Kongruencje modulo liczba pierwsza

Bartłomiej BZDĘGA

Jeśli a jest liczbą całkowitą oraz $p \nmid a$, to istnieje taka liczba całkowita a', że $aa' \equiv 1 \pmod p$ (por. kącik 29. w Δ_{21}^5). Liczbę a' nazywamy odwrotnością a modulo p. Dzięki temu faktowi możemy udowodnić

Twierdzenie Wilsona. Liczba $n \geqslant 2$ jest pierwsza wtedy i tylko wtedy, gdy $(n-1)! \equiv -1 \pmod n$.

Dowód. Dla $n \in \{2,3,4\}$ sprawdzamy bezpośrednio, że teza jest prawdziwa. W dalszej części zakładamy więc, że $n \geqslant 5$.
($\Rightarrow$) Niech $n = p \geqslant 5$ będzie pierwsze. Reszta $r \in \{1,2,\ldots,p-1\}$ jest swoją własną odwrotnością modulo p wtedy i tylko wtedy, gdy $r^2 \equiv 1 \pmod p$, równoważnie $p \mid r^2 - 1 = (r-1)(r+1)$. Ma to miejsce dla $r = 1$ i $r = p-1$. Pozostałe liczby ze zbioru $2, 3, \ldots, p-2$ możemy pogrupować w pary (r_i, r_i') – liczba i jej odwrotność modulo p. Niech $p = 2k+1$. Otrzymujemy stąd

$$p! = 1 \cdot r_1 r_1' \cdot r_2 r_2' \cdot \ldots \cdot r_{k-1} r_{k-1}' \cdot (p-1) \equiv -1 \pmod p,$$

ponieważ $r_i r_i' \equiv 1 \pmod p$ dla $k = 1, 2, \ldots, k-1$.
($\Leftarrow$) Niech $n \geqslant 6$ będzie złożona – wówczas albo $n = ab$ dla pewnych liczb naturalnych $1 < a < b < n$, albo $n = p^2$ dla pewnej liczby pierwszej $p \geqslant 3$. W pierwszym przypadku w iloczynie $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot (n-1)$ występują liczby a i b, w drugim – liczby p i $2p$. W obu przypadkach $n \mid (n-1)!$, czyli $(n-1)! \equiv 0 \pmod n$.

W zadaniach związanych z kongruencjami modulo liczba pierwsza przydatny bywa poniższy

Lemat o ciągu arytmetycznym. Niech p będzie liczbą pierwszą i niech $(a_0, a_1, \ldots, a_{p-1})$ będzie ciągiem arytmetycznym liczb całkowitych o różnicy r. Wówczas jeśli $p \nmid r$, to każda z liczb $a_0, a_1, \ldots, a_{p-1}$ daje inną resztę z dzielenia przez p; resztami są wszystkie liczby całkowite od 0 do $p-1$.

Dowód. Przypuśćmy dla dowodu nie wprost, że $a_i \equiv a_j \pmod p$ oraz $0 \leqslant i < j \leqslant p-1$. Wtedy $p \mid a_j - a_i = (j-i)r$. Jednak $p \nmid r$ oraz $p \nmid j-i$, gdyż $0 < j-i < p$. Z tego wynika, że w ciągu $(a_0, a_1, \ldots, a_{p-1})$ każdy wyraz ma inną resztę z dzielenia przez p. Wyrazów jest p, więc muszą to być wszystkie możliwe reszty od 0 do $p-1$.

W kąciku pod takim tytułem nie mogłoby zabraknąć najsłynniejszego bodaj twierdzenia związanego z kongruencjami modulo liczba pierwsza:

Małe twierdzenie Fermata. Jeśli p jest liczbą pierwszą, n jest liczbą całkowitą oraz $p \nmid n$, to $n^{p-1} \equiv 1 \pmod p$.

Dowód. Niech $r_1, r_2, \ldots, r_{p-1}$ będą resztami z dzielenia przez p liczb $n, 2n, 3n \ldots, (p-1)n$. Na mocy poprzedniego lematu ($a_0 = 0$, $r = n$) otrzymujemy $\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}$ (kolejność oczywiście może być inna). Mnożąc stronami kongruencje $in \equiv r_i \pmod p$ dla $i = 1, 2, \ldots, p-1$, otrzymamy

$$(p-1)! n^{p-1} = n(2n)(3n)\ldots((p-1)n) \equiv r_1 r_2 r_3 \ldots r_{p-1} = (p-1)! \pmod p.$$

Teraz wystarczy skorzystać z twierdzenia Wilsona albo po prostu podzielić obustronnie powyższą kongruencję przez $(p-1)!$, co można zrobić, gdyż jest to liczba względnie pierwsza z p.

Małe twierdzenie Fermata można wyrazić w innej postaci, bez warunku $p \nmid n$: jeśli p jest liczbą pierwszą, a n liczbą całkowitą, to $n^p \equiv n \pmod p$.

Zadania

1. Wykazać, że jeśli n jest liczbą całkowitą oraz p, q, r są liczbami pierwszymi, to $\frac{qn^p + pn^q - (p+q)n}{pq}$ również jest liczbą całkowitą.
2. Liczby całkowite nieujemne a, b, c spełniają dla każdej liczby całkowitej $n \geqslant 2$ podzielność $n \mid a^n + b^n + c^n$. Dowieść, że $a = b = c = 0$.
3. W zależności od liczby pierwszej $p \neq 2, 5$ wyznaczyć p-tą cyfrę po przecinku w rozwinięciu dziesiętnym ułamka $\frac{1}{p}$.
4. W zależności od liczby pierwszej $p \geqslant 5$ wyznaczyć reszty z dzielenia przez p liczb:
   (a) $(p-2)!$, (b) $(p-3)!$, (c) $2 \cdot 4 \cdot \ldots \cdot (2p-2)$, (d) $1 \cdot 3 \cdot \ldots \cdot (2p-1)$.
5. Niech $(p_1, p_2, \ldots, p_{10})$ będzie rosnącym ciągiem arytmetycznym liczb pierwszych. Wykazać, że $p_{10} > 2022$.
6. Rozwiązać równanie $2^x + 17 = y^4$ w liczbach całkowitych dodatnich x, y.
7. Dowieść, że równanie $a^{11} + b^{11} + c^{11} = 111$ nie ma rozwiązań w liczbach całkowitych a, b, c.

Wskazówki do zadań

1. Liczby $\frac{n^p - n}{p}$ i $\frac{n^q - n}{q}$ są całkowite na mocy małego twierdzenia Fermata.
2. Jeśli p jest liczbą pierwszą, to $a^p + b^p + c^p \equiv a + b + c \pmod p$.
3. Z małego twierdzenia Fermata wynika, że $p \mid 10^{p-1} - 1$. Stąd $\frac{1}{p} = \frac{a}{10^{p-1}-1} = 0{,}(a)$, przy czym a oznacza tu liczbę $(p-1)$-cyfrową z dopuszczalnymi zerami początkowymi.
4. (a) Odwrotnością liczby $p-1$ modulo p jest $p-1$.
   (b) Odwrotnością liczby $p-2$ modulo p jest $-(p+1)/2$.
   (c) $2^{p-1}(p-1)!$.
   (d) Tu nie trzeba żadnych twierdzeń.
5. Trzeba dość sprytnie zastosować lemat o ciągu arytmetycznym, by wykazać, że różnica ciągu dzieli się przez 210 (kłopot może sprawić np. to, że jeśli $7 \mid p_i$, to niekoniecznie p_i jest liczbą złożoną). Jeśli ta różnica jest większa od 210 (tzn. równa co najmniej 420), teza jest oczywista. W przeciwnym wypadku pozostaje jeszcze uzasadnić, że $p_1 > 132$. Ponieważ $210 \equiv 1 \pmod{11}$, mamy $p_i \in \{0, 1\} \pmod{11}$. Analogicznie, $210 \equiv 2 \pmod{13}$, więc $p_1 \in \{0, 2, 4, 6\} \pmod{13}$. Jedyną liczbą pierwszą $p_1 \leqslant 132$ spełniającą te warunki jest 67, ale wtedy nie otrzymamy ciągu samych liczb pierwszych. (Ciekawostka: $p_1 = 199$ jest najmniejsze, dla którego otrzymamy ciąg liczb pierwszych o różnicy 210.)
6. Z danego równania wynika, że $2^x \equiv y^4 \pmod{17}$. Można podnieść tę kongruencję obustronnie do czwartej potęgi i skorzystać z małego twierdzenia Fermata dla $p = 17$.
7. Zamiast równości rozważyć kongruencję modulo 23.