příjmení : **Matematické algoritmy - varianta I**

jméno : *10. ledna 2008*

skupina : *doba řešení 60 minut*

1. S použitím čínské věty o zbytcích nalezněte obecné řešení x kongruencí

$$\begin{aligned} x &\equiv 1 (\mathrm{mod}\, 3), \\ x &\equiv 2 (\mathrm{mod}\, 5), \\ x &\equiv 3 (\mathrm{mod}\, 7). \end{aligned}$$

2. Dokažte, že každé číslo $2^{4m} - 1$ je dělitelné 3×5.

3. Mezi možné generátory prvočísel patří také výraz $V_n = 2n^2+11$, který nabývá prvočíselné hodnoty pro $n = 0, 1, 2, 3, \ldots, 10$. Ukažte, že pro $n = 11$ je V_n číslo složené.

4. Tak zvaná *afinní šifra* je definována šifrovací transformací $\mathcal{C}(m) = a \cdot m + b \,(\mathrm{mod}\, n)$ a dešifrovací transformací $\mathcal{D}(c) = a^{-1} \cdot (c - b) \,(\mathrm{mod}\, n)$, přičemž musí existovat multiplikativní inverze a^{-1} a musí tedy platit, že $\gcd(a, n) = 1$. Zprávy šifrujeme a dešifrujeme po jednotlivých znacích.

   Přiřadíme-li jednotlivým znakům anglické abecedy ($n = 26$) jejich numerické ekvivalenty podle následující tabulky,

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

   a zvolíme-li $a = 7$ a $b = 3$, obdržíme po zakódování textu šifrovanou zprávu MXSY ESFMFRG, přičemž mezery se zachovávají.

   Jaké bylo znění původního textu?

1. K zadaným kongruencím

$$\begin{aligned} x &\equiv 1 (\mathrm{mod}\, 3), \\ x &\equiv 2 (\mathrm{mod}\, 5), \\ x &\equiv 3 (\mathrm{mod}\, 7). \end{aligned}$$

vytvoříme nulové a jednotkové zbytkové třídy pro kombinace původních modulů $m_i = 3, 5, 7$

$$\begin{aligned} 70 &\equiv 0 (\mathrm{mod}\, 5 \times 7) \quad 70 \equiv 1 (\mathrm{mod}\, 3), \\ 21 &\equiv 0 (\mathrm{mod}\, 3 \times 7) \quad 21 \equiv 1 (\mathrm{mod}\, 5), \\ 15 &\equiv 0 (\mathrm{mod}\, 3 \times 5) \quad 15 \equiv 1 (\mathrm{mod}\, 7). \end{aligned}$$

Řešením uvedených kongruencí je

$$\hat{x} = 1 \times 70 + 2 \times 21 + 3 \times 15 = 157$$

a příslušná zbytková třída je

$$x = 157 \equiv 52 (\mathrm{mod}\, 105)$$

takže obecné řešení má tvar

$$x = 52 + n \times 105$$

2. Protože platí

$$\begin{aligned} 2^{4m} \equiv 1 (\mathrm{mod}\, 3 \times 5) \Leftrightarrow 16^m &\equiv 1 (\mathrm{mod}\, 15), \\ 16 &\equiv 1 (\mathrm{mod}\, 15), \\ &\times \\ &\vdots \\ 16 &\equiv 1 (\mathrm{mod}\, 15), \end{aligned}$$

je potom

$$\begin{aligned} 2^{4m} &\equiv 1 (\mathrm{mod}\, 3 \times 5), \\ 2^{4m} - 1 &\equiv 0 (\mathrm{mod}\, 3 \times 5). \end{aligned}$$

3. Dešifrovací transformace je $\mathcal{D}(c) = 7^{-1}(c - 3) \,(\mathrm{mod}\, 26)$, a platí $7^{-1} \equiv 15 \,(\mathrm{mod}\, 26)$, je tedy

$$\mathcal{D}(c) = 15c - 19 \,(\mathrm{mod}\, 26).$$

	M	S	X	Y		M	G	X	X	A	J	
c	12	18	20	E		G	H	I	J	K	L	
$(c-3) (\mathrm{mod}\, 26)$	9	12	13	4		6	7	8	9	10	11	
$15(c-3) (\mathrm{mod}\, 26)$	5	4	13	R		T	U	V	W	X	Y	
	F	O	R	D		P	R	E	F	E	C	T