Instrucciones

Fecha de entrega: 25 de febrero 2019.
Nota: Toda tarea escrita a LaTeX tendrá un ejericio "gratis" de su elección; este ejercicio gratis no es obligatorio y puntúa como un ejericio correctamente resuelto.

1 Divisibilidad

Ejercicio 1.1. Definimos la siguiente relación:

$$a \preccurlyeq b \quad \overset{\text{def}}{\iff} \quad a \mid b.$$

Prueba que $\preccurlyeq$ es un orden parcial sobre $\mathbb{Z}^+ = \{1, 2, \ldots\}$, es decir que $(\mathbb{Z}^+, \preccurlyeq)$. Explica porqué no es un orden parcial sobre $\mathbb{Z}$.

Ejercicio 1.2. Sobre las unidades de un anillo:

a. Sea A un anillo conmutativo con 1 y $U(A) = \{u \in A \mid \exists v \in A \text{ tal que } uv = 1\}$ su conjunto de unidades. Definimos la siguiente relación:

$$a \sim b \quad \overset{\text{def}}{\iff} \quad \exists u \in U(A) \text{ tal que } a = ub$$

Prueba que $\sim$ es una relación de equivalencia. Si $a \sim b$, decimos que a y b son *asociados*. ¿Qué conjunto es el espacio cociente $\mathbb{Z}/_\sim$?

b. Sea $p \in \mathbb{Z}$ un número primo. Prueba que $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ es un anillo con las operaciones usuales de $\mathbb{Q}$ y describe el conjunto $U(\mathbb{Z}_{(p)})$.

c. Prueba que cuales quiera dos elementos primos de $\mathbb{Z}_{(p)}$ son asociados (un elemento q en cualquier anillo conmutativo con 1 es primo si no es una unidad y además cumple que $q \mid ab \implies q \mid a$ ó $q \mid b$).

d. Prueba que si $\frac{a}{b} \in \mathbb{Z}_{(p)}$ no es una unidad, entonces $\frac{a}{b} + 1 \in U(\mathbb{Z}_{(p)})$. Explica porque la prueba de Euclides de la infinitud de los números primos falla para $\mathbb{Z}_{(p)}$.

Ejercicio 1.3. Sean $a, b, c \in \mathbb{Z}$. Prueba las siguientes propiedades:

a. $a \mid b \implies ac \mid bc$ para toda $c \in \mathbb{Z}$ y si $c \neq 0$, entonces $ac \mid bc \implies a \mid b$.

b. Si $a \mid a'$ y $b \mid b'$, entonces $ab \mid a'b'$.

c. Si $a \mid c$, $b \mid c$ y $(a, b) = 1$, entonces $ab \mid c$. Muestra un contraejemplo de esta propiedad si $(a, b) > 1$.

d. $(a + n, n) \mid n$ para toda $n \in \mathbb{Z}$.

e. Si $(a, b) = 1$ entonces $(a + b, a - b) = 1$ ó 2.

f. $(a + tb, b) = (a, b)$ para toda $t \in \mathbb{Z}$.

g. Si $a' \mid a$, $b' \mid b$ y $(a, b) = 1$ entonces $(a', b') = 1$. En palabras esto es: si a y b son primos relativos, entonces sus divisores son primos relativos entre ellos.

h. Si $(a, b) = d$ entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

i. Si $(a, b) = 1 = (a, c)$, entonces $(a, bc) = 1$.

j. Sea $a_0, a_1, a_2, \ldots$ la sucesión de Fermat 1,1,2,3,5.... definida recursivamente como $a_{n+1} := a_n + a_{n-1}$ donde $a_0 = 1 = a_1$. Prueba que $(a_n, a_{n+1}) = 1$ para toda n.

Ejercicio 1.4. Un *mínimo común múltiplo* de dos enteros $a, b \in \mathbb{Z}$ se define como un entero $m > 0$ que cumple las siguientes dos propiedades:

(•) $a \mid m$ y $b \mid m$.

(••) Si $m' \in \mathbb{Z}$ es tal que $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$.

Fija $a, b, c \in \mathbb{Z}$. Prueba las siguientes propiedades del mínimo común múltiplo (mcm):

a. Prueba que el mcm de a, b es único; gracias a esto lo denotamos por $[a, b]$.

b. $[ab, ac] = a[b, c]$

c. $(a, b) = [a, b] \implies a = b$

d. $ab = (a, b)[a, b]$

e. $(a + b, [a, b]) = (a, b)$

Ejercicio 1.5. Sean $a \in \mathbb{Z}$ y $d \in \mathbb{Z}^+$ fijos y considera el sistema de ecuaciones

$$(\star) \begin{cases} (x, y) = d \\ xy = a \end{cases}$$

Prueba que $(\star)$ tiene una solución $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ si y solamente si $d^2 \mid a$.

Ejercicio 1.6. Sea D_n el conjunto de divisores positivos de n, ie. $D_n = \{d > 0 : d \mid n\}$. Ahora sea $F : D_a \times D_b \to D_{ab}$ la función definida por $F(d, d') = dd'$. Prueba que si $(a, b) = 1$, entonces F es una función bien definida y que es biyectiva. Si $(a, b) > 1$, ¿deja de ser biyectiva la función? Explica tu respuesta.

Ejercicio 1.7. Sean $n, m, x, y \in \mathbb{Z}$ fijos tales que $n = ax + by$ y $m = cx + dy$ para algunas $a, b, c, d \in \mathbb{Z}$. Si $ad - bc = \pm 1$, prueba que $(n, m) = (x, y)$.

Ejercicio 1.8. Fija tres enteros $a, b, c \in \mathbb{Z}$. Prueba que la ecuación $ax + by = c$ tiene solución si y solamente si $(a, b) \mid c$. Además, si (x_0, y_0) es una solución ¿de qué forma son el resto de las soluciones?

Ejercicio 1.9. Prueba que todo entero mayor que 6 se puede expresar como suma de dos enteros primos relativos.

$(*)$**Ejercicio 1.10.** Demuestra que para todo $a > 1$ y exponentes $n, m > 0$ se cumple que $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.

$(*)$**Ejercicio 1.11.** Los números armónicos no son enteros.

a. Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ fracciones irreducibles, es decir $(a, b) = 1 = (c, d)$. Prueba que

$$\frac{a}{b} + \frac{c}{d} \in \mathbb{Z} \quad \implies \quad b = \pm d.$$

b. Los número' armónicos H_n se definen como las sumas parciales de la serie armónica, es decir

$$H_n := \sum_{k=1}^{n} \frac{1}{k}.$$

Prueba que $H_n \notin \mathbb{Z}$ para toda $n > 1$.