Matematyka dyskretna I
Zestaw 5

1. Przypiszmy literom alfabetu angielskiego (a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z) wartości liczbowe ze zbioru $X := \{0, 1, \ldots, 25\}$ zgodnie z następująca regułą: $a \leftrightarrow 0$, $b \leftrightarrow 1$, $c \leftrightarrow 2$, ... Niech $f : X \to X$ będzie funkcją szyfrującą daną wzorem $f(\alpha) := M\alpha + N \pmod{26}$ dla pewnych $M, N \in X$, $(M, 26) = 1$. Wyznaczyć wartości M i N wykorzystując analizę częstości, fakt, że w języku angielskim najczęściej występującą literą jest „e", a następnie „t", oraz że następujący komunikat nadany w języku angielskim został zaszyfrowany powyższą funkcją (odstępy i znaki przestankowe pozostały niezmienione).

```
uj kxt ujm tsjmrwe, az xsunwj zasj, djivwp tjivw, ywjw djast
pa  mke pfkp pfwe ywjw djwzwqpre xajukr, pfkxo eas vwje usqf.
pfwe  ywjw pfw rkmp dwadrw eas yasrt wbdwqp pa nw ixvarvwt ix
kxepfixc mpjkxcw aj uempwjiasm, nwqksmw pfwe lsmp tit xap
fart yipf msqf.
```

Odczytać oryginalny komunikat.

2. Złamać system kryptograficzny RSA, w którym $n = 9991$, zaś jawnym kluczem szyfrującym jest liczba 37.

3. Udowodnić, że dla każdej liczby naturalnej $n \geq 1$ mamy

$$\sum_{m=1}^{n} \mu(m) \lfloor \frac{n}{m} \rfloor = 1.$$

W s k a z ó w k a. Wykorzystać następującą obserwację:

$$\text{jeśli } g(n) = \sum_{d|n} f(d), \text{ to } \sum_{m=1}^{n} g(m) = \sum_{d=1}^{n} f(d) \lfloor \frac{n}{d} \rfloor.$$

4. Dowody z wykładu pozostawione jako ćwiczenie.