Números Inteiros e Criptografia - Lista 1
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

1)
a. Sempre que um número inteiro é par e maior que 2, ele é a soma de dois primos.

n = número inteiro
P(n) = inteiro par
M(n) = inteiro maior que 2
S(n) = inteiro que é a soma de dois números primos

$\forall n(P(n) \wedge M(n)) \text{ -> } S(n)$

b)Todo dia eu como manga ou tomo leite, mas nunca ambos no mesmo dia.

x: dia
m(x): comer manga
l(x): tomar leite

$\forall x[(m(x) \wedge \neg l(x)) \vee (\neg m(x) \wedge l(x))]$

2)
a)$p \rightarrow (q \rightarrow p)$

q	p	$q \rightarrow p$	$p \rightarrow (q \rightarrow p)$
v	v	v	v
v	f	f	v
f	v	v	v
f	f	v	v

b)

$[(p \rightarrow q) \land (r \rightarrow s)] \rightarrow [(p \lor r) \rightarrow (q \lor s)]$

p	q	r	s	$p \rightarrow q$	$r \rightarrow s$	$(p \rightarrow q) \land (r \rightarrow s$	$p \lor r$	$q \lor s$	$(p \lor r) \rightarrow (q \lor s)$	$[(p \rightarrow q) \land (r \rightarrow s)] \rightarrow [(p \lor r) \rightarrow (q \lor s)]$
v	v	v	v	v	v	v	v	v	v	v
v	v	v	f	v	f	f	v	v	v	v
v	v	f	v	v	v	v	v	v	v	v
v	v	f	f	v	v	v	v	v	v	v
v	f	v	v	f	v	f	v	v	v	v
v	f	v	f	f	f	f	v	f	f	v
v	f	f	v	f	v	f	v	v	v	v
v	f	f	f	f	v	f	v	f	f	v
f	v	v	v	v	v	v	v	v	v	v
f	v	v	f	v	f	f	v	v	v	v
f	v	f	v	v	v	v	f	v	v	v
f	v	f	f	v	v	v	f	v	v	v
f	f	v	v	v	v	v	v	v	v	v
f	f	v	f	v	f	f	v	f	f	v
f	f	f	v	v	v	v	f	v	v	v
f	f	f	f	v	v	v	f	f	v	v

c) [p → (q → r)] ←→ [(p ∧ q) → r]

p	q	r	(q->r)	(p^q)	(p->(q->r))	[(p^q)->r]	[p → (q → r)] ←→ [(p ∧ q) → r]
v	v	v	v	v	v	v	v
v	v	f	f	v	f	f	v
v	f	v	v	f	v	v	v
v	f	f	v	f	v	v	v
f	v	v	v	f	v	v	v
f	v	f	f	f	v	v	v
f	f	v	v	f	v	v	v
f	f	f	v	f	v	v	v

d)
[p ∧ (p → q)] → q

p	q	p → q	p ∧ (p → q)	[p ∧ (p → q)] → q
v	v	v	v	v
v	f	f	f	v
f	v	v	f	v
f	f	v	f	v

3)

a) Existem pelo menos dois x tais que φ(x).
∃x(φ(x)) ∧ ∀y∀z[(φ(y) ∧ φ(z)) → y =/= z].

b) Existem no máximo dois x tais que φ(x)
∃x(φ(x)) ∧ ∀y∀z∀k[{(φ(y) ∧ φ(z) ∧ φ(k))} → y =/= z = k].

c) Existem exatamente dois x tais que φ(x).
∃x(φ(x)) ∧ ∀y∀z∀k∀q[{(φ(y) ∧ φ(z) ∧ φ(k) ∧ φ(q)} → q = y =/= z = k].

4)
a) Existe um número inteiro que é primo ou igual a 15

Todo número inteiro não é primo e difere e 15

b) Todo número real é o resultado da divisão de dois inteiros.

Existe um número real que não é resultado da divisão de dois inteiros.

c) Para qualquer número real não-nulo x existe um número real y tal que o produto de x e y é igual a 1.

Existe um número real-não nulo x para todo número real y tal que o produto de x e y não é igual a 1.

5) Considerando que
a as variáveis x e y sejam todas os carros.
R(x, y) significa “x é pelo menos tão rápido quanto y”,
C(x, y) significa “x é pelo menos tão caro quanto y”
V (x, y) significa “x é pelo menos tão velho quanto y”

a) $\forall x \exists y[V(y, x) \land C(y, x) \land R(x, y)]$

O carro y é tão velho e caro quanto todos carros x, que são tão rápidos quanto ele.

b) $\exists x \forall y(V(y, x))$

Um carro x é tão velho quanto os carros y.

c) $\neg[\forall x \forall y(R(x, y) \longleftrightarrow C(x, y))]$

Ou todo carro x é tão rápido quanto y, mas não tão caro quanto ou todo carro x não é tão rápido quanto y, mas é tão caro quanto.

6-)Seja x um número real. Dizemos que x é gelatinoso se ele é fleumático e para todo número natural n existe algum número real y tal que y^2 encapsula superiormente x ou y + n encapsula inferiormente x. Como você caracterizaria um número real não-gelatinoso?

g(x): x é gelatinoso
f(x): x é fleumático
S(n,y): $\forall n \exists y$[y^2 encapsula superiormente x]
I(n,y): $\forall n \exists y$[y+n encapsula inferiormente x]

Então: $[F(x) \land (S(n,y) \lor I(n,y))] \rightarrow G(x)$

$\neg G(x) \rightarrow \neg[F(x) \land (S(n,y) \lor I(n,y))]$
Podemos dizer que x não é gelatinoso se ele for não for fleumático ou existir pelo menos um número natural n para todo número real y tal que y^2 encapsula superiormente x e y+n encapsula inferiormente x.

7) (X ∪ Y) \ X = Y \ (X ∩ Y) = Y\ X.

(X ∪ Y) \ X = Y \ (X ∩ Y)

{n; n∈X v n∈Y}^¬{n; n∈X} = {n; n∈Y}^¬{n; n∈X ^ n∈Y}

(X v Y) ^(¬ X) = (Y^(¬(x^Y)))

x	y	X v Y	¬ X	(X v Y) ^(¬ X)
v	v	v	f	f
v	f	v	f	f
f	v	v	v	v
f	f	f	v	f

x	y	x^Y	¬(x^Y)	(Y^(¬(x^Y)))
v	v	v	f	f
v	f	f	v	f
f	v	f	v	v
f	f	f	v	f

Y \ (X ∩ Y) = Y \ X.

{n; n∈Y} ^¬ {n; n∈X ^ n∈Y} = {n; n∈Y} ^¬ {n;n∈X}

(Y^(¬(X^Y))) = (Y ^(¬X))

X	Y	(X^Y)	¬(X^Y)	(Y^(¬(X^Y)))
v	v	v	f	f
v	f	f	v	f
f	v	f	v	v
f	f	f	v	f

x	y	¬X	(Y ^(¬X))
v	v	f	f
v	f	f	f

f	v	v	v
f	f	v	f

(X ∪ Y) \ X = Y \ X

{n; n∈X v n∈Y} ^¬ {n; n∈X} = {n; n∈Y} ^¬ {n; n∈X}

(x v Y) ^¬ X = Y ^¬X

x	y	x v y	¬X	(x v Y) ^¬ X
v	v	v	f	f
v	f	v	f	f
f	v	v	v	v
f	f	f	v	f

x	y	¬X	Y ^¬X
v	v	f	f
v	f	f	f
f	v	v	v
f	f	v	f

Como a tabela verdade resultou no mesmo resultado para todas as igualdades, provamos que as afirmações.

8) a)p ∧ (q ∨ r) = (p ∧ q) ∨ (p ∧ r)

p	q	r	q ∨ r	p ∧ (q ∨ r)
v	v	v	v	v

v	v	f	v	v
v	f	v	v	v
v	f	f	f	f
f	v	v	v	f
f	v	f	v	f
f	f	v	v	f
f	f	f	f	f

p	q	r	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
v	v	v	v	v	v
v	v	f	v	f	v
v	f	v	f	v	v
v	f	f	f	f	f
f	v	v	f	f	f
f	v	f	f	f	f
f	f	v	f	f	f
f	f	f	f	f	f

b)
$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R)$.
$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$

Pela definição de união, sabemos que o elemento x qualquer está Q ou R, exatamente como $x \in Q \vee x \in R$
$Q \cup R = \{x; x \in Q \vee x \in R\}$

Pela definição de intersecção, sabemos que o elemento x qualquer está P ($x \in P$) e na união de Q com R ($x \in Q \vee x \in R$)
$P \cap (Q \cup R) = \{x; x \in P \wedge (x \in Q \vee x \in R)\}$

$(P \cap Q) = \{x; x \in P \wedge x \in Q\}$

$(P \cap R) = \{x;\ x \in P \wedge x \in R\}$

$(P \cap Q) \cup (P \cap R) = \{x;\ x \in P \wedge x \in Q\} \vee \{x;\ x \in P \wedge x \in R\}$

$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R)$.
$\{x;\ x \in P \wedge (x \in Q \vee x \in R)\} = \{x;\ x \in P \wedge x \in Q\} \vee \{x;\ x \in P \wedge x \in R\}$

Como podemos traduzir "$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R)$" para "$\{x;\ x \in P \wedge (x \in Q \vee x \in R)\} = \{x;\ x \in P \wedge x \in Q\} \vee \{x;\ x \in P \wedge x \in R\}$", observamos certa semelhança com a fórmula "$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$". Podemos assim, provar que "$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R)$" é verdadeira pelas tabelas verdade do item a)