1. Soustavy lineárních kongruencí 19.3.

1. Skupině třinácti pirátů se podařilo uloupit bednu zlatých mincí. Zkusili je rozdělit rovným dílem na třináct hromádek, ale deset mincí jim zbylo. O zbylé mince se strhla rvačka, při níž jednoho piráta propíchli. Přestali tedy bojovat a zkusili mezi sebe znovu rozdělit mince rovným dílem. Tentokrát zbyly tři mince, o které opět začali bojovat. V boji zahynul další pirát a tak si ostatní opět zkusili mince spravedlivě rozdělit, tentokrát úspěšně. Kolik bylo nejméně mincí, které piráti ukradli?

2. Vyřešte lineární kongruenci $3446x \equiv 8642 \pmod{208}$.

2. Kongruence vyšších řádů, primitivní kořeny, testy prvočíselnosti 2.4.

1. Vyřešte $7x^4 + 19x + 25 \equiv 0 \pmod{27}$.

2. Ukažte, že neexistují primitivní kořeny modulo 8.

3. Nalezněte všechny primitivní kořenymodulo 41 a vyřešte $7x^{17} \equiv 11 \pmod{41}$.

4. Vyřešte $x^2 - 23 \equiv 0 \pmod{77}$.

5. Dokažte, že čísla 2465, 2821 a 6601 jsou tzv. Carmichaelova.

6. Ukažte, že číslo 341 je Fermatovo pseudoprvočíslo o základu 2, ale že není Euler-Jacobiho pseudoprvočíslo o základu 2. Dále, že číslo 561 je E-J pseudoprvočíslo o základu 2, ale ne o základu 3 a že naopak číslo 121 není E-J pseudoprvočíslo o základu 2, ale je o základu 3.

3. Testy prvočíselnosti 9.4.

1. Pomocí Pocklington-Lehmer testu ukažte, že 1321 je prvočíslo.

Řešení. $N - 1 = 1320 = 2^3.3.5.11$
$F := 2^3.3.5 = 120$, $U := 11 \Rightarrow (F, U) = (120, 11) = 1$
$(2^{\frac{1320}{2}}, 1321) = 1$, $(2^{\frac{1320}{3}}, 1321) = 1$, $(2^{\frac{1320}{5}}, 1321) = 1$ a $2^{1320} \equiv 1 \bmod(1321) \Rightarrow$ Svědkové prvočíselnosti jsou $a_2 = a_3 = a_5 = 2$.

2. Pomocí Pollardova rho algoritmu najděte faktorizaci čísla 221. [využijte funkci $f(x) = x^2 + 1$, poč. podm. $x_0 = 2$]

Řešení. $x = y = 2$

$x := f(x)$	$y := f(f(y))$	$(\lvert x - y\rvert, 221)$	$\bmod(221)$
5	26	1	
26	197	1	
14	104	1	
197	145	13	

$\rightsquigarrow 221 = 13.17$

4. Booleovy algebry

Příkladem užitečné algebraické struktury je tzv. Booleova algebra - viz přednáška. Tato abstraktní struktura pomáhá řešit různé konkrétní problémy, např. v teorii množin nebo v logice. Množinový výraz či logickou formuli můžeme přepsat do formálního výrazu v Booleově algebře, využít identit v této algebře k úpravě výrazu a výsledek formulovat zpět jako množinový výraz nebo logickou formuli, viz příklady níže.

1. Zjednodušte výraz $((A \wedge B) \vee (A \Rightarrow B)) \wedge ((B' \Rightarrow C) \vee (B \wedge C'))$.

Řešení. Přepsáním do Booleovy algebry dostáváme

$$(a.b + a' + b).(b + c + b.c') = \cdots = a'.c + b.$$

To znamená, že výše uvedená formule je ekvivalentní výroku $(A' \wedge C) \vee B$.

2. Anna, Bára, Kateřina a Dana chtějí jet na výlet. Rozhodněte, která z děvčat pojedou, mají-li být dodrženy tyto zásady: Pojede aspoň jedna z dvojice Bára/Dana, nejvýše jedna z dvojice Anna/Kateřina, aspoň jedna z dvojice Anna/Dana a nejvýše jedna z dvojice Bára/Kateřina. Dále je jisté, že Bára nepojede bez Anny a že Kateřina pojede, pojede-li Dana.

Řešení. Přepsáním do Booleovy algebry, úpravou a přepsáním zpět dostaneme, že na výlet pojede buď právě Anna s Bárou nebo právě Kateřina s Danou.

5. Kódování

Příkladem využití jiné algebraické struktury, konkrétně okruhu polynomů nad $\mathbb{Z}_2$ (či jiným konečným polem), jsou (n, p) kódy - viz přednáška a příklady níže.

1. Uvažujme $(5, 3)$ kód nad $\mathbb{Z}_2$ generovaný polynomem $x^2 + x + 1$. Vypište všechna kódová slova, najděte generující matici a matici kontroly parity.

Řešení. $p(x) = x^2 + x + 1$. Kódová slova jsou právě násobky generujícího polynomu:

$$0.p, 1.p, x.p, (x+1).p, x^2.p, (x^2+1).p, (x^2+x).p, (x^2+x+1).p$$

neboli

$$0, x^2 + x + 1, x^3 + x^2 + x, x^3 + 1, x^4 + x^3 + x^2, x^4 + x^3 + x + 1, x^4 + x, x^4 + x^2 + 1$$

neboli

$$00000, 11100, 01110, 10010, 00111, 11011, 01001, 10101$$

Bázové vektory vynásobené $x^{5-3} = x^2$ dávají $\mathrm{mod}(p)$:

$$\begin{aligned} x^2 &\equiv x + 1 \\ x^3 &= x.x^2 \equiv x(x+1) = x^2 + x \equiv 1 \\ x^4 &\equiv x \end{aligned}$$

To znamená, že bázové vektory se zakódují následovně

$$\begin{array}{lcl} 1 \mapsto x^2 + x + 1 & & 100 \mapsto 11100 \\ x \mapsto x^3 + x & \text{tj.} & 010 \mapsto 10010 \\ x^2 \mapsto x^4 + 1 & & 001 \mapsto 01001 \end{array}$$

a proto je generující matice

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

a matice kontroly parity

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

2. Udělejte to samé se $(7, 4)$ kódem nad $\mathbb{Z}_2$ generovaným polynomem $x^3 + x + 1$.

Řešení.

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

6. Vytvořující funkce

1. Pomocí vytvořující funkce určete počet jedniček v náhodném binárním řetězci.

Řešení. Oynačme B množinu řetězců, pro řetězec $b \in B$ $|b|$ počet jeho bitů a $j(b)$ počet jedniček. Vytvořující funkce má tvar

$$B(x) = \sum_{b \in B} x^{|b|} = \sum_{n \geq 0} 2^n x^n = \frac{1}{1-2x}$$

Vytvořující funkce pro počet jedniček je

$$C(x) = \sum_{b \in B} j(b) x^{|b|}$$

Řetězec b dostaneme z o jeden bit kratšího b' přidáním jedné nuly nebo jedničky, tj. $j(b)$ je součtem $j(b')$ jedniček a $j(b')+1$ jedniček. Takže

$$C(x) = \sum_{b' \in B} (1 + 2j(b'))x^{|b'|+1} = \sum_{b' \in B} x^{|b'|+1} + 2\sum_{b' \in B} j(b')x^{|b'|+1} = xB(x) + 2xC(x)$$

Odtud

$$C(x) = \frac{x}{(1-2x)^2} = x(1-2x)^{-2}$$

a n-tý koeficient je $c_n = 2^{n-1}\binom{-2}{n-1} = n2^{n-1}$. Toto číslo udává počet jedniček v bitech délky n. Těch je $b_n = 2^n$. V jednom řetězci je tedy $\frac{c_n}{b_n} = \frac{n}{2}$ jedniček. To je samozřejmě očekávaný výsledek.

7. Bodované příklady, odevzdat do 21.5.

1. Pomocí přepisu do Booleovy algebry vyřešte následující úlohu:

Při vyšetřování vraždy bylo zajištěno pět podezřelých Kalina, Nováček, Obrátil, Pražák, Ryvola. V době činu byl na místě Obrátil nebo Pražák, ale nejvýše jeden z dvojice Kalina, Nováček a aspoň jeden z dvojice Kalina, Obrátil. Podezřelý Ryvola tam mohl být jen v přítomnosti Pražáka, ale pokud tam Ryvola byl, nechyběl ani Obrátil. Lze vyloučit spolupráci Nováčka s Pražákem, zato Nováček a Obrátil tvoří nerozlučnou dvojici. Kdo z podezřelých vraždu spáchal?

Řešení. Přepisem do Booleovské algebry, podle prvních písmen jména, dostáváme

$$(o+p)(k'+n')(k+o)(p+r')(r'+o)(n'+p')no$$

a s využitím $x^2 = x$, $xx' = 0$ dostaneme $r'p'nok'$. Vinni jsou teda Nováček a Obrátil.

Poslední podmínka v zadání by se ovšem měla pochopit tak, že buď tam byli oba nebo ani jeden (Nováček a Obrátil). Tím pádem bude konec výrazu v Booleovské algebře $\ldots(no + n'o')$ místo $\ldots no$. Tím nám na konci po úpravě přibude člen $r'pn'o'k$. Vraždu tedy mohl rovněž spáchat Kalina s Pražákem.

2. Uvažme $(15, 11)$ kód generovaný polynomem $1 + x^3 + x^4$. Přijali jsme kód 011101110111001. Určete původní 11-bitovou zprávu předpokládáme-li, že při přenosu došlo k chybě na jednom bitu.

Řešení. Řetězec je kódové slovo, právě tehdy, když je dělitelný generujícím polynomem, tj. v našem případě $1 + x^3 + x^4$. Přijatý řetězec odpovídá polynomu $x+x^2+x^3+x^5+x^6+x^7+x^9+x^{10}+x^{11}+x^{14}$. Tento polynom dává po dělení $1+x^3+x^4$ zbytek $x+1$. To znamená, že při přenosu došlo k chybě. Předpokládáme-li, že chyba je jen na jednom bitu, musí existovat mocnina x, která je rovna tomuto zbytku modulo $1 + x^3 + x^4$. Proto počítáme $x^4 \equiv x^3 + 1, x^5 \equiv x^3 + x + 1, \ldots, x^{12} \equiv x + 1$. Chyba tedy nastala na třináctém bitu a originální zpráva byla 01110111101.

Můžeme si příklad i víc rozebrat. Když si spočítáme všechny mocniny x, dostaneme

$$\begin{aligned}
x^4 &\equiv x^3 + 1\\
x^5 &\equiv x^3 + x + 1\\
x^6 &\equiv x^3 + x^2 + x + 1\\
x^7 &\equiv x^2 + x + 1\\
x^8 &\equiv x^3 + x^2 + x\\
x^9 &\equiv x^2 + 1\\
x^{10} &\equiv x^3 + x\\
x^{11} &\equiv x^3 + x^2 + 1\\
x^{12} &\equiv x + 1\\
x^{13} &\equiv x^2 + x\\
x^{14} &\equiv x^3 + x^2
\end{aligned}$$

a generující matice je tedy

$$G = \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0\\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0\\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1\\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

Můžeme si ověřit, že vynásobením 01110111101 dostaneme kódové slovo 011101110111101, které se liší od přijatého řetězce 011101110111001 právě na tom třináctém bitu.

3. Pomocí vytvořující funkce vyřešte následující rekurenci:

$$\begin{aligned}
&a_0 = 1, a_1 = 2\\
&a_n = 5a_{n-1} - 4a_{n-2} \quad n \geq 2
\end{aligned}$$

Řešení. Univerzální formule má tvar

$$a_n = 5a_{n-1} - 4a_{n-2} - 3[n = 1] + [n = 0]$$

Vynásobením obou stran x^n a sečtením přes všechna n dostaneme

$$A(x) = 5xA(x) - 4x^2A(x) - 3x + 1$$

Odtud

$$A(x) = \frac{1 - 3x}{(1 - 4x)(1 - x)} = \frac{2}{3}\frac{1}{1 - x} + \frac{1}{3}\frac{1}{1 - 4x}$$

a

$$a_n = \frac{2}{3}\binom{-1}{n} + \frac{2}{3}\binom{-1}{n}(-4)^n = \frac{4^n + 2}{3}.$$