22.05.2024

Matematyka dyskretna, zestaw 8.

8.1. Korzystając z własności kongruencji modulo oraz twierdzenia Eulera (i uzasadniając przy tym, że to ostatnie można zastosować), oblicz

(a) dwie ostatnie cyfry liczby $2 + 39^{82}$ w systemie dziesiętnym,

(b) sześć ostatnich cyfry liczby 77^{33} w systemie binarnym.

8.2. Rozwiąż układ liniowych kongruencji

$$\begin{cases} x \equiv 3 \pmod{2}, \\ x \equiv 5 \pmod{3}, \\ x \equiv 7 \pmod{5}. \end{cases}$$

8.3. Pokaż, że układ liniowych kongruencji

$$\begin{cases} x \equiv 2 \pmod{8}, \\ x \equiv 6 \pmod{12}, \\ x \equiv 8 \pmod{28}, \end{cases}$$

nie ma rozwiązania.

8.4. Korzystając z małego twierdzenia Fermata (dlaczego to możliwe?) oraz dokonując dalszych rachunków, znajdź wszystkie rozwiązania nieliniowej kongruencji

$$x^{14} \equiv 9 \pmod{13}.$$

8.5. Test pierwszości Fermata pozwala sprawdzić (chociaż tylko z pewnym prawdopodobieństwem), czy dana liczba jest pierwsza, co jest przydatne przy szukaniu dużych liczb pierwszych potrzebnych w kryptografii. W tym celu rozważmy zaprzeczenie małego twierdzenia Fermata:

$$a^{p-1} \neq 1 \bmod p \implies p \mid a \ \vee \ p \notin \mathbb{P}\,.$$

Wynika stąd, że jeżeli weźmiemy dowolne a mniejsze od p (wykluczając w ten sposób możliwość $p \mid a$), a równość $a^{p-1} = 1 \bmod p$ nie zachodzi, to p na pewno nie jest liczbą pierwszą. Z drugiej strony, jeżeli $a^{p-1} = 1 \bmod p$, to z dużym prawdopodobieństwem p jest pierwsze – aczkolwiek nie ma pewności.

Należy zatem wybrać liczbę $a \in [2, p-2]$ i sprawdzić, czy zachodzi $a^{p-1} = 1 \bmod p$; jeżeli nie, to p jest liczbą złożoną, a jeżeli tak, to należy wziąć inne a i powtórzyć poprzedni krok. Kiedy równość jest nadal spełniona po k powtórzeniach (tj. tylu, ile uznamy za wystarczające), to wówczas możemy ostrożnie przyjąć, że p jest pierwsze.

Sprawdź działanie testu Fermata dla $p = 71$ i $p = 84$, z $k = 5$.

8.6. Protokół Diffiego-Hellmana pozwala na ustalenie pomiędzy dwiema stronami (zwyczajowo nazywanymi Alicją i Bobem) wspólnego prywatnego klucza przy użyciu publicznego kanału komunikacji. Wykorzystuje on zbiór $\mathbb{Z}_p^* := \{1, 2, ..., p-1\}$, gdzie p to liczba pierwsza, na którym jest zdefiniowane działanie mnożenia modulo p:

$$\forall a, b \in \mathbb{Z}_p^* \quad a \circ b := (ab) \bmod p \tag{1}$$

($\mathbb{Z}_p^*$ wraz z działaniem $\circ$ stanowi grupę – por. wykład 7.). Oto protokół:

(a) Alicja i Bob ustalają publicznie zbiór $\mathbb{Z}_p^*$, na którym będą działać, oraz element $g \in \mathbb{Z}_p^*$. Rozważymy przypadek: $p = 23$, $g = 5$.

(b) Alicja wybiera taki losowy element $a \in \mathbb{Z}_p^*$, że $1 < a < p$.

(c) Alicja oblicza potęgę $A = g^{\circ a}$ w sensie działania $\circ$, tzn. $A = g^a \bmod p$.

(d) Bob postępuje tak samo – wybiera losowy element $b \in \mathbb{Z}_p^*$ i oblicza $B = g^{\circ b}$.

(e) Elementy a i b są znane tylko, odpowiednio, Alicji i Bobowi, natomiast A i B zostają wymienione publicznym kanałem. Bob następnie oblicza $k_B = A^{\circ b}$ (czyli $A^b \bmod p$), zaś Alicja oblicza $k_A = B^{\circ a}$ (czyli $B^a \bmod p$)

Otrzymane przez Alicję i Boba klucze k_A i k_B są sobie równe, niezależnie od wyboru elementów a i b, oraz nieznane innym osobom (poznanie ich jest teoretycznie możliwe, ale wymaga ogromnej mocy obliczeniowej, nieosiągalnej współcześnie przy wyborze odpowiednio dużych p, a i b). Wykonaj powyższy algorytm wybierając jakieś wartości a i b i potwierdź, że otrzymane klucze są identyczne ($k_A = k_B$). Ponadto udowodnij, że będą one sobie równe dla dowolnego wyboru a i b.

8.7. System kryptograficzny RSA w uproszczeniu opiera się na tym, że wiadomość wyrażona w postaci liczby $m \in \mathbb{N}$ zostaje zapisana jako szyfrogram

$$c := m^e \bmod n\,,$$

gdzie para liczb (n, e), taka że $n \perp m$ oraz $e \perp \varphi(n)$, tworzy tzw. klucz publiczny (przy czym n jest generowana losowo jako iloczyn dwóch dużych liczb pierwszych, które trzymane są w tajemnicy; φ oznacza funkcję Eulera, a $\perp$ względną pierwszość danych liczb). Klucz prywatny, złożony z n i takiej liczby d, że $e\,d \equiv 1 \pmod{\varphi(n)}$, pozwala odszyfrować wiadomość poprzez obliczenie $c^d \bmod n$. Wyjaśnij, dlaczego to działa, oraz przelicz odręcznie trywialny przykład z $n = 21$ i $e = 5$ dla $m = 4$.

Michał Bujak
Piotr Czarnik
Andrzej Kapanowski
Alicja Kawala
Jakub Mielczarek
Andrzej Rostworowski