** **
Zadania PDF.

Źródło zadań w texu.

% File: podstawy-tl.tex % Created: Sun Dec 11 11:00 PM 2011 C % Last Change: Sun Dec 11 11:00 PM 2011 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{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-ml.sty} defsectionwidth{10cm} defheadpicture{fireworks.png} defauthor{czyli kolejny fascynujący tytuł.\Joachim Jelisiejew} defdate{12 grudnia 2011} begin{document} setlength{topmargin}{-2cm} section{Teoria liczb~--- powtórka} subsection{Powtórzenie teorii} paragraph{Reszty modulo n} Cel: chcemy stwierdzić, czy równanie ma rozwiązanie w~liczbach całkowitych. Moglibyśmy sprawdzić wszystkie, ale jest ich nieskończenie wieledots Natomiast reszt z~dzielenia przez n jest skończenie wiele, więc możemy sprawdzić wszystkie. Na resztach da się sensownie działać: jeżeli $a equiv b$ i~$c equiv d$ (wszystko $mod n$) to [a + c equiv b + d mod nquad a - c equiv b - d mod n,quad ac equiv bd mod n, quad a^m equiv b^m mod n hbox{ dla każdego }min mathbb{Z}_+]

Z~dzieleniem trzeba ostrożnie: mamy $2cdot 2 equiv 4cdot 2 mod 4$, ale $2 notequiv 4 mod 4$. Jednak: begin{center} jeżeli $NWD(a, n)= 1$ i~$ak equiv al mod n$, to $kequiv lmod n$. end{center} Udowodniliśmy także begin{thm}[Małe twierdzenie Fermata] Jeżeli p jest liczbą pierwszą, a~a jest całkowite, to [a^p equiv a mod p.] Jeżeli $pnotbig| a$, to $a^{p-1} equiv 1 mod p$, innymi słowy $acdot a^{p-2} equiv 1 mod p$, więc a^{p-2} możemy NIEFORMALNIE (na razie) traktować jako ``$a^{-1}mod p$''. Kiedyś może pokażemy, że to ma sens, a~jeśli nie, to na studiach. end{thm} subsection{Zadania} begin{problem} Pokaż, że jeżeli p jest pierwsza, to jedynymi rozwiązaniami równania $x^2 equiv 1 mod p$ są $1mod p$ i~$-1mod p$ (emph{tzn. każda liczba całkowita x spełniająca $x^2 equiv 1$, przystaje do 1 lub -1 modulo p}).

Podaj przykład, że bez założenia, że p jest pierwsza, teza zadania nie byłaby prawdziwa. end{problem} begin{problem} Udowodnij, że jeśli p jest pierwsza, a~a całkowita niepodzielna przez p, to [a^{frac{p-1}{2}} equiv 1 mod phbox{ lub }a^{frac{p-1}{2}}equiv -1 mod p.] Wywnioskuj, że sześciany liczb całkowitych dają z~dzielenia przez 7 reszty ze zbioru ${0, 1, -1}$. Co można powiedzieć o~5 potęgach, 6 potęgach itd.? end{problem} begin{problem} Udowodnij, że równanie $x^3 - y^3 = 2012$ nie ma rozwiązań w~liczbach całkowitych x, y. emph{Wskazówka: skorzystać z~wyniku poprzedniego zadania.} end{problem} begin{problem} Udowodnij, że równanie $x^5 - y^5 = 2010$ nie ma rozwiązań w~liczbach całkowitych x, y. emph{Wskazówka: skorzystać z~wyniku poprzedniego poprzedniego zadania.} end{problem} begin{problem} Niech $p>3$ będzie liczbą pierwszą, udowodnić, że [pbig|6^{p-2} + 3^{p-2} + 2^{p-2} - 1.] emph{(bardzo nieformalnie znaczy to: $1/6 +1/2 + 1/3 - 1 = 0$.) trzeba skorzystać z~twierdzenia Fermata, więc trzeba wymnożyć przez cośdots} end{problem} end{document}