$\mathbb{Z}_p$ i lemat o rzędzie

KÓŁKO I LO BIAŁYSTOK
27 LUTEGO 2012

1.1 Teoria

1. **Twierdzenie 1.1 (Małe twierdzenie Fermata)** *Dla każdej liczby pierwszej p i liczby całkowitej a, takiej, że $p \not| a$ zachodzi*
$$a^{p-1} \equiv 1 \mod p$$

2. **Definicja 1.2** *Niech a, n będą liczbami naturalnymi względnie pierwszymi.* Rzędem *liczby $a \mod n$ nazywamy najmniejsze $k \in \mathbb{Z}_+$, takie, że*
$$a^k \equiv 1 \mod n$$
Rząd ten oznaczamy przez $\mathrm{ord}(a, n)$ lub, gdy n jest znane, $\mathrm{ord}(a)$.

   Twierdzenie 1.3 (Lemat o rzędzie) *Jeżeli a, k', n są takie, że*
$$a^{k'} \equiv 1 \mod n$$
to $\mathrm{ord}(a, n) | k'$.

   Wniosek 1.4 *Jeżeli p jest liczbą pierwszą, zaś a jest liczbą całkowitą niepodzielną przez p, to*
$$\mathrm{ord}(a, p) | p - 1$$

3. **Twierdzenie 1.5 (Chińskie o resztach)** *Jeżeli n_1, n_2 są względnie pierwsze, a r_1, r_2 dowolne to istnieje M takie, że*
$$M \equiv r_1 \mod n_1 \quad M \equiv r_2 \mod n_2.$$
   W ramach ciekawostki: tak naprawdę, jest to fakt geometryczny, w pewnym dziwnym świecie.

1.2 Zadania

Dzisiaj zadania są trudniejsze niż zwykle, stąd jest do nich dużo wskazówek.

Zadanie 1
Policz rzędy liczb $\mod 5$. Policz rzędy liczb $\mod 6$. Policz rząd liczby 2 modulo wszystkie liczby względnie pierwsze z nią mniejsze od 10.

Zadanie 2
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 $2 \mod 27$.

Zadanie 3
Liczba n jest całkowita, a liczba a jest taka, że

1. $a^{26} \equiv 1 \mod n$ i $a^{2011} \equiv 1 \mod n$,
2. $a^{26} \equiv -1 \mod n$ i $a^{2011} \equiv 1 \mod n$.

Uzasadnij, że $a \mod n = 1 \mod n$.

Zadanie 4
Liczba pierwsza p daje resztę 2 z dzielenia przez 3. Uzasadnij, że przyporządkowanie $a \mapsto a^3$ jest bijekcją na zbiorze (ciele) $\{1 \mod p, 2 \mod p, \ldots, p-1 \mod p\}$. Pokaż, że nie jest to prawdą, jeżeli $p \equiv 1 \mod 3$.

Wskazówka: pamiętaj, że dla każdego a istnieje jego "odwrotność". Wykorzystaj to, by zredukować tezę zadania do "jeżeli $a^3 \equiv 1$ to $a \equiv 1$".

Zadanie 5
Liczba pierwsza p daje resztę 2 z dzielenia przez 3. Niech

$$a_k := k^2 + k + 1 \text{ dla } k = 1, 2, \ldots, p-1.$$

Wykaż, że iloczyn $a_1 \cdot a_2 \cdot \ldots \cdot a_{p-1}$ daje resztę 3 z dzielenia przez p.

Wskazówki: uzasadnij, że $\prod_{k=2,3,\ldots,p-1}(k^3 - 1)$ *jest równy* $\mod p$ *iloczynowi* $\prod_{k=2,3,\ldots,p-1}(k-1)$. *Przedstaw (prawie) iloczyn z zadania w terminach tych produktów.*

Zadanie 6
Uzasadnij, że każdy dzielnik liczby $F_n = 2^{2^n} + 1$ jest postaci $2^{n+1} \cdot k + 1$ dla pewnego k całkowitego.

Wskazówka: wystarczy to zrobić dla dzielników pierwszych (dlaczego?). Oblicz, że $\operatorname{ord}(2, p) = 2^{n+1}$.

Zadanie 7
Udowodnij, że dla liczby pierwszej p istnieje nieskończenie wiele liczb naturalnych n takich, że

$$p | 2^n - n$$

Źródło: Staszic, uwaga: nie potrzeba lematu o rzędzie.

Wskazówka: pokaż, jak zmieniają się reszty z dzielenia przez p liczb 2^n i n. Skorzystaj z chińskiego twierdzenia o resztach.

Zadanie z $\star$ 8
Znajdź wszystkie liczby naturalne n takie, że

$$n^2 | 3^n + 1$$

Źródło: Staszic

Wskazówki.

1. Niech p będzie **najmniejszym** dzielnikiem pierwszym n.
2. Niech d_1 będzie rzędem $3 \mod p$. Uzasadnij, że d_1 ma sens, $d_1 | 2n$.
3. Uzasadnij, że $d_1 | p - 1$, stąd d_1 jest względnie pierwsze z n, czyli $d_1 | 2$.
4. Udowodnij stąd, że $p = 2$, czyli $2 | n$. Pokaż, że to daje sprzeczność.
5. Jakie zatem są rozwiązania?