** **
Zadania PDF.

Źródło zadań w texu.

% File: zad.tex % Created: Wed Nov 03 10:00 PM 2010 C % Last Change: Wed Nov 03 10:00 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} setlength{topmargin}{-1cm} section{Generator} subsection{Teoria} renewcommand{thethm}{} begin{thm}[Istnienie generatora] Niech p będzie liczbą pierwszą. Istnieje liczba całkowita g, taka, że potęgi g dają wszystkie niezerowe reszty z dzielenia przez p, tzn. [{g mod p, g^2 mod p, dots, g^{p-1} mod p} = {1, 2, dots, p-1}.] end{thm} begin{cor} Dla g,p jak wyżej jeżeli $g^n equiv 1 mod p$ to $p-1Big|n$. end{cor} begin{cor} Dla dowolnej liczby pierwszej p nie ma liczby $n < p-1$ takiej, że $x^n equiv 1 mod p$ dla każdego x niepodzielnego przez p textbf{---} ``małe twierdzenie Fermata jest optymalne". end{cor} subsection{Zadania bez generatora} begin{enumerate} item begin{problem} Udowodnij, że równanie $3x^2 + 2 = y^2$ nie ma rozwiązań w~liczbach całkowitych. end{problem} item begin{problem} Udowodnij, że równanie $7x^3 + 2 = y^3$

nie ma rozwiązań w~liczbach całkowitych. end{problem} item begin{problem} (twierdzenie Wilsona) Niech p będzie liczbą pierwszą większą od 2. begin{enumerate} item Pokaż, że jedynymi rozwiązaniami równania $x^2 equiv 1 mod p$ są liczby x dające resztę -1 lub 1 z dzielenia przez p. item Przypomnij sobie, że dla każdej liczby całkowitej $ain {1,2,dots,p-1}$ istnieje dokładnie jedna liczba b ze zbioru ${1,2,dots,p-1}$ taka, że $abequiv 1mod p$, którą oznaczam a^{-1}. Udowodnij, że przy tak przyjętych oznaczeniach $(a^{-1})^{-1} = a$. item Wywnioskuj, że jeżeli $x equiv x^{-1} mod p$ to $xequiv1$ lub $xequiv-1$. item Uzasadnij, że [(p-1)! equiv -1cdot 1 = -1 mod p.] grupując elementy iloczynu po lewej w pary (x,x^{-1}). item Policz, że (zupełnym przypadkiem) to samo zachodzi dla $p=2$. end{enumerate} end{problem} item begin{problem} Niech p będzie liczbą pierwszą większą od 2. Uzasadnić, że istnieje dokładnie $frac{p+1}{2}$ reszt kwadratowych $mod p$ tzn. zbiór ${0^2,1^2,dots,(p-1)^2}$ ma dokładnie $frac{p+1}{2}$ elementów. end{problem} item begin{problem} Uzasadnij, że jeżeli $p>2$ jest pierwsze, a n takie, że $NWD(n,p-1) = 1$, to [a^n equiv b^n mod p hbox{ implikuje } aequiv bmod p.] emph{Wskazówka użyj małego twierdzenia Fermata.} end{problem} item begin{problem} Uzasadnij (bez użycia teorii generatora!), że jeżeli p jest nieparzystą liczbą pierwszą, a $NWD(n, p-1) = 1$ to [pBig|1^n + 2^n + dots + (p-1)^n.] emph{Wskazówka: skorzystaj z poprzedniego zadania, by zobaczyć, że liczby $1^n,2^n,ldots,(p-1)^n$ są różne.} Ile wynosi $1^n + 2^n + dots + (p-1)^n$ gdy $p-1Big|n$? end{problem} end{enumerate} subsection{* Zadania na generator} begin{enumerate} item begin{problem} Korzystając z tego, że 2 jest generatorem dla liczby 29 znajdź, bez zgadywania, rozwiązania równania $x^7 equiv 1 mod 29$. end{problem} item begin{problem} Udowodnij, że dla 8 nie istnieje odpowiednik generatora tzn. taka liczba g, że ${g mod 8, g^2 mod 8, g^3mod 8,g^4 mod 8} = {1,3,5,7}$. end{problem} item begin{problem} Niech p będzie pierwsze, a n będzie liczbą całkowitą niepodzielną przez $p-1$. Udowodnić, że [pBig|1^n + 2^n + dots + (p-1)^n.] Ile wynosi $1^n + 2^n + dots + (p-1)^n$ jeżeli $p-1Big|n$? end{problem} item begin{problem} Liczba $p>2$ jest pierwsza. Wielomian $P(x) = a_{p-1}x^{p-1} + dots + a_1x + a_0$ jest taki, że p nie dzieli $P(a) - P(b)$ o ile a,b są całkowite i $pnotBig|a-b$. Wykazać, że $p|a_{p-1}$. begin{enumerate} item Wykaż, że ${P(0)mod p,P(1)mod p,dots,P(p-1)mod p} = {0,1,dots,p-1}$. item Zakonkluduj, że $p Big|P(0) + dots + P(p-1)$. item Rozpisz współczynniki i policz, że właśnie udowodniłeś, że $p Big| a_{p-1}$. end{enumerate} end{problem} item begin{problem} Niech p będzie liczbą pierwszą większą od 2. Uzasadnić, że istnieje dokładnie $frac{p+1}{2}$ reszt kwadratowych $mod p$ tzn. zbiór ${0^2,1^2,dots,(p-1)^2}$ ma dokładnie $frac{p+1}{2}$ elementów. end{problem} item begin{problem} Niech p będzie liczbą pierwszą. Wtedy a^k może daje dokładnie $frac{p-1}{NWD(k,p-1)} + 1$ różnych reszt $mod p$. end{problem} end{enumerate} end{document}