Universidade Federal da Bahia
Departamento de Matemática

Matemática Discreta II
Prof. Ciro Russo
Primeira unidade, segunda chamada – 20 de dezembro de 2017

Atenção: é preciso justificar todas as respostas.

1. Seja $\prec$ a relação binária em $\mathbb{N} \times \mathbb{N}$ definida por

$$(a, b) \prec (c, d) \text{ se, e somente se, } (a \mid c) \wedge (b \geq d)).$$

Verifique quais, entre as propriedades reflexiva, irreflexiva, simétrica, antissimétrica e transitiva, valem para $\prec$. Consequentemente, determine se ela é uma relação de equivalência, de ordem, de ordem estrita, ou nenhuma dessas.

2. Demonstre, usando o princípio de indução, que o cubo de todo número natural ímpar é ímpar, ou seja, que em $\mathbb{N}$ vale:

$$\forall n \exists a((2n + 1)^3 = 2a + 1).$$

3. Demonstre, usando apenas os axiomas da Aritmética de Peano e a propriedade comutativa da soma, a seguinte formula:

$$\forall x \exists y((x = y + y) \vee (x = s(y + y)).$$

4. Verifique que as seguintes equações diofantinas são solucionáveis e encontre os conjuntos das soluções.

(a) $25x + 30y = 40$;

(b) $110x + 76y = 6$.

Escreva, também, as duas equações congruenciais (uma na incógnita x e a outra em y) associadas a cada equação diofantina, com os respectivos conjuntos de soluções.

SOLUÇÕES.

1. Primeiramente, observe-se que, em $\mathbb{N}$, tanto $|$ quanto $\leq$ são relações de ordem, ou seja, são reflexivas, antissimétricas e transitivas.

$\forall a, b \in \mathbb{N}$, $a \mid a$ e $a \leq a$, então $(a, b) \prec (a, b)$ e $\prec$ é reflexiva. Portanto não é irreflexiva.

$\prec$ não é simétrica pois, por exemplo, $(1, 0) \prec (0, 0)$ mas $(0, 0) \not\prec (1, 0)$ uma vex que 0 não divide 1.

$\forall a, b, c, d \in \mathbb{N}$, se $(a, b) \prec (c, d)$ e $(c, d) \prec (a, b)$, então $a \mid c$, $c \mid a$, $b \leq d$ e $d \leq b$. Como $|$ e $\leq$ são antissimétricas, isso implica que $a = c$ e $b = d$. Logo, $(a, b) = (c, d)$ e, então, $\prec$ é antissimétrica.

Sejam $a, b, c, d, e, f \in \mathbb{N}$ tais que $(a, b) \prec (c, d)$ e $(c, d) \prec (e, f)$. Então $a \mid c$, $c \mid e$, $b \leq d$ e $d \leq f$. Pela transitividade de $|$ e $\leq$, seguem $a \mid e$ e $b \leq f$. Logo, $(a, b) \prec (e, f)$ e $\prec$ é transitiva.

Concluindo, $\prec$ é uma relação de ordem.

2. É preciso provar a seguinte:

$$\forall n \exists a((2n + 1)^3 = 2a + 1).$$

Base de indução: $n = 0$.

$$(2 \cdot 0 + 1)^3 = 1 = 2 \cdot 0 + 1 \quad \text{verificada.}$$

Hipótese de indução: $n = k$.

$$\exists a((2k + 1)^3 = 2a + 1).$$

Tese: $n = k + 1$.

$$\exists a'((2(k + 1) + 1)^3 = 2a' + 1).$$

Vamos calcular $(2(k + 1) + 1)^3$:

$$\begin{aligned}
&(2(k + 1) + 1)^3 = \\
&= (2k + 3)^3 = \\
&= 8k^3 + 36k^2 + 54k + 27 = \\
&= (8k^3 + 12k^2 + 6k + 1) + 24k^2 + 48k + 26 \overset{\text{HP}}{=} \\
&\overset{\text{HP}}{=} 2a + 1 + 2(12k^2 + 24k + 13) = \\
&= 2(a + 12k^2 + 24k + 13) + 1.
\end{aligned}$$

Então a tese vale com $a' = a + 12k^2 + 24k + 13$.

3. Vamos usar o princípio de indução (PA7) na variável x (que, por sinal, é única que podemos usar, pois é a única quantificada universalmente).

Base: $x = 0$.

$0 \overset{PA3}{=} 0 + 0$, então a base de indução é verificada, com $y = 0$.

Hipótese de indução: $x = k$. $\exists y((k = y + y) \vee (k = s(y + y))$.

Tese: $x = s(k)$. $\exists z((s(k) = z + z) \vee (s(k) = s(z + z))$.

Como a hipótese de indução contém uma disjunção, vamos distinguir dois casos: $k = y + y$ e $k = s(y + y)$.

No primeiro caso, $s(k) = s(y + y)$, então a tese é verificada de maneira óbvia. No segundo caso, $s(k) = s(s(y + y)) \overset{PA4}{=} s(y + s(y)) \overset{C}{=} s(s(y) + y) \overset{PA4}{=} s(y) + s(y)$, então a tese vale com $z = s(y)$.

Logo, a tese de indução vale em todo caso, e portanto a asserção segue do axioma PA7.

4. (a) O mdc positivo de 25 e 30 é 5, e $40 = 8 \cdot 5$. Então a equação é solucionável. Temos, também: $25 = 5 \cdot 5$ e $30 = 6 \cdot 5$.

O algoritmo das divisões sucessivas de Euclides retorna $5 = 25 \cdot (-1) + 30 \cdot 1$, o que implica $25 \cdot (-8) + 30 \cdot 8 = 40$. Logo, o conjunto das soluções é

$$\{(-8 + 6k, 8 - 5k) : k \in \mathbb{Z}\}.$$

As equações congruenciais associadas à equação diofantina dada são as seguintes:

$25x \equiv 40 (\mathrm{mod}\, 30)$, cujo conjunto das soluções é

$$\{-8 + 6k : k \in \mathbb{Z}\}, \text{ e}$$

$30y \equiv 40 (\mathrm{mod}\, 25)$, cujo conjunto das soluções é

$$\{8 + 5k : k \in \mathbb{Z}\}.$$

(b) O mdc positivo de 110 e 76 é 2, e $6 = 3 \cdot 2$. Então a equação é solucionável. Temos, também: $110 = 55 \cdot 2$ e $76 = 38 \cdot 2$.

O algoritmo das divisões sucessivas de Euclides retorna $2 = 110 \cdot 9 + 76 \cdot (-13)$, o que implica $6 = 110 \cdot 27 + 76 \cdot (-39)$. Logo, o conjunto das soluções é

$$\{(27 + 38k, -39 - 55k) : k \in \mathbb{Z}\}.$$

As equações congruencias associadas à equação diofantina dada são as seguintes:

$110x \equiv 6 (\mathrm{mod}\, 76)$, cujo conjunto das soluções é

$$\{27 + 38k : k \in \mathbb{Z}\}, \text{ e}$$

$76y \equiv 6 (\mathrm{mod}\, 110)$, cujo conjunto das soluções é

$$\{-39 + 55k : k \in \mathbb{Z}\}.$$