Teoria liczb I – kongruencje

1.1 Teoria

Wszystkie liczby są całkowite, chyba, że powiedziano inaczej.

Dla dowolnych rzeczy, na których mamy sensownie zdefiniowane mnożenie (np. dla liczb całkowitych) mówimy, że a **dzieli** b, równoważnie b **jest podzielna przez** a co zapisujemy

$$a \Big| b$$

jeżeli istnieje takie c, że

$$b = ca.$$

Relacja podzielności niestety nie jest zbyt poręczna, jeżeli rozpatrujemy wiele podzielności przez tę samą liczbę. Stosujemy wtedy **kongruencje**.

Definicja 1.1 *Mówimy, że*

$$a \equiv b \mod n$$

co czytamy "a przystaje do b modulo n", jeżeli

$$n \Big| a - b.$$

Np. $3 \equiv 5 \mod 2$, $7 \equiv -4 \mod 11$ bo $2|5-3$ i $11|7-(-4)$. Jak widać, żadnej magii tutaj nie ma.

Relacja przystawania modulo n ma jednak własności bardzo podobne do relacji równości:

1. $a \equiv a \mod n$,
2. Jeżeli $a \equiv b \mod n$ to
   $b \equiv a \mod n$,
3. Jeżeli $a \equiv b \mod n$ i $b \equiv c \mod n$ to
   $a \equiv c \mod n$,
4. Jeżeli $a_1 \equiv a_2 \mod n$ i $b_1 \equiv b_2 \mod n$ to
   $a_1 + b_1 \equiv a_2 + b_2 \mod n$
   $a_1 - b_1 \equiv a_2 - b_2 \mod n$
   $a_1 b_1 \equiv a_2 b_2 \mod n$
5. Z poprzednich własności wynika, że jeżeli $b_1 \equiv b_2 \mod n$ to $ab_1 \equiv ab_2 \mod n$.

Niestety nie ma podobnie łatwych relacji jeżeli chodzi o dzielenie.

Wszystkie własności kongruencji dowodzimy korzystając z definicji. Udowodnimy dla przykładu ostatnią własność, a raczej trzy własności:

Dowód.

Wiemy, że $a_1 \equiv a_2 \mod n$, czyli z definicji $n \Big| a_1 - a_2$ oraz $b_1 \equiv b_2 \mod n$ czyli $n \Big| b_1 - b_2$.

Oczywiście wynika z tego $n \Big| (a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$. Korzystając ponownie z definicji zachodzi $a_1 + b_1 \equiv a_2 + b_2 \mod n$.

Analogicznie $n \Big| (a_1 - a_2) - (b_1 - b_2) = (a_1 - b_1) - (a_2 - b_2)$, czyli $a_1 - b_1 \equiv a_2 - b_2 \mod n$.

Nieco trudniej dowodzi się ostatniej własności (*ale to dobrze, bo ma ona dzięki temu niezerowy sens*):

Skoro $n \Big| a_1 - a_2$ to $n \Big| (a_1 - a_2)b_1$ i skoro $n \Big| b_1 - b_2$ to $n \Big| a_2(b_1 - b_2)$, a więc

$$n \Big| (a_1 - a_2)b_1 + a_2(b_1 - b_2) = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_2 \text{ stąd } a_1 b_1 \equiv a_2 b_2 \mod n$$

■

Definicja 1.2 *Symbolem* $a \mod n$ *oznaczamy resztę z dzielenia liczby* a *przez* n. *Ma to wystarczająco dużo wspólnego z* $a \equiv b \mod n$, *żeby używać tej notacji, ale mimo wszystko* $a \mod n$ *to zupełnie co innego niż* $a \equiv b \mod n$ – *pierwsze to pewna liczba a drugie to pewne twierdzenie.*

1.2 Zadania

Część teoretycznie trudniejszych zadań jest oznaczona gwiazdką.

1. Zadanie

   (a) Udowodnij, że reszta z dzielenia przez 10 liczby 33^{100} jest taka sama jak reszta z dzielenia przez 10 liczby 3^{100}.

   (b) Oblicz resztę z dzielenia 3^{100} przez 100.

   (c) Oblicz resztę z dzielenia $2^{70}, 3^{70}, 4^{70}, 5^{70}$ przez 71.

   (d) Wykaż, że
   $$13 \Big| 2^{70} + 3^{70}.$$

2. Zadanie
   Udowodnij własności kongruencji z listy z teorii. Wykaż też, że jeżeli liczba d jest względnie pierwsza z n, a, b są takimi całkowitymi podzielnymi przez d, że $a \equiv b \mod n$, to
   $$\frac{a}{d} \equiv \frac{b}{d} \mod n.$$

3. Zadanie
   Oblicz resztę z dzielenia $17, 17^2, 17^3, \ldots, 17^{21}$ przez 11. Spróbuj znaleźć wśród otrzymanych reszt jakieś regularności.

   (*) Oblicz resztę z dzielenia
   $$17^{17^{17}}$$
   przez 11.

4. Zadanie
   Udowodnij wzory skróconego mnożenia:

   (a) $x - y \Big| x^n - y^n$ dla dowolnej liczby naturalnej n,

   (b) $x + y \Big| x^n + y^n$ dla dowolnej **nieparzystej** liczby naturalnej n.

   Oczywiście istnieją ładne dowody za pomocą kongruencji i inne dowody więc jeżeli ktoś zna inny dowód, to niech spróbuje udowodnić za pomocą kongruencji, a jeżeli nie to niech wymyśli cokolwiek :)