Teoria liczb
zadanie domowe 1, na 30.03

Rozwiązanie zadania należy spisać i przysłać, można papierowo lub elektronicznie. Zadanie są na zaliczenie: warto oddawać również częściowo rozwiązane zadanie. Rozwiązanie może (a czasem nawet powinno) korzystać z zadań z ćwiczeń oraz z materiału z wykładu. Dopuszczalne jest konsultowanie się z kolegami, natomiast bardzo proszę oddawać wyłącznie rozwiązania spisane przez siebie i zrozumiane przez siebie (niekoniecznie wymyślone przez siebie).

Zadanie 1. Niech $n = p_1^{e_1} \dots p_k^{e_k}$ będzie rozkładem liczby n na czynniki pierwsze. Niech

$$d = \mathrm{NWW}(p_1^{e_1-1}(p_1-1),\ p_2^{e_2-1}(p_2-1),\ \dots,\ p_k^{e_k-1}(p_k-1)).$$

(a) Pokaż, że dla każdego $x \in \mathbb{Z}_n^*$ zachodzi

$$x^d \equiv 1 \pmod{n}.$$

(b) Pokaż, że jeśli $\mathbb{Z}_n^*$ jest cykliczna, to n jest postaci $2^{e_1}p_2^{e_2}$, gdzie $p_2 > 2$ jest pierwsza oraz $e_1, e_2 \geq 0$ są całkowite.

(c) Pokaż, że $\mathbb{Z}_n^*$ jest cykliczna wtedy i tylko wtedy, gdy n spełnia jeden z warunków: $n = 2$ lub $n = 4$ lub $n = p^e$ lub $n = 2p^e$, gdzie $p > 2$ jest pierwsza i $e > 0$ jest całkowita.