INF152 Estructuras Discretas
Profesores: R. Astudillo – M. Bugueño
Universidad Técnica Federico Santa María
Departamento de Informática – Septiembre 2, 2020.

Nombre: Maximiliano Sepúlveda
Rol: 201973536-5 **Paralelo**: 200

Certamen 1 – Pregunta 2

Esta evaluación tiene como máximo 25 puntos del C1.

a) Sean a, b y c enteros positivos, tales que a divide a b y b divide a c. Demuestre que a divide a c. [**8 pts**]

Respuesta:

Primero, cuando se dice que "un numero a **divide** a otro numero b", se está diciendo que b puede representarse como la multiplicación de algún otro numero k con a; en otras palabras, a es un factor de b. Con lo anterior, se define entonces:

$$\boxed{\forall a, b \in \mathbb{Z}^+ \, (a \mid b \iff \exists k \in \mathbb{Z}^+, \, b = a \cdot k)}$$

"a divide a b, si y solo si, existe un numero k tal que $b = a \cdot k$"

Formalización:

A continuación se definen las siguientes proposiciones para la demostración:

Con $a, b, c \in \mathbb{Z}^+$:

- $p : (a \mid b) \land (b \mid c)$
  "a divide a b, y b divide a c"
- $q : a \mid c$
  "a divide a c"

Demostración:

*Se utilizará demostración directa. $p \implies q$

Supondremos que $p \equiv \mathbf{V}$, y con ello, se va a intentar llegar a q. Por definición, se cumple que:

1) $\forall a, b \in \mathbb{Z}^+ \, (a \mid b \iff \exists k \in \mathbb{Z}^+, \, b = a \cdot k)$
2) $\forall b, c \in \mathbb{Z}^+ \, (b \mid c \iff \exists w \in \mathbb{Z}^+, \, c = b \cdot w)$

Y queremos llegar a:

3) $\forall a, c \in \mathbb{Z}^+ \, (a \mid c \iff \exists g \in \mathbb{Z}^+, \, c = a \cdot g)$

Como se esta considerando **para cualquier numero** en $\mathbb{Z}^+$, se puede hacer una particularización universal y considerar a, b, c números arbitrarios de $\mathbb{Z}^+$.

Por la proposición 1, se tiene entonces que $b = a \cdot k$, y en la proposición 2, se tiene que $c = b \cdot w$. Como en la proposición 2 se encuentra b, se puede reemplazar directamente (ya que lo consideramos como verdadero).

$$\begin{aligned} c &= b \cdot w \\ c &= (a \cdot k) \cdot w \\ c &= a \cdot (k \cdot w) \end{aligned}$$

Tenemos en cuenta que también existen los valores de k y w en $\mathbb{Z}^+$, por lo tanto $k \cdot w$ también existe, y también pertenece a $\mathbb{Z}^+$, y se le puede definir una variable nueva.

$$c = a \cdot (k \cdot w)$$

$$\boxed{c = a \cdot g, \qquad g = k \cdot w}$$

Conclusión:

Acabamos de encontrar el valor de g para que la tesis se cumpla. **Si existe** g tal que $c = a \cdot g$. Y además, como son números arbitrarios en $\mathbb{Z}^+$, se puede generalizar para cualquier numero en $\mathbb{Z}^+$.

$$\boxed{\forall a, c \in \mathbb{Z}^+ \, (a \mid c \iff \exists g \in \mathbb{Z}^+, \, c = a \cdot g)}$$

$\therefore$ Si a divide a b, y b divide a c, **es verdad** que a también va a dividir a c. $\blacksquare$

b) Demuestre formalmente lo siguiente: **[8 pts]**

$$(a\,[a\,[k]] = a\,[b\,[j]]) \rightarrow \exists x \exists y (x = a\,[k] \wedge (y = b\,[j]) \wedge (a\,[x] = a\,[y])))$$

Respuesta:

Formalización:

Se consideran las siguientes proposiciones para la demostración: $p \implies q$

- $p : a\Big[a[k]\Big] = a\Big[b[j]\Big]$
- $q : \exists x \exists y \Big((x = a\,[k]) \wedge (y = b\,[j]) \wedge (a\,[x] = a\,[y])\Big)$

Demostración:

Si consideramos que $a[k]$ y $b[j]$ son elementos específicos de algún conjunto. A la proposición p se le puede aplicar una generalización existencial:

$$\frac{a\Big[a[k]\Big] = a\Big[b[j]\Big]}{\exists x, y\,(a[x] = a[y])}$$

Los elementos que existen para x e y, son precisamente $a[k]$ y $b[j]$ respectivamente.

$$\boxed{\exists x\,(x = a[k]) \wedge \exists y\,(y = b[j]) \wedge (a[x] = a[y])}$$

Conclusión:

La proposición muestra básicamente como una generalización existencial puede expresar los argumentos de $a[x]$ en general, con otras variables.

$\therefore$ Por formalizacion, la expresion $a\Big[a[k]\Big] = a\Big[b[j]\Big]$ tambien se puede expresar como:

$$\boxed{\exists x \exists y \Big((x = a\,[k]) \wedge (y = b\,[j]) \wedge (a\,[x] = a\,[y])\Big)} \blacksquare$$

c) Demuestre que si n no es un entero divisible por 3, $n^2 - 1$ sí lo es. **[9 pts]**

Respuesta:

Formalización:

Se definen las siguientes proposiciones para la demostración $p \implies q$:

Con $n \in \mathbb{Z}$:

- $p : n$ no es divisible por 3.
- $q : n^2 - 1$ si es divisible por 3.

Demostración:

*Se utilizará demostración por contradicción. $(p \wedge \neg q) \implies \mathbf{F}$

Supongamos que $p \equiv \mathbf{V}$ y $\neg q \equiv \mathbf{V}$. Es decir, asumir verdad que:

1) $p : n$ no es divisible por 3.
2) $\neg q : n^2 - 1$ **no** es divisible por 3.

De la proposición 1, se sabe que n no es divisible por 3, es decir, que 3 no divide a n:

$$\boxed{\forall n \in \mathbb{Z} \left((3 \nmid n) \iff (\nexists k \in \mathbb{Z},\, n = 3 \cdot k)\right)}$$

De la proposición 2, de la misma forma, dice que 3 no divide a $n^2 - 1$:

$$\boxed{\forall n \in \mathbb{Z} \left((3 \nmid (n^2 - 1)) \iff (\nexists m \in \mathbb{Z},\, n^2 - 1 = 3 \cdot m)\right)}$$

Como se considera un $n \in \mathbb{Z}$ arbitrario, se puede utilizar una particularización universal. Por ejemplo, de la proposición 1, se puede asumir $\boxed{n = 2}$.

Es valido, ya que no existe ningún numero $k \in \mathbb{Z}$ tal que al multiplicarlo por 3, me dé 2.

Pero si ahora evaluamos la proposición 2:

$$\begin{aligned} n^2 - 1 &= 3 \cdot m \\ (2)^2 - 1 &= 3 \cdot m \\ 4 - 1 &= 3 \cdot m \\ 3 &= 3 \cdot m \end{aligned}$$

$$\boxed{1 = m \quad \rightarrow\!\!\times\!\!\leftarrow \quad \nexists m \in \mathbb{Z}}$$

Conclusión:

Habíamos supuesto que $\neg q$ era verdad. Es decir, que **no existe** un numero m tal que $n^2 - 1 = 3 \cdot m$, pero por la proposición 1 dijimos que $n = 2$, al final, al unirlo con la proposición 2, nos dio una **contradicción**.

Es decir, nuestro supuesto inicial acerca de $\neg q$ estaba errónea, es decir que $\neg q \equiv \mathbf{F}$, por lo tanto $q \equiv \mathbf{V}$.

Como se consideraba un $n \in \mathbb{Z}$ arbitrario, esto se puede generalizar para todo n.

$\therefore$ Por contradicción, si n no es divisible por 3, entonces $n^2 - 1$ si sera divisible por 3. $\blacksquare$