** **
Zadania PDF.

Źródło zadań w texu.

documentclass[10pt]{article} usepackage{amssymb} usepackage{amsmath} textwidth 16cm textheight 26cm 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{useless}[thm]{} defmb#1{mathbb{#1}} defsource#1{$ $\Źródło: #1} defo{operatorname{ord}} newenvironment{sol}[1][Rozwiązanie.]{ vskip 3mm noindentemph{#1} } {hfillpar} newcounter{problem} newenvironment{problem}[1][Zadanie]{ stepcounter{problem} vskip 3mm noindent{textsc{bfseries #1 theproblem}}\} {hfillpar} defabs #1{leftvert #1rightvert} renewcommand{angle}{sphericalangle} renewcommand{vec}[1]{overrightarrow{#1}} renewcommand{leq}{leqslant} renewcommand{geq}{geqslant} renewcommand{dots}{ldots} subimport{../}{style.sty} defsectionwidth{8cm} %include{style} defheadpicture{../micek-2cm.jpg} defauthor{kółko I~LO Białystok} defdate{27 lutego 2012} begin{document} setlength{topmargin}{-0.5in} section{$mathbb{Z}_p$ i~lemat o rzędzie} subsection{Teoria} begin{enumerate} item begin{thm}[Małe twierdzenie Fermata] Dla każdej liczby pierwszej p i liczby całkowitej a, takiej, że $pnot|a$ zachodzi [a^{p-1} equiv 1 mod p] end{thm} item begin{defn} Niech a, n będą liczbami naturalnymi względnie pierwszymi. emph{Rzędem} liczby $a mod n$ nazywamy najmniejsze $kinmb{Z}_+$, takie, że $$a^k equiv 1 mod n$$ Rząd ten oznaczamy przez $o(a, n)$ lub, gdy n jest znane, $o(a)$. end{defn} begin{thm}[Lemat o rzędzie] Jeżeli a, k', n są takie, że $$a^{k'} equiv 1

mod n$$ to $displaystyle{o(a, n) | k'}$. end{thm} begin{cor} Jeżeli p jest liczbą pierwszą, zaś a jest liczbą całkowitą niepodzielną przez p, to $$o(a, p)|p-1$$ end{cor} item begin{thm}[Chińskie o~resztach] Jeżeli n_1, n_2 są względnie pierwsze, a~r_1,r_2 dowolne to istnieje M takie, że [M equiv r_1 mod n_1quad M equiv r_2 mod n_2.] emph{W~ramach ciekawostki: tak naprawdę, jest to fakt geometryczny, w~pewnym dziwnym świecie.} end{thm} end{enumerate} subsection{Zadania} Dzisiaj zadania są trudniejsze niż zwykle, stąd jest do nich dużo wskazówek. begin{problem} Policz rzędy liczb $mod 5$. Policz rzędy liczb $mod 6$. Policz rząd liczby 2 modulo wszystkie liczby względnie pierwsze z~nią mniejsze od 10. end{problem} begin{problem} Przypomnij sobie twierdzenie Eulera i~sformułuj tezę wniosku z~punktu 2. dla liczb złożonych, a~nie tylko pierwszych. Spróbuj policzyć, jaki może być rząd liczby $2mod 27$. end{problem} begin{problem} Liczba n jest całkowita, a~liczba a jest taka, że begin{enumerate} item $a^{26} equiv 1mod n$ i~$a^{2011} equiv 1 mod n$, item $a^{26} equiv -1 mod n$ i~$a^{2011} equiv 1 mod n$. end{enumerate} Uzasadnij, że $a mod n = 1 mod n$. end{problem} begin{problem} Liczba pierwsza p daje resztę 2 z~dzielenia przez 3. Uzasadnij, że przyporządkowanie $amapsto a^3$ jest bijekcją na zbiorze (ciele) ${1mod p, 2mod p, dots, p-1 mod p}$. Pokaż, że nie jest to prawdą, jeżeli $pequiv 1 mod 3$. emph{Wskazówka: pamiętaj, że dla każdego a istnieje jego ``odwrotność''. Wykorzystaj to, by zredukować tezę zadania do ``jeżeli $a^3 equiv 1$ to $aequiv 1$''.} end{problem} begin{problem} Liczba pierwsza p daje resztę 2 z~dzielenia przez 3. Niech [a_{k} := k^2 + k + 1hbox{ dla } k=1,2,dots,p-1.] Wykaż, że iloczyn $a_1cdot a_2cdot dots cdot a_{p-1}$ daje resztę 3 z~dzielenia przez p. emph{Wskazówki: uzasadnij, że $prod_{k=2,3,dots,p-1} (k^3 - 1)$ jest równy $mod p$ iloczynowi $prod_{k=2,3,dots, p-1} (k-1)$. Przedstaw (prawie) iloczyn z~zadania w~terminach tych produktów.} end{problem} begin{problem} Uzasadnij, że każdy dzielnik liczby $F_n = 2^{2^n} + 1$ jest postaci $2^{n+1}cdot k + 1$ dla pewnego k całkowitego. emph{Wskazówka: wystarczy to zrobić dla dzielników pierwszych (dlaczego?). Oblicz, że $o(2, p) = 2^{n+1}$.} end{problem} begin{problem} Udowodnij, że dla liczby pierwszej p istnieje nieskończenie wiele liczb naturalnych n takich, że $$p|2^n - n$$ source{Staszic, uwaga: nie potrzeba lematu o~rzędzie.} emph{Wskazówka: pokaż, jak zmieniają się reszty z~dzielenia przez p liczb 2^n i~n. Skorzystaj z~chińskiego twierdzenia o~resztach.} end{problem} begin{problem}[Zadanie z~$star$] Znajdź wszystkie liczby naturalne n takie, że [n^2 | 3^n + 1] source{Staszic} emph{Wskazówki.} begin{enumerate} item Niech p będzie textbf{najmniejszym} dzielnikiem pierwszym n. item Niech d_1 będzie rzędem $3 mod p$. Uzasadnij, że d_1 ma sens, $d_1 big|2n$. item Uzasadnij, że $d_1big| p-1$, stąd d_1 jest względnie pierwsze z~n, czyli $d_1 big| 2$. item Udowodnij stąd, że $p=2$, czyli $2big|n$. Pokaż, że to daje sprzeczność. item Jakie zatem są rozwiązania? end{enumerate} end{problem} end{document}