

### Zadanie 3. Potęgowanie modulo

Rozważmy operację potęgowania modularnego stosowaną np. w algorytmie RSA.

Liczbę  $a$  podnosimy do potęgi  $x$ , po czym bierzemy resztę z dzielenia otrzymanej liczby przez ustaloną liczbę  $M$ , dzięki czemu otrzymujemy wynik

$$b = a^x \bmod M,$$

gdzie  $a$ ,  $M$  – dodatnie liczby całkowite,  $x$  – nieujemna liczba całkowita.

Mówimy wtedy, że  $a^x$  modulo  $M$  równa się  $b$ .

#### Przykład:

Dla  $a = 2$ ,  $x = 5$ ,  $M = 7$  liczymy resztę z dzielenia  $2^5$  (czyli 32) przez 7, zatem  $b = 4$ .

Dla  $a = 3$ ,  $x = 3$  i  $M = 11$  mamy  $b = 3^3 \bmod 11 = 5$ ,

natomiast dla  $a = 10$ ,  $x = 2$  i  $M = 13$  wynikiem jest  $b = 10^2 \bmod 13 = 9$ .

Wypełnia egzaminator	Nr zadania	2.1.	2.2	2.3.
	Maks. liczba pkt.	2	2	2
	Uzyskana liczba pkt.			