Universidade Federal da Bahia
Departamento de Matemática

Matemática Discreta II
Prof. Ciro Russo
Segunda unidade – 1 de agosto de 2018

Atenção: é preciso justificar todas as respostas.

1. Verifique se o seguinte sistema de equações congruenciais é solucionável e, em caso afirmativo, encontre o conjunto das soluções:

$$\begin{cases} x \equiv 12 \pmod 5 \\ x \equiv 7 \pmod 4 \\ x \equiv 22 \pmod 7 \end{cases}.$$

2. Considere a menor solução positiva n do Exercício 1 e, usando os critérios de divisibilidade e o crivo de Eratóstenes, encontre a decomposição de n no produto de potências de primos. Encontre também a expressão na base 13 de $14 \cdot n$ (algarismos: $0, \ldots, 9, A, B, C$).

3. Seja $I_2 = \{0, 1\}$, ordenado com a ordem usual dos números naturais $\leq$, e consideremos $I_2^3 = \{(x, y, z) : x, y, z \in \{0, 1\}\}$ com a ordem produto (ou seja, $(x_1, x_2, x_3) \leq (y_1, y_2, y_3)$ sse $x_i \leq y_i$ $\forall i = 1, 2, 3$).

(a) Verifique que I_2^3, com essa ordem, é uma álgebra de Boole e determine quais são as suas operações $\vee, \wedge$ e $\neg$, e as suas constantes 0 e 1.

(b) Defina um isomorfismo de álgebras de Boole entre I_2^3 e $\wp(X)$, onde $X = \{a_1, a_2, a_3\}$.

(c) Defina uma imersão de álgebras de Boole de D_{77} em I_2^3.

(d) Defina uma imersão de reticulados de D_{77} em I_2^3 que não preserve $\neg$.

(e) Determine todas as subálgebras de Boole de D_{77}.

$\boxed{1}$

$$\begin{cases} x \equiv 12 \pmod 5 \\ x \equiv 7 \pmod 4 \\ x \equiv 22 \pmod 7 \end{cases} \qquad m_1 = 5,\ m_2 = 2^2,\ m_3 = 7$$

Os m_i são dois a dois primos entre si, então o sistema é solucionável.

1. Simplificar (se possível):

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 7 \end{cases}$$

2. Calcular m'_1, m'_2, m'_3 e m: $m = 5 \cdot 4 \cdot 7 = 140$, $m'_1 = 4 \cdot 7 = 28$, $m'_2 = 5 \cdot 7 = 35$,

$$m'_3 = 5 \cdot 4 = 20$$

3. Escrever as equações "auxiliárias" $\left(m'_i\, x \equiv 1 \pmod{m_i}\right)$:

$28x \equiv 1 \pmod 5$, $35x \equiv 1 \pmod 4$, $20x \equiv 1 \pmod 7$

$3x \equiv 1 \pmod 5$, $3x \equiv 1 \pmod 4$, $-1 \cdot x \equiv 1 \pmod 7$

4. Solucionar tais equações

$$\begin{array}{c|c|c|c} 5 & 3 & 2 & 1 \\ \hline & 1 & 1 & \end{array} \qquad 1 = 3 - 2 = 3 - (5 - 3) = -1 \cdot 5 + 2 \cdot 3 \Rightarrow c_1 = 2$$

$$\begin{array}{c|c|c} 4 & 3 & 1 \\ \hline & 1 & \end{array} \qquad 1 = 4 - 3 = 1 \cdot 4 + (-1) \cdot 3 \Rightarrow c_2 = -1$$

$$c_3 = -1$$

5. Calcular $c = \sum_{i=1}^{n} b_i m'_i c_i$:

$$c = 2 \cdot 28 \cdot 2 + 3 \cdot 35 \cdot (-1) + 1 \cdot 20 \cdot (-1) = 112 - 105 - 20 = -13$$

6. Conjunto das soluções: $S = \{c + mk : k \in \mathbb{Z}\}$

$$S = \{-13 + 140k : k \in \mathbb{Z}\}.$$

$\boxed{2}$

A menor solução positiva do ex. 1 é dada por $k=1$ e é 127.

$2 \mid 127$? Não, pois 7 é ímpar.

$3 \mid 127$? $1+2+7=10$ que não é múltiplo de 3, então $3 \nmid 127$

$5 \nmid 127$ pois $7 \notin \{0,5\}$

$7 \mid 127$? $\quad 12 + 5 \cdot 7 = 47$ e $7 \nmid 47 \Rightarrow 7 \nmid 127$

$11 \mid 127$? $\quad (7+1)-2 = 6$ e $11 \nmid 6 \Rightarrow 11 \nmid 127$

O primo seguinte é 13. Como nenhum primo < 13 divide 127, para 13 dividir 127 é necessário que 127 seja $\geqslant 13^2$. Mas $13^2 = 169 > 127$. Logo, 127 é primo pois nenhum primo $\leq \sqrt{127}$ divide 127.

Vamos encontrar a expansão de $14 \cdot 127$ na base 13.

$14 \cdot 127 = 1778 \;\underline{|\,13}$

$\quad 47 \qquad 136 \;\underline{|\,13}$

$\quad 88 \qquad\; 6 \qquad 10 \;\underline{|\,13}$

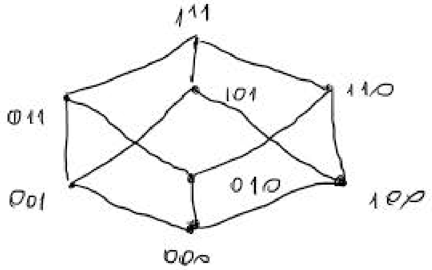
$\quad \boxed{10} \qquad \boxed{6} \qquad\quad 0$

$\qquad\qquad\qquad\quad \boxed{10}$

$$(1778)_{10} = (A6A)_{13}$$

$\boxed{3}$ $\left(\underbrace{\{0,1\}^3}_{S}, \leq\right)$

$S = \{(0,0,0), (0,0,1), (0,1,0), (1,0,0), (0,1,1), (1,0,1), (1,1,0), (1,1,1)\}$



S é limitado, $\max S = 111$
$\min S = 000$

$(x,y,z) \vee (x',y',z') = (x \vee x', y \vee y', z \vee z')$

$(x,y,z) \wedge (x',y',z') = (x \wedge x', y \wedge y', z \wedge z')$

$(\{0,1\}, \leq)$ é reticulado distributivo

$$((x,y,z) \vee (x',y',z')) \wedge (x'',y'',z'') = ((x \vee x') \wedge x'', (y \vee y') \wedge y'', (z \vee z') \wedge z'') =$$

$$= ((x \wedge x'') \vee (x' \wedge x''), (y \wedge y'') \vee (y' \wedge y''), (z \wedge z'') \vee (z' \wedge z'')) =$$

$$= (x \wedge x'', y \wedge y'', z \wedge z'') \vee (x' \wedge x'', y' \wedge y'', z' \wedge z'') =$$

$$= ((x,y,z) \wedge (x'',y'',z'')) \vee ((x',y',\cancel{z}z') \wedge (x'',y'',z'')) \Rightarrow S \text{ é distributivo.}$$

$\forall (x,y,z), (x',y',z') \in S \quad (x',y',z') = \neg(x,y,\cancel{z}z)$ sse

sse $(x,y,z) \vee (x',y',z') = (1,1,1)$ e $(x,y,z) \wedge (x',y',z') = (0,0,0)$ sse

sse $(x \vee x', y \vee y', z \vee z') = (1,1,1)$ e $(x \wedge x', y \wedge y', z \wedge z') = (0,0,0)$ sse

sse $x' = \neg x$, $y' = \neg y$, $z' = \neg z$ sse $x' = 1-x$, $y' = 1-y$, $z' = 1-z$.

Então S é complementado e $\neg(x,y,z) = (1-x, 1-y, 1-z)$ $\forall (x,y,z) \in S$.

Logo, S é uma álgebra de Boole.

$\boxed{3\,(b)}$ Defina um isomorfismo entre S e $\mathcal{P}(X)$,
$X = \{a_1, a_2, a_3\}$

$$f: \mathcal{P}(X) \to S$$
$$Y \mapsto (x_1, x_2, x_3) \text{ t.q. } x_i = \begin{cases} 0 \text{ se } a_i \notin Y \\ 1 \text{ se } a_i \in Y \end{cases}$$

$f(\emptyset) = (0,0,0) \Rightarrow f(\min \mathcal{P}(X)) = \min S$ ✓

$f(Y^c) = (x_1', x_2', x_3')$ com $x_i' = \begin{cases} 0 \text{ se } a_i \notin Y^c \text{ sse } a_i \in Y \\ 1 \text{ se } a_i \in Y^c \text{ sse } a_i \notin Y \end{cases}$

$\Rightarrow x_i' = \neg x_i \quad (i = 1, 2, 3) \Rightarrow f(Y^c) = \neg f(Y)$ ✓

$f(Y) = (y_1, y_2, y_3)$, $f(Z) = (z_1, z_2, z_3)$, $f(Y \cup Z) = (x_1, x_2, x_3)$

$x_i = 0$ sse $a_i \notin Y \cup Z$ sse $(a_i \notin Y$ e $a_i \notin Z)$ sse $(y_i = 0$ e $z_i = 0)$ e, então,
$x_i = 1$ sse $a_i \in Y \cup Z$ sse $(a_i \in Y$ ou $a_i \in Z)$ sse $(y_i = 1$ ou $z_i = 1)$

$x_i = y_i \vee z_i \Rightarrow f(Y \cup Z) = (y_1, y_2, y_3) \vee (z_1, z_2, z_3) = f(Y) \vee f(Z)$.

Logo, f é um homom. de álgebras de Boole.

Se $Y \neq Z \in \mathcal{P}(X)$, então $\exists\, i \leq 3$ t.q. $a_i \in Y \setminus Z$ ou $a_i \in Z \setminus Y$.
Sem perda, podemos supor $a_i \in Y \setminus Z$. Então $y_i = 1$ e $z_i = 0 \Rightarrow$
$\Rightarrow f(Y) \neq f(Z)$. Logo, f é injetora.

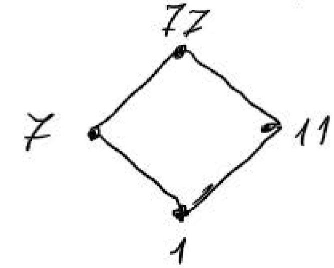
$\forall (y_1, y_2, y_3) \in S$, seja $Y = \{a_i \in X : y_i = 1\}$.

$f(Y) = (y_1', y_2', y_3')$ com $y_i' = \begin{cases} 0 \text{ sse } a_i \notin Y \text{ sse } y_i = 0 \\ 1 \text{ sse } a_i \in Y \text{ sse } y_i = 1 \end{cases} \Rightarrow y_i' = y_i$.

Segue que f é sobrej., então bijetora e, portanto, um isomorfismo.

$\boxed{3(c)}$ Defina uma imersão de álgebras de Boole de $\left(D_{77}, \mathrm{mmc}, \mathrm{mdc}, {}^{77}/\cdot, 1, 77\right)$ para S.

$D_{77} = \{1, 7, 11, 77\}$



$f: D_{77} \to S$ é imersão de álgebras de Boole sse f é hom. injetor de álgebras de Boole.

Como f tem que preservar min e max, $f(1) = (0,0,0)$ e $f(77) = (1,1,1)$.

Seja $f(7) = (1,0,1)$. Como $11 = {}^{77}/_{7}$, $f(11)$ tem que ser $\neg f(7)$, e então, $f(11) = (0,1,0)$.

Desta forma defini um f que é injetora e preserva min e $\neg$.

$f(\mathrm{mdc}(7,11)) = f(1) = (0,0,0)$ e $f(7) \wedge f(11) = (1,0,1) \wedge (0,1,0) = (0,0,0)$ ✓

f é imersão de álg. de Boole.

$\boxed{3(d)}$ Encontre todas as subálgebras de D_{77}.

A é subálgebra de D_{77} sse $1, 77 \in A$ e $\forall x, y \in A$,

$x \vee y \in A$ e $\neg x \in A$.

D_{77} é subálg. de D_{77}.

$A = \{1, 77\}$ também pois $1 \vee 77 = 77 \in A$, $\neg 1 = 77 \in A$.

Se $7 \in B$ subálg. de D_{77} $\Rightarrow 11 \in B \Rightarrow B = D_{77}$.

Se $11 \in B$ subálg. de D_{77} $\Rightarrow 7 = \neg 11 \in B \Rightarrow B = D_{77}$.

Logo, D_{77} e $\{1, 77\}$ são as únicas subálgebras de D_{77}.