $y = 0$, tj. rozpatrujemy punkty osi odciętych. Jeśli „linie" $y \equiv F(x) \pmod m$ przecinają w punktach kraty $x_1, x_2, x_3, \ldots$ oś odciętych, to odcięte tych punktów spełniają kongruencjonał $F(x) \equiv 0 \pmod m$. Jest to pierwsza metoda, którą zilustrujemy na przykładach. Weźmy cytowany wcześniej kongruencjonał $2x+1 \equiv 0 \pmod 3$. Wykonujemy wykres wyrażenia $y \equiv 2x+1 \pmod 3$, a następnie zaznaczamy punkty przecięcia z osią odciętych „prostych" wykresu. Jak widać na rys. 1, nasz kongruencjonał spełniają liczby: $\ldots, -2, 1, 4, \ldots$, a więc pierwiastek ma postać $x_1 \equiv 1 \pmod 3$. Kongruencjonał kwadratowy $x^2-1 \equiv 0 \pmod 2$ rozwiążemy graficznie na rys. 2. Widać stąd, że kongruencjonał ten spełniają liczby $\ldots, -3, -1, 1, 3, \ldots$, a więc pierwiastki stanowią kongruencje: $x_1 \equiv 1 \pmod 2$ i $x_2 \equiv -1 \pmod 2$. Zauważmy, że $-1 \equiv 1 \pmod 2$, a więc $x_1 \equiv x_2 \equiv 1 \pmod 2$. Metoda druga — przypominająca rozwiązywanie układów równań — polega na tym, że wielomian w kongruencjonale danym rozkładamy na sumę dwóch wielomianów $A(x)$ i $B(x)$ i kładziemy y zamiast jednego z wielomianów sumy (np. $A(x)$). Wykonujemy następnie wykres wyrażenia $y \equiv -B(x) \pmod m$ i wykres funkcji $y \equiv A(x) \pmod m$. Jeżeli punktami przecięcia otrzymanych „linii" są punkty kraty, to ich odcięte spełniają dany kongruencjonał. Rozwiążemy tą metodą wcześniej cytowane kongruencjonały. Mamy $2x+1 \equiv 0 \pmod 3$. Kładziemy $y = 2x$, stąd $y \equiv -1 \pmod 3$. Wykonujemy wykresy (rys. 3) i dochodzimy do tego samego wniosku, co metodą pierwszą graficzną, jak i algebraiczną. Metoda druga znajduje zastosowanie głównie przy rozwiązywaniu kongruencjonałów nieliniowych o module pierwszym. Weźmy $x^2-1 \equiv 0 \pmod 2$. Kładziemy $y = x^2$, a więc $y \equiv 1 \pmod 2$ (rys. 4). Mamy stąd identyczny wynik jak w pierwszej metodzie.

Celem rozważań powyższych było wskazanie analogii i różnic pomiędzy kongruencjonałami a równaniami o współczynnikach całkowitych. Można się było zorientować, że zapisy $F(x) = 0$ i $F(x) \equiv 0 \pmod m$ mają wiele cech wspólnych. Aż dziw, że tak na pozór różne relacje, jak relacja równości i kongruencji, a co za tym idzie, i podzielności, okazały się tak podobne. Rozszerzając to stwierdzenie należy zauważyć, że można relację kongruencji traktować jako uogólnienie relacji równości określonej w zbiorze liczb całkowitych.

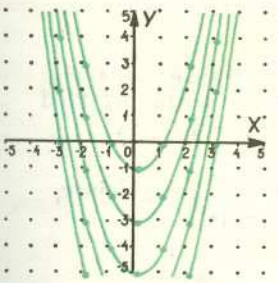


Rys. 1

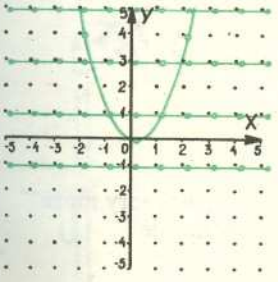


Rys. 2

Gdy moduł jest liczbą złożoną, to prócz „normalnych" pierwiastków pojawiają się jeszcze dodatkowe liczby spełniające ów kongruencjonał.



Rys. 3



Rys. 4