Universidad San Pablo - CEU

Fundamentos Matemáticos de Ingeniería Biomédica 3

Ejercicios

Profesor:
Rodrigo García Carmona

Curso 2013-2014

Temas 1 y 2: Lógica y Demostraciones

Ejercicio 1

Tenemos el siguiente teorema:

Teorema 1:

$$(\exists a \in A, \forall b \in B, P(a,b)) \implies (\forall b \in B, \exists a \in A, P(a,b))$$

Vamos a darle significado a los diferentes conjuntos y elementos del teorema:

$$A = \{ \text{ estudiantes de FM3 } \}$$
$$B = \{ \text{ clases de FM3 } \}$$
$$P(a,b) = \text{"estudiante } a \text{ se duerme durante la clase } b\text{"}$$

El siguiente teorema es similar al anterior:

Teorema 2:

$$(\forall b \in B, \exists a \in A, P(a,b)) \implies (\exists a \in A, \forall b \in B, P(a,b))$$

Preguntas:

1. ¿Cómo se podría escribir en lenguaje natural el lado a la izquierda de la implicación del teorema 1?
2. ¿Cómo se podría escribir en lenguaje natural el lado a la derecha de la implicación del teorema 1?
3. Averigüe si el teorema 1 es cierto o no, y demuéstrelo.
4. Averigüe si el teorema 2 es cierto o no, y demuéstrelo.

Solución

1. Existe un estudiante que se duerme en todas las clases de FM3.
2. En todas las clases de FM3 se duerme algún estudiante.
3. Es cierto. Consideramos dos casos posibles. Por agotamiento:
   - **Caso 1:** Supongamos que el lado izquierdo de la implicación es falso. En este caso el predicado es cierto por definición de implicación.
   - **Caso 2:** Supongamos que el lado izquierdo de la implicación es cierto. En este caso existe un elemento $a_0 \in A$ tal que $P(a_0, b)$ es cierto para todo $b \in B$. Por tanto, para todo $b \in B$ existe un $a \in A$ (que hemos llamado a_0) tal que $P(a_0, b)$ es cierto. Por tanto, el lado derecho de la implicación también es cierto.

   Como se dan ambos casos, el lado izquierdo implica el lado derecho, así que el teorema es cierto. □

4. Es falso. Encontramos un contraejemplo. Según el lado izquierdo de la implicación, pueden $\exists a_0, a_1 \in A$ y $\exists b_0, b_1 \in B$, tal que $a_0 \neq a1$ y $b_0 \neq b1$, y para los que $P(a_0, b_0)$ y $P(a_1, b_1)$ sean ciertos, pero que hagan $P(a_0, b_1)$ y $P(a_1, b_y)$ falsos. Por tanto, en este caso no existiría un $a_x \in A$ que hiciera $P(a_x, b)$ cierto para todo $b \in B$.

Ejercicio 2

Una pequeña sociedad secreta dentro de la EPS tiene aviesas intenciones: hacer que el examen final de FM3 sea *obscenamente difícil*, con enunciados del estilo *"Demuestre que un conjunto de axiomas no puede ser a la vez consistente y completo."* o *"Demuestre el último teorema de Fermat."* La única forma de acabar con sus malvados planes es determinar con exactitud quién forma parte de dicha sociedad secreta. Tras intensas investigaciones se ha conseguido reducir el grupo de profesores de la EPS sospechosos a tan solo nueve personas:

$$\{Abraham, Ana, Carlos, Gabriel, Gianluca, Teo, Mariano, Rodrigo, Victor\}$$

La sociedad secreta es un subconjunto de estos nueve. Se ha encontrado una lista con los participantes en el complot, pero está cifrada utilizando notación lógica, para evitar que los descubran (pues saben que los alumnos de FM3 no podran resolver un problema así). El predicado *miembro* indica quién forma parte de la sociedad. Esto es: $miembro(x)$ es cierto si y sólo si x es miembro de la sociedad.

Los contenidos de la lista se encuentran a continuación. Traduzca a lenguaje natural cada uno de los predicados siguientes y deduzca quién forma parte de la sociedad secreta.

1. $\exists x, \exists y, \exists z, (x \neq y \wedge x \neq z \wedge y \neq z \wedge miembro(x) \wedge miembro(y) \wedge miembro(z))$
2. $\neg(miembro(Ana) \wedge miembro(Gianluca))$
3. $(miembro(Mariano) \vee miembro(Gabriel)) \implies \forall x, miembro(x)$
4. $miembro(Ana) \implies miembro(Gianluca)$
5. $miembro(Carlos) \implies miembro(Mariano)$
6. $(miembro(Abraham) \vee miembro(Teo)) \implies \neg miembro(Victor)$
7. $(miembro(Abraham) \vee miembro(Gianluca)) \implies \neg miembro(Rodrigo)$

Solución

1. $\exists x, \exists y, \exists z, (x \neq y \wedge x \neq z \wedge y \neq z \wedge miembro(x) \wedge miembro(y) \wedge miembro(z))$
   Esto se puede traducir por: "Existe un conjunto de 3 personas, a las que llamaremos x, y y z, diferentes entre sí, que pertenecen a la sociedad secreta." Otra forma más natural de decir esto seria omintir el nombrado de las personas: "Existen 3 personas que pertenecen a la sociedad secreta." O, de forma aún más simple: "La sociedad secreta cuenta con, al menos, 3 personas."

2. $\neg(miembro(Ana) \wedge miembro(Gianluca))$
   "Es imposible que tanto Ana como Gianluca formen parte de la sociedad" O, dicho de otra forma: "O Ana o Gianluca no forman parte de la sociedad."

3. $(miembro(Mariano) \vee miembro(Gabriel)) \implies \forall x, miembro(x)$
   "Si Mariano o Gabriel forman parte de la sociedad, entonces todo el mundo forma parte de la sociedad."

4. $miembro(Ana) \implies miembro(Gianluca)$
   "Si Ana forma parte de la sociedad, entonces Gianluca también."

5. $miembro(Carlos) \implies miembro(Mariano)$
   "Si Carlos forma parte de la sociedad, entonces Mariano también."

6. $(miembro(Abraham) \vee miembro(Teo)) \implies \neg miembro(Victor)$
   "Si Abraham o Mariano forman parte de la sociedad, entonces Víctor no." O, dicho de otra forma: "Si Víctor forma parte de la sociedad, entonces ni Abraham ni Teo forman parte."

7. $(miembro(Abraham) \vee miembro(Gianluca)) \implies \neg miembro(Rodrigo)$
   "Si Abraham o Gianluca forman parte de la sociedad, entonces Rodrigo no." O, dicho de otra forma: "Si Rodrigor forma parte de la sociedad, entonces ni Abraham ni Gianluca forman parte."

Y ahora que ya tenemos las traducciones, vamos a argumentar por qué la sociedad secreta sélo puede estar compuesta por exactamente tres miembros: Abraham, Gianluca y Teo.

Fijándonos en (2) podemos deducir que existe al menos una persona, ya sea Ana o Gianluca, que no forma parte de la sociedad secreta. Pero también sabemos, por (3), que si Mariano o Gabriel formaran parte de la sociedad, entonces todo el mundo lo haría. Por lo que, por contradicción, concluimos que:

Mariano y Gabriel no forman parte de la sociedad secreta.

Ahora consideremos que (5) implica su contrapositivo: Si Mariano no forma parte de la sociedad, entonces tampoco Carlos forma parte. Por tanto, como Mariano no forma parte de la sociedad secreta:

Carlos no forma parte de la sociedad secreta.

Después nos fijamos en (4). Vemos que si Ana formara paerte de la sociedad, entonces Gianluca también, lo cual llevaría la contraria a (2). Así que, por contradicción, concluimos que:

Ana no forma parte de la sociedad secreta.

Ahora, supongamos que Víctor forma parte de la sociedad. Entonces, según (6), ni Abraham ni Teo formarían parte. Ya sabemos que Mariano, Gabriel, Carlos y Ana no forman parte de la sociedad secreta, por lo que, si suponemos que Víctor forma parte de la sociedad entonces solo habría tres personas que podrían pertenecer a ella: Víctor, Rodrigo y Gianluca. Como indica (1), la sociedad secreta tiene que estar compuesta por al menos 3 miembros, por lo que la sociedad tendría que estar formada por exactamente estos tres. Esto demuestra:

Lema 1: *Si Víctor forma parte de la sociedad, entonces Rodrigo y Gianluca también son miembros.*

Pero observando (7), vemos que si Gianluca forma parte de la sociedad, entonces Rodrigo no puede hacerlo, por lo que:

Lema 2: *Es imposible que tanto Gianluca como Rodrigo formen parte de la sociedad.*

Por tanto, a partir del Lema 2 concluimos que el Lema 1 es falso. Por lo que, por el contrapositivo, demostramos que la hipótesis del Lema 1 es falsa. Es decir, que:

Víctor no forma parte de la sociedad secreta.

Por último, supongamos que Rodrigo forma parte de la sociedad. Entonces, por (7), ni Abraham ni Gianluca formarían parte, y ya sabemos que Mariano, Gabriel, Carlos, Ana y Víctor no forman parte tampoco. Por tanto, en esta suposición la sociedad estaría compuesta de, como mucho, dos personas (Rodrigo y Teo). Esto contradice a (1), asi que concluimos que:

Rodrigo no forma parte de la sociedad secreta.

Es decir, que las únicas personas que podrían forman parte de la sociedad son Abraham, Gianluca y Teo. Como la sociedad tiene q ue contar con al menos 3 miembros, podemos concluir que:

Lema 3:*No hay ninguna sociedad secreta posible excepto la compuesta por Abraham, Gianluca y Teo.*

Pero aún no hemos terminado. Nos queda demostrar que la sociedad secreta compuesta por Abraham, Gianluca y Teo satisface las 7 condiciones que hemos expuesto. Así que definamos el conjunto $A = \{Abraham, Gianluca, Teo\}$ y demostremos la siguiente proposición:

Proposición: $\{Abraham, Gianluca, Teo\}$ *es la* ***única*** *sociedad secreta que satisface las condiciones (1)-(7).*

- $|A| = 3$ (Cardinalidad de A es 3), por lo que A satisface (1).
- $Ana \notin A$, por lo que A satisface (2) y (4).
- $Mariano, Gabriel \notin A$, por lo que la hipótesis de (3) es falsa, así que A satisface (3).
- $Carlos \notin A$, por lo que A satisface (5).
- Por último, $Victor, Rodrigo \notin A$, asi que las conclusiones tanto de (6) como de (7) son ciertas, por lo que A satisface (6) y (7).

Por tanto, $\{Abraham, Gianluca, Teo\}$ satisface las condiciones (1)-(7). Antes (Lema 3) hemos demostrado que esta sociedad secreta es la única que lo hace. □

Ejercicio 3

Traduzca las siguientes frases del español a lenguaje de lógica de predicados. El dominio sobre el que se trabaja es X, el conjunto de todas las personasl. Puede utilizar las siguientes funciones:

- $F(x)$: indica que x ha sido estudiante de FM3.
- $S(x)$: indica que x ha sacado sobresaliente en FM3.
- $J(x)$: indica que x le ha regalado un jamón a Rodrigo.
- $E(x, y)$: indica que x e y son la misma persona.

Las frases a traducir son las que siguen:

1. Hay gente que ha sido estudiante de FM3 y ha sacado sobresaliente en FM3.
2. Todos los que han cursado FM3 y le han regalado un jamón a Rodrigo han sacado sobresaliente en FM3.
3. No hay nadie que le haya regalado un jamón a Rodrigo y que no haya sacado sobresaliente en FM3.
4. Hay al menos tres personas que le han regalado un jamón a Rodrigo y no han cursado FM3.

Solución

1. $\exists x \in X, (F(x) \wedge S(x)$
2. $\forall x \in X, (F(x) \wedge J(x)) \implies S(x)$
3. $\nexists x \in X, (J(x) \wedge \neg S(x))$
4. $\exists x, y, z \in X, (\neg E(x, y) \wedge \neg E(x, z) \wedge \neg E(y, z))$
   $\wedge (J(x) \wedge \neg F(x)) \wedge (J(y) \wedge \neg F(y)) \wedge (J(z) \wedge \neg F(z))$

Ejercicio 4

Use una tabla de verdad para demostrar si las siguientes proposicones son o no ciertas:

1. $\neg(P \vee (Q \wedge R)) = (\neg P) \wedge (\neg Q \vee \neg R)$
2. $\neg(P \wedge (Q \vee R)) = (\neg P) \vee (\neg Q \wedge \neg R)$

Solución

1. Demostramos que el lado izquierdo:

P	Q	R	$Q \wedge R$	$\neg(P \vee (Q \wedge R))$
T	T	T	T	F
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F
F	T	T	T	F
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

Y el lado derecho coinciden en todas las combinaciones posibles:

$\neg P$	$\neg Q$	$\neg R$	$\neg Q \vee \neg R$	$(\neg P) \wedge (\neg Q \vee \neg R)$
F	F	F	F	F
F	F	T	T	F
F	T	F	T	F
F	T	T	T	F
T	F	F	F	F
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

2. Demostramos que el lado izquierdo:

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$\neg(P \wedge (Q \vee R))$
T	T	T	T	T	F
T	T	F	T	T	F
T	F	T	T	T	F
T	F	F	F	F	T
F	T	T	T	F	T
F	T	F	T	F	T
F	F	T	T	F	T
F	F	F	F	F	T

Y el lado derecho coinciden en todas las combinaciones posibles:

$\neg P$	$\neg Q$	$\neg R$	$\neg Q \wedge \neg R$	$(\neg P) \vee (\neg Q \wedge \neg R)$
F	F	F	F	F
F	F	T	F	F
F	T	F	F	F
F	T	T	T	T
T	F	F	F	T
T	F	T	F	T
T	T	F	F	T
T	T	T	T	T

Ejercicio 5

Los conectores binarios $\wedge$ (*and*), $\vee$ (*or*) y $\implies$ (*implies*) aparecen multitud de veces en expresiones lógicas. Sin embargo, a la hora de diseñar chips y circuitos electronicos, suele ser mucho más económico construir la lógica del sistema utilizando únicamente otra operación: ***nand***, ya que ésta es más sencilla de representar en un circuito. Aquí tienes la tabla de verdad para la operación *nand*:

P	Q	P nand Q
T	T	F
T	F	T
F	T	T
F	F	T

Vamos a trabajar con esta operación lógica. Para cada una de las expresiones que siguen, encuentre una expresión equivalente usando únicamente *nand* y $\neg$ (*not*), así como cualesquiera paréntesis crea necesarios para especificar el orden en el que se aplican las operaciones. Puedes utilizar A, B y los operadores tantas veces como desee:

1. $A \wedge B$
2. $A \vee B$
3. $A \implies B$

Por otra parte, como es posible expresar cualquier expresión lógica usando únicamente *nand* (sin necesidad de usar $\neg$), encuentre una expresión equivalente a $(\neg A)$ utilizando sólo *nand* y, de ser necesario, paréntesis.

Es más, incluso las constantes T y F pueden ser expresadas únicamente recurriendo a *nand*. Construya una expresión gracias a la cual, a partir de una proposición arbitraria A y uno o más *nand*, dé como resultado siempre T, cualesquiera valores tome A. Construya también otra expresión que a partir de A y uno o más *nand*, dé como resultado siempre F, cualesquiera valores tome A.

Solución

Consideramos los tres casos planteados:

1. Este primer caso es automático, pues *nand* es lo opuesto a *and* ($\wedge$). Por tanto:

$$A \wedge B = \neg(A \, nand \, B)$$

2. Para este caso planteamos la tabla de verdad de $A \vee B$ frente a la de $A \, nand \, B$ y buscamos que combinación de entradas (A, B, $\neg A$ y $\neg B$) que la pueden construir:

A	B	$\neg A$	$\neg B$	$A \vee B$	$A \, nand \, B$	$(\neg A) \, nand \, (\neg B)$
T	T	F	F	T	F	T
T	F	F	T	T	T	T
F	T	T	F	T	T	T
F	F	T	T	F	T	F

Así que tenemos que:

$$A \vee B = (\neg A)\ nand\ (\neg B)$$

3. Para este caso, sabemos que podemos expresar la implicación de la siguiente manera:

$$A \implies B = (\neg A) \vee B$$

Y, dado que sabemos cómo expresar una unión ($\vee$) con *nand* por el punto 2, podemos expresar la implicación de la siguiente manera:

$$A \implies B = A\ nand\ (\neg B)$$

Para expresar la negación ($\neg$) planteamos una tabla de verdad únicamente con A y $\neg A$ que nos permita deducir cómo construir esta última a partir de *nand*. Pensemos en que *nand* es F si sus dos entradas son T, por lo que:

A	$\neg A$	$A\ nand\ A$
T	F	F
F	T	T

Asi que concluimos que:

$$\neg A = A\ nand\ A$$

Finalmente, para expresar las constantes T y F, recurrimos de nuevo a una tabla de verdad, esta vez mostrando A y $\neg A$, y buscando qué combinación de entradas a *nand* utilizándolas (pues ya sabemos que podemos expresar $\neg A$ como $A\ nand\ A$) nos da el resultado pedido.

Para T, buscamos que las dos entradadas a *nand* sean siempre distintas, pues eso hace el resultado siempre T:

A	$\neg A$	$(\neg A)\ nand\ A$
T	F	T
F	T	T

Con lo que:

$$T = (\neg A)\ nand\ A$$

Y, sustituyendo $\neg A$:

$$T = (A\ nand\ A)\ nand\ A$$

Para F, sabemos que la única forma de que *nand* de como resultado F es que las dos entradas sean T. Y como sabemos cómo expresar T a partir de *nand*, A y $\neg A$, concluimos que:

$$F = [(\neg A)\ nand\ A]\ nand\ [(\neg A)\ nand\ A]$$

Y, sustituyendo $\neg A$:

$$F = [(A\ nand\ A)\ nand\ A]\ nand\ [(A\ nand\ A)\ nand\ A]$$

Ejercicio 6

Dado un $x \in \mathbb{Z}$, demuestre que si $x^3 + x^2 + x$ es impar $\implies$ x es impar. ¿Qué tipo de demostración ha utilizado?

Solución

Utilizaremos el método del contrapositivo. Demostraremos que:

$$\text{Si } x \text{ es par} \implies x^3 + x^2 + x \text{ es par.}$$

Demostración: Si x es par, entonces $x = 2k$ para algún $k \in \mathbb{Z}$. Por tanto:

$$x^3 + x^2 + x = (2k)^3 + (2k)^2 + 2k = 8k^3 + 4k^2 + 2k = 2(4k^3 + 2k^2 + k)$$

Como $2(4k^3 + 2k^2 + k)$ es par, entonces $x^3 + x^2 + x$ es par. $\square$

Tema 3: Inducción

Ejercicio 1

Considere la siguiente función:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + ... + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

Recurra a la inducción para demostrar que la fórmula es correcta $\forall n \in \mathbb{N}^+$.

Solución

Demostración: Utilizamos inducción. Definimos $P(n)$ como el hecho de que la siguiente ecuación sea cierta $\forall n \in \mathbb{N}^+$:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + ... + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

Caso base: $P(1)$ es cierto porque ambos lados de la ecuación valen 2.

Paso inductivo: Debemos mostrar que $P(n) \implies P(n+1), \forall n \geq 1$. Asumimos que $P(n)$ es cierto, dónde n denota cualquier entero positivo. Buscamos, por tanto, demostrar que $P(n+1)$, que se puede ver a continuación, es cierto:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + ... + (n+1)(n+2) = \frac{(n+1)(n+2)(n+3)}{3}$$

Razonamos de la siguiente manera:

$$\begin{aligned}
&1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + ... + (n+1)(n+2) \\
&= [1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + ... + n(n+1)] + (n+1)(n+2) \\
&= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \\
&= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3} \\
&= \frac{(n+1)(n+2)(n+3)}{3}
\end{aligned}$$

La primera igualdad surge de extraer el lado izquierdo $P(n)$ del lado izquierdo de $P(n+1)$. Después sustituimos el lado izquierdo de $P(n)$ por su lado derecho, y el resto de pasos son simplificaciones que acaban llevando al lado derecho de $P(n+1)$. Esto acaba con la demostración de que $P(n+1)$ es cierto, ya que tenemos como resultado la ecuación que se corresponde a $P(n+1)$. $\square$

Ejercicio 2

Considere la siguiente función, una serie geométrica:

$$1 + r + r^2 + r^3 + ... + r^n = \frac{1 - r^{n+1}}{1 - r}$$

Recurra a la inducción para demostrar que la fórmula es correcta $\forall r \in \mathbb{R}$ con $r \neq 1$.

Solución

Demostración: Utilizamos inducción. Definimos $P(n)$ como el hecho de que la siguiente ecuación sea cierta $\forall r \neq 1$:

$$1 + r + r^2 + r^3 + ... + r^n = \frac{1 - r^{n+1}}{1 - r}$$

Caso base: $P(0)$ es cierto porque ambos lados de la ecuación valen 1.

Paso inductivo: Debemos mostrar que $P(n) \implies P(n+1), \forall n \in \mathbb{N}$. Asumimos que $P(n)$ es cierto, dónde n denota cualquier número natural. Buscamos, por tanto, demostrar que $P(n+1)$, que se puede ver a continuación, es cierto:

$$1 + r + r^2 + r^3 + ... + r^{n+1} = \frac{1 - r^{n+2}}{1 - r}$$

Razonamos de la siguiente manera:

$$\begin{aligned} 1 + r + r^2 + r^3 + ... + r^n + r^{n+1} &= \frac{1 - r^{n+1}}{1 - r} + r^{n+1} \\ &= \frac{1 - r^{n+1} + (1 - r)r^{n+1}}{1 - r} \\ &= \frac{1 - r^{n+2}}{1 - r} \end{aligned}$$

La primera ecuación nace de la asunción de que $P(n)$ es cierto. Sumamos a ambos lados de la ecuación el término r^{n+1}, y el resto de pasos son simplificaciones sobre dicha ecuación. Esto acaba con la demostración de que $P(n+1)$ es cierto, ya que tenemos como resultado la ecuación que se corresponde a $P(n+1)$. □

Ejercicio 3

Use la inducción para demostrar que, para todo entero positivo n, $6^n - 1$ es divisible por 5.

Solución

Demostración: Utilizamos inducción. Definimos $P(n)$ como $(5|6^n - 1)\ \forall n \in \mathbb{N}, n \geq 1$.

Caso base: $P(1)$:

$$6^1 - 1 = 6 - 1 = 5$$

Paso inductivo: Debemos mostrar que $P(n) \implies P(n+1), \forall n \geq 1$. Asumimos que $P(n)$ es cierto. Buscamos, por tanto, demostrar que $P(n+1)$, que se puede ver a continuación, es cierto:

$$(5|6^{n+1} - 1)$$

Razonamos de la siguiente manera:

$$\begin{aligned} 6^{n+1} - 1 &= 6(6^n) - 1 \\ &= 6(6^n - 1) - 1 + 6 \\ &= 6(6^n - 1) + 5 \end{aligned}$$

Por $P(n)$ sabemos que $6(6^k - 1)$ es divisible por 5, por lo que al sumarle 5 sigue siéndolo. Por tanto, $P(n+1)$ es cierto. □

Ejercicio 4

Como parte de un nuevo *reality show*, un grupo de concursantes son abandonados en una isla remota. Los concursantes han estado de acuerdo en, antes de que empiece la emisión del programa, tatuarse en medio de la frente un pequeño dibujo en forma de ojo, de color rojo o morado. Ninguno de los concursantes sabe el color de su tercer ojo, ni cuántos ojos morados y rojos hay en total. En la isla no hay ningún espejo, y se prohíbe a los concursantes hablar sobre los tatuajes. Por tanto, todo el mundo sabe el color del tatuaje de todos los demás, pero no del suyo propio.

El primer día del concurso, para sorpresa de los ilusionados concursantes, el presentador se presenta ante ellos y les dice, con voz grave y misteriosa:

Contáis con provisiones para sobrevivir tantos días como personas sois.
No recibiréis más.
Al menos uno de vosotros posee un ojo púrpura.
Debéis obedecer las siguientes reglas:
1.- Los tatuados con un ojo púrpura sólo podrán abandonar la isla cuando puedan demostrar que ése es el color de su ojo.
2.- Los tatuados con un ojo rojo abandonarán la isla automáticamente cuando no quede nadie con un ojo púrpura.

El presentador, y la maligna cadena televisiva que le produce, esperan que, tras esta ominosa revelación, la convivencia entre los concursantes se vuelva imposible. Las tensiones internas deberían crear multitud de dramas personales y, en consecuencia, disparar los índices de audiencia.

Sin embargo, los creadores del programa no contaban con que todos los concursantes han cursado FM3 y son, por consiguiente, unos maestros en el uso de la lógica. Así que lo que al final sucede es que los concursantes pasan los días en alegre convivencia, hasta que un día (antes de que se acaben las provisiones), todos los que poseen un ojo púrpura demuestran esta circunstancia y abandonan la isla a la vez, terminando con el concurso.

Podemos representar esta situación con el siguiente teorema:

Teorema: Todos los concursantes con un ojo púrpura tatuado abandonan la isla el día p, dónde p es el número de concursantes con un ojo púrpura. $p \geq 1$

Demuestre, utilizando la inducción, que este teorema es cierto, al igual que hicieron los concursantes para salvar su vida. Como pista, sugerimos una hipótesis $P(n)$ que verifique que todos los siguientes casos son ciertos para el día n:

1. Si $p > n$, entonces _____
2. Si $p = n$, entonces _____
3. Si $p < n$, entonces _____

Para poder llevar a cabo la demostración deberá rellenar los espacios en blanco.

Solución

Demostración: Utilizamos inducción. Definimos $P(n)$ como:

1. Si $p > n$, entonces ningún concursante con un ojo púrpura abandona aún la isla.
2. Si $p = n$, entonces todos los concursantes con un ojo púrpura abandonan la isla este día.
3. Si $p < n$, entonces ya no queda ningún concursante con un ojo púrpura en la isla.

Caso base: Tenemos que comprobar que las tres partes se dan en $P(1)$:

1. Supongamos $p > 1$: pongámonos en el lugar de un concursante con un ojo púrpura. Como el presentador ha dicho que hay al menos una persona con un ojo púrpura, y yo veo a al menos otro con un ojo púrpura (ya que $p > 1$), entonces yo no tengo por qué tener un ojo púrpura, bien podría tenerlo rojo. Así que no debo abandonar la isla.
2. Supongamos $p = 1$: pongámonos en el lugar de un concursante con un ojo púrpura. Como el presentador ha dicho que hay al menos una persona con un ojo púrpura, y yo no veo a nadie con un ojo púrpura, entonces el único con un ojo púrpura soy yo. Así que debo abandonar la isla.
3. Supongamos $p < 1$: siempre es cierto, ya que nunca se va a dar que $p < 1$ (siempre hay al menos un concursante con un ojo púrpura), y $P \implies Q$ es cierto si $P = F$.

Por tanto, $P(1)$ es cierto.

Paso inductivo: Asumimos que $P(n)$ es cierto. Tenemos, sabiendo esto, que comprobar que las tres partes se dan en $P(n+1)$:

1. Supongamos $p > n+1$: como $p > n$, sabemos que nadie ha abandonado la isla aún (parte 1 de $P(n)$). Pongámonos en el lugar de todos los concursantes con un ojo púrpura. Como ven a al menos otros $n+1$ concursantes con un ojo púrpura, todos concluyen que ellos no tienen por qué tener un ojo púrpura, así que no abandonan la isla.
2. Supongamos $p = n+1$: como $p > n$, sabemos que nadie ha abandonado la isla aún (parte 1 de $P(n)$). Pongámonos en el lugar de todos los concursantes con un ojo púrpura. Como ven a exactamente otros n concursantes con un ojo púrpura, todos concluyen que ellos tienen un ojo púrpura (pues todos los demás concursantes con un ojo púrpura ven a su vez a n concursantes con el ojo púrpura), así que abandonan la isla.

3. Supongamos $p < n + 1$: aquí puede ser que $p = n$, en cuyo caso todos los concursantes con ojo púrpura habrán abandonado ya la isla (parte 2 de $P(n)$), o $p < n$, en cuyo caso no quedará ya ningún concursante con un ojo púrpura (parte 3 de $P(n)$).

Por tanto, hemos demostrado que si $P(n)$ es cierto, se cumple que $P(n) \implies P(n+1)$. $\square$

Si resulta complicado entender el razonamiento lógico que llevan a cabo los concursantes en $P(n)$, sería recomendable intentar traducirlo a $n = 2$, luego $n = 3$, y así sucesivamente, para así comprender el problema.

Por ejemplo, con $n = 2$, durante el segundo día los dos concursantes con un ojo púrpura ven exactamente a otro concursante con un ojo púrpura. En ese momento ambos saben que el total de ojos púrpura es dos, y ambos tienen un ojo púrpura. La explicación es la siguiente, desde el punto de vista de cada concursante con un ojo púrpura:

1. Si hubiera sólo un ojo púrpura, el concursante con un ojo púrpura al que veo habría abandonado la isla ayer, al no ver éste a ninguna otra persona con un ojo púrpura.

2. Si hubiera tres o más ojos púrpuras, vería a dos o más concursantes con un ojo púrpura, pero sólo veo a uno. Luego es imposible.

3. Por tanto, sólo puede haber dos ojos púrpuras, y yo soy uno de ellos.

Ejercicio 5

Use la inducción para demostrar que, para todo entero positivo n:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

Solución

Demostración: Utilizamos inducción. Definimos $P(n)$ como el hecho de que se cumpla la igualdad del enunciado.

Caso base: $P(1)$:

$$\sum_{i=1}^{1} \frac{1}{i(i+1)} = \frac{1}{1 \cdot 2} = \frac{1}{2} = \frac{1}{1+1}$$

Paso inductivo: Debemos mostrar que $P(n) \implies P(n+1), \forall n \geq 1$. Asumimos que $P(n)$ es cierto. Buscamos, por tanto, demostrar que $P(n+1)$, que se puede ver a continuación, es cierto:

$$\sum_{i=1}^{n+1} \frac{1}{i(i+1)} = \frac{n+1}{n+2}$$

Razonamos de la siguiente manera:

$$\begin{aligned}\sum_{i=1}^{n+1}\frac{1}{i(i+1)} &= \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+...+\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)}\\ &= \frac{n}{n+1}+\frac{1}{(n+1)(n+2)}\\ &= \frac{n(n+2)}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)}\\ &= \frac{n(n+2)+1}{(n+1)(n+2)}\\ &= \frac{n^2+2n+1}{(n+1)(n+2)}\\ &= \frac{(n+1)(n+1)}{(n+1)(n+2)}\\ &= \frac{(n+1)}{(n+2)}\end{aligned}$$

Por tanto, $P(n)$ es cierto para todo $n \geq 1$. □

Ejercicio 6

Use la inducción para demostrar que, para todo entero $n \geq 3$, $n^2 - 7n + 12$ no es negativo.

Solución

Demostración: Utilizamos inducción. Definimos $P(n)$ como $n^2-7n+12 > 0$ para todo entero $n \geq 3$.

Caso base: $P(3)$:

$$n^2 - 7n + 12 = 3^2 - 7\cdot 3 + 12 = 9 - 21 + 12 = 0$$

Paso inductivo: Debemos mostrar que $P(n) \implies P(n+1), \forall n \geq 3$. Asumimos que $P(n)$ es cierto. Buscamos, por tanto, demostrar que $P(n+1)$, que se puede ver a continuación, es cierto:

$$(n+1)^2 - 7(n+1) + 12 > 0$$

Razonamos de la siguiente manera:

$$\begin{aligned}(n+1)^2 - 7(n+1) + 12 &= n^2 + 2n + 1 - 7n - 7 + 12\\ &= (n^2 - 7n + 12) + (2n - 6)\\ &\geq 2n - 6\\ &\geq 2\cdot 3 - 6 \leftarrow \text{Porque } n \geq 3.\\ &= 0\end{aligned}$$

Por tanto, $P(n)$ es cierto para todo $n \geq 3$. □

Ejercicio 7

Use la inducción para demostrar que, para todo entero no negativo n, tal que $n \neq 2$ y $n \neq 3$, se cumple que $n^2 \leq n!$ es cierto.

Solución

Demostración: Antes de nada, tengamos en cuenta lo siguiente:

- Si $n = 0$, entonces $0^2 = 0$ y $0! = 1$.
- Si $n = 1$, entonces $1^2 = 1$ y $1! = 1$.

Ahora utilizamos inducción para el resto de valores posibles de n. Definimos $P(n)$ como el hecho de que $n^2 \leq n!$ es cierto para todo $n \geq 4$.

Caso base: $P(4)$: $4^2 = 16$ y $4! = 24$. Por tanto: $16 < 24$

Paso inductivo: Debemos mostrar que $P(n) \implies P(n+1), \forall n \geq 4$. Asumimos que $P(n)$ es cierto. Buscamos, por tanto, demostrar que $P(n+1)$, que se puede ver a continuación, es cierto:

$$(n+1)^2 \leq (n+1)!$$

Razonamos de la siguiente manera:

$$\begin{aligned}
(n+1)! &= (n+1)n! \\
&\geq (n+1)n^2 \leftarrow \text{Por } P(n). \\
&= n^2 \cdot n + n^2 \\
&\geq 4^2 \cdot n + n^2 \leftarrow \text{Porque } n \geq 4. \\
&= 14n + 2n + n^2 \\
&= 14n + 2n + n^2 + 1 - 1 \\
&= 14n + (n+1)^2 - 1 \\
&\geq (n+1)^2
\end{aligned}$$

Por tanto, $P(n)$ es cierto para todo $n \geq 4$. □

Ejercicio 8

Cuentan las leyendas que, perdido en medio de un valle secreto en el Tíbet, yace un lugar de peregrinación y sabiduría conocido como el Templo de la Eternidad. A él acuden aquellos monjes que buscan obtener la iluminación, para así convertirse en *bodhisattvas*, seres iluminados que sienten una gran compasión por el universo. Pero para alcanzar tal estado no basta con penetrar en el Templo de la Eternidad, sino que también se deben superar las pruebas que se encuentran en su interior.

Cada vez que un monje entra en el Templo de la Eternidad se le entrega un cuenco con 15 cuentas rojas y 12 cuentas verdes. Los monjes deben entonces meditar frente al impresionante Gong del Tiempo y, cada vez que este taña, decidir entre hacer una de las siguientes dos cosas:

- **Intercambiar:** Si un monje tiene al menos 3 cuentas rojas, podrá cambiar 3 cuentas rojas por 2 cuentas verdes.
- **Permutar:** Un monje puede cambiar todas sus cuentas rojas por verdes y todas sus cuentas verdes por rojas. Es decir, que si tiene i cuentas rojas y j cuentas verdes, tras acabar de permutar tendrá j cuentas rojas e i cuentas verdes.

Un monje sólo podrá abandonar el Templo de la Eternidad cuando tenga exactamente 5 cuentas rojas y 5 cuentas verdes en su cuenco. Momento en que, suponemos, habrá alcanzado la iluminación. Represente la situación descrita mediante una máquina de estados, y más concretamente:

1. Indique cómo se pueden representar los estados de dicha máquina de estados.
2. Use la notación que ha desarrollado para representar las transiciones posibles.
3. Dibuje un diagrama que represente los primeros 3 o 4 niveles de esta máquina de estados. No olvide indicar de qué tipo es cada transición.

Pero, ¡oh desgracia! La prueba a la que someten a los monjes en el Templo de la Eternidad no tiene solución, ya que el estado pedido (5 cuentas rojas y 5 verdes) viola un invariante de la máquina de estados presentada. Por tanto, deberá demostrar, utilizando la inducción, que se cumple el siguiente teorema.

Teorema 1: *Nadie abandona jamás el Templo de la Eternidad.*

Para demostrarlo, busque un invariante que se cumpla en el estado inicial y se mantenga tras cada transición, pero que no cumpla el estado que permite a los monjes salir del templo.

Aprovechando que estamos analizando la máquina de estados que representa el Templo de la Eternidad, demuestre también que se cumple el siguiente teorema:

Teorema 2: *El número de estados alcanzable en la máquina de estados del Templo de la Eternidad es finito.*

Para lograrlo, encuentre un invariante que sugiera un límite superior a la cantidad de estados alcanzables y demuestre que se cumple.

Y ahora volvamos nuestra atención de nuevo hacia los monjes. En el interior del Templo de la Eternidad el Gong del Tiempo sigue sonando, una y otra vez. Como cabría imaginar, los monjes empiezan a darse cuenta de que no importa cuántas veces intercambien o permuten sus cuentas, ¡siempre acaban repitiendo algún estado anterior!

Esto no es algo tan terrible como podría parecer, ya que esta súbita revelación hace que unos cuantos monjes alcancen la iluminación, su objetivo inicial cuando entraron en el templo. Sin embargo, para el resto las tribulaciones soportadas aún no son suficientes, y el conocimiento recién adquirido no hace sino minar su voluntad. Simplemente se deprimen. Dándose cuenta de esto, el abad del templo decide presentarse ante ellos y proponerles lo siguiente:

Si algún monje consigue visitar los 108 estados[1] *únicos en los que puede encontrarse su cuenco, entonces podrá abandonar el Templo de la Eternidad.*

¿Tienen los monjes alguna oportunidad de abandonar el Templo de la Eternidad? La respuesta, desafortunadamente, es que no. Demuestre el siguiente teorema, buscando una contradicción:

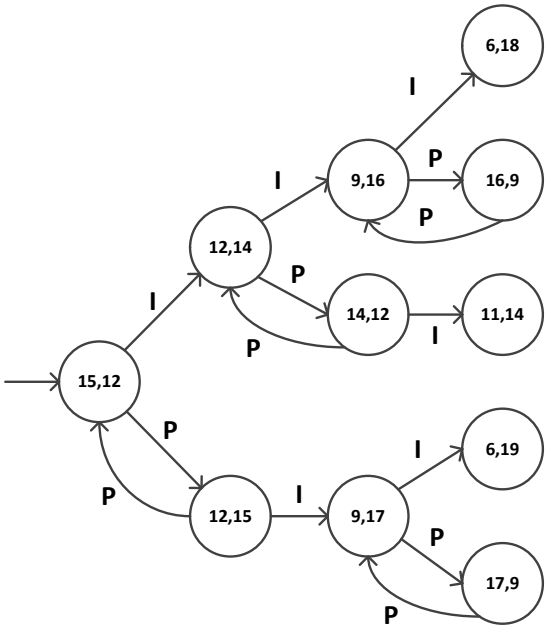
Teorema 3: *No es posible visitar 108 estados distintos en la máquina de estados del Templo de la Eternidad.*

¿Cuál es el máximo número de estados que se pueden alcanzar? ¿Cómo?

Solución

En primer lugar, veamos cómo representar la máquina de estados:

1. Podemos utilizar una variable r para representar el número de cuentas rojas, y una varible v para representar el número de cuentas verdes. Sabiendo esto, podemos representar los estados como parejas (r, v) para $r \geq 0$ y $v \geq 0$.
2. Existen dos tipos de transiciones posibles:
   - *Intercambiar*: $(x, y) \to (x - 3, y + 2), x \geq 3$
   - *Permutar:* $(x, y) \to (y, x)$
3. El diagrama de los primeros 4 niveles puede verse a continuación:



[1] 108 es el número místico que representa la totalidad de la existencia, pues sus dígitos son 1, que representa una cosa; 0, que representa la nada; y 8, que representa la eternidad (el infinito). 108 fueron también las preguntas que hizo Buda, y además 108 = 42 + 24 + 42

La máquina de estados que representa el Templo de la Eternidad modela todas las formas en las que los monjes pueden cambiar sus cuentas respetando las reglas. Ahora queremos saber si dicha máquina puede alcanzar el estado $(5, 5)$. Si es así, decimos que dicho estado es *alcanzable*. Una forma bastante práctica de determinar si un estado es alcanzable o no es identificar los invariantes de la máquina de estados. En este caso el invariante es el siguiente:

En todos los estados alcanzables, el número de cuentas rojas menos el número de cuentas verdes en el cuenco de un monje sigue la fórmula $5k + 2$ *o la fórmula* $5k + 3$ *siendo* k *un entero.*

Este invariante lo hemos encontrado tras una observación cuidadosa del diagrama que se ha mostrado anteriormente. El siguiente paso es demostrar que dicho invariante se cumple para todos los estados alcanzables del sistema, así que recurrimos al método de la inducción.

Proposición: $P(n)$*: Tras* n *transiciones, en el estado* (x, y)*,* $x - y = 5k + 2$ *o* $x - y = 5k + 3$*, siendo* k *un entero.*

Caso base: $P(0)$ es cierto porque para el estado $(15, 12)$, $15 - 12 = 5 \cdot 0 + 3$

Paso inductivo: Asumimos que $P(n)$ es cierto. Analicemos los posible casos para el estado $P(n + 1)$, considerando que (x, y) es el estado para $P(n)$:

- Si $x \geq 3$, entonces el monje puede haber intercambiado 3 cuentas rojas por 2 cuentas verdes. Por tanto, el número de cuentas rojas menos el número de cuentas verdes es el siguiente: $(x - 3) - (y + 2) = (x - y) - 5$. Aquí tenemos dos posibilidades:

  1. Que, por $P(n)$, $x - y = 5k + 2$, en cuyo caso:
     $(x - y) - 5 = 5k + 2 - 5 = 5k - 3 = 5(k - 1) + 2 = 5k' + 2$
  2. Que, por $P(n)$, $x - y = 5k + 3$, en cuyo caso:
     $(x - y) - 5 = 5k + 3 - 5 = 5k - 2 = 5(k - 1) + 3 = 5k' + 3$

- La otra opción es que el monje haya permutado las cuentas rojas por las verdes. Si ha sucedido esto, el nuevo estado es (y, x). Aquí tenemos dos posibilidades:

  1. Que, por $P(n)$, $x - y = 5k + 2$, en cuyo caso:
     $(y - x) = -5k - 2 = 5(-k - 1) + 3 = 5k' + 3$
  2. Que, por $P(n)$, $x - y = 5k + 3$, en cuyo caso:
     $(y - x) = -5k - 3 = 5(-k - 1) + 2 = 5k' + 2$

Por tanto, en todos los casos posibles $P(n+1)$ es cierto. Por lo que $P(n) \implies P(n+1)$. Por inducción, hemos demostrado que el invariante se cumple, y como no se cumple que $0 = 5k + 2$ o que $0 = 5k + 3$, entonces el estado $(5, 5)$ no es alcanzable. Por tanto, nadie abandonará jamás el Templo de la Eternidad. Con ese nombre, deberían haberlo sospechado. □

Ahora es el momento de demostrar el siguiente teorema:

Teorema 2: *El número de estados alcanzable en la máquina de estados del Templo de la Eternidad es finito.*

Para demostrarlo utilizamos el siguiente invariante:

En todos los estados alcanzables, la suma de las cuentas rojas y las cuentas verdes en el cuenco de un monje ($r + v$) es como mucho 27.

Para encontrar este invariante nos hemos limitado a contar el número máximo de cuentas en el diagrama que aparecía antes. Recurrimos a la inducción para demostrar el invariante. $P(n)$ en este caso es que, tras n estados, $r+g \leq 27$.

Caso base: $P(0)$ es cierto porque para el estado $(15, 12)$, $15 + 12 = 27$

Paso inductivo: Asumimos que $P(n)$ es cierto. Analicemos los posible casos para el estado $P(n+1)$, considerando que (x, y) es el estado para $P(n)$. Tenemos dos situaciones posibles:

- Si $x \geq 3$, entonces el monje puede haber intercambiado 3 cuentas rojas por 2 cuentas verdes. Por tanto, el número de cuentas rojas más el número de cuentas verdes es el siguiente: $(x - 3) + (y + 2) = (x + y) - 1$. Como por $P(n)$ sabemos que $x + y \leq 27$, entonces $(x + y) - 1 < 27$.
- La otra opción es que el monje haya permutado las cuentas rojas por las verdes. Si ha sucedido esto, el nuevo estado es (y, x). Por tanto, el número de cuentas rojas más el número de cuentas verdes es el siguiente: $y + x$. Como por $P(n)$ sabemos que $x + y \leq 27$, entonces $y + x \leq 27$.

Por tanto, en todos los casos posibles $P(n+1)$ es cierto. Por lo que $P(n) \implies P(n+1)$. Por inducción, hemos demostrado que el invariante se cumple, asi que nunca se pueden tener en total más de 27 cuentas.

Por fin estamos equipados para demostrar el teorema 2, que hay un límite superior al número de estados alcanzables en la máquina de estados. Lo demostramos por razonamiento directo. Sabemos que el máximo de cuentas es 27, y sólo hay 28 formas de que r y v sumen 27, 27 formas de que r y v sumen 26, y así sucesivamente. Por tanto, como:

$$28 + 27 + 26 + ... + 2 + 1 = \frac{29 \cdot 28}{2} = 406$$

Habrá como mucho 406 estados posibles: una cantidad finita. □

Como 406 es más que 108, los pobres monjes piensan que quizá puedan alcanzar los 108 estados pedidos. Pero no es así.

Teorema 3: *No es posible visitar 108 estados distintos en la máquina de estados del Templo de la Eternidad.*

Demostremos este teorema encontrando una contradicción. Supongamos que es posible visitar 108 estados únicos en una ejecución de la máquina de estados, y consideremos la secuencia de movimientos que sería necesario seguir para ello. Cada movimiento de la secuencia debe ser obligatoriamente un intercambio o una permutación. Al hacer una permutación la suma de cuentas rojas y verdes no cambia. Al hacer un intercambio la suma de cuentas rojas y verdes se reduce en 1:

$$(r - 3) + (v + 2) = (r + v) - 1$$

También sabemos que $r + v$ tiene que ser al menos 3 para poder hacer un intercambio. Con todo esto concluimos que, como mucho, podemos hacer 25 intercambios $(27 - 2)$. Por contra, a partir de cada estado podemos hacer infinitas permutaciones, pero esto no es realmente cierto, ya que de ellas sólo una (la primera para cada estado) nos llevará a un estado no visitado. Es decir, que si en el estado k hacemos dos permutaciones consecutivas, el nuevo estado $k + 2$ será el mismo que k.

Por tanto, el límite superior de estados alcanzables es $1 + 25 + 25 + 1 = 52$ (el estado inicial, 25 intercambios, 25 permutaciones, y el estado final). Como $52 < 108$, no es posible visitar 108 estados, así que ningún monje abandonará jamás el Templo de la Eternidad. □

Para alcanzar estos 52 estados un monje debe empezar haciendo una permutación para alcanzar el estado $(12, 15)$, luego hacer otra permutación para volver al estado inicial, y después seguir con una serie de 25 parejas intercambio/permutación hasta llegar a $(0, 2)$, momento en el que hacer una última permutación para llegar hasta $(2, 0)$.

Ejercicio 9

Probablemente uno de los tipos de robots más populares ahora mismo en el mercado sean los robots-aspiradora. Su cometido es, como se puede deducir a partir del nombre, aspirar el polvo del suelo de una casa. Para este problema consideraremos uno de los primeros prototipos de este robot, para el cual se han programado una serie de movimientos que deberían permitirle cubrir todo el suelo de una habitación.

Desde el punto de vista del robot, la habitación es una rejilla bidimensional, siendo la posición inicial del robot $(0, 0)$, dónde el primer valor representa la coordenada x y el segundo la y. A partir de esta posición inicial, el robot puede moverse en cualquiera de las cuatro diagonales. Es decir, que puede aumentar o reducir su x en 1 y aumentar o reducir su y en 1. Es decir, que el robot no puede moverse simplemente a la derecha, izquierda, arriba o abajo, sino que tendrá que hacerlo en diagonal.

Demuestre, utilizando inducción, que éste es un mal programa para el robot, pues nunca podrá alcanzar la posición $(1, 0)$.

Solución

Representaremos el robot del problema como una máquina de estados con dos valores x, e y, que representan su posición en un momento dado. A partir de esta máquina de estados buscamos un invariante que todos los estados posibles cumplan pero que no sea posible en el estado $(1, 0)$. Para ello tenemos en cuenta algunos de los estados posibles: $(0, 0)$, $(1, 1)$, $(2, 2)$, $(1, 3)$, $(0, 2)$...

Vemos que, en todos ellos, la suma $x + y$ siempre es un número par, así que plantemos el siguiente invariante:

Teorema: *La suma de la coordenada x y la coordenada y del robot en un estado cualquiera siempre es par.*

En efecto, el estado $(1, 0)$ no cumple con esta condición, por lo que si podemos demostrar el invariante habremos resuelto el problema. Demostramos usando inducción.

Proposición: $P(n)$*: Tras* n *transiciones, en el estado* (x, y)*,* $x + y$ *es par.*

Caso base: $P(0)$ es cierto porque para el estado $(0, 0)$, $0 + 0 = 0$, que es par.
Paso inductivo: Asumimos que $P(n)$ es cierto. Analicemos los posible casos para el estado $P(n + 1)$, considerando que (x, y) es el estado para $P(n)$:

- Si el robot se mueve a $(x + 1, y + 1)$, la nueva suma de coordenadas es $x + y + 2$, que es par, ya que $x + y$ es par.
- Si el robot se mueve a $(x + 1, y - 1)$, la nueva suma de coordenadas es $x + y$, que ya sabemos que es par.
- Si el robot se mueve a $(x - 1, y + 1)$, la nueva suma de coordenadas es $x + y$, que ya sabemos que es par.
- Si el robot se mueve a $(x - 1, y - 1)$, la nueva suma de coordenadas es $x + y - 2$, que es par, ya que $x + y$ es par.

Por tanto, en todos los casos posibles $P(n+1)$ es cierto. Por lo que $P(n) \implies P(n+1)$. Por inducción, hemos demostrado que el invariante se cumple, y como no se cumple que el estado $(1, 0)$ no es alcanzable. □

Tema 4: Teoría de números

Ejercicio 1

Encuentre el $mcd(10933, 832)$.

Solución

$$\begin{aligned} mcd(10933, 832) &= mcd(832, res(10933, 832)) \\ 10933 &= 832 \cdot 13 + 117 \rightarrow mcd(832, 117) \\ mcd(832, 117) &= mcd(117, res(832, 117)) \\ 832 &= 117 \cdot 7 + 13 \rightarrow mcd(117, 13) \\ mcd(117, 13) &= mcd(13, res(117, 13)) \\ 117 &= 13 \cdot 9 + 0 \rightarrow mcd(13, 0) \\ mcd(13, 0) &= 13 \end{aligned}$$

Por tanto: $mcd(10933, 832) = 13$

Ejercicio 2

Considere la siguiente ecuación:

$$13x = 60y + 1.$$

Utilizando el algoritmo del Pulverizador, encuentre la pareja de valores x e y solución de la ecuación con la x positiva más pequeña posible. La variable y puede ser negativa. Tanto x como y deben ser enteros.

Solución

Podemos escribir $13x = 60y + 1$ como $13x - 60y = 1$, dándonos así cuenta de que x e y son una combinación lineal de 1. Planteamos el Pulverizador con $a = 13$ y $b = 60$:

a	b	res	$= a - q \cdot y$
60	13	8	$= 60 - 4 \cdot 13$
13	8	5	$= 13 - 1 \cdot 8 = 13 - 60 + 4 \cdot 13 = -60 + 5 \cdot 13$
8	5	3	$= 8 - 1 \cdot 5 = 60 - 4 \cdot 13 - 5 \cdot 13 + 60 = 2 \cdot 60 - 9 \cdot 13$
5	3	2	$= 5 - 1 \cdot 3 = 5 \cdot 13 - 60 - 2 \cdot 60 + 9 \cdot 13 = -3 \cdot 60 + 14 \cdot 13$
3	2	1	$= 3 - 1 \cdot 2 = 2 \cdot 60 - 9 \cdot 13 + 3 \cdot 60 - 14 \cdot 13 = 5 \cdot 60 - 23 \cdot 13$

Por tanto, tenemos que $x = -23$ e $y = 5$. Como queremos que $x \geq 1$, hacemos la siguiente operación:

$$1 = -23 \cdot 13 + 5 \cdot 60 = -23 \cdot 13 + 5 \cdot 60 + 60 \cdot 13 - 13 \cdot 60 = 37 \cdot 13 - 8 \cdot 60$$

Asi que la pareja buscada es $x = 37$ e $y = -8$.

Ejercicio 3

Calcule el residuo de $12^{43} \pmod{713}$.

Solución

En primer lugar, descomponemos el exponente (43) en potencias de dos:

$$43 = 2^5 + 2^3 + 2^1 + 2^0 = 32 + 8 + 2 + 1$$

Por tanto:

$$12^{43} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12$$

Recurriendo a ellas, calculamos por fin el residuo de $12^{43} \pmod{713}$.

$$\begin{aligned}
12^2 &= 12^2 = 144 && \pmod{713} \\
12^4 &= (12^2)^2 = 144^2 = 20736 \equiv 59 && \pmod{713} \\
12^8 &= (12^4)^2 \equiv 59^2 = 3481 \equiv 629 && \pmod{713} \\
12^{16} &= (12^8)^2 \equiv 629^2 = 395641 \equiv 639 && \pmod{713} \\
12^{32} &= (12^{16})^2 \equiv 639^2 = 408321 \equiv 485 && \pmod{713} \\
12^{43} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12 &\equiv 485 \cdot 629 \cdot 144 \cdot 12 = 527152320 \equiv 48 && \pmod{713}
\end{aligned}$$

Por tanto: $12^{43} \equiv 48 \pmod{713}$

Ejercicio 4

Recurriendo a la aritmética modular, demuestre que $100|(11^{10} - 1)$.

Solución

Operamos utilizando aritmética modular con módulo 100. Podemos resolver el problema de varias formas. Podemos, por ejemplo, calcular el residuo de $11^{10} \pmod{100}$ de forma directa:

$$\begin{aligned}
11^2 &= 11 \cdot 11 = 121 \equiv 21 && \pmod{100} \\
11^3 &= 11^2 \cdot 11 \equiv 21 \cdot 11 = 231 \equiv 31 && \pmod{100} \\
11^4 &= 11^3 \cdot 11 \equiv 31 \cdot 11 = 341 \equiv 41 && \pmod{100} \\
11^5 &= 11^4 \cdot 11 \equiv 41 \cdot 11 = 451 \equiv 51 && \pmod{100} \\
11^6 &= 11^5 \cdot 11 \equiv 51 \cdot 11 = 561 \equiv 61 && \pmod{100} \\
11^7 &= 11^6 \cdot 11 \equiv 61 \cdot 11 = 671 \equiv 71 && \pmod{100} \\
11^8 &= 11^7 \cdot 11 \equiv 71 \cdot 11 = 781 \equiv 81 && \pmod{100} \\
11^9 &= 11^8 \cdot 11 \equiv 81 \cdot 11 = 891 \equiv 91 && \pmod{100} \\
11^{10} &= 11^9 \cdot 11 \equiv 91 \cdot 11 = 1001 \equiv 1 && \pmod{100}
\end{aligned}$$

También podemos recurrir a las potencias de 2. Pues sabemos que $10 = 8+4$ y, por tanto: $11^{10} = 11^8 \cdot 11^2$. Sabiendo esto, podemos calcular el residuo de 11^{10} (mód 100) de la siguiente forma:

$$\begin{aligned} 11^2 = 11 \cdot 11 = 121 \equiv 21 \pmod{100} \\ 11^4 = (11^2)^2 \equiv 21^2 = 441 \equiv 41 \pmod{100} \\ 11^8 = (11^4)^2 \equiv 41^2 = 1681 \equiv 81 \pmod{100} \\ 11^{10} = 11^8 \cdot 11^2 \equiv 81 \cdot 21 = 1701 \equiv 1 \pmod{100} \end{aligned}$$

Para ambos casos, como $11^{10} \equiv 1 \pmod{100}$, entonces $(11^{10} - 1) \equiv 0 \pmod{100}$. Es decir, que $100|(11^{10} - 1)$. □

Ejercicio 5

Recurriendo a la aritmética modular, demuestre que $7|(2222^{5555} + 5555^{2222})$.

Solución

Operamos utilizando aritmética modular con módulo 7. En primer lugar, simplificamos las bases de las potencias a su residuo módulo 7:

$$\begin{aligned} 2222 \equiv 3 \pmod{7} \\ 5555 \equiv 4 \pmod{7} \\ 2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod{7} \end{aligned}$$

Por el pequeño teorema de Fermat sabemos que, dado un primo p y un k que no sea múltiplo de p, se cumple que $k^{p-1} \equiv 1 \pmod{p}$. Por tanto, y dado que 7 es un número primo y $k_1 = 3$ y $k_2 = 4$ no son múltiplos de p, entonces se cumple que:

$$\begin{aligned} 3^6 \equiv 1 \pmod{7} \\ 4^6 \equiv 1 \pmod{7} \end{aligned}$$

Y como:

$$\begin{aligned} 5555 = 925 \cdot 6 + 5 \\ 2222 = 370 \cdot 6 + 2 \end{aligned}$$

Tenemos que:

$$\begin{aligned} 3^{5555} + 4^{2222} \equiv (3^6)^{925} \cdot 3^5 + (4^6)^{370} \cdot 4^2 \pmod{7} \\ (3^6)^{925} \cdot 3^5 + (4^6)^{370} \cdot 4^2 \equiv 3^5 + 4^2 \pmod{7} \\ 3^5 + 4^2 \equiv 243 + 16 \equiv 5 + 2 = 7 \equiv 0 \pmod{7} \end{aligned}$$

Como $3^{5555} + 4^{2222} \equiv 0 \pmod{7}$, eso implica que $7|(2222^{5555} + 5555^{2222})$. □

Ejercicio 6

Demuestre que $7^{11}|(3^{6\cdot 7^{10}}-1)$.

Solución

Pensamos en el teorema de Euler, que dice que, dados unos k y n primos relativos: $k^{\phi(n)} \equiv 1 \pmod{n}$. Esto mismo, escrito de otra forma:

$$n|(k^{\phi(n)}-1)$$

Nos fijamos en que el divisor es 7^{11}, y aplicamos sobre él la función indicatriz de Euler:

$$\phi(7^{11}) = 7^{11}(1-\frac{1}{7}) = 6\cdot 7^{10}$$

Por tanto:

$$3^{6\cdot 7^{10}} = 3^{\phi(7^{11})}$$

Así que comprobamos que $n = 7^{11}$ y $k = 3$ son primos relativos:

$$mcd(7,3) = 1$$
$$mcd(7^{11},3) = 1$$

Por tanto, hemos demostrado que podemos aplicar el teorema de Euler sobre $n =$ y $k = 3$, por lo que:

$$3^{\phi(7^{11})} \equiv 1 \pmod{7^{11}}$$
$$7^{11}|(3^{\phi(7^{11})}-1)$$
$$7^{11}|(3^{6\cdot 7^{10}}-1)\ \square$$

Ejercicio 7

Tenemos una hoja de papel, y se nos permite cortarla en 7 trozos distintos. Podemos repetir este proceso tantas veces deseemos. Es decir, podemos cortar uno de los 7 trozos obtenidos en otros 7, y así sucesivamente. Demuestre, utilizando artimética modular, que no se pueden lograr dividir la hoja en 1997 trozos mediante este proceso.

Solución

Cada vez que cortamos un trozo de papel en 7 estamos añadiendo 6 al total de trozos. Por tanto, todos los posibles números de trozos que puedo conseguir son congruentes entre sí módulo 6. Por ejemplo:

$$\begin{aligned} 7 &\equiv 1 \pmod 6 \\ 13 \equiv 7 &\equiv 1 \pmod 6 \\ 19 \equiv 13 \equiv 715 \equiv 7 &\equiv 1 \pmod 6 \\ &\vdots \end{aligned}$$

Buscamos el residuo de 1997 (los trozos pedidos) módulo 6:

$$1997 \equiv 5 \pmod 6$$

Como el residuo es distinto a 1, eso quiere decir que es imposible conseguir 1997 trozos usando el método indicado. □