Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Departamento de Matemáticas

Álgebra I

Segundo Cuatrimestre 2020

Guia Práctica 5

Ejercicios entregables

Isaac Edgar Camacho Ocampo

Buenos Aires, 2020

Índice general

Capítulo 1

Práctica 1 - Conjuntos, Relaciones y Funciones

1.1. Guia 1

1.2. Resolución

1. I **verdadero** de forma trivial.

   II **verdadero**, Recordar que $\{C \subseteq D \Leftrightarrow \forall x \in C \Rightarrow x \in D\}$ y podemos ver que 1 esta en ambos connjuntos.

   III **verdadero**, el razonamiento es idéntico, solo hay que tener en cuenta que para conjuntos no es relevante ni las repeticiones de elementos ni el órden.

   IV **falso**, porque el conjunto cuyos únicos elementos son 1,3 no esta en A, $\{1,3\} \notin A$ aqui hay que tener en cuenta que se esta usando el pertenece y no la inclusión de conjuntos.

   V **falso** por la misma razón que el item anterior.

2. 2

3. 3

4. 4

5. I **Recordemos que** $B \triangle C$ son todos los elementos que estan en B o en C pero no en ambos.
   $B \triangle C = \{1, \{3\}, 10, -2, \{1,2,3\}, 3\}$
   $A \cap (B \triangle C) = \{1, -2, 3\}$

   II $A \cap B = \{1\}$ y $A \cap C = \{-2, 3\} \Rightarrow (A \cap B) \triangle (A \cap C) = \{1, -2, 3\}$
   Notar que el resultado es igual que I porque $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ ambos resultados son equivalentes solo hay que distribuir.

   III **Usando la ley de De Morgan**

$$\begin{aligned} A^c \cap B^c \cap C^c = (A \cup B \cup C)^c &\Rightarrow A \cup B \cup C = \{1, \{3\}, -2, 7, 10, \{1,2,3\}, 3\} \\ &\Rightarrow (A \cup B \cup C) = V \\ &\Rightarrow (A \cup B \cup C)^c = \{\emptyset\} \end{aligned}$$

6. 6

7. 7

8. I Podemos ver a la parte subrayada del gráfico como la unión de tres conjuntos,
   $A \cup \{(A \cap C) - B\} \cup \{(B \cup C) - A\}$

   II Este es claramente la diferencia simétrica entre A y C, quitandole ademas todos lo elementos de B
   $(A \triangle C) - B$

   III Tambien lo podemos mirar como la unión de tres subconjuntos
   $\{(A \cap B) - C\} \cup \{(B \cap C) - A\} \cup \{(A \cap C) - B\}$

9. 9

10.

$$\begin{aligned} P(A) \subseteq P(B) \quad &\Rightarrow \quad A \subseteq B \\ A \underbrace{\subseteq}_{definicion} P(A) \quad &\Rightarrow \quad A \underbrace{\subseteq}_{Hipótesis} P(B) \end{aligned}$$

Pero $P(B) \subseteq B$ ya que $\forall x \in P(B) \Rightarrow x \in B$

$\Rightarrow A \subseteq B$

$$\begin{aligned} A \subseteq B \quad &\Rightarrow \quad P(A) \subseteq P(B) \\ \forall x \in A \quad &\Rightarrow \quad x \in P(A) \\ \forall x \in A \quad &\Rightarrow \quad x \in B \subseteq P(B) \\ \forall x \in P(A) \quad &\Rightarrow \quad x \in P(B) \end{aligned}$$

$\Rightarrow P(A) \subseteq P(B)$

11. 11

12. I a) **falso**, tomar el contraejemplo, n = 2.
    b) **verdadero**, porque me dice que existe algún n natural que cumple la condición, no es una proposición categórica, sino singular.
    c) **verdadera**, porque los intervalos incluyen a todos los Naturales, $[5, +\infty] \cup [1, 8]$
    d) **verdadera**, porque no es un intervalo vacío $[5, 8] \neq \emptyset$
    e) **verdadera**, porque cualquiera sea n, eligiendo m = n+1 se verifica la proposición.
    f) **falso**, lo que me quiere decir, es que existe un n que verifica, que es menor estrícto para todo m, y eso es falso porque si n = 1, y m = 1 $\Rightarrow$ 1 no es menor estricto que 1.

    II

    III

13. 13

14. 14

15. 15

16. 16

17. 17 R = (1, 1), (1, 3), (1, 7), (3, 1), (3, 5)

18. i) **verdadero**
    ii) **falso**, porque en el elemento (3, 2), $2 \notin B$
    iii) **verdadera**
    iv) **verdadera**
    v) **verdadera**
    vi) **verdadera**

19. i) $R = \{(1,1),(1,3),(1,5),(1,7),(2,2),(2,3),(2,5),(2,7),(3,3),(3,5),(3,7)\}$
    ii) $R = \{(2,1),(3,1)\}$
    iii) $R = \{(2,1),(2,3),(2,5),(2,7)\}$
    iv) $R = \{(1,7),(2,5),(2,7),(3,5),(3,7)\}$

20.

21.

22. **Ejercicio 18**

    i) **No es función** porque el 1 tiene varias imagenes.
    ii) **no es función** idem.
    iii) **no es función**
    iv) **no es función**
    v) **si es función** $\forall x \in A \Rightarrow \ \exists!\ y \in B \ \ |(x,y) \in R$
    vi) **si es función**

Capítulo 2

Práctica 2 - Números Naturales e Inducción

2.1. Resolución

1. I) a) $\sum_{i=1}^{100} i$ (es la sumatoria trivial).
   b) $\sum_{i=1}^{11} 2^{i-1}$
   c) $\sum_{i=1}^{12} (-1)^{i-1} \cdot i^2$
   d) $\sum_{i=1}^{21} (2i-1)^2$
   e) $\sum_{i=0}^{n} (2i+1)$
   f) $\sum_{i=1}^{n} (i \cdot n)$

   II) a) $\prod_{i=5}^{100} i = 5 \cdot 6 \cdots 100$
   b) $\prod_{i=0}^{10} 2^i$
   c) $\prod_{i=1}^{n} (i \cdot n)$

2. I)
$$\sum_{i=6}^{n} 2(i-5) = 2(6-5) + 2(7-5) + \cdots + 2(n-1-5) + 2(n-5)$$

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

   III)
$$\sum_{i=1}^{n} \frac{n+i}{2i} = \frac{n+1}{2 \cdot 1} + \frac{n+2}{2 \cdot 2} + \cdots + \frac{(n-1)+1}{2 \cdot (n-1)} + \frac{n+n}{2 \cdot n}$$

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

   V)
$$\prod_{i=1}^{n} \frac{n+i}{2i-3} = \frac{n+1}{2 \cdot 1 - 3} \cdot \frac{n+2}{2 \cdot 2 - 3} \cdots \frac{n+(n-1)}{2(n-1)-3} \cdot \frac{n+n}{2n-3}$$

3. i) Usamos inducción, primero para n=1

$$\sum_{i=1}^{1} i = 1 \text{ (ahora verificamos la fórmula) } \frac{n(n+1)}{2}, \text{ con n = 1,}$$

$$\frac{1(1+1)}{2} = 1, \text{ se verifica la propiedad para n = 1. } \Rightarrow P(1) = True$$

Hipótesis inductiva

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

Tésis inductiva

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

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

$$\underbrace{\sum_{i=1}^{n} i}_{\frac{n(n+1)}{2}} + (n+1) \underbrace{=}_{\text{por HI}} \frac{n(n+1)}{2} + (n+1)$$

$$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} \qquad \text{(factor común (n+1))}$$

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

probamos que $\Rightarrow \sum_{i=1}^{n+1} i = \frac{(n+1)(n+1+1)}{2} \qquad \forall n \in \mathbb{N}$

ii) De igual manera probaremos, por inducción la igualdad

$$2 + 4 + 6 + \cdots + 2n = \sum_{i=1}^{n} 2i = n(n+1)$$

para ello probamos que cumple para n=1, $P(1) \Rightarrow \sum_{i=1}^{1} 2i = 1(1+1) = 2$, luego probamos el paso inductivo, suponiendo que P(n) es verdadero, $\sum_{i=1}^{n} 2i = n(n+1)$ probamos que es verdadero P(n+1) o $\sum_{i=1}^{n+1} 2i = (n+1)(n+2)$.
Partimos de $\sum_{i=1}^{n+1} 2i$ y trataremos de llegar lógicamente a $(n+1)(n+2)$,
$\Rightarrow \sum_{i=1}^{n+1} 2i = \sum_{i=1}^{n} 2i + 2(n+1)$ pero usando la HI, $n(n+1) + 2(n+1)$ y sacando factor común (n+1) llegamos a, $(n+1)(n+2)$ que era justo lo que queriamos probar.

4.

5. Se trata de una serie geométrica.

$$\sum_{i=0}^{n} 2^i = 1 + 2 + 4 + 6 + \cdots + 2^n$$

si multiplico ambos miembros por 2 y resto convenientemente

$$\sum_{i=0}^{n} 2^i = 1 + 2 + 4 + 6 + \cdots + 2^n$$

$$2 \cdot (\sum_{i=0}^{n} 2^i) = 2 \cdot (1 + 2 + 4 + 6 + \cdots + 2^n)$$

$$2 \cdot (\sum_{i=0}^{n} 2^i) - (\sum_{i=0}^{n} 2^i) = (2 + 4 + 6 + \cdots + 2^n + 2^{n+1}) - (1 + 2 + 4 + 6 + \cdots + 2^n)$$

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Capítulo 3

Práctica 3 - Números enteros (Parte 2)

3.1. Guia 3

Álgebra I
Práctica 3 - Combinatoria de Conjuntos, Relaciones y Funciones

Cardinal de conjuntos y cantidad de relaciones y funciones

1. Dado el conjunto referencial $V = \{n \in \mathbb{N} \,/\, n \text{ es múltiplo de } 15\}$, determinar el cardinal del complemento del subconjunto A de V definido por $A = \{n \in V \,/\, n \geq 132\}$.

2. ¿Cuántos números naturales hay menores o iguales que 1000 que no son ni múltiplos de 3 ni múltiplos de 5?

3. Dados subconjuntos finitos A, B, C de un conjunto referencial V, calcular $\#(A \cup B \cup C)$ en términos de los cardinales de A, B, C y sus intersecciones.

4.
i) Una compañía tiene 420 empleados de los cuales 60 obtuvieron un aumento y un ascenso, 240 obtuvieron solo un aumento y 115 obtuvieron solo un ascenso. ¿Cuántos empleados no obtuvieron ni aumento ni ascenso?

ii) En el listado de inscripciones de un grupo de 150 estudiantes, figuran 83 inscripciones en Análisis y 67 en Álgebra. Además se sabe que 45 de los estudiantes se anotaron en ambas materias. ¿Cuántos de los estudiantes no están inscriptos en ningún curso?

iii) En un instituto de idiomas donde hay 110 alumnos, las clases de inglés tienen 63 inscriptos, las de alemán 30 y las de francés 50. Se sabe que 7 alumnos estudian los tres idiomas, 30 solo estudian inglés, 13 solo estudian alemán y 25 solo estudian francés. ¿Cuántos alumnos estudian exactamente dos idiomas? ¿Cuántos inglés y alemán pero no francés? ¿Cuántos no estudian ninguno de esos idiomas?

5. Si hay 3 rutas distintas para ir de Buenos Aires a Rosario, 4 rutas distintas para ir de Rosario a Santa Fe, y 2 para ir de Santa Fe a Reconquista ¿cuántos formas distintas hay para ir de Buenos Aires a Reconquista pasando por las dos ciudades intermedias?

6.
i) ¿Cuántos números de exactamente 4 cifras (no pueden empezar con 0) hay que no contienen al dígito 5?

ii) ¿Cuántos números de exactamente 4 cifras hay que contienen al dígito 7?

7. María tiene una colección de 17 libros distintos que quiere guardar en 3 cajas: una roja, una amarilla y una azul. ¿De cuántas maneras distintas puede distribuir los libros en las cajas?

8. Un estudiante puede elegir qué cursar entre 5 materias que se dictan este cuatrimestre. ¿De cuántas maneras distintas puede elegir qué materias cursar, incluyendo como posibilidad no cursar ninguna materia? ¿Y si tiene que cursar al menos dos materias?

9. Si A es un conjunto con n elementos ¿Cuántas relaciones en A hay? ¿Cuántas de ellas son reflexivas? ¿Cuántas de ellas son simétricas? ¿Cuántas de ellas son reflexivas y simétricas?

10. Sean $A = \{1, 2, 3, 4, 5\}$ y $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Sea $\mathcal{F}$ el conjunto de todas las funciones $f : A \to B$.

i) ¿Cuántos elementos tiene el conjunto $\mathcal{F}$?

ii) ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : 10 \notin \mathrm{Im}(f)\}$?

iii) ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : 10 \in \mathrm{Im}(f)\}$?

iv) ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : f(1) \in \{2, 4, 6\}\}$?

11. Sean $A = \{1, 2, 3, 4, 5, 6, 7\}$ y $B = \{8, 9, 10, 11, 12, 13, 14\}$.

i) ¿Cuántas funciones biyectivas $f : A \to B$ hay?

ii) ¿Cuántas funciones biyectivas $f : A \to B$ hay tales que $f(\{1, 2, 3\}) = \{12, 13, 14\}$?

12. ¿De cuántas formas se pueden permutar los números $1, 2, 3, 4, 5$ y 6? Por ejemplo, todas las permutaciones de $1, 2, 3$ son

$$1, 2, 3; \qquad 1, 3, 2; \qquad 2, 1, 3; \qquad 2, 3, 1; \qquad 3, 1, 2; \qquad 3, 2, 1.$$

13. ¿Cuántos números de 5 cifras distintas se pueden armar usando los dígitos del 1 al 5? ¿Y usando los dígitos del 1 al 7? ¿Y usando los dígitos del 1 al 7 de manera que el dígito de las centenas no sea el 2?

14. ¿Cuántos anagramas tiene la palabra *estudio*? ¿Y la palabra *murciélago*? Por ejemplo, todos los anagramas de la palabra *aro* son aro, aor, rao, roa, oar y ora.

15. Sean $A = \{1, 2, 3, 4, 5, 6, 7\}$ y $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

i) ¿Cuántas funciones inyectivas $f : A \to B$ hay?

ii) ¿Cuántas de ellas son tales que $f(1)$ es par?

iii) ¿Cuántas de ellas son tales que $f(1)$ y $f(2)$ son pares?

16. ¿Cuántas funciones biyectivas $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{1, 2, 3, 4, 5, 6, 7\}$ tales que $f(\{1, 2, 3\}) \subseteq \{3, 4, 5, 6, 7\}$ hay?

17. Sea $A = \{f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4, 5, 6, 7, 8\}$ tal que f es una función inyectiva$\}$.

Sea $\mathcal{R}$ la relación en A definida por:

$$f \,\mathcal{R}\, g \iff f(1) + f(2) = g(1) + g(2)$$

i) Probar que $\mathcal{R}$ es una relación de equivalencia.

ii) Sea $f \in A$ la función definida por $f(n) = n + 2$.
¿Cuántos elementos tiene su clase de equivalencia?

<u>*Número combinatorio*</u>

18. i) ¿Cuántos subconjuntos de 4 elementos tiene el conjunto $\{1, 2, 3, 4, 5, 6, 7\}$?

ii) ¿Y si se pide que 1 pertenezca al subconjunto?

iii) ¿Y si se pide que 1 no pertenezca al subconjunto?

iv) ¿Y si se pide que 1 o 2 pertenezcan al subconjunto pero no simultáneamente los dos?

19. Sea $A = \{n \in \mathbb{N} : n \leq 20\}$. Calcular la cantidad de subconjuntos $B \subseteq A$ que cumplen las siguientes condiciones:

i) B tiene 10 elementos y contiene exactamente 4 múltiplos de 3.

ii) B tiene 5 elementos y no hay dos elementos de B cuya suma sea impar.

20. Dadas dos rectas paralelas en el plano, se marcan n puntos distintos sobre una y m puntos distintos sobre la otra. ¿Cuántos triángulos se pueden formar con vértices en esos puntos?

21. ¿Cuántos anagramas tienen las palabras *elementos* y *combinatorio*?

22. Probar que $\binom{2n}{n} > n\, 2^n, \ \forall\, n \geq 4$.

23. Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por

$$a_1 = 2 \quad \text{y} \quad a_{n+1} = 4a_n - 2\frac{(2n)!}{(n+1)!\, n!} \qquad (n \in \mathbb{N})$$

Probar que $a_n = \binom{2n}{n}$.

24. Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por

$$a_1 = 1 \quad \text{y} \quad a_{n+1} = \frac{2n+1}{n+1}\, a_n \qquad (n \in \mathbb{N})$$

i) Probar que $a_n \leq \dfrac{1}{2n}\binom{2n}{n}$ para todo $n \in \mathbb{N}$.

ii) Probar que $a_n > \dfrac{1}{3^{n-1}}\binom{2n}{n}$ para todo $n \geq 3$.

25. En este ejercicio no hace falta usar inducción: se puede pensar en el significado combinatorio de $\binom{n}{k}$ (como la cantidad de subconjuntos de k elementos en un conjunto de n elementos).

i) Probar que $\displaystyle\sum_{k=0}^{2n}\binom{2n}{k} = 4^n$ y deducir que $\displaystyle\binom{2n}{n} < 4^n$.

ii) Calcular $\displaystyle\sum_{k=0}^{n}\binom{2n+1}{k}$.

iii) Probar que $\displaystyle\sum_{k=1}^{n} k\binom{n}{k} = n\,2^{n-1}$ $\left(\text{sug: } k\binom{n}{k} = n\binom{n-1}{k-1}\right)$.

iv) Probar que $\displaystyle\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}$ $\left(\text{sug: } \binom{n}{k} = \binom{n}{n-k}\right)$.

26. Probar que $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$ (sug: no hace falta usar inducción, aplicar el binomio de Newton).

27. Derivar a izquierda y derecha la igualdad $(x+1)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$ y evaluar lo obtenido en $x = 1$. ¿Qué se obtiene?

28. Sea $X = \{1, 2, 3, 4, 5, 5, 7, 8, 9, 10\}$, y sea $\mathcal{R}$ la relación de equivalencia en $\mathcal{P}(X)$ definida por:

$$A\,\mathcal{R}\,B \iff A \cap \{1,2,3\} = B \cap \{1,2,3\}.$$

¿Cuántos conjuntos $B \in \mathcal{P}(X)$ de exactamente 5 elementos tiene la clase de equivalencia $\overline{A}$ de $A = \{1, 3, 5\}$?

29. Sea $X = \{1, 2, \ldots, 20\}$, y sea $\mathcal{R}$ la relación de orden en $\mathcal{P}(X)$ definida por:

$$A\,\mathcal{R}\,B \iff A - B = \emptyset$$

¿Cuántos conjuntos $A \in \mathcal{P}(X)$ cumplen simultáneamente $\#A = 6$ y $A\,\mathcal{R}\,\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$?

30. i) Sea A un conjunto con $2n$ elementos. ¿Cuántas relaciones de equivalencia pueden definirse en A que cumplan la condición de que para todo $a \in A$ la clase de equivalencia de a tenga n elementos?

ii) Sea A un conjunto con $3n$ elementos. ¿Cuántas relaciones de equivalencia pueden definirse en A que cumplan la condición de que para todo $a \in A$ la clase de equivalencia de a tenga n elementos?

3.2. Resolución

Capítulo 4

Práctica 4 - Números enteros (Parte 2)

4.1. Guia 4

Álgebra I
Práctica 4 - Números enteros (Parte 1)

Divisibilidad

1. Decidir cuáles de las siguientes afirmaciones son verdaderas $\forall\, a, b, c \in \mathbb{Z}$

i) $a \cdot b \mid c \Rightarrow a \mid c$ y $b \mid c$
ii) $4 \mid a^2 \Rightarrow 2 \mid a$
iii) $2 \mid a \cdot b \Rightarrow 2 \mid a$ ó $2 \mid b$
iv) $9 \mid a \cdot b \Rightarrow 9 \mid a$ ó $9 \mid b$
v) $a \mid b + c \Rightarrow a \mid b$ ó $a \mid c$
vi) $a \mid c$ y $b \mid c \Rightarrow a \cdot b \mid c$
vii) $a \mid b \Rightarrow a \leq b$
viii) $a \mid b \Rightarrow |a| \leq |b|$
ix) $a \mid b + a^2 \Rightarrow a \mid b$
x) $a \mid b \Rightarrow a^n \mid b^n$, $\forall\, n \in \mathbb{N}$

2. Hallar todos los $n \in \mathbb{N}$ tales que

i) $3n - 1 \mid n + 7$
ii) $3n - 2 \mid 5n - 8$
iii) $2n + 1 \mid n^2 + 5$
iv) $n - 2 \mid n^3 - 8$

3. Sean $a, b \in \mathbb{Z}$.

i) Probar que $a - b \mid a^n - b^n$ para todo $n \in \mathbb{N}$ y $a \neq b \in \mathbb{Z}$.
ii) Probar que si n es un número natural par y $a \neq -b$, entonces $a + b \mid a^n - b^n$.
iii) Probar que si n es un número natural impar y $a \neq -b$, entonces $a + b \mid a^n + b^n$.

4. Sea a un entero impar. Probar que $2^{n+2} \mid a^{2^n} - 1$ para todo $n \in \mathbb{N}$.

5. Sea $n \in \mathbb{N}$.

i) Probar que si n es compuesto, entonces $2^n - 1$ es compuesto.
(Los primos de la forma $2^p - 1$ para p primo se llaman *primos de Mersenne*, por Marin Mersenne, monje y filósofo francés, 1588-1648. Se conjetura que existen infinitos primos de Mersenne, pero aún no se sabe. Se conocen a la fecha 49 primos de Mersenne (Enero 2017). El más grande producido hasta ahora es $2^{74207281} - 1$, que tiene 22338618 dígitos, y es el número primo más grande conocido a la fecha.)

ii) Probar que si $2^n + 1$ es primo, entonces n es una potencia de 2.
(Los números de la forma $\mathcal{F}_n = 2^{2^n} + 1$ se llaman *números de Fermat*, por Pierre de Fermat, juez y matemático francés, 1601-1665. Fermat conjeturó que cualquiera sea $n \in \mathbb{N}_0$, $\mathcal{F}_n$ era primo, pero esto resultó falso: los primeros $\mathcal{F}_0 = 3$, $\mathcal{F}_1 = 5$, $\mathcal{F}_2 = 17$, $\mathcal{F}_3 = 257$, $\mathcal{F}_4 = 65537$, son todos primos, pero $\mathcal{F}_5 = 4294967297 = 641 \times 6700417$. Hasta ahora no se conocen más primos de Fermat que los 5 primeros mencionados.)

6. i) Probar que el producto de n enteros consecutivos es divisible por $n!$.

ii) Probar que $\binom{2n}{n}$ es divisible por 2.

iii) Probar que $\binom{2n}{n}$ es divisible por $n + 1$ (sugerencia: probar que $(2n+1)\binom{2n}{n} = (n+1)\binom{2n+1}{n}$ y observar que $\binom{2n}{n} = (2n+2)\binom{2n}{n} - (2n+1)\binom{2n}{n}$).

7. Probar que las siguientes afirmaciones son verdaderas para todo $n \in \mathbb{N}$

i) $99 \mid 10^{2n} + 197$

ii) $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$

iii) $56 \mid 13^{2n} + 28n^2 - 84n - 1$

iv) $256 \mid 7^{2n} + 208n - 1$

Algoritmo de División

8. Calcular el cociente y el resto de la división de a por b en los casos

i) $a = 133, \quad b = -14$

ii) $a = 13, \quad b = 111$

iii) $a = 3b + 7, \quad b \neq 0$

iv) $a = b^2 - 6, \quad b \neq 0$

v) $a = n^2 + 5, \quad b = n + 2 \ (n \in \mathbb{N})$

vi) $a = n + 3, \quad b = n^2 + 1 \ (n \in \mathbb{N})$

9. Sabiendo que el resto de la división de un entero a por 18 es 5, calcular el resto de la división de

i) la división de $a^2 - 3a + 11$ por 18

ii) la división de a por 3

iii) la división de $4a + 1$ por 9

iv) la división de $a^2 + 7$ por 36

v) la división de $7a^2 + 12$ por 28

vi) la división de $1 - 3a$ por 27

10. i) Si $a \equiv 22 \ (14)$, hallar el resto de dividir a a por 14, por 2 y por 7.

ii) Si $a \equiv 13 \ (5)$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

iii) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

11. i) Hallar todos los $a \in \mathbb{Z}$ tales que $a^2 \equiv 3 \ (11)$.

ii) Probar que no existe ningún entero a tal que $a^3 \equiv -3 \ (13)$.

iii) Probar que $a^2 \equiv -1 \ (5) \Leftrightarrow a \equiv 2 \ (5)$ ó $a \equiv 3 \ (5)$.

iv) Probar que $a^7 \equiv a \ (7)$ para todo $a \in \mathbb{Z}$.

v) Probar que $7 \mid a^2 + b^2 \Leftrightarrow 7 \mid a$ y $7 \mid b$.

vi) Probar que $5 \mid a^2 + b^2 + 1 \Rightarrow 5 \mid a$ ó $5 \mid b$.

12. i) Probar que $2^{5n} \equiv 1 \ (31)$ para todo $n \in \mathbb{N}$.

ii) Hallar el resto de la división de 2^{51833} por 31.

iii) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39 \ (31)$, hallar el resto de la división de k por 5.

iv) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

Sistemas de numeración

13. i) Hallar el desarrollo en base 2 de

(a) 1365 (b) 2800 (c) $3 \cdot 2^{13}$ (d) $13 \cdot 2^n + 5 \cdot 2^{n-1}$

ii) Hallar el desarrollo en base 16 de 2800.

14. Sea $a \in N_0$. Probar que si el desarrollo en base 10 de a termina en k ceros entonces el desarrollo en base 5 de a termina en por lo menos k ceros.

15. i) ¿Cuáles son los números naturales más chico y más grande que se pueden escribir con exactamente n "dígitos" en base $d > 1$?

ii) Probar que $a \in \mathbb{N}_0$ tiene a lo sumo $[\log_2(a)] + 1$ bits cuando se escribe su desarrollo binario. (Para $x \in \mathbb{R}_{\geq 0}$, $[x]$ es la *parte entera de* x, es decir el mayor número natural (o cero) que es menor o igual que x.)

16. Sea $a = (a_d a_{d-1} \dots a_1 a_0)_2$ un número escrito en base 2 (o sea escrito en bits). Determinar simplemente cómo son las escrituras en base 2 del número $2a$ y del número $a/2$ cuando a es par, o sea las operaciones "multiplicar por 2" y "dividir por 2" cuando se puede. Esas operaciones se llaman *shift* en inglés, o sea corrimiento, y son operaciones que una computadora hace en forma sencilla.

17. Enunciar y demostrar criterios de divisibilidad por 8, 9 y 11.

Máximo común divisor

18. En cada uno de los siguientes casos calcular el máximo común divisor entre a y b y escribirlo como combinación lineal entera de a y b:

i) $a = 2532$, $b = 63$

ii) $a = 5335$, $b = 110$

iii) $a = 131$, $b = 23$

iv) $a = n^2 + 1$, $b = n + 2$ $(n \in \mathbb{N})$

19. Sean $a, b \in \mathbb{Z}$. Sabiendo que el resto de dividir a a por b es 27 y que el resto de dividir b por 27 es 21, calcular $(a : b)$.

20. Sea $a \in \mathbb{Z}$.

i) Probar que $(5a + 8 : 7a + 3) = 1$ o 41. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 23$ da 41.

ii) Probar que $(2a^2 + 3a - 1 : 5a + 6) = 1$ o 43. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 16$ da 41.

21. Sean $a, b \in \mathbb{Z}$ coprimos. Probar que $7a - 3b$ y $2a - b$ son coprimos.

22. Sean $a, b \in \mathbb{Z}$ con $(a : b) = 2$. Probar que los valores posibles para $(7a + 3b : 4a - 5b)$ son 2 y 94. Exhibir valores de a y b para los cuales da 2 y para los cuales da 94.

23.

i) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{b+4}{a} + \dfrac{5}{b} \in \mathbb{Z}$.

ii) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{9a}{b} + \dfrac{7a^2}{b^2} \in \mathbb{Z}$.

iii) Determinar todos los $a \in \mathbb{Z}$ tales que $\dfrac{2a+3}{a+1} + \dfrac{a+2}{4} \in \mathbb{Z}$.

Primos y factorización

24.

i) Probar que un número natural n es compuesto si y sólo si es divisible por algún primo positivo $p \leq \sqrt{n}$.

ii) Determinar cuáles de los siguientes enteros son primos: 91, 209, 307, 791, 1001, 3001.

iii) Hallar todos los primos menores o iguales que 100.

25. Probar que existen infinitos primos congruentes a 3 módulo 4.
Sugerencia: probar primero que si $a \neq \pm 1$ satisface $a \equiv 3 \pmod 4$, entonces existe p primo, $p \equiv 3 \pmod 4$ tal que $p \mid a$. Luego probar que si existieran sólo finitos primos congruentes a 3 módulo 4, digamos $p_1, p_2, \dots, p_n$, entonces $a = -1 + 4 \prod_{i=1}^{n} p_i$ sería un entero distinto de 1 y -1 que no es divisible por ningún primo congruente a 3 módulo 4.

26. Sea p primo positivo.

i) Probar que si $0 < k < p$, entonces $p \mid \binom{p}{k}$.

ii) Probar que si $a, b \in \mathbb{Z}$, entonces $(a + b)^p \equiv a^p + b^p \pmod p$.

27. Decidir si existen enteros a y b no nulos que satisfagan

i) $a^2 = 8b^2$ ii) $a^2 = 3b^3$ iii) $7a^2 = 11b^2$

28. Sea $n \in \mathbb{N}$, $n \geq 2$. Probar que si p es un primo positivo entonces $\sqrt[n]{p} \notin \mathbb{Q}$.

29. Sean p y q primos positivos distintos y sea $n \in \mathbb{N}$. Probar que si $p\,q \mid a^n$ entonces $p\,q \mid a$.

30. Sean $a, b \in \mathbb{Z}$. Probar que si ab es un cuadrado en $\mathbb{Z}$ y $(a : b) = 1$, entonces tanto a como b son cuadrados en $\mathbb{Z}$.

31. Determinar cuántos divisores positivos tienen 9000, $15^4 \cdot 42^3 \cdot 56^5$ y $10^n \cdot 11^{n+1}$. ¿ Y cuántos divisores en total ?

32. Hallar la suma de los divisores positivos de $2^4 \cdot 5^{123}$ y de $10^n \cdot 11^{n+1}$.

33. Hallar el menor número natural n tal que $6552\,n$ sea un cuadrado.

34. Hallar todos los $n \in \mathbb{N}$ tales que

i) $(n : 945) = 63$, $(n : 1176) = 84$ y $n \leq 2800$

ii) $(n : 1260) = 70$ y n tiene 30 divisores positivos

35. Hallar el menor número natural n tal que $(n : 3150) = 45$ y n tenga exactamente 12 divisores positivos.

36. Sea $n \in \mathbb{N}$. Probar que

i) $(2^n + 7^n : 2^n - 7^n) = 1$,

ii) $(2^n + 5^{n+1} : 2^{n+1} + 5^n) = 3$ ó 9, y dar un ejemplo para cada caso.

iii) $(3^n + 5^{n+1} : 3^{n+1} + 5^n) = 2$ ó 14, y dar un ejemplo para cada caso.

37. Sean $a, b \in \mathbb{Z}$. Probar que si $(a : b) = 1$ entonces $(a^2 \cdot b^3 : a + b) = 1$.

38. Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 5$.

i) Calcular los posibles valores de $(ab : 5a - 10b)$ y dar un ejemplo para cada uno de ellos.

ii) Para cada $n \in \mathbb{N}$, calcular $(a^{n-1}b : a^n + b^n)$.

39. Hallar todos los $n \in \mathbb{N}$ tales que

i) $[n : 130] = 260$. ii) $[n : 420] = 7560$.

40. Hallar todos los $a, b \in \mathbb{Z}$ tales que

i) $(a : b) = 10$ y $[\,a : b\,] = 1500$ ii) $3 \mid a$, $(a : b) = 20$ y $[a : b] = 9000$

4.2. Resolución

Capítulo 5

Práctica 5 - Números enteros (Parte 2)

5.1. Guia 5

Álgebra I
Práctica 5 - Números enteros (Parte 2)

Ecuaciones diofánticas y de congruencia

1. Determinar, cuando existan, todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen

i) $5a + 8b = 3$ iii) $24a + 14b = 7$ v) $39a - 24b = 6$

ii) $7a + 11b = 10$ iv) $20a + 16b = 36$ vi) $1555a - 300b = 11$

2. Determinar todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen simultáneamente $4 \mid a$, $8 \mid b$ y $33a + 9b = 120$.

3. Si se sabe que cada unidad de un cierto producto A cuesta 39 pesos y que cada unidad de un cierto producto B cuesta 48 pesos, ¿cuántas unidades de cada producto se pueden comprar con 135 pesos?

4. Hallar, cuando existan, todas las soluciones de las siguientes ecuaciones de congruencia

i) $17X \equiv 3\ (11)$ ii) $56X \equiv 28\ (35)$ iii) $56X \equiv 2\ (884)$ iv) $33X \equiv 27\ (45)$

5. Determinar todos los $b \in \mathbb{Z}$ para los cuales existe $a \equiv 4\ (5)$ tal que $6a + 21b = 15$.

6. Hallar todos los $(a, b) \in \mathbb{Z}^2$ tales que $b \equiv 2a \pmod 5$ y $28a + 10b = 26$.

7. Hallar el resto de la división de un entero a por 18, sabiendo que el resto de la división de $7a$ por 18 es 5.

8. Hallar todos los $a \in \mathbb{Z}$ para los cuales $(7a + 1 : 5a + 4) \neq 1$.

9. Describir los valores de $(5a + 8 : 7a + 3)$ en función de los valores de $a \in \mathbb{Z}$.

Teorema chino del resto

10. i) ¿Existe algún entero a cuyo resto en la división por 15 sea 13 y cuyo resto en la división por 35 sea 22?

ii) ¿Existe algún entero a cuyo resto en la división por 15 sea 2 y cuyo resto en la división por 18 sea 8?

11. Hallar, cuando existan, todos los enteros a que satisfacen simultáneamente:

i) $\begin{cases} a \equiv 0 & (8) \\ a \equiv 2 & (5) \\ a \equiv 1 & (21) \end{cases}$ ii) $\begin{cases} a \equiv 3 & (10) \\ a \equiv 2 & (7) \\ a \equiv 5 & (9) \end{cases}$ iii) $\begin{cases} a \equiv 1 & (6) \\ a \equiv 2 & (20) \\ a \equiv 3 & (9) \end{cases}$ iv) $\begin{cases} a \equiv 1 & (12) \\ a \equiv 7 & (10) \\ a \equiv 4 & (9) \end{cases}$

12. Hallar, cuando existan, todos los enteros a que satisfacen simultáneamente:

i) $\begin{cases} 3\,a \equiv 4 & (5) \\ 5\,a \equiv 4 & (6) \\ 6\,a \equiv 2 & (7) \end{cases}$ ii) $\begin{cases} 3\,a \equiv 1 & (10) \\ 5\,a \equiv 3 & (6) \\ 9\,a \equiv 1 & (14) \end{cases}$ iii) $\begin{cases} 15\,a \equiv 10 & (35) \\ 21\,a \equiv 15 & (8) \\ 18\,a \equiv 24 & (30) \end{cases}$

13. i) Sabiendo que los restos de la división de un entero a por 3, 5 y 8 son 2, 3 y 5 respectivamente, hallar el resto de la división de a por 120.

ii) Sabiendo que los restos de la división de un entero a por 6, 10 y 8 son 5, 3 y 5 respectivamente, hallar los posibles restos de la división de a por 480.

14. i) Hallar el menor entero positivo a tal que el resto de la división de a por 21 es 13 y el resto de la división de $6a$ por 15 es 9.

ii) Hallar un entero a entre 60 y 90 tal que el resto de la división de $2a$ por 3 es 1 y el resto de la división de $7a$ por 10 es 8.

Pequeño teorema de Fermat

15. Hallar el resto de la división de a por p en los casos

i) $a = 33^{1427}$, $p = 5$

ii) $a = 71^{22283}$, $p = 11$

iii) $a = 5 \cdot 7^{2451} + 3 \cdot 65^{2345} - 23 \cdot 8^{138}$, $p = 13$

16. Resolver en $\mathbb{Z}$ las ecuaciones de congruencia

i) $7^{13}X \equiv 5\ (11)$

ii) $2^{194}X \equiv 7\ (97)$

17. Probar que para todo $a \in \mathbb{Z}$ vale

i) $728 \mid a^{27} - a^3$

ii) $\dfrac{2a^7}{35} + \dfrac{a}{7} - \dfrac{a^3}{5} \in \mathbb{Z}$

18. *Seudoprimos o números de Carmichael (Robert Carmichael, 1879-1967, matemático estadounidense).* Se dice que $n \in \mathbb{Z}$ es un número de Carmichael si satisface el pequeño Teorema de Fermat sin ser primo, es decir, si a es un entero coprimo con n, entonces $a^{n-1} \equiv 1 \pmod{n}$. Probar que 561 es un número de Carmichael. En 1994 se probó finalmente que hay infinitos números de Carmichael, luego de que esta conjetura quedara abierta por muchos años.

19. Resolver en $\mathbb{Z}$ los siguientes sistemas lineales de ecuaciones de congruencia

i) $\begin{cases} 2^{2013}X \equiv 6 \ \ (13) \\ 5^{2013}X \equiv 4 \ \ (7) \\ 7^{2013}X \equiv 2 \ \ (5) \end{cases}$

ii) $\begin{cases} 10^{49}X \equiv 17 \ \ (39) \\ 5X \equiv 7 \ \ (9) \end{cases}$

20. Hallar el resto de la división de

i) $3 \cdot 7^{135} + 24^{78} + 11^{222}$ por 70

ii) 3^{385} por 400

iii) $\displaystyle\sum_{i=1}^{1759} i^{42}$ por 56

21. Hallar todos los $a \in \mathbb{Z}$ tales que

i) $539 \mid 3^{253}a + 5^{44}$

ii) $a^{236} \equiv 6\ (19)$

22. Hallar el resto de la división de 2^{2^n} por 13 para cada $n \in \mathbb{N}$.

23. Resolver en $\mathbb{Z}$ la ecuación de congruencia $7\,X^{45} \equiv 1 \pmod{46}$.

24. Hallar todos los divisores positivos de 25^{70} que sean congruentes a 2 módulo 9 y a 3 módulo 11.

El anillo $\mathbb{Z}/m\mathbb{Z}$

25. Escribir las tablas de suma y producto en $\mathbb{Z}/m\mathbb{Z}$ para $m = 5$, 6, 7 y 8. ¿Cuáles de estos anillos son cuerpos?

26. Un elemento $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ es un *cuadrado* (en $\mathbb{Z}/m\mathbb{Z}$) si existe $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\overline{a} = \overline{b}^2$ en $\mathbb{Z}/m\mathbb{Z}$.

i) Calcular los cuadrados de $\mathbb{Z}/m\mathbb{Z}$ para $m = 2$, 3, 4, 5, 6, 7, 8, 9, 11 y 13. ¿Cuántos hay en cada caso?

ii) Probar que si $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$ son cuadrados, entonces $\overline{a} \cdot \overline{b}$ es un cuadrado también.

iii) Probar que si $\overline{a}$ es un elemento inversible de $\mathbb{Z}/m\mathbb{Z}$ tal que $\overline{a} = \overline{b}^2$, entonces $\overline{b}$ es inversible también en $\mathbb{Z}/m\mathbb{Z}$ y $\overline{a}^{-1}$ es un cuadrado también.

iv) Sea p primo positivo. Probar que, en $\mathbb{Z}/p\mathbb{Z}$, si $\overline{a}^2 = \overline{b}^2$ entonces $\overline{a} = \overline{b}$ ó $\overline{a} = -\overline{b}$. Deducir que si p es impar, entonces hay exactamente $\dfrac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}/p\mathbb{Z}$.

27. Sea p un primo. Probar que en $\mathbb{Z}/p\mathbb{Z}$ vale que $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$, $\forall\, \overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ (sug: ver Ej. 26 Práctica 3). ¿Vale lo mismo en $\mathbb{Z}/m\mathbb{Z}$ si m no es primo?

28. *Test de primalidad de Wilson,* por el mátemático inglés John Wilson, 1741-1793. Este test era conocido mucho antes por los árabes, y fue de hecho probado por primera vez por el matemático italiano Joseph-Louis Lagrange en 1771. Dice que si $n \in \mathbb{N}$ es distinto de 1, entonces

$$(n-1)! \equiv -1 \pmod{n} \iff n \text{ es primo .}$$

i) Probar que si $n \geq 5$ es compuesto, entonces $(n-1)! \equiv 0 \pmod{n}$. ¿Qué implicación se prueba con esto?

ii) Sea p un primo positivo. Se recuerda que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Probar que $\overline{a} = \overline{a}^{-1}$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\overline{a} = \pm\overline{1}$. Deducir que $(p-1)! \equiv -1 \pmod{p}$.

29. i) Describir el conjunto $\{\overline{3}^n;\ n \in \mathbb{N}\}$ en $\mathbb{Z}/7\mathbb{Z}$ y en $\mathbb{Z}/11\mathbb{Z}$. Observar la diferencia que hay en el primer caso con respecto al segundo caso, y hallar si se puede un elemento $\overline{a} \in \mathbb{Z}/11\mathbb{Z}$ que cumpla que $\{\overline{a}^n;\ n \in \mathbb{N}\} = \mathbb{Z}/11\mathbb{Z} - \{\overline{0}\}$.

ii) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\ (7)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 4\ (7)$.

iii) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\ (11)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 9\ (11)$.

iv) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 53\ (77)$.

5.2. Resolución

hola mundo

Para demostrar la corrección del programa en SmallLang con respecto a la especificación, debemos probar que:

$$Post \Rightarrow wp(\ \textbf{código previo al ciclo}\ , Pc) \tag{5.1}$$
$$Pc \Rightarrow wp(\ \textbf{ciclo}, Qc) \tag{5.2}$$
$$Qc \Rightarrow wp(\ \textbf{código posterior al ciclo}\ , Post) \tag{5.3}$$

La parte 2.2 con el teoréma del invariante. Si probamos estas tres implicaciones, por el principio de monotonía sabemos que $Pre \Rightarrow wp(programacompleto, Post)$ y por lo tanto el programa es correcto, respecto a su especificación

5.3. Definición de Qc, Pc, I, fv

Primero vamos a definir los predicados que necesitamos para la demostracion.

$$\begin{aligned}
Pre &\quad \{True\} \\
Post = &\quad \{r = True \leftrightarrow ((\exists k : \mathbb{Z})(0 \leq k < |s|) \wedge_L s[k] = e)\} \\
Pc = &\quad (i = 0) \wedge (j = -1) \\
Qc = &\quad (j \neq -1) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k <| s \mid \ \wedge_L s[k] = e) \\
I = &\quad 0 \leq i \leq| s |) \wedge (j \neq -1) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = e) \wedge (s[i] = e \rightarrow i = j) \\
fv = &\quad (| s | -i) \\
B = &\quad (i <| s |)
\end{aligned}$$

5.3.1. Pre ⇒ wp(código previo al ciclo, Pc)

$$
\begin{aligned}
Pre \to wp(i := 0; j := -1, Pc) \equiv \quad & wp(i := 0; wp(j := -1, Pc)) \\
\\
Calculamos\ wp(j := -1, Pc) & \\
wp(j := -1, Pc) \equiv \quad & def(-1) \wedge_L Pc^j_{-1} \\
\equiv \quad & wp(j := -1, ((i = 0) \wedge (j = -1))^j_{(-1)}) \\
\equiv \quad & def(-1) \wedge (i = 0) \wedge (-1 = -1) \\
E1 \equiv \quad & (i = 0) \\
\\
Calculamos\ wp(i := 0, E1) & \\
wp(i := 0, E1) \equiv \quad & def(0) \wedge_L E1^i_0 \\
\equiv \quad & True \wedge_L (i = 0)^i_0 \\
\equiv \quad & (0 = 0) \\
E2 \equiv \quad & True
\end{aligned}
$$

Por lo tanto demostramos que:

$$Pre \Rightarrow wp(\ \textbf{código previo al ciclo}\ , Pc)$$

5.3.2. Qc ⇒ wp(if..then..else..fi, Post)

Recordamos la post

$$Post = \{r = True \leftrightarrow ((\exists k : \mathbb{Z})(0 \leq k < |s|) \wedge_L s[k] = e)\}$$

Calculamos:

$$
\begin{aligned}
wp(if.....endif, Post) &\equiv wp(if(j \neq -1) then\ r := True\ else\ r := False\ endif, Post) \\
&\equiv def(j \neq -1) \wedge_L [(j \neq -1) \wedge wp(r := True, Post)] \vee [(j = -1) \wedge wp(r := False, Post)] \\
&\equiv \underbrace{def(j \neq -1)}_{\text{True}} \wedge_L \quad [\qquad\qquad " \qquad\qquad] \vee [\qquad\qquad " \qquad\qquad] \\
&\equiv (j \leq -1 \wedge wp(r := True, Post)) \vee (j = -1 \wedge wp(r := False, Post)) \\
&\equiv (j \leq -1 \wedge wp(r := True, Post)) \vee (j = -1 \wedge wp(r := False, Post))
\end{aligned}
$$

$$\begin{aligned} wp(r := True, Post) &\equiv def(True) \wedge_L Post^r_{true} \\ &\equiv (True = True) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e) \\ wp(r := True, Post) &\equiv (\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e) \end{aligned}$$

$$\begin{aligned} wp(r := False, Post) &\equiv def(False) \wedge_L Post^r_{false} \\ &\equiv \underbrace{(false = True)}_{\text{False}} \leftrightarrow \underbrace{(\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e)}_{(*)} \end{aligned}$$

$(*)$ *entonces como* $(\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e)$ debe ser Falso, invierto desigualdad

$$wp(r := False, Post) \equiv (\forall k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] \neq e)$$

$$\begin{aligned} wp(if...endif, Post) &\equiv (j \neq -1) \wedge (\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e) \vee \\ &\quad (j = -1) \wedge (\forall k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] \neq e) \\ &\quad (aplico\ (p \wedge q) \vee (\neg p \wedge \neg q) \equiv p \leftrightarrow q) \\ E3 &\equiv (j \neq -1) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e) \end{aligned}$$

Chequeamos $Qc \rightarrow E3$

$$Qc \equiv j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e) \equiv E3$$

Por lo tanto demostramos que:

$$Qc \Rightarrow E3$$

Capítulo 6

Demostración de la corrección del ciclo

6.0.1. Qc ⇒ wp(ciclo, Qc)

Teorema. Sean un predicado I y una función $fv : \mathbb{V} \to \mathbb{Z}$ (donde $\mathbb{V}$ es el producto cartesiano de los dominios de las variables del programa), y supongamos que I → def(B). Si se cumplen:

1) $PC \Rightarrow I$,
2) $\{I \wedge B\} S \{I\}$,
3) $I \wedge \neg B \Rightarrow Qc$,
4) $\{I \wedge B \wedge v_0 = fv\} S \{fv < v_0\}$,
5) $I \wedge fv \leq 0 \Rightarrow \neg B$,

... entonces la siguiente tripla de Hoare es válida: {PC } while B do S endwhile {QC }

6.0.2. $Pc \ \to I$

$$
\begin{aligned}
Pc = \quad & (i = 0) \wedge (j = -1) \\
I = \quad & 0 \leq i \leq |\ s\ | \wedge (j \neq -1) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i \to_L s[k] = e) \wedge (s[i] = e \to i = j) \\
\equiv \quad & (i = 0) \wedge (j = -1) \to (0 \leq i \leq |\ s\ |) \ \checkmark (\textit{trivial}) \\
\equiv \quad & (j \neq -1 \wedge (\exists k : \mathbb{Z})(0 \leq k < i \wedge_L s[k] = e)) \vee (j = -1 \wedge (\forall k : \mathbb{Z})(0 \leq k < i \wedge_L s[k] \neq e)) \checkmark
\end{aligned}
$$

(porque se cumple trivialmente que $(j = -1)$ y por vacuidad $(j = -1 \wedge (\forall k : \mathbb{Z})(0 \leq k < i \wedge_L s[k] \neq e))$ ya que no hay ningún número que sea mayor o igual a cero y menor a cero a la vez)

6.0.3. $(I \ \wedge \neg B) \rightarrow Qc$

$$Q_c \equiv (j \neq -1) \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e)$$
$$B \equiv (i < |s|)$$
$$I \equiv 0 \leq i \leq |s| \wedge j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i \Rightarrow_L s[k] = e) \wedge (s[i] = e \rightarrow i = j)$$

Q_c✓

(porque $I \wedge \neg B$ implica que $i = |s|$ ya que por I, $i \leq |s|$ y por $\neg B$ $i \geq |s|$ y si aplico esto a I me queda Q_c)

6.0.4. $\{I \wedge B\}$ ciclo $\{I\}$

$$I = \quad (0 \leq i \leq |\ s\ |) \wedge (j \neq -1) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = e) \wedge (s[i] = e \rightarrow i = j)$$
$$B \equiv \quad (i < |s|)$$

Ciclo

$if(s[i] = e)then$
$\quad j := i$
$else$
$\quad skip$
$endif$
$i := i + 1$

Veamos si $(I \wedge B) \Rightarrow wp(\text{if...then..else..fi}, i := i + 1, I)$

$$wp(if..fi, i := i + 1, I) \equiv wp(if..fi, \underbrace{wp(i := i + 1, I)}_{debo\ calcular})$$

$$wp(i := i + 1, I) \equiv \underbrace{def(i + 1)}_{True} \wedge_L I^i_{i+1}$$
$$\equiv (0 \leq i + 1 \leq |s|) \wedge_L (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z}))(0 \leq k < i + 1 \Rightarrow_L s[k] = e)) \wedge$$
$$(s[i + 1] = e \rightarrow i + 1 = j)$$

$$E4 \equiv (0 \leq i + 1 \leq |s|) \wedge_L (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z}))(0 \leq k < i + 1 \Rightarrow_L s[k] = e)) \wedge$$
$$(s[i + 1] = e \rightarrow i + 1 = j)$$

Calculo $wp(if...then..else..fi, E4)$

$$
\begin{aligned}
wp(if..fi, E4) &\equiv \underbrace{def(s[i] = e)}_{True} \wedge_L \ [\ s[i] = e \wedge wp(j := i, E4)\ ] \vee [\ s[i] \neq e \wedge wp(skip, E_4)] \\
&\equiv (s[i] = e \wedge \underbrace{def(i)}_{True} \wedge E4_i^j) \vee (s[i] \neq e \wedge E4) \\
&\equiv (s[i] = e \wedge E4_i^j) \vee (s[i] \neq e \wedge E4) \\
&\equiv (s[i] = e) \quad \wedge \\
&\quad (0 \leq i+1 \leq |s|) \wedge_L (i \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e)) \wedge \\
&\quad (s[i+1] = e \rightarrow i+1 = i) \qquad \vee \\
&\quad (s[i] \neq e) \quad \wedge \\
&\quad (0 \leq i+1 \leq |s| \wedge_L (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k \leq i+1 \Rightarrow_L s[k] = e)) \wedge \\
&\quad (s[i+1] = e \rightarrow i+1 = j)
\end{aligned}
$$

$$
\begin{aligned}
E5 \equiv\ & (0 \leq i+1 \leq |s|) \wedge_L \\
& (s[i] = e \wedge (i \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e)) \wedge \\
& (s[i+1] = e \rightarrow i+1 = i)) \\
& \vee \\
& (s[i] \neq e \wedge (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k \leq i+1 \Rightarrow_L s[k] = e)) \wedge \\
& (s[i+1] = e \rightarrow i+1 = j))
\end{aligned}
$$

Segun el invariante $(s[i] = e \rightarrow i = j)$, y usando la equivalencia $(p \wedge q) \vee (\neg p \wedge q) \equiv q$

$$
\begin{aligned}
E5 \equiv\ & (0 \leq i+1 \leq |s|) \wedge_L \\
& (\underbrace{s[i] = e}_{\text{por I}} \wedge (\underbrace{i \neq -1}_{\text{i=j}} \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e)) \wedge \\
& (s[i+1] = e \rightarrow \underbrace{i+1 = i}_{i=j})) \\
& \vee \\
& (s[i] \neq e \wedge (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k \leq i+1 \Rightarrow_L s[k] = e)) \wedge \\
& (s[i+1] = e \rightarrow i+1 = j))
\end{aligned}
$$

$$
\begin{aligned}
E5 \equiv\ & (0 \leq i+1 \leq |s|) \wedge_L \\
& (s[i] = e \wedge (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e)) \wedge \\
& (s[i+1] = e \rightarrow i+1 = j)) \\
& \vee \\
& (s[i] \neq e \wedge (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k \leq i+1 \Rightarrow_L s[k] = e)) \wedge \\
& (s[i+1] = e \rightarrow i+1 = j))
\end{aligned}
$$

$$
\begin{aligned}
&\textit{usando}(p \wedge q) \vee (\neg p \wedge q) \equiv q \\
E5 \equiv\ & (0 \leq i+1 \leq |s|) \wedge_L \\
& (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e) \wedge \\
& (s[i+1] = e \rightarrow i+1 = j)
\end{aligned}
$$

Ahora veamos si $\{I \wedge B\} \Rightarrow E5$

Hipótesis:

1. $B \equiv \quad (i < |s|)$
2. $I = \quad (0 \leq i \leq |\ s\ |)$
3. $(j \neq -1) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = e)$
4. $(s[i] = e \rightarrow i = j)$

Tésis

1. $(0 \leq i+1 \leq |s|)$
2. $(j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e)$
3. $(s[i+1] = e \rightarrow i+1 = j)$

Comenzamos por la tésis 1 $(0 \leq i+1 \leq |s|)$

$$
\begin{aligned}
\textbf{segun la hip 2} \ &\Rightarrow \quad 0 \leq i \\
&\Rightarrow \quad 0 \leq i+1 \\
\textbf{segun la hip 1} \ &\Rightarrow \quad i < |s| \\
&\Rightarrow \quad i+1 < |s|+1 \\
&\Rightarrow \quad i+1 \leq |s|
\end{aligned}
$$

Por lo tanto se cumple la tésis 1 $(0 \leq i+1 \leq |s|)$

Continuamos por la tésis 2

$$(j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e)$$

$$
\begin{aligned}
0 \leq k < i+1 \quad &\equiv \quad 0 \leq k \leq i \\
\textbf{sabemos que} \quad i < |s| \quad &\equiv \quad 0 \leq k \leq i < |s| \\
(*) \quad &\equiv \quad 0 \leq k < |s| \\
(j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i+1 \Rightarrow_L s[k] = e) \quad &\equiv \quad (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(\underbrace{0 \leq k < |s|}_{(*)} \Rightarrow_L s[k] = e) \\
&\equiv \quad (j \neq -1 \Leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < |s| \Rightarrow_L s[k] = e)
\end{aligned}
$$

Esto significa que j sera distinto de -1 cuando exista un k que estando en rango verifique que el elemento en la posicion k sea e, y sera falso cuando e no este en la secuencia.

Continuamos por la tésis 3

$$(s[i+1] = e \leftrightarrow i+1 = j)$$

$$
\begin{aligned}
\textbf{segun la hip 4} \quad i = j \quad &\leftrightarrow \quad s[i] = e \\
&\leftrightarrow \quad s[j] = e \\
\textbf{pero si} \quad j = i+1 \quad &\leftrightarrow \quad s[i+1] = e \\
\textbf{de igual forma si} \quad s[i] = e \quad &\leftrightarrow \quad j = i \\
s[i+1] = e \quad &\leftrightarrow \quad j = i+1
\end{aligned}
$$

Esto dice que si e esta en la posicion i+1, entonces j debe ser i+1, ya que j era igual a i.

Por lo tanto se cumple

$$(s[i+1] = e \leftrightarrow i+1 = j)$$

6.0.5. $I \wedge f_v \leq 0 \rightarrow \neg B$

Queremos demostrar que cuando la función variante llega a un valor determinado entonces se termina el ciclo o dicho de otra forma la guarda se hace falsa.

Hipótesis

$$
\begin{aligned}
I = \quad & (0 \leq i \leq |\ s\ |) \wedge (j \neq -1) \leftrightarrow (\exists k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = e) \wedge (s[i] = e \rightarrow i = j) \\
fv = \quad & (|\ s\ | - i) \leq 0
\end{aligned}
$$

Tésis

$$\neg B \equiv \quad (i \geq |s|)$$

Demostración

$$
\begin{aligned}
fv \equiv \quad & |\ s\ | - i \leq 0 \\
\equiv \quad & |\ s\ | \leq i \\
\equiv \quad & (i \geq |s|) \qquad (\ \textbf{que es}\ \neg B)
\end{aligned}
$$

Por lo tanto se cumple la tésis $(I \wedge f_v \leq 0) \rightarrow \neg B$

6.0.6. $\{I \wedge B \wedge v_0 = fv\} S \{fv < v_0\}$

Finalemente vamos a demostrar que la funcion variante decrece, esto equivale a decir que si estamos al principio del ciclo en donde valen, tanto el invariante, la guarda y donde la funcion variante toma cierto valor v_0, despues de ejecutar el cuerpo del ciclo la fv va a tomar un valor estrictamente menor a v_0 .

Ciclo
S1 $if(s[i] = e) then$
$j := i$
$else$
$skip$
$endif$
S2 $i := i + 1$

Si llamamos **S1 al if..endif** y **S2 a i:=i+1**. Debemos hallar $wp(S1; S2, fv < v_0)$

$$
\begin{aligned}
wp(S1;S2, fv < v_0) &\equiv wp(S1,\ wp(S2, |s| - i < v_0)) \\
wp(S2, |s| - i < v_0) &\equiv wp(i := i+1, |s| - i < v_0) \\
&\equiv \underbrace{def(i+1)}_{True} \wedge_L (|s| - i < v_0)^i_{i+1} \\
&\equiv (|s| - i < v_0)^i_{i+1} \\
E2 \equiv wp(S2, |s| - i < v_0) &\equiv (|s| - (i+1) < v_0)
\end{aligned}
$$

Calculamos la precondición más débil del if..fi respecto de E2.

$$
\begin{aligned}
wp(S1, E2) &\equiv wp(if..fi, E2) \\
&\equiv \underbrace{def(s[i] = e)}_{True} \wedge_L \ [\ s[i] = e \wedge wp(j := i, E2)\ ] \vee [\ s[i] \neq e \wedge wp(skip, E2)] \\
&\equiv [\ s[i] = e \wedge wp(j := i, E2)\ ] \vee [\ s[i] \neq e \wedge E2] \\
&\equiv (\ s[i] = e \wedge (def(i) \wedge_L E2^j_i)\ ) \vee (\ s[i] \neq e \wedge E2) \\
&\equiv (\ s[i] = e \wedge (E2^j_i)\ ) \vee (\ s[i] \neq e \wedge E2) \\
&\equiv (\ s[i] = e \wedge (|s| - (i+1) < v_0)\ ) \vee (\ s[i] \neq e \wedge (|s| - (i+1) < v_0)) \\
&usando (p \wedge q) \vee (\neg p \wedge q) \equiv q \\
E1 &\equiv (|s| - (i+1) < v_0) \\
E1 &\equiv (|s| - i - 1 < v_0)
\end{aligned}
$$

Por lo tanto la precondición más débil que queriamos calular es E1, ahora debemos verificar que

$$\{I \wedge B \wedge v_0 = fv\} \Rightarrow E1$$

$$\begin{array}{rcll} fv & = & v_0 & \\ |s| - i & = & v_0 & (\text{ restando 1 a ambos miembros obtenemos}) \\ |s| - i - 1 & = & v_0 - 1 & (\text{ pero } (v_0 - 1) < v_0) \\ |s| - i - 1 & = & v_0 - 1 < v_0 & \\ |s| - i - 1 & < & v_0 & \end{array}$$

Por lo tanto nuestra funcion variante decrece y

$$\{I \wedge B \wedge v_0 = fv\} \Rightarrow E1$$

Capítulo 7

Conclusiones

Estamos en condiciones de afirmar que nuestro programa, habiendo demostrado a través del teorema de invarinate que el ciclo es correcto respecto de su espeficicación y a través del teorema de terminacion del ciclo, que el mismo finaliza siempre y ademas termina en un estado en que vale la postcondicion del ciclo.
Con todo esto probado y por el principio de monotonia probamos que el programa completo es correcto respecto de la especificación dada.