Ejercicios 7

1 **Teo B** (*Formas normales para* **nat**)
Sea $X = \{n:\mathbf{nat} \mid n=0 \vee (\exists m:nat \mid: n=S.m)\}$.
Claramente, $0 \in X$. Además, si $x \in X$, también $S.x \in X$, porque $S.x=S.x$ y, por tanto $(\exists m:\mathbf{nat} \mid: S.x = S.m)$. El Axioma e permite afirmar que $X = \mathbf{nat}$.

2 **Teo**: Principio del Buen Orden ≡ Axioma e.
(⇒) Supóngase el Principio del Buen Orden. Sea A un subconjunto de **nat** para el que $0 \in A$ y, si $x \in A$, se tenga que $S.x \in A$. Considérese A^c, el complemento de A con respecto a **nat**. Si $A^c \neq \emptyset$, el Principio del Buen Orden garantiza que A^c tiene un primer elemento a. Por el Teo B: $a=0 \vee (\exists m:nat \mid: a=S.m)$. Como $0 \in A$, debe ser $a \neq 0$ y debe existir $m \in \mathbf{nat}$ tal que $S.m=a$. Ahora, $m \notin A^c$, porque a es el menor elemento de A^c. Entonces $m \in A$. Pero entonces, $S.m=a \in A$, lo que es una contradicción. Por lo tanto, $A^c=\emptyset$ y, así mismo, $A = \mathbf{nat}$.
(⇐) Sea X un subconjunto no vacío de **nat**. Supóngase que X no tiene un primer elemento. Para $n \in \mathbf{nat}$, sea B_n el intervalo $0..n$. Nótese que $B_0 \subseteq X^c$, porque $B_0=\{0\}$ y $0 \notin X$ porque, de lo contrario, 0 sería un primer elemento para X. Más aún, si $B_n \subseteq X^c$, entonces $n+1 \in X^c$ porque, en otro caso, $n+1 \in X$ y $n+1 \leq x$ para todos los elementos de X, de modo que $x+1$ sería un primer elemento.
Sea $C = \{n:\mathbf{nat} \mid B_n \subseteq X^c\}$. Por la anterior discusión, $0 \in C$ y, si $n \in C$, también $n+1 \in C$. Por el Axioma e, $C = \mathbf{nat}$. Sea $B = (\cup n:\mathbf{nat} \mid: X^c \cap B_n)$. Entonces, $B = X^c \cap (\cup n:\mathbf{nat} \mid: B_n) = X^c \cap \mathbf{nat} = X^c$. Por otro lado, $X^c \cap B_n = B_n$, ya que $C=\mathbf{nat}$. Por tanto: $B = (\cup n:\mathbf{nat} \mid: B_n) = \mathbf{nat}$. Es decir, $X^c = \mathbf{nat}$ y, consecuentemente, $X=\emptyset$. Como esto sería una contradicción, X debe tener un primer elemento.

3 Muestre que $(\mathbf{nat},<)$ es un conjunto bien ordenado.
Hay que mostrar que $(\mathbf{nat},<)$ es un conjunto ordenado ($<$ es irreflexiva y transitiva) en el que no pueden darse cadenas descendentes infinitas. Para esto último, si hubiera una cadena descendente infinita de la forma $x_0>x_1>\ldots>x_k>\ldots$ los elementos de la cadena formarían un conjunto que debería tener un primer elemento, que sería menor que todos los de la cadena. Si este elemento fuera x_k, se tendría la contradicción de que $x_k>x_{k+1}$, por ser cadena descendente, pero $x_k \leq x_{k+1}$ por ser x_k primer elemento.

Ejercicios 7.1

1 **Teorema 7.1.A**

1 $a|b \Rightarrow a|b*c$
Dem:
Hip: $a*d=b$
$b*c$
$=$ ⟨Hip: $a*d=b$⟩
$a*(d*c)$
$\Rightarrow$ ⟨Def $|$⟩
$a|b*c$

2 $a|b \wedge b|c \Rightarrow a|c$
Dem:

```
Hip: a*d=b, b*e=c
  c
=    ⟨Hip: b*e=c⟩
  b*e
=    ⟨Hip: a*d=b⟩
  a*(d*e)
⇒    ⟨Def |⟩
  a|c
```

3 $a|b \wedge a|c \Rightarrow a|(m*b + n*c)$

Dem:

```
Lema: m*b + n*c = a*(m*d + n*c)
Hip: a*d=b, a*e=c
  m*b + n*c
=    ⟨Hip: a*d=b ∧ a*e=c⟩
  m*a*d + n*a*e
=    ⟨Distr. */+⟩
  a*(m*d + n*c)
```

Ahora, por el lema

```
  m*b + n*c = a*(m*d + n*c)
⇒    ⟨Def |⟩
  a|(m*b + nc)
```

4 $c \neq 0 \Rightarrow (c*a|c*b \equiv a|b)$

Dem:

```
Hip: c≠0
  c*a|c*b
=    ⟨Def. |⟩
  (∃d|: c*a*d=c*b)
=    ⟨Hip: c≠0; aritmética⟩
  (∃d|: a*d=b)
=    ⟨Def. |⟩
  a|b
```

5 $a|b \wedge a>0 \wedge b>0 \Rightarrow a \leq b$

Dem:

(Esta demostración usa propiedades de aritmética supuestamente conocidas).

```
Hip: a|b, a>0, b>0
  true
=    ⟨Hip: a|b⟩
  b=a*d
⇒    ⟨Hip: a>0, b>0; aritmética⟩
  1≤d
```

Ahora:

```
  a = a*d/d = b/d ≤ b
```

2 Sea $\mathbf{nat}^+ = \mathbf{nat} \setminus \{0\}$. Muestre que $(\mathbf{nat}^+, |)$ es un orden parcial.

Hay que mostrar que $|$ es una relación reflexiva, transitiva y antisimétrica.

Reflexividad:

```
  a|a
⇐    ⟨Def |⟩
  a*1=a
=    ⟨aritmética⟩
```

`true`

Transitividad: Teorema 7.1.A.2.
Antisimetría: Teorema 7.1.A.5.

Ejercicios 7.2

1 Indique en dónde se usa, en la demostración del Teorema 7.2.A, la hipótesis de que `d>0`.
Observe que `r = (min k:int| 0≤n-k*d: n-k*d)`. Si `d=0`, se tendrá que `r=(min k:int| 0≤n: n) = n`. En ese caso, `q` puede ser cualquier entero, ya que `n = q*0 + r`. Enseguida se requiere que `d≠0` para mostrar que `0≤r<d`.

2 Si en el algoritmo que se da para construir el cociente y el residuo de una división entera cuestan `1` las asignaciones, ¿cuánto cuesta ejecutar el algoritmo en el caso general?
Si el dividendo es `n≥0` y el divisor es `d>0`, el algoritmo efectúa `2+2*q` asignaciones (`2` antes del ciclo y `2` por cada iteración en el ciclo, con `q` iteraciones). Es decir, en términos de los datos iniciales, hay `2+2*(n÷d)` asignaciones.

Ejercicios 7.3

1 Para las siguientes parejas de números `p` y `q`, encuentre `mcd(p,q)` y números `n` y `m` tales que: `mcd(p,q)=n*p + m*q`
a `mcd(20,19) = 1; n=1, m=-1.`
b `mcd(121,99) = 11; n=-4, m=5`
c `mcd(333,153) = 9; n=6, m=-13`
d `mcd(741,299) = 13; n=-2, m=5`
e `mcd(975,630) = 15; n=11, m=-17`

2 Muestre que: `y>0 ⇒ mcd(x,y) = mcd(y,x mod y)`. Use este resultado para mostrar que el invariante se mantiene en el Algoritmo de Euclides que usa divisiones.
Dem: Por el algoritmo de la división: `x = y*(x÷y) + (x mod y)`. Si `d|x` y `d|y` entonces `d|y` y `d|(x mod y)` y también vale en la dirección contraria. Entonces `mcd(x,y) = mcd(y,x mod y)`.
El cuerpo del Algoritmo de Euclides con divisiones hace, precisamente, esta operación de cambiar `(x,y)` por `(y,x mod y)`, por lo que el invariante se mantiene.

3 En la versión del Algoritmo de Euclides, incluya en el invariante una variable `t` que guarde el valor de la pareja `(x,y)`. Considere el orden lexicográfico sobre $\mathbf{nat}^+ \times \mathbf{nat}^+$ definido a partir del orden estricto $(\mathbf{nat}^+, |)$ (cf. Ejercicio 7.1.2). Muestre que, en cada iteración, `t` cambia a un valor `t'` tal que $t' <_{lex} t$. ¿Cómo puede usarse esta observación para argumentar la terminación de los algoritmos?

Se entra a iterar con `t=(x,y)` y se sale con `t'=(x',y')`.

En el algoritmo de restas:
Si `x>y`: $t'=(x',y') = (x-y,y) <_{lex} (x,y) = t$.
Si `x<y`: $t'=(x',y') = (x,y-x) <_{lex} (x,y) = t$.
El programa progresa pasando por una secuencia de estados para los que `t` va descendiendo estrictamente en cada iteración. El proceso debe terminar, porque el orden lexicográfico en cuestión no permite cadenas descendentes infinitas, i.e., es un orden bien fundado.

En la versión de divisiones, si `b<c`, la primera iteración invierte los valores de `(x,y)` a `(y,x)`. En cualquier caso se puede suponer que `x≥y` de un momento en adelante (primera o segunda iteración). En este caso la primera componente cambia de `(x,y)` a `(y,x mod y)`, con `x≥y`. Si `x=y`, el estado

después de la iteración es $(y,0)$, de modo que $(x,y) >_{lex} (y,0)$. Si $x>y$, el estado cambia a $(y, x \bmod y)$ y también $(x,y) >_{lex} (y, x \bmod y)$.

Ejercicios 7.4

⟨No se incluyen soluciones⟩

Ejercicios 7.5

1

d Nótese que $10 \equiv_2 0$. Usando repetidamente propiedades de las congruencias, se muestra que $10^k \equiv_2 0$, para k, $0<k<r$. También: $d_k * 10^k \equiv_2 0$, $0<k<r$. Por tanto:

$$
\begin{aligned}
& n \\
= & \\
& (+k \mid 0 \le k < r : d_k * 10^k) \\
= & \\
& d_0 + (+k \mid 0 < k < r : d_k * 10^k) \\
\equiv_2 & \\
& d_0 + (+k \mid 0 \le k < r : 0) \\
= & \\
& d_0
\end{aligned}
$$

2 Utilice los resultados de **1** para decidir si las siguientes afirmaciones son ciertas o falsas:

a $11 \mid 121121$. Verdadero: $11 \mid (1+1+2-2-1-1)$
b $9 \mid 123456789$. Verdadero: $9 \mid (1+2+3+4+5+6+7+8+9)$
c $2 \mid 1465413$. Falso: $\neg(2 \mid 3)$
d $5 \mid 1231230$. Verdadero: $5 \mid 0$
e $9 \mid 364234$. Falso: $\neg(9 \mid (3+6+4+2+3+4)$
f $9 \mid 364239$. Verdadero: $9 \mid (3+6+4+2+3+9)$
g $11 \mid 3454$. Verdadero: $11 \mid (3+5-4-4)$
h $11 \mid 204081$. Falso: $\neg(11 \mid (1+0+0-8-4-2)$.

3 Calcule las siguientes expresiones (recuerde que $n \bmod d$ es el residuo de la división entera $n \div d$):

a $5^{422} \bmod 7$
Por el Teorema de Fermat (7 primo que no divide a 5): $5^6 \equiv_7 1$. Como $422 = 6*70+2$, se tiene que $5^{422} \equiv_7 5^2 \equiv_7 4$.

b $5^{422} \bmod 8$
Por el Teorema de Euler (8 y 5 primos relativos): $5^{\varphi(8)} \equiv_8 1$. Ahora: $\varphi(8)=8*(1-1/2)=4$. Así: $5^4 \equiv_8 1$. Como $422 = 4*55+2$, se tiene que $5^{422} \equiv_8 5^2 \equiv_8 1$.

4

a

$$
\begin{aligned}
& 9*x \equiv_7 12 \\
\equiv & \quad \langle 2 \equiv_7 9,\ 12 \equiv_7 5 \rangle \\
& 2*x \equiv_7 5
\end{aligned}
$$

Usando el método sugerido en el texto: $x \equiv_7 2^{6-1}*5 \equiv_7 160 \equiv_7 6$.

1 Para $a,b \in \mathbf{z}_n$ muestre que $a +_n b \equiv_n a+b$.

Dem:

Sean q_a, r_a, q_b, r_b tales que $a = q_a*n+r_a$, $b = q_b*n+r_b$, con $0 \le r_a, r_b < n$. Es decir, $a \equiv_n r_a$ y $b \equiv_n r_b$. Ahora: $a+b = (q_a+q_b)*n+(r_a+r_b)$, con $0 \le r_a+r_b < 2*n$.

Si $0 \le r_a+r_b < n$, se tiene que: $a +_n b \equiv_n r_a+r_b \equiv_n a+b$.

Si $n \le r_a+r_b < 2*n$, entonces $0 \le r_a+r_b-n < n$ y, por tanto $a +_n b \equiv_n r_a+r_b-n \equiv_n r_a+r_b \equiv_n a+b$.

2 Pruebe que $(\mathbf{z}_n, +_n, 0)$ es un grupo abeliano.

$\mathbf{z}_n = 0..n-1$.

Para $x,y \in \mathbf{z}_n$: $x +_n y \equiv_n (x+y)$.

(i) Como se sabe que hay un r único, $0 \le r < n$, tal que $r \equiv_n x+y$, $+_n$ *es una operación cerrada en* $\mathbf{z}_n$.

(ii) $+_n$ *es asociativa*:

$$
\begin{array}{ll}
 & x +_n (y +_n z) \\
\equiv_n & \quad \langle\ a +_n b \equiv_n a + b\ \rangle \\
 & x +_n (y + z) \\
\equiv_n & \quad \langle\ a +_n b \equiv_n a + b\ \rangle \\
 & x + (y + z) \\
\equiv_n & \quad \langle + \text{ asociatividad} \rangle \\
 & (x + y) + z \\
\equiv_n & \quad \langle\ a +_n b \equiv_n a + b\ \rangle \\
 & (x + y) +_n z \\
\equiv_n & \quad \langle\ a +_n b \equiv_n a + b\ \rangle \\
 & (x +_n y) +_n z
\end{array}
$$

(iii) Hay un elemento neutro.

$$
\begin{array}{ll}
 & x +_n 0 \\
\equiv_n & \quad \langle\ a +_n b \equiv_n a + b\ \rangle \\
 & x+0 \\
= & \\
 & x
\end{array}
$$

(iv) $+_n$ *es conmutativa*:

$$
\begin{array}{ll}
 & x +_n y \\
\equiv_n & \quad \langle\ a +_n b \equiv_n a + b\ \rangle \\
 & x + y \\
= & \\
 & y + x \\
\equiv_n & \quad \langle\ a +_n b \equiv_n a + b\ \rangle \\
 & y +_n x
\end{array}
$$

(v) Hay *inversos*: Sea $x \in Z_n$. Entonces, $0 \le x < n$. Sea $y \equiv_n n-x$. Claramente, $0 \le y < n$. Además, $x+y \equiv_n x+(n-x) \equiv_n n \equiv_n 0$. Por tanto, $x +_n (n-x) = 0$.

4 En $(\mathbf{z}_{13}^*, *_{13}, 1)$ determine los inversos de cada uno de los elementos en $\mathbf{z}_{13}^*$.

Sea x^{-1} el inverso de x en $\mathbf{z}_{13}^*$. Entonces:

$1^{-1}= 1$	$2^{-1}= 7$	$3^{-1}= 9$	$4^{-1}= 10$
$5^{-1}= 8$	$6^{-1}= 11$	$7^{-1}= 2$	$8^{-1}= 5$
$9^{-1}= 3$	$10^{-1}= 4$	$11^{-1}= 6$	$12^{-1}= 12$