



[](#)
[Zadania PDF.](#)

Źródło zadań w texu.

```
%      File: skrypt.tex %      Created: Thu Oct 28 12:00 PM 2010 C % Last Change: Thu Oct
28 12:00 PM 2010 C documentclass[10pt]{article} usepackage{amssymb}
usepackage{amsmath} textwidth 16cm textheight 24cm oddsidemargin 0cm topmargin 0pt
headheight 0pt headsep 0pt usepackage[polish]{babel} usepackage[utf8]{inputenc}
usepackage[T1]{fontenc} usepackage{import} %usepackage{MnSymbol} %
----- vfuzz4pt % Don't report over-full v-boxes if
over-edge is small hfuzz4pt % Don't report over-full h-boxes if over-edge is small %
THEOREMS ----- newtheorem{thm}{Twierdzenie}[section]
newtheorem{cor}[thm]{Wniosek} newtheorem{lem}[thm]{Lemat}
newtheorem{defn}[thm]{Definicja} newtheorem{tozs}[thm]{Tożsamość}
newtheorem{hyp}[thm]{Hipoteza} newtheorem{useless}[thm]{}
newenvironment{proof}[1][Dowód. ]{noindenttextsc{#1}}{nolinebreak[4]hfill$\blacksquare$\par}
newenvironment{sol}[1][Rozwiązanie. ]{noindenttextsc{#1}}{hfillpar}
newenvironment{problem}{noindenttextsc{Zadanie}}{hfillpar} defdeg{^{\circ}}
defsource#1{\Źródło: #1} subimport{../}{style} %include{style} begin{document}
section{Koniec o $\mathbb{Z}$ $\rightarrow$ $\mathbb{Z}_p$} subsection{Teoria} Nieraz
stykamy się z problemem: udowodnić, że dane równanie postaci $\cos \quad \cdot x^k + \cos_2 y^m$
+ $\cos\_jeszcze = 0$ nie ma rozwiązań w liczbach całkowitych. Warto wtedy popatrzeć na
to równanie $\mod$ pewna liczba całkowita (emph{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: [begin{array}[c]{l} \hline
n \quad & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \backslash \quad \hline
n \mod 8 & 0 & 1 & 4 & 1 & 0 & 1 & 4 & 1 \backslash \quad \hline
end{array}] Zatem $\mathbb{Z}_8$ może przyjmować jedynie wartości $0$,
$1$, $4$, stąd też wniosek, że $\mathbb{Z}_4$ może przyjmować jedynie wartości $0, 1$.
Typowe rozumowania: begin{problem} Udowodnić, że równanie $x^2 + 4y^2 = 2011$
nie rozwiązań w liczbach całkowitych dodatnich. end{problem} begin{sol}
```

Zauważmy, że $2011 \equiv 3 \pmod{4}$, zatem gdyby x i y spełniały to równanie to $x^2 \equiv x^2 + 4y^2 = 2011 \equiv 3 \pmod{4}$, a kwadraty nie dają reszty $3 \pmod{4}$.
 Udowodnić, że równanie $x^2 + 2y^2 = 4^k$ nie ma rozwiązań w liczbach całkowitych dodatnich, dla żadnego k naturalnego.
 Zauważmy, że rozwiązanie w liczbach całkowitych istnieją -- np. rozwiązanie $x=2^k, y=0$. Zatem nachamowe liczenie $\pmod{4}$ 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 $x^2 + 2y^2 \equiv 4^k \pmod{4}$. Oczywiście $4^k \equiv 0 \pmod{4}$, zatem $x^2 + 2y^2 \equiv 0 \pmod{8}$. Jakie reszty może dawać $x^2 + 2y^2 \pmod{8}$? Ano wszystkie kombinacje $a + 2b \pmod{4}$ 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 $4 \mid x^2$ i $4 \mid y^2$, czyli gdy $2 \mid x$ i $2 \mid y$.
 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.
 Zadania
 1. Udowodnij, że liczba $3^n + 3 \cdot 17^n$ nie jest kwadratem liczby naturalnej dla każdego $n \in \mathbb{N}$.
 2. Wyznacz wszystkie $n \in \mathbb{N}$ takie, że $5 \mid 1^n + 2^n + 3^n + 4^n$.
 3. Rozwiąż równanie $x^3 + 3y^3 = 9z^3$ w liczbach całkowitych.
 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 $M \in \{0, 1, \dots, kl\}$ taka, że $M \equiv r_1 \pmod{k}$ i $M \equiv r_2 \pmod{l}$.
 Intuicyjnie: reszty z dzielenia przez k i l są zupełnie niezależne od siebie.
 Sugerowane kroki:
 1. Udowodnić, że reszty liczb z ciągu $\{0, k, 2k, 3k, \dots, (l-1)k\}$ są parami różne, zauważyć, że w związku z tym każda reszta pojawia się w tym ciągu.
 2. zrobić to samo dla ciągu $\{a, k+a, 2k+a, 3k+a, \dots, (l-1)k+a\}$.
 3. zauważyć, że właśnie udowodniło się to, co trzeba ;)
 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 kółka.
 Jak cały czas w teorii liczb, można zobaczyć znacznie więcej patrząc przez szkiełko algebry, można znacznie ułatwić sobie życie i uniknąć błędów obliczeniowych, wybierając od razu te "bardziej obiecujące" liczby do brania $\pmod{p}$.
 Niech p będzie liczbą pierwszą. Wtedy a^k może dawać dokładnie $\frac{p-1}{\text{NWD}(k, p-1)} + 1$ różnych reszt $\pmod{p}$.
 Wymaga użycia faktu o istnieniu generatora, ale przy znajomości tego faktu i lematu o rzędzie jest bardzo proste. Dowód na życzenie.
 Nie ma sensu np. rozważać reszt z dzielenia przez 5 liczb n^3 , bo, jak głosi powyższe twierdzenie, jest ich $\frac{4}{\text{NWD}(3, 4)} + 1 = 5$, czyli są to po prostu wszystkie możliwe reszty.
 Ogólniej sensowniej rozważać takie p , żeby $\text{NWD}(k, p-1)$ było jak największe. Pokazuje to, że np. $\pmod{7}$ świetnie sprawdza się w kontaktach z sześciannymi, bo $n^3 \pmod{7}$ daje dokładnie $\frac{6}{3} + 1 = 3$ reszty $\pmod{7}$ (są to

zresztą $-1, 0, 1$, co przeliczamy już bezpośrednio). $\end{cor}$ 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.
 $\end{document}$