závěrečná písemka 23.1.2023, skupina **A**

Obecné doporučení: Čtěte pozorně, často jsou v textu informace, které Vám počítání zjednoduší. Navíc se po Vás také často chce několik věcí, tak na žádnou nezapomeňte.

1. Zbytková třída 5 modulo 47 je primitivní kořen (nemusíte to ověřovat). Z přednášky se nám bude hodit

$$a^s \equiv a^t \pmod{n} \Leftrightarrow s \equiv t \pmod{\operatorname{ord}_n a}, \tag{$\star$}$$

kde $\operatorname{ord}_n a$ značí řád zbytkové třídy $a \pmod{n}$.

a) **Dokažte**, že zbytková třída 10 modulo 23 je také primitivní kořen. **Rozhodněte**, která ze dvou odpovídajících zbytkových tříd $10 \pmod{46}$, $33 \pmod{46}$ je primitivním kořenem a vysvětlete proč (není potřeba za tímto účelem počítat mocniny modulo 46, stačí počítat zvlášť modulo 2 a 23). Označme tuto zbytkovou třídu $g \pmod{46}$.

b) **Rozhodněte** s využitím ($\star$), která z kongruencí

$$5^{(g^x)} \equiv 25 \pmod{47}, \quad 25^{(g^x)} \equiv 25 \pmod{47}$$

má a která nemá řešení.

c) **Dokažte** $k \mid l \Rightarrow \varphi(k) \mid \varphi(l)$.

d) V tomto bodě jsou a, b parametry splňující $(a, 47) = 1$, $(b, 46) = 1$. Vztah ($\star$) říká, že výraz $a^s \pmod{47}$ nabývá právě $\operatorname{ord}_{47} a$ různých hodnot – pro $\operatorname{ord}_{47} a$ různých zbytkových tříd $s \pmod{\operatorname{ord}_{47} a}$. **Určete** podobně počet m různých hodnot výrazu $a^{(b^x)} \pmod{47}$. Kongruence $a^{(b^x)} \equiv c \pmod{47}$ pak buď nebude mít žádné řešení nebo řešením bude jediná zbytková třída modulo m. S využitím $\operatorname{ord}_n a \mid \varphi(n)$ a části c) **dokažte** $m \mid \varphi(\varphi(47))$.

e) Pro každou ze čtyř možných hodnot $m \mid \varphi(\varphi(47))$ **najděte** hodnotu parametru b tak, aby kongruence

$$5^{(b^x)} \equiv 5 \pmod{47},$$

měla jediné řešení modulo m (kterým pak samozřejmě bude $x \equiv 0 \pmod{m}$). **Kolik** řešení bude v každém případě existovat modulo $\varphi(\varphi(47))$?

(18 bodů)

2. Albert a Bedřich chtějí komunikovat Rabinovou šifrou. Albert si zvolil jako soukromý klíč prvočísla $p = 19$, $q = 23$ a jim příslušný veřejný klíč – modul $n = p \cdot q = 437$. Bedřich mu poslal veřejným kanálem zašifrovanou zprávu $c \equiv 328 \pmod{437}$. **Dešifrujte** Bedřichovu zprávu. Asi budete chtít počítat prvně zvlášť modulo 19, 23 a tyto částečné výsledky pak dát dohromady.

(12 bodů)

3. Polynom $1 + x + x^4$ je primitivní, takže jím generovaný lineární $(12, 8)$-kód rozpoznává dvojité chyby (to by platilo dokonce i pro delší kód).

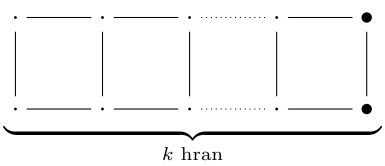
a) **Demonstrujte** explicitně na konkrétním příkladu, že tento kód nerozpoznává trojité chyby.

b) **Demonstrujte** explicitně na konkrétním příkladu, že tento kód neopravuje dvojité chyby.

c) **Dekódujte** obdržená slova 1100 | 10010001 a 0111 | 10010001 za předpokladu nejmenšího možného počtu chyb.

(12 bodů)

4. Cílem tohoto příkladu je určení počtu obarvení následujícího grafu dvěma barvami, ve kterých každý čtverec obsahuje vrcholy obou barev.



Označme a_k počet takových obarvení, ve kterých jsou (zvýrazněné) vrcholy na pravé straně obarveny dvěma různými barvami, pevně zvolenými (počet obarvení na tomto výběru nezáleží). Protože je k počet vodorovných hran, máme $a_0 = 1$. Označme b_k počet takových obarvení, ve kterých jsou vrcholy na pravé straně obarveny jednou barvou, opět pevně zvolenou. Protože je k počet vodorovných hran, máme $b_0 = 1$.

a) V obou případech si zvolte libovolné vyhovující obarvení na pravé straně a (např. vypsáním všech možností pro sousedy) **odvoďte** rekurence pro a_k, b_k pomocí a_{k-1}, b_{k-1}, která platí i pro $k = 0$. Dokažte, že platí $a_k = b_k + b_{k-1}$ a pomocí této substituce **nahraďte** systém rekurencí jedinou rekurencí pro posloupnost b_k (odkazující se ovšem nyní na b_{k-1}, b_{k-2}).

b) **Vyřešte** tuto rekurenci bez explicitního dopočítávání koeficientů a **odvoďte** asymptotické chování $b_k \approx C \cdot B^k$, ve kterém **určete** základ B (pokud bude výraz pro B obsahovat $\sqrt{17}$, bude pravděpodobně dobře). **Rozhodněte**, zda $\lim_{k\to\infty} |b_k - C \cdot B^k| = 0$.

Poznamenejme, že počet všech obarvení je $2 \cdot a_k + 2 \cdot b_k$ a asymptoticky vypadá stejně, jen pro jiný koeficient C. Samozřejmě se jej můžete pokusit odvodit.

(12 bodů)