Teoria liczb I

1 Teoria

1. **Definicja.** Mówimy, że a przystaje do b modulo n, jeśli dają takie same reszty z dzielenia przez n. Zapisujemy $a \equiv b \pmod{n}$. **Własności:**
   - $a \equiv a\ (mod\ n)$
   - $a \equiv b\ (mod\ n) \Rightarrow b \equiv a\ (mod\ n)$
   - $(a \equiv b\ (mod\ n) \wedge b \equiv c\ (mod\ n)) \Rightarrow a \equiv c\ (mod\ n)$
   - $(a \equiv b\ (mod\ n) \wedge c \equiv d\ (mod\ n)) \Rightarrow (a + c \equiv b + d\ (mod\ n) \wedge a \cdot c \equiv b \cdot d\ (mod\ n))$
   - $a \equiv b\ (mod\ n) \Rightarrow a^m \equiv b^m\ (mod\ n)$
2. **Twierdzenie** (Algorytm Euklidesa) Dla dowolnych naturalnych $a > b$ jeżeli $m|a$ oraz $m|b$ to $m|(a - b)$. Powtarzając to rozumowanie możemy wyznaczyć $\mathrm{NWD}(a, b)$.
3. **Twierdzenie** (Małe Fermata) Dla dowolnego $a \in \mathbb{Z}$ oraz dla dowolnego $p \in \mathbb{P}$ zachodzi $p|a^p - a$. Jeżli ponadto $p \perp a$, to $p|a^{p-1} - 1$
4. **Twierdzenie** (Twierdzenie chińskie o resztach) Niech $n_1, n_2, ..., n_k \in \mathbb{N}$,$n_i \perp n_j$ dla $i \neq j$, $a_1, a_2, ..., a_n \in \mathbb{N}$. Wtedy istnieje dokładnie jedna liczba $a \in \mathbb{N}$, $0 \leqslant a < n_1 n_2 ... n_k$ taka, że $a \equiv a_i \pmod{n_i}$

2 Przykłady do twierdzeń

1. Udowodnić, że liczba $93^{93} - 33^{33}$ jest podzielna przez 10.
2. Wyznacz NWD(282, 78)
3. Udowodnij, że jeżeli liczba pierwsza p dzieli liczbę 11...1 (p razy), to $p = 3$.
4. Rozwiąż układ kongruencji:

$$\begin{aligned} x &\equiv 0\ (mod\ 1996) \\ x &\equiv -6\ (mod\ 1998) \\ x &\equiv -4\ (mod\ 2000) \\ x &\equiv 0\ (mod\ 2004) \end{aligned}$$

3 Zadania

1. Udowodnij, że dla liczby pierwszej p oraz liczb całkowitych $a_1, a_2 \ldots a_n$ zachodzi

$$p|a_1^p + a_2^p + \cdots + a_n^p \iff p|a_1 + a_2 + \cdots + a_n \tag{1}$$

2. Wykazać, że dla nieskończenie wielu liczb całkowitych dodatnich n, liczba $1 + 2^{4^n} + 2^{5^n}$ jest złożona.
3. Udowodnij, że równanie $x^{1996} + y^{1998} + z^{2000} = t^{2004}$ ma rozwiązanie w liczbach całkowitych.

4. Dla jakich naturalnych k liczba $k^{k+1} + (k+1)^k$ jest podzielna przez 3?

5. Wyznaczyć największą możliwą długość ciągu kolejnych liczb całkowitych, z których każdą można przedstawić w postaci $x^3 + 2y^2$ dla pewnych liczb całkowitych x, y.

6. Rozwiązać w liczbach całkowitych x, y równanie

$$2^x + 17 = y^4 \tag{2}$$

7. Wykaż, że $7|13^n + 6$ jeśli n jest całkowitą liczbą parzystą.

8. Znaleźć wszystkie pary liczb całkowitych dodatnich x, y spełniających równanie $y^x = x^{50}$.

9. Jakie cyfry należy umieścić zamiast zer na trzecim i piątym miejscu w liczbie 3000003, aby otrzymać liczbę podzielną przez 13?