Koniec o $\mathbb{Z} \to \mathbb{Z}_p$

1.1 Teoria

Nieraz stykamy się z problemem: udowodnić, że dane równanie postaci $cos \cdot x^k + cos_2 y^m + cos\_jeszcze = 0$ nie ma rozwiązań w liczbach całkowitych.

Warto wtedy popatrzeć na to równanie $\mod$ pewna liczba całkowita (*ma to też sens algebraiczny – chodzi o to, że obrazami algebraicznymi $\mathbb{Z}$ są dokładnie zbiory reszt $\mathbb{Z}_n$*).

Przeliczmy bodaj najczęściej stosowany przykład:

n	0	1	2	3	4	5	6	7
$n \mod 8$	0	1	4	1	0	1	4	1

Zatem $n^2 \mod 8$ może przyjmować jedynie wartości $0, 1, 4$, stąd też wniosek, że $n^2 \mod 4$ może przyjmować jedynie wartości $0, 1$.

Typowe rozumowania:

Zadanie

Udowodnić, że równanie $x^2 + 4y^2 = 2011$ nie rozwiązań w liczbach całkowitych dodatnich.

Rozwiązanie.

Zauważmy, że $2011 \equiv 3 \mod 4$, zatem gdyby x i y spełniały to równanie to $x^2 \equiv x^2 + 4y^2 = 2011 \equiv 3 \mod 4$, a kwadraty nie dają reszty 3 z dzielenia przez 4.

Zadanie

Udowodnić, że równanie $x^2 + 2y^2 = 4^k$ nie ma rozwiązań w liczbach całkowitych dodatnich, dla żadnego k naturalnego.

Rozwiązanie.

Zauważmy, że rozwiązanie w liczbach ***całkowitych*** *istnieją – np. rozwiązanie $x = 2^k, y = 0$. Zatem nachamowe liczenie $\mod$ nie zadziała.*

Załóżmy, że takie rozwiązania istnieją, niech (x, y) będzie takim rozwiązaniem, przy czym x **jest najmniejsze możliwe** wśród wszystkich rozwiązań x, y dla wszystkich k.

Liczby x i y spełniają równanie $x^2 + 2y^2 \equiv 4^k \mod 4$. Oczywiście $4^k \equiv 0 \mod 4$, zatem $x^2 + 2y^2 \equiv 0 \mod 4$. Jakie reszty może dawać $x^2 + 2y^2$? Ano wszystkie kombinacje $a + 2b \mod 4$ gdzie $a, b \in \{0, 1\}$. Przeliczamy, że są to $0 + 2 \cdot 0 \equiv 0, 0 + 2 = 2, 1 + 0 = 1, 1 + 2 \cdot 1 = 3$. Zatem zgadza się tylko, jeżeli $a = 0$ i $b = 0$, czyli gdy $4 \Big| x^2$ i $4 \Big| y^2$, czyli gdy $2 \Big| x$ i $2 \Big| y$.

Liczby $x/2$ i $y/2$ są więc całkowite i spełniają:

$$\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 = 4^{k-1}.$$

a więc $x/2, y/2$ są rozwiązaniem równania i oczywiście skoro $x > 0$ to $x/2 < x$. Otrzymujemy sprzeczność z założeniem, że x było najmniejsze wśród wszystkich rozwiązań.

1.2 Zadania

1. Zadanie
   Udowodnij, że liczba $3^n + 3 \cdot 17^n$ nie jest kwadratem liczby naturalnej dla każdego $n \in \mathbb{N}$.

2. Zadanie
   Wyznacz wszystkie $n \in \mathbb{N}$ takie, że

$$5 \Big| 1^n + 2^n + 3^n + 4^n.$$

3. Zadanie
   Rozwiąż równanie $x^3 + 3y^3 = 9z^3$ w liczbach całkowitych.

4. Zadanie
   Chińskie twierdzenie o resztach.

   Celem jest udowodnienie, że jeżeli liczby k i l są względnie pierwsze, a r_1 i r_2 są całkowite, to istnieje dokładnie jedna liczba $M \in \{0, 1, \ldots, kl-1\}$ taka, że
   $M \equiv r_1 \mod k$
   $M \equiv r_2 \mod l$.

   Intuicyjnie: reszty z dzielenia przez k i l są zupełnie niezależne od siebie.

   Sugerowane kroki:

   (a) Udowodnić, że reszty liczb z ciągu $\{0, k, 2k, 3k, \ldots, (l-1)k\}$ są parami różne, zauważyć, że w związku z tym każda reszta pojawia się w tym ciągu.

   (b) zrobić to samo dla ciągu $\{a, k+a, 2k+a, 3k+a, \ldots, (l-1)k+a\}$.

   (c) zauważyć, że właśnie udowodniło się to, co trzeba ;)

1.3 Teoria 2.0

Ten paragraf jest (niestety; kiedyś się może zdrażnię i zrobię porządny kurs algebry) poza jakimkolwiek programem tego kółka, jego zrozumienie pozostawiam najwyżej uczestnikom zeszłorocznego kółka.

Jak cały czas w teorii liczb, można zobaczyć znacznie więcej patrząc przez szkiełko algebry, można znaczniej ułatwić sobie życie i uniknąć błędów obliczeniowych, wybierając od razu te "bardziej obiecujące" liczby do brania $\mod$.

Twierdzenie 1.1 *Niech p będzie liczbą pierwszą. Wtedy a^k może daje dokładnie $\frac{p-1}{NWD(k,p-1)}+1$ różnych reszt $\mod p$.*

Dowód. Wymaga użycia faktu o istnieniu generatora, ale przy znajomości tego faktu i lematu o rzędzie jest bardzo proste. Dowód na życzenie. ■

Wniosek 1.2 *Nie ma sensu np. rozważać reszt z dzielenia przez 5 liczb n^3, bo, jak głosi powyższe twierdzenie, jest ich $\frac{4}{NWD(3,4)}+1 = 5$, czyli są to po prostu wszystkie możliwe reszty.*

Ogólniej sensownie rozważać takie p, żeby $NWD(k, p-1)$ było jak największe. Pokazuje to, że np. $\mod 7$ *świetnie sprawdza się w kontaktach z sześcianami, bo n^3 daje dokładnie $\frac{6}{3}+1 = 3$ reszty* $\mod 7$ *(są to zresztą $-1, 0, 1$, co przeliczamy już bezpośrednio).*

Z liczbami niepierwszymi jak zawsze jest większy problem, tym niemniej można sobie poradzić przez izomorfizm $\mathbb{Z}_{kl} \simeq \mathbb{Z}_k \times \mathbb{Z}_l$ $(k \perp l)$ oraz istnienie generatora w $\mathbb{Z}_{p^\alpha}$ gdzie p – pierwsze, α dodatnie.