Poniżej teoria i zadania do przeczytania i zrobienia na najbliższe kółko (21.10.10). Wyjątkowo "wykład" jest również "do domu". Gdybyście mieli jakieś pytania (niekoniecznie mądre), piszcie na maila, pomyślimy wspólnie :)

Miłego, Joachim (Yogi)

** **
Zadania PDF.

**Źródło zadań w texu.**

```
 %       File: zad.tex
%     Created: Sat Oct 16 04:00 PM 2010 C
% Last Change: Sat Oct 16 04:00 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}}


subimport{../}{style}
%include{style}

begin{document}
section{Teoria liczb I -- kongruencje}

subsection{Teoria}
Wszystkie liczby są całkowite, chyba, że powiedziano inaczej.

Dla dowolnych rzeczy, na których mamy sensownie zdefiniowane mnożenie (np.
dla liczb całkowitych) mówimy, że $a$textbf{ dzieli }$b$, równoważnie $b$
textbf{jest podzielna przez }$a$ co zapisujemy
[
aBig|b
]
jeżeli istnieje takie $c$, że
[
b = ca.
]

Relacja podzielności niestety nie jest zbyt poręczna, jeżeli rozpatrujemy
```

wiele podzielności przez tę samą liczbę. Stosujemy wtedy
textbf{kongruencje}.

begin{defn}
Mówimy, że
[
a equiv b mod n
]
co czytamy ``$a$ przystaje do $b$ modulo $n$'', jeżeli
[
nBig| a - b.
]
end{defn}

Np. $3 equiv 5 mod 2$, $7 equiv -4 mod 11$ bo $2 | 5 - 3$ i $11 | 7 -
(-4)$. Jak widać, żadnej magii tutaj nie ma.

Relacja przystawania modulo $n$ ma jednak własności bardzo podobne do
relacji równości:
begin{enumerate}
item $a equiv a mod n$,
item Jeżeli $a equiv b mod n$ to\
$b equiv a mod n$,
item Jeżeli $a equiv b mod n$ i $b equiv cmod n$ to\
$a equiv c mod n$,
item Jeżeli $a_1equiv a_2 mod n$ i $b_1 equiv b_2 mod n$ to\
$a_1 + b_1 equiv a_2 + b_2 mod n$\
$a_1 - b_1 equiv a_2 - b_2 mod n$\
$a_1b_1 equiv a_2b_2 mod n$
item Z poprzednich własności wynika, że jeżeli $b_1 equiv b_2 mod n$ to
$ab_1 equiv ab_2 mod n$.
end{enumerate}
Niestety nie ma podobnie łatwych relacji jeżeli chodzi o dzielenie.

Wszystkie własności kongruencji dowodzimy korzystając z definicji.
Udowodnimy dla przykładu ostatnią własność, a raczej trzy własności:

begin{proof}

Wiemy, że $a_1 equiv a_2 mod n$, czyli z definicji $nBig| a_1 - a_2$ oraz $b_1
equiv b_2 mod n$ czyli $nBig| b_1 - b_2$.

Oczywiście wynika z tego $nBig|(a_1 - a_2) + (b_1 - b_2) = (a_1 +
b_1) - (a_2 + b_2)$. Korzystając ponownie z definicji zachodzi $a_1 +
b_1 equiv a_2 + b_2 mod n$.

Analogicznie $nBig|(a_1 - a_2) - (b_1 - b_2) = (a_1 - b_1) - (a_2 - b_2)$, czyli $a_1 - b_1 equiv a_2 - b_2 mod n$.

Nieco trudniej dowodzi się ostatniej własności (emph{ale to dobrze, bo ma ona dzięki temu niezerowy sens}):

Skoro $nBig|a_1 - a_2$ to $nBig|(a_1 - a_2)b_1$ i skoro $nBig|b_1 - b_2$ to $nBig|a_2(b_1 - b_2)$, a więc
[
nBig|(a_1 - a_2)b_1 + a_2(b_1 - b_2) = a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2 = a_1b_1 - a_2b_2hbox{ stąd }a_1b_1 equiv a_2b_2 mod n
]
end{proof}

begin{defn}
Symbolem $a mod n$ oznaczamy resztę z dzielenia liczby $a$ przez $n$. Ma to wystarczająco dużo wspólnego z $a equiv b mod n$, żeby używać tej notacji, ale mimo wszystko $amod n$ to zupełnie co innego niż $a equiv bmod n$ -- pierwsze to pewna liczba a drugie to pewne twierdzenie.
end{defn}

subsection{Zadania}

Część teoretycznie trudniejszych zadań jest oznaczona gwiazdką.

begin{enumerate}
item
begin{problem}
begin{enumerate}
item Udowodnij, że reszta z dzielenia przez $10$ liczby $33^{100}$ jest taka sama jak reszta z dzielenia przez $10$ liczby $3^{100}$.
item Oblicz resztę z dzielenia $3^{100}$ przez $100$.
item Oblicz resztę z dzielenia $2^{70}, 3^{70}, 4^{70}, 5^{70}$ przez $71$.
item Wykaż, że
[
13Big|2^{70} + 3^{70}.
]
end{enumerate}
end{problem}
item begin{problem}
Udowodnij własności kongruencji z listy z teorii. Wykaż też, że jeżeli liczba $d$ jest względnie pierwsza z $n$, $a,b$ są takimi całkowitymi podzielnymi przez $d$, że $a equiv bmod n$, to

[
frac{a}{d} equiv frac{b}{d} mod n.
]
end{problem}
item
begin{problem}
Oblicz resztę z dzielenia $17, 17^{2}, 17^{3}, dots,
17^{21}$ przez $11$. Spróbuj znaleźć wśród otrzymanych reszt jakieś
regularności.

(*) Oblicz resztę z dzielenia
[
17^{17^{17}}
]
przez $11$.
end{problem}
item
begin{problem}
Udowodnij wzory skróconego mnożenia:
begin{enumerate}
item $x-yBig|x^n - y^n$ dla dowolnej liczby naturalnej $n$,
item $x+yBig|x^n + y^n$ dla dowolnej textbf{nieparzystej}
liczby naturalnej $n$.
end{enumerate}
emph{Oczywiście istnieją ładne dowody za pomocą kongruencji i
inne dowody więc jeżeli ktoś zna inny dowód, to niech spróbuje
udowodnić za pomocą kongruencji, a jeżeli nie to niech wymyśli
cokolwiek :)}
end{problem}
end{enumerate}

end{document}