



Kongruencje w akcji

Bartłomiej BZDEGA

Uniwersytet im. A. Mickiewicza w Poznaniu

Kongruencje pojawiały się już kilka razy w Kąciku, ale zawsze grały rolę co najwyżej drugoplanową. Tym razem będzie inaczej.

Niech a, b i n będą liczbami całkowitymi. Kongruencję $a \equiv b \pmod{n}$ (czytaj: a przystaje do b modulo n) możemy zdefiniować na dwa równoważne sposoby:

- (1) Liczby a, b dają tę samą resztę z dzielenia przez n .
- (2) Liczba n dzieli $a - b$.

Będziemy tutaj używać krótszej notacji: $a \equiv_n b$.

Z (1) natychmiast wynikają własności:

$$a \equiv_n a, \quad a \equiv_n b \Rightarrow b \equiv_n a, \quad a \equiv_n b \wedge b \equiv_n c \Rightarrow a \equiv_n c.$$

Kongruencje modulo n możemy dodawać, odejmować i mnożyć stronami, czyli jeśli $a \equiv_n b$ oraz $c \equiv_n d$, to

$$a \pm c \equiv_n b \pm d \quad \text{oraz} \quad ac \equiv_n bd.$$

Dla dowodu wystarczy zauważyć, że liczby $(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$ oraz $ac - bd = c(a - b) + b(c - d)$ są podzielne przez n na mocy (2).

Dzięki możliwości mnożenia kongruencji stronami można wykazać indukcyjnie, że jeśli $a \equiv_n b$, to $a^k \equiv_n b^k$ dla naturalnych k .

Pierwiastkowania kongruencji na ogół wykonywać nie można. Na przykład zachodzi $8 \equiv_7 1$, ale po wyciągnięciu obu stronnie pierwiastka sześciennego otrzymamy nieprawdziwą kongruencję $2 \equiv_7 1$.

Najogólniejszym wnioskiem z powyższych faktów jest następujące twierdzenie: dla wielomianu P o współczynnikach całkowitych zachodzi implikacja

$$x \equiv_n y \Rightarrow P(x) \equiv_n P(y).$$

Dla dowodu niech $P(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d$. Z kongruencji $x \equiv_n y$ otrzymujemy $x^k \equiv_n y^k$, a po pomnożeniu przez a_k mamy $a_kx^k \equiv_n a_ky^k$. Wystarczy teraz zsumować ostatnią kongruencję dla $k = 0, 1, 2, \dots, d$.

Jeśli $n = x - y \neq 0$, to oczywiście $x \equiv_n y$. Wnioskiem z tego jest podzielność $x - y \mid P(x) - P(y)$ dla $x \neq y$ (jest to twierdzenie 2 z Kącika 12. w Δ_{19}^{12} – tam można znaleźć inny dowód).

Z dzieleniem jest trochę trudniej – można je wykonać tylko w szczególnych okolicznościach. Niech $a \equiv_n b$ oraz $c \equiv_n d$. Przyjmijmy, że $c \mid a$ i $d \mid b$. Jeśli dodatkowo $\text{NWD}(c, n) = 1$, to wówczas $\frac{a}{c} \equiv_n \frac{b}{d}$. Aby to wykazać, zauważmy, że $a - b = c \cdot \frac{a}{c} - d \cdot \frac{b}{d} \equiv_n c \cdot \frac{a}{c} - c \cdot \frac{b}{d} = c(\frac{a}{c} - \frac{b}{d})$. Ostatnia liczba jest podzielna przez n oraz $\text{NWD}(c, n) = 1$, więc $n \mid \frac{a}{c} - \frac{b}{d}$ (zobacz (1) w 29. Kąciku, w Δ_{21}^5).

Z powyższej własności najczęściej korzysta się w szczególnym przypadku $c = d$ oraz gdy n jest liczbą pierwszą.

Zadania

1. Liczby a_1, a_2, \dots, a_n są całkowite. Niech d będzie wspólnym dzielnikiem liczb $a_1 - 1, a_2 - 1, \dots, a_n - 1$. Udowodnić, że $d \mid a_1 a_2 \dots a_n - 1$.
2. Dane są takie liczby całkowite dodatnie d, m, n , że $d \mid mn^4 - 1$ i $d \mid m^4n - 1$. Wykazać, że $d \mid n^{15} - 1$.
3. Liczby naturalne n i k są nieparzyste. Dowieść, że liczba $1^k + 2^k + \dots + n^k$ dzieli się przez n .
4. Liczby a, b, c są całkowite. Liczba nieparzysta n jest dzielnikiem liczb $a + b + c$ i $a^2 + b^2 + c^2$. Wykazać, że liczby a^3, b^3, c^3 dają takie same reszty z dzielenia przez n .
5. Niech P będzie wielomianem o współczynnikach całkowitych. Liczby całkowite x, y, z spełniają równości: $P(x) = y, P(y) = z, P(z) = x$. Wykazać, że $x = y = z$.
6. Niech p będzie liczbą pierwszą. Liczby całkowite x_1, x_2, \dots, x_p spełniają podzielności $p \mid x_1 x_2 \dots x_k - k$ dla $k = 1, 2, \dots, p$. Udowodnić, że liczby x_1, x_2, \dots, x_p są różne.
7. Liczby a i b są całkowite, a $p > 2$ jest liczbą pierwszą, która nie dzieli ab . Liczby $a^2 + b^2$ i $a^3 + b^3$ dają resztę 1 z dzielenia przez p . Dowieść, że $p \mid a + b + 2$.

Wskazówki do zadań
 1. Pomnożyć stronami kongruencje $a_i \equiv_n d$ dla $i = 1, 2, \dots, n$.
 2. Kongruencję $mx^k \equiv_n d$ i podnieść obie strony do potęgi 4. Sprawdzić, że tak otrzymane równanie można podzielić przez m^4n .
 3. Uzasadnić, że $k^k + (n - k)^k \equiv_n 0$ i zsumować dla $k = 0, 1, 2, \dots, [n/2]$.
 4. Kongruencję $-a \equiv_n b + c$ podnieść do kwadratu i odjąć od niej $-a^2 \equiv_n b^2 + c^2$. Można stąd otrzymać $a^3 \equiv_n abc$.
 5. Jeśli pewne dwie liczby x, y, z są równe, to $x = y = z$. Przypuśćmy, że są to trzy różne liczby. Wtedy $x - y \mid P(x) - P(y) = x - y$ i $x - y \mid P(x) - P(y) = x - y$, zachodząca też dwie analogiczne podzielności. Wnioskujeśmy, że $|x - y| = |y - z| = |z - x|$, co daje $x = y = z$.
 6. Zauważamy, że $x^k \equiv_n d$ dla $k > 1$ mamy $k^k \equiv_n x^k \equiv_n d$.
 7. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 8. Dla $k > 1$ mamy $k^k \equiv_n d$.
 9. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 10. Dla $k > 1$ mamy $k^k \equiv_n d$.
 11. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 12. Dla $k > 1$ mamy $k^k \equiv_n d$.
 13. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 14. Dla $k > 1$ mamy $k^k \equiv_n d$.
 15. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 16. Dla $k > 1$ mamy $k^k \equiv_n d$.
 17. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 18. Dla $k > 1$ mamy $k^k \equiv_n d$.
 19. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 20. Dla $k > 1$ mamy $k^k \equiv_n d$.
 21. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 22. Dla $k > 1$ mamy $k^k \equiv_n d$.
 23. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 24. Dla $k > 1$ mamy $k^k \equiv_n d$.
 25. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 26. Dla $k > 1$ mamy $k^k \equiv_n d$.
 27. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 28. Dla $k > 1$ mamy $k^k \equiv_n d$.
 29. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 30. Dla $k > 1$ mamy $k^k \equiv_n d$.
 31. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 32. Dla $k > 1$ mamy $k^k \equiv_n d$.
 33. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 34. Dla $k > 1$ mamy $k^k \equiv_n d$.
 35. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 36. Dla $k > 1$ mamy $k^k \equiv_n d$.
 37. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 38. Dla $k > 1$ mamy $k^k \equiv_n d$.
 39. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 40. Dla $k > 1$ mamy $k^k \equiv_n d$.
 41. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 42. Dla $k > 1$ mamy $k^k \equiv_n d$.
 43. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 44. Dla $k > 1$ mamy $k^k \equiv_n d$.
 45. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 46. Dla $k > 1$ mamy $k^k \equiv_n d$.
 47. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 48. Dla $k > 1$ mamy $k^k \equiv_n d$.
 49. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 50. Dla $k > 1$ mamy $k^k \equiv_n d$.
 51. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 52. Dla $k > 1$ mamy $k^k \equiv_n d$.
 53. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 54. Dla $k > 1$ mamy $k^k \equiv_n d$.
 55. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 56. Dla $k > 1$ mamy $k^k \equiv_n d$.
 57. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 58. Dla $k > 1$ mamy $k^k \equiv_n d$.
 59. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 60. Dla $k > 1$ mamy $k^k \equiv_n d$.
 61. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 62. Dla $k > 1$ mamy $k^k \equiv_n d$.
 63. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 64. Dla $k > 1$ mamy $k^k \equiv_n d$.
 65. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 66. Dla $k > 1$ mamy $k^k \equiv_n d$.
 67. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 68. Dla $k > 1$ mamy $k^k \equiv_n d$.
 69. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 70. Dla $k > 1$ mamy $k^k \equiv_n d$.
 71. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 72. Dla $k > 1$ mamy $k^k \equiv_n d$.
 73. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 74. Dla $k > 1$ mamy $k^k \equiv_n d$.
 75. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 76. Dla $k > 1$ mamy $k^k \equiv_n d$.
 77. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 78. Dla $k > 1$ mamy $k^k \equiv_n d$.
 79. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 80. Dla $k > 1$ mamy $k^k \equiv_n d$.
 81. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 82. Dla $k > 1$ mamy $k^k \equiv_n d$.
 83. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 84. Dla $k > 1$ mamy $k^k \equiv_n d$.
 85. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 86. Dla $k > 1$ mamy $k^k \equiv_n d$.
 87. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 88. Dla $k > 1$ mamy $k^k \equiv_n d$.
 89. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 90. Dla $k > 1$ mamy $k^k \equiv_n d$.
 91. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 92. Dla $k > 1$ mamy $k^k \equiv_n d$.
 93. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 94. Dla $k > 1$ mamy $k^k \equiv_n d$.
 95. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 96. Dla $k > 1$ mamy $k^k \equiv_n d$.
 97. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 98. Dla $k > 1$ mamy $k^k \equiv_n d$.
 99. Jeśli $k \neq d$, to $k^k \not\equiv_n d$.
 100. Dla $k > 1$ mamy $k^k \equiv_n d$.