

Z_p i (nie)skończone schodzenie

Wpisany przez Joachim Jelisiejew
poniedziałek, 06 lutego 2012 21:47 -



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

Źródło zadań w texu.

```
% File: starsi.tex % Created: Sun Feb 05 08:00 PM 2012 C % Last Change: Sun Feb
05 08:00 PM 2012 C documentclass[10pt]{article} usepackage{amssymb}
usepackage{amsmath} usepackage{amsthm} textwidth 16cm textheight 24cm oddsidemargin
0cm topmargin 0pt headheight 0pt headsep 0pt usepackage[polish]{babel}
usepackage[utf8]{inputenc} usepackage[T1]{fontenc} usepackage{polski} 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{example}[thm]{Przykład} newtheorem{useless}[thm]{}
newenvironment{sol}[1][Rozwiązanie. ]{ vskip 3mm noindentemph{#1} } {hfillpar}
newcounter{problem} newenvironment{problem}[1][Zadanie]{ stepcounter{problem} vskip
3mm noindent{textsc{bfseries #1 theproblem}}\} {hfillpar} defabs #1{leftvert #1rightvert}
renewcommand{angle}{sphericalangle} renewcommand{vec}[1]{\overrightarrow{#1}}
renewcommand{leq}{leqslant} renewcommand{geq}{geqslant} renewcommand{dots}{\ldots}
subimport{../}{style.sty} defsectionwidth{10cm} %include{style}
defheadpicture{../micek-2cm.jpg} defauthor{kółko l~LO Białystok} defdate{6 lutego 2012}
begin{document} section{Large Dlaczego reszty  $\pmod p$  są fajne?Krótkie przypomnienie
teorii liczb} subsection{Ogólnorozwojowa teoria} Oznaczmy przez  $\mathbb{Z}_n$  zbiór
reszt  $\pmod n$ , który można uznawać za  $\{0, 1, 2, \dots, n-1\}$ . Porównanie  $\mathbb{Q}$ 
 $i \sim \mathbb{Z}_p$ , gdzie jest  $p$  pierwsza. Poniżej  $x, y$  in  $\mathbb{Q}$ ,  $a$ , bin  $\mathbb{Z}$ .
begin{tabular}[]{| p{7cm} | p{7cm} |} \hline  $\mathbb{Q}$  &  $\mathbb{Z}_p$  \hline &
jeżeli  $x \cdot y = 0$ , to  $x = 0$  lub  $y = 0$  & jeżeli  $a \cdot b \equiv 0 \pmod p$  to  $a \equiv
0 \pmod p$  lub  $b \equiv 0 \pmod p$  & jeżeli  $x \neq 0$ , to istnieje  $x^{-1}$  in  $\mathbb{Q}$  takie,
```

Z_p i (nie)skończone schodzenie

Wpisany przez Joachim Jelisiejew
poniedziałek, 06 lutego 2012 21:47 -

że $x^{-1} = 1$ & jeżeli $a \not\equiv 0 \pmod{p}$, to istnieje $b \in \mathbb{Z}$ takie, że $a \cdot b \equiv 1 \pmod{p}$. Możemy to b oznaczać " $a^{-1} \pmod{p}$ " & $x^{-1} + y^{-1} = (x + y) \cdot (xy)^{-1}$ i ogólnie wszystkie działania zachowują się tak, jak wiemy & $a^{-1} + b^{-1} \equiv (a+b) \cdot (ab)^{-1} \pmod{p}$ i ogólnie wszystko jest dobrze, tylko trzeba pamiętać, że nie istnieje nic takiego jak $p^{-1} \pmod{p}$ albo $(2p)^{-1} \pmod{p}$.

Dlaczego ten punkt widzenia opłaca się?

Udowodnij, że jeżeli p jest pierwsza, $a \in \mathbb{Z}$ niepodzielna przez p , to $\{a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)\}$ dają różne reszty z dzielenia przez p .

Wiemy, że $a \not\equiv 0 \pmod{p}$. Rozważamy liczby $\{a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)\}$. Chcemy pokazać, że one dają różne reszty \pmod{p} . Więc mnożymy je wszystkie przez $a^{-1} \pmod{p}$. Otrzymujemy liczby $\{0, 1, 2, \dots, p-1\}$ które dają różne reszty. A więc oryginalne liczby dawały różne reszty.

To jest TYLKO intuicyjne porównanie!!

Wiemy, że $a \neq 0$. Rozważamy liczby $\{a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)\}$. Chcemy pokazać, że są one parami różne. Więc mnożymy je wszystkie przez a^{-1} . Otrzymujemy liczby $\{0, 1, 2, \dots, p-1\}$ które są różne. A więc oryginalne liczby były różne.

Jeżeli $p > 3$ jest liczbą pierwszą to $p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

Jeżeli $p > 5$ jest pierwsze, to $p \mid 2^{p-2} + 5^{p-2} - 7 \cdot 10^{p-2}$.

Uzasadnij, że jeśli $p > 2$ jest pierwsze, to $p \mid 2^{p-2} + (p-2)^{p-2}$.

Uzasadnij, że jeśli $p > 40$ jest pierwsze, to $p \mid 2^{p-40} + (p-2)^{p-40}$.

Praktyka

Znajdź wszystkie rozwiązania równania $8x^4 + 4y^4 + 2z^4 = t^4$ w liczbach całkowitych nieujemnych.

Znajdź wszystkie rozwiązania równania $x^2 + y^2 + z^2 + u^2 = 2xyzu$ w liczbach \mathbb{N}_+ .

Udowodnij, że 7^n nie da się przedstawić w postaci sumy trzech kwadratów liczb wymiernych dodatnich.

Udowodnij, że liczba postaci $4^n(8k-1)$, gdzie $k, n \in \mathbb{N}_+$ nie może być przedstawiona jako suma 1, 2 lub 3 kwadratów liczb naturalnych dodatnich.

Udowodnić, że dla dowolnych dodatnich liczb całkowitych $x_1, \dots, x_{2011}, y_1, \dots, y_{2011}$ iloczyn $[(2x_1^2 + 3y_1^2) \cdot (2x_2^2 + 3y_2^2) \cdot \dots \cdot (2x_{2011}^2 + 3y_{2011}^2)]$ nie jest kwadratem liczby całkowitej.

Ciąg a_1, \dots, a_n ($a_i \in \mathbb{N}_+$) zamieniamy na ciąg postaci $[\frac{a_1 + a_2}{2}, \frac{a_2 + a_3}{2}, \dots, \frac{a_{n-1} + a_n}{2}, \frac{a_n + a_1}{2}]$ ten ciąg zmieniamy analogicznie itd. Udowodnij, że po pewnej liczbie takich operacji albo otrzymany ciąg będzie stały, albo będzie on zawierać wyrazy niecałkowite.