Universidad Nacional Autónoma de México
Facultad de Ciencias
Teoría de los Números I

Tarea 1

Ángel Iván Gladín García
No. cuenta: 313112470
angelgladin@ciencias.unam.mx

25 de Febrero 2019

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 $\mathbb{Z}$.

<u>**Solución:**</u> Antes de empezar procederemos dando unas definiciones.

Definición 1. Un **orden parcial** es una relación binaria R sobre un conjunto X que es reflexiva, antisimétrica, y transitiva, es decir, para cualesquiera a, b, y c en X se tiene que:

a. aRa (reflexividad).

b. Si aRb y bRa, entonces $a = b$ (antisimetría).

c. Si aRb y bRc, entonces aRc (transitividad).

Definición 2. Sean $a, b \in \mathbb{Z}$, decimos que a **divide** a b si existe un entero $k \in \mathbb{Z}$ tal que $b = ak$.

$$a \mid b \quad \overset{\text{def}}{\iff} \quad \exists k \in \mathbb{Z} \ni b = ak$$

Por demostrar que $(\mathbb{Z}^+, \preccurlyeq)$. Para esto hay que probar las tres propiedades descritas anteriormente.

- <u>Reflexividad</u>. Sea $a \in \mathbb{Z}$, por demostrar que $a \preccurlyeq a$. Por definición se tiene que $\exists k \in \mathbb{Z} \ni a = ak$ y k debe ser una unidad en $\mathbb{Z}$ por lo que $a1 = a$. Por tanto $a \preccurlyeq a$.

- <u>Antisimetría</u>. Sean $a, b \in \mathbb{Z}$. Si $a \preccurlyeq b$ y $b \preccurlyeq a$ por demostrar que $a = b$. Por definición de $\preccurlyeq$ tenemos que $\exists p \in \mathbb{Z} \ni b = ap$ y $\exists q \in \mathbb{Z} \ni a = bq$ entonces sustituyendo a tenemos que $b = (bq)p$, asociando $b = b(qp)$, entonces $qp = 1$. Por tanto $a = b$.

- <u>Transitividad</u>. Sean $a, b, c \in \mathbb{Z}$. Si $a \preccurlyeq b$ y $b \preccurlyeq c$ por demostrar que $a \preccurlyeq c$. Por definición de $\preccurlyeq$ tenemos que $\exists p \in \mathbb{Z} \ni b = ap$ y $\exists q \in \mathbb{Z} \ni c = bq$, sustituyendo b tenemos que $c = (ap)q$, asociando $c = a(pq)$. Por tanto $a \preccurlyeq b$.

Ahora bien $(\mathbb{Z}, \preccurlyeq)$ no es un orden parcial porque no cumple la antisimetría y se dará un contraejemplo. Sean $a, b \in \mathbb{Z}$. Si $a \preccurlyeq b$ y $b \preccurlyeq a$. Por definición de $\preccurlyeq$ tenemos que $\exists p \in \mathbb{Z} \ni b = ap$ y $\exists q \in \mathbb{Z} \ni b = aq$ pero si tomamos a $a = 1$ y $b = -1$ (s.p.d.g), no se cumple $\preccurlyeq$ porque $a \neq b$.

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:

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

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 $\mathbb{Z}/_\sim$?
<u>Solución</u>: TODO

b. Sea $p \in \mathbb{Z}$ un número primo. Prueba que $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \not| \ b\}$ es un anillo con las operaciones usuales de $\mathbb{Q}$ y describe el conjunto $U(\mathbb{Z}_{(p)})$.
<u>Solución</u>: TODO

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 $q \mid ab \Longrightarrow q \mid a$ ó $q \mid b$).
<u>Solución</u>: TODO

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 $\mathbb{Z}_{(p)}$.
<u>Solución</u>: TODO

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

a. $a \mid b \Longrightarrow ac \mid bc$ para toda $c \in \mathbb{Z}$ y si $c \neq 0$, entonces $ac \mid bc \Longrightarrow a \mid b$.
<u>Solución</u>: Como por hipótesis y aplicando la definición de divisibilidad tenemos que $\exists p, q$ tales que si $ap = b$ entonces $acq = bc$. Entonces basta con dividir $acq = bc$ entres c ya que es un factor común teniendo $\frac{acq}{c} = \frac{bc}{c}$, teniendo entonces $aq = b$. Por tanto $a \mid b$

b. Si $a \mid a'$ y $b \mid b'$, entonces $ab \mid a'b'$.
<u>Solución</u>: Basta escribir a $a \mid a'$ y $b \mid b'$, usando la definición de divisibilidad tenemos entonces $p, q \in \mathbb{Z}$ tal que $ap = a'$ y $bq = b'$. Multiplicando ambas igualdades tenemos que $apbq = a'b'$ y asociando $ab(pq) = a'b'$. Por tanto $ab \mid a'b'$.

c. Si $a \mid c$, $b \mid c$ y $(a, b) = 1$, entonces $ab \mid c$. Muestra un contraejemplo de esta propiedad si $(a, b) > 1$.
<u>Solución</u>: Tomando $a = 2$, $b = 4$ y $c = 4$. Porque $(a, b) = (2, 4) = 2$ y tenemos que $2 \mid 4$ y $4 \mid 4$, pero no se cumple $ab \mid c$ ya que $8 \nmid 4$.

d. $(a + n, n) \mid n$ para toda $n \in \mathbb{Z}$.
<u>Solución</u>: Sabemos por un teorema, que el máximo común divisor de dos números cualesquiera puede ser expresado como la mínima combinación lineal. Sabiendo éso, podemos expresar a $(a + n, n) = d$ como $p(a + n) + qn = d$ con $p, q \in \mathbb{Z}$. Ahora bien, por el inciso h) sabemos que si $(a, b) = d$, entonces $(\frac{a}{d}, \frac{b}{d}) = 1$. Aplicando el resultado previo, tenemos que $(\frac{a+n}{d}, \frac{n}{d}) = 1$, reescribiendo como combinación lineal se tiene que $r\frac{a+n}{d} + s\frac{n}{d} = 1$ para algún $r, s \in \mathbb{Z}$, multiplicando ambos lados por n se tiene $nr\frac{a+n}{d} + ns\frac{n}{d} = n$ y factorizando n tenemos $n(r\frac{a+n}{d} + s\frac{n}{d}) = n$, lo que implica que $(r\frac{a+n}{d} + s\frac{n}{d}) = 1$. Por tanto, aplicando la definición de divisibilidad se tiene que $(a + n, n) \mid n$.

e. Si $(a, b) = 1$ entonces $(a + b, a - b) = 1$ ó 2.
Solución: Si $(a, b) = d$ por definición se tiene que $d \mid a$ y $d \mid b$. Entonces regresando a la expresión a probar se tiene que $d \mid a + b, a - b$, si tomamos la suma y diferencia de ambos términos tenemos que $d \mid (a+b)+(a-b) = 2a$ y $d \mid (a+b)(a-b) = 2b$, teniedo entonces que $d \mid (2a, 2b) = 2(a, b) = 2$. Ergo $d = 1$ o $d = 2$.

f. $(a + tb, b) = (a, b)$ para toda $t \in \mathbb{Z}$.
Solución: Sabemos que podemos expresar a $(a, b) = d$ como la menor combinación lineal positiva. Entonces expresamos a $(a + tb, b) = d$ como dicha combinación teniendo entonces $(a + tb)m + bn = d$ con $m, n \in \mathbb{Z}$, expandiendo el producto y asociando tenemos $am + (tm + n)b = d$ y por otro lado tenemos que $ap' + bq' = d$. Por tanto, podemos expresar a ambos $(a+tb, b)$ y (a, b) como la menor combinación lineal positiva y ambos tienen el mismo máximo común divisor. Ergo $(a + tb, b) = (a, b)$ 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.
Solución: TODO

h. Si $(a, b) = d$ entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
Solución: Sea $\left(\frac{a}{d}, \frac{b}{d}\right) = d'$. Por demostrar que $d' = 1$. Como d' es un factor común de $\frac{a}{d}$ y de $\frac{b}{d}$, entonces $\exists l, m$ tales que $\frac{a}{d} = ld'$ y $\frac{b}{d} = md'$. Entonces $a = ldd'$ y $b = mdd'$, entonces dd' es un factor común de a y b. Entonces, por definición de máximo común divisor tenemos que $dd' \leq d$, entonces $d' = 1$. Por tanto d' es un entero positivo tal que $d' = 1$. Ergo si $(a, b) = d$ entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

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

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.
Solución: TODO

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:

($\bullet$) $a \mid m$ y $b \mid m$.

($\bullet\bullet$) 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 $[a, b]$.
Solución: Prueba por unicidad y existencia.
Empecemos por suponer $n, m \in \mathbb{Z}$ que satisfacen ($\bullet$) y ($\bullet\bullet$). Como m es un m.c.d. de a y b y como n satisface ($\bullet\bullet$) entonces $n \mid m$. Sin perdida de generalidad, intercambiamos las variables y tenemos que $m \mid n$. Lo que implica que si $n \mid m$ y $m \mid n$, entonces $n = m$ y con esto hemos provado la unicidad.
Para provar la existencia, denotaremos a $S = x \in \mathbb{N} : a \mid x \wedge b \mid x$. Por el principio del buen orden se tiene que S tiene un elemento mínimo m. Por tanto tenemos que $a \mid m$ y $b \mid m$, con ésto hemos provado ($\bullet$). Para probar ($\bullet\bullet$) denotaremos a $x \in \mathbb{Z}$ tal que $a \mid x \wedge b \mid x$. Por el

algorítmo de la división tenemos que $\exists! q, r \in \mathbb{Z}$ tal que $x = mq + r, \quad 0 < r \leq m$. Dado que $a \mid x$ y $a \mid x$ entonces $x = aq_1$ para algún $q_1 \in \mathbb{Z}$. Como $a \mid m$ entonces por definición $m = aq_2$ para alguna $q_2 \in \mathbb{Z}$. Se sigue que $aq_1 = aq_2 + r$ y reescribiendo $a(q_1 - q_2) = r$. Lo que implica que $a \mid r$ (por definición). Si $r > 0$ entonces $r \in S$ y contradice la definición de m. Ergo $r = 0$. Para b la prueba es totalmente análoga.

b. $[ab, ac] = a[b, c]$
<u>Solución</u>: TODO

c. $(a, b) = [a, b]$ $enta = b$
<u>Solución</u>: Tenemos por el inciso $d)$ que $[a, b] = \frac{ab}{(a,b)}$. Sabiendo eso, rescribiremos al m.c.m. como $[a, b] = \frac{ab}{(a,b)}$ pero por hipótesis se tiene que $(a, b) = [a, b]$, sustituyendo $[a, b]$ se tiene que $(a, b) = \frac{ab}{(a,b)}$, despejando se sigue que $(a, b)^2 = ab \iff a = b$ porque ab tiene que ser cuadrado.

d. $ab = (a, b)[a, b]$
<u>Solución</u>: Antes de probarlo, enunciaremos los siguiente Lemas. Sean a y b dos enteros positivos expresaremos al m.c.m y m.c.d. con la siguiente descomposición canónica.

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \quad \wedge \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \ni a_i, b_i \geq 0$$

(Asumimos que ambas descomposiciones contienen exactamente las mismas bases primas p_i). Entonces podemos expresar al m.c.m y m.c.d como .

$$[a, b] = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \cdots p_n^{max(a_n,b_n)}$$

$$(a, b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \cdots p_n^{min(a_n,b_n)}$$

Ahora bien, teniendo los lema anteriores procederemos con la demostración.
Tenemos que $ab = (a, b)[a, b]$, reacomodando tenemos demostrar que $[a, b] = \frac{ab}{(a,b)}$. Sea $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ y $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{bn}$ la descomposición canónica de a y b. Entonces tenemos

$$[a, b] = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \cdots p_n^{max(a_n,b_n)}$$

y

$$(a, b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \cdots p_n^{min(a_n,b_n)}$$

Por consiguiente,

$$\begin{aligned}
(a, b)[a, b] &= p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \cdots p_n^{min(a_n,b_n)} \cdot p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \cdots p_n^{max(a_n,b_n)} \\
&= p_1^{min(a_1,b_1)+max(a_1,b_1)} \cdots p_n^{max(a_n,b_n)+max(a_n,b_n)} \\
&= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n} \\
&= (p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})(p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}) \\
&= ab
\end{aligned}$$

Ergo $[a, b] = \frac{ab}{(a,b)} \iff ab = (a, b)[a, b]$

e. $(a + b, [a, b]) = (a, b)$
<u>Solución</u>: TODO

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 $d^2 \mid a$.
<u>**Solución:**</u> $\Longrightarrow$) Por demostrar que $d^2 \mid a$. Tomando $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ como una solución particular de la forma $x_0 = d$ y $y_0 = \frac{a}{d}$, de esta forma se satisface en la segunda ec. que:

$$d\frac{a}{d} = a \quad a = a$$

Por definición de divisivilidad $\exists k \in \mathbb{Z} \ni d^2k = a$ y escibiendo a como (x, y) como combinación lineal de la forma $xs + yt = d$ p.a. $s, t \in \mathbb{Z}$ se sigue que:

$$\begin{aligned}
a &= kd^2 \\
&= k(xs + yt)^2 && \text{(Sutituyendo } d = xs + yt) \\
&= k(ds + \frac{a}{d}t)^2 && \text{(Reescribiendo } x = d \text{ y } y = \frac{a}{d}) \\
&= k(d^2s^2 + 2ds\frac{a}{d}t + \frac{a^2}{d^2}t) && \text{(Expandiendo el binomio)} \\
&= k(d^2s^2 + 2ds\frac{xy}{d}t + \frac{a^2}{d^2}t^2) && \text{(Reescribiendo } a = xy) \\
&= k(d^2s^2 + 2ds\frac{dy}{d}t + \frac{a^2}{d^2}t^2) && \text{(Reescribiendo } x = y) \\
&= k(d^2s^2 + d^2\frac{2syt}{d} + \frac{a^2}{d^2}t^2) && \text{(Asociando y conmutando)} \\
&= k(d^2s^2 + d^2\frac{2syt}{d} + \frac{x^2y^2}{d^2}t^2) && \text{(Reescribiendo } a = xy) \\
&= k(d^2s^2 + d^2\frac{2syt}{d} + d^2\frac{y^2t^2}{d^2}) && \text{(Reescribiendo } x = d \text{ y asociando)} \\
&= kd^2(s^2 + \frac{2syt}{d} + \frac{y^2t^2}{d^2}) && \text{(Factorizando } d^2) \\
&= m'd^2 && \text{Sea } m' = k(s^2 + \frac{2syt}{d} + \frac{y^2t^2}{d^2})
\end{aligned}$$

Por definición de divisivilidad, ergo $d^2 \mid a$.
$\Longleftarrow$) Por demostrar que $(\star)$ tiene una solución $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$. Como $d^2 \mid a$ entonces $d^2p = a$ para alguna $p \in \mathbb{Z}$. Entonces tiene solucion

$$\begin{aligned}
&\Longleftrightarrow xy = d^2p \\
&\Longleftrightarrow d^2p = a \\
&\Longleftrightarrow x = d^2 \wedge y = \frac{a}{d^2} \\
&\Longleftrightarrow p = y = \frac{a}{d^2}
\end{aligned}$$

Por tanto, $(\star)$ tiene una solución $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$.

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.
Solución: TODO

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 $(m, n) = (x, y)$.
Solución: Sea $d = (m, n)$, entonces podemos expresar a d como $d = sn + tm$ p.a. $s, t \in \mathbb{Z}$, sea $d' = (x, y)$. Como por hipótesis dejamos fijos $n = ax + by$ y $m = cx + dy$, entonces $d = s(ax + by) + t(cx + dy) = sax + sby + tcx + tdy = x(sa + tc) + y(sb + td)$. Por tanto se sigue que $d \mid d'$ porque tanto d y d' se pueden expresar como combinaciones lineales en términos de x y y. Una transformación lineal por $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ es invertible si $\Delta \neq 0$, pero como por hipótesis se tiene que $ad - bc = \pm 1$, entonces podemos escribir a x y y como combinaciones lineales de m y n, entonces se sigue que $x = dm - bn$ y $y = -cm + an$. $\exists p, q \ni px + qy = d'$. Se tiene que:

$$\begin{aligned} d' &= px + qy \\ &= p(dm - bn) + q(-cm + an) \\ &= m(pd - qc) + n(-qb + qa) \end{aligned}$$

Por tanto, se tiene que $d' \mid d$.
Si $(m, n) \mid (x, y)$ y $(x, y) \mid (m, n)$, (como el máximo común divisor es positivo) entonces $(m, n) = (x, y)$.

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?
Solución: $\Rightarrow$) TODO

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

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

($*$)**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

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

Solución: TODO

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 $n > 1$.
Solución: TODO

Referencias

[1] Notas tomadas en clase del curso de Teoría de los Números I (2019-2).

[2] Thomas Koshy. *Elementary Number Theory with Applications. 2nd Edition.* Addison-Wesley, Reading, Massachusetts, 1993. Academic Press. 8th May 2007.

[3] Apostol, Tom M. *Introduction to Analytic Number Theory.* Springer-Verlag, New York, 1976.