This is a reprint of the paper
¿Cuándo son dos números primos entre sí?
by Ricardo Palacios
published in **Lecturas Matemáticas**
15 (1994), pp. 221–226

¿CUÁNDO SON DOS NÚMEROS PRIMOS ENTRE SÍ?

Ricardo Palacios*

Universidad Nacional de Colombia, Bogotá

Abstract. Different characterizations of 'two elements being relatively prime' are examined and connections between them are established in general domains and in principal and factorial domains.

Resumen. Se examinan caracterizaciones diferentes de la propiedad 'ser primos entre sí' y se establecen conexiones entre ellas en el contexto de dominios generales, de los anillos principales y de los anillos factoriales.

La idea central de esta nota es la de recoger las diferentes caracterizaciones encontradas en la literatura de la noción de *coprimalidad* en el anillo $\mathbb{Z}$ de los números enteros y estudiar sus eventuales equivalencias en el marco general de los dominios de integridad unitarios. Al final de la nota y como consecuencia de este estudio establecemos que $\mathbb{Z}[X]$ y $K[X_1, X_2, ..., X_n]$ $(n \geq 2)$, donde K es un cuerpo conmutativo, no son anillos principales y, por tanto, tampoco euclídeos para ningún algoritmo.

En un dominio de integridad arbitrario A podemos definir la siguiente relacion, conocida como la *relación de divisibilidad*: Dados a y b en A, $a \mid b$ si existe $x \in A$ tal que $b = ax$. En tal caso, $a \mid b$ se lee *a divide a b*, o, *a es un divisor de b*. Esta es una relación de *pre–orden*, es decir, satisface las condiciones

(i) $a \mid a$ para todo $a \in A$,
(ii) si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

* El autor es estudiante de la carrera de Matemáticas en la Universidad Nacional de Colombia, Bogotá.

Los divisores del elemento $1 \in A$ se denominan las *unidades* de A. Si se tiene simultáneamente que $a \mid b$ y $b \mid a$, es fácil comprobar que existe una unidad u de A tal que $a = bu$, en cuyo caso diremos que a y b son *asociados* o que a y b *difieren* en una unidad.

Las siguientes son diferentes nociones de coprimalidad en un dominio de integridad unitario A, las cuales se pueden encontrar en las referencias [1] a [6] al final:

- (a) Dos elementos $a, b \in A \setminus \{0\}$ *no tienen divisores comunes* si todo divisor común u de a y b es una unidad de A. Para expresar esto se suele decir también que a y b son *débilmente coprimos* [2, pág. 140], [4].
- (b) a *es primo con* b si para todo $x \in A$ tal que $b \mid ax$ se tiene que $b \mid x$ [2, pág. 140].
- (c) a y b son *coprimos*, o primos relativos en el sentido de Bezout, si satisfacen una relación de Bezout, es decir, si existen x, $y \in A$ tales que $ax + by = 1$.
- (c') a y b son *comaximales* si $(a, b) = (a) + (b) = A$, donde (a), (b) y (a, b) son los ideales de A generados por a, b y $\{a, b\}$ respectivamente.
- (d) Dados $a, b \in A$, se dice que un elemento $d \in A$ es un *máximo común divisor* de a y b (lo que indicamos con $d = \mathrm{mcd}(a, b)$) si
  - (i) $d \mid a$ y $d \mid b$, y
  - (ii) si $e \mid a$ y $e \mid b$, entonces $e \mid d$.

Diremos entonces que a y b son *primos entre sí*, si su máximo común divisor, $\mathrm{mcd}(a, b)$, es una unidad de A. (Es fácil verificar que dos $\mathrm{mcd}(a, b)$ son *asociados*).

La caracterización (b) fue utilizada por Hasse en un trabajo muy interesante [3] en el que se considera establecer la factorialidad (ver adelante) de un dominio mediante la generalización de la noción de *algoritmo euclídeo.* Esta caractrización es aparentemente menos simétrica que las demás indicadas arriba, lo que ha conducido a algunos autores a afirmar que a puede ser primo con b sin que b lo sea con a [5, pág. 182]. Veamos, sin embargo, que éste no es el caso. En efecto, si a es primo con b entonces, para todo $x \in A$ tal que $b \mid ax$, tendremos que $b \mid x$. Supongamos ahora que $a \mid by$, es decir, que $by = ax$ para algún $x \in A$. Como $b \mid x$, tenemos que $x = bq$ para algún $q \in A$, así que $y = aq$; en consecuencia, a divide a y. Entonces, b es también primo con a.

Estableceremos ahora las relaciones existentes en un dominio de integridad unitario entre las diferentes caracterizaciones enunciadas arriba.

Proposición 1. *En cualquier dominio de integridad unitario A se tienen las siguientes implicacions y equivalencias:*

$$\begin{array}{ccccc} & & (b) & \Longrightarrow & (a) \\ & & \Uparrow & & \Updownarrow \\ (c') & \Longleftrightarrow & (c) & \Longrightarrow & (d) \end{array}$$

Demostración.

- $(b) \Rightarrow (a)$ Sea x un divisor común de a y b, de modo que existen $y, w \in A$ tales que $xy = a$, $xw = b$. Entonces $aw = xyw = by$, así que $b \mid aw$. Como por hipótesis a es primo con b, tendremos también que $bz = w$ para algún $z \in A$. Entonces $b = xw = b(zx)$, y, por consiguiente, $xz = 1$. Entonces, x es una unidad de A.

$(c) \Rightarrow$ (b) Supongamos que a y b satisfacen una relación de BEZOUT $ax + by = 1$, donde $x, y \in A$. Supongamos además que b divide a az, es decir, que $az = bw$ para algún $w \in A$. Entonces $z = z1 = (az)x + (bz)y = b[wx + zy]$, así que $b \mid z$. Se concluye que a es primo con b.

$(d) \Leftrightarrow$ (a) Supóngase que $\mathrm{mcd}(a, b) = u$ es una unidad de A, y sea x un divisor común de a y b. Como, por (ii), todo divisor común de a y b es un divisor de u, resulta que $u = xy$ para algún $y \in A$. Entonces $1 = u^{-1}u = (u^{-1}y)x$, y x es una unidad de A. Lo recíproco es claro, pues $\mathrm{mcd}(a, b)$ es una unidad de A cuando a y b no tienen divisores comunes.

$(c) \Rightarrow$ (d) Supongamos que a y b satisfacen una relación de BEZOUT $ax + by = 1$ y que e es un divisor común de a y b, de modo que $a = ez$ y $b = ew$, $z, w \in A$. Entonces $1 = (ez)x + (ew)y = e(xz + wy)$, y, por consiguiente, e es una unidad de A. Entonces, todo divisor común de a y b es una unidad. En particular, $\mathrm{mcd}(a, b)$ es una unidad.

$(c') \Leftrightarrow$ (c) Si $A = (a) + (b)$, existen $x, y \in A$ tales que $1 = ax + by$. Recíprocamente, si $1 = ax + by$ tenemos que $w = w.1 = (wx)a + (wy)b$ para todo $w \in A$, así que $A = (a) + (b)$. $\square$

Corolario 1. *Si el dominio de integridad unitario A es principal, todas las anteriores nociones de coprimalidad son equivalentes. En particular son equivalentes en $K[X]$, donde K es un cuerpo conmutativo, y en $\mathbb{Z}$.*

Demostración. Basta demostrar que $(a) \Longrightarrow (c')$. Sean, pues, $a, b \in A$. Como A es principal, existe $w \in A$ tal que $(a) + (b) = (w)$. Entonces $a, b \in (w)$, de manera que $a = wt$, $b = wy$, $t, y \in A$, así que w es un divisor común de a y b, y, por hipótesis, debe ser una unidad de A. Entonces, $(w) = A$. Finalmente, como $\mathbb{Z}$ y $K[X]$ son anillos euclídeos, son también principales [1, pág. 39]. $\square$

Antes de enunciar otro colorario de la proposición anterior, recordemos que en todo dominio de integridad unitario A, un elemento $p \neq 0$ es irreducible si no es una unidad y si cada vez que $p = ab$ entonces a es una unidad o b es una unidad. Recordemos también que un dominio de integridad unitario A es un anillo *factorial* (o un dominio de *factorización única en irreducibles*) si todo elemento $x \in A$, $x \neq 0$, que no sea una unidad, puede escribirse unívocamente como un producto finito de elementos irreducibles:

$$x = p_1 p_2 \cdots p_r \qquad (p_i \text{ irreducible}).$$

Corolario 2. *Si A es un dominio factorial, $(a), (b)$ y (d) son equivalentes.*

Demostración. Basta demostrar que $(a) \Longrightarrow (b)$. Supongamos, pues, que a y b no tienen divisores comunes. En particular, ningún irreducible p de A es divisor común de a y b. Si ahora b es un divisor de ax, entonces $ax = by$ para algún $x \in A$, y todo irreducible p que figure en la descomposición de b en irreducibles con multiplicidad $m > 0$ deberá figurar en la de ax y, por fuerza, en la de x, con la misma multiplicidad. Entonces b divide a x y, en consecuencia a es primo con b. $\square$

Consideremos ahora un dominio factorial A. Sabemos [1, pág. 47] que el domino $A[Y]$ de los polinomios en la indeterminada Y y coeficientes en A también es factorial. Si p es un irreducible de A, entonces Y y $Y+p$ son irreducibles distintos de $A[Y]$ y, por consiguiente, no tienen divisores comunes. Es decir Y y $Y+p$ satisfacen (a). Sin embargo, no satisfacen (c), pues si

$$1 = Y \cdot a(Y) + (Y+p)b(Y) = Y[a(Y) + (b(Y)] + pb(Y), \qquad (*)$$

donde $a(Y), b(Y) \in A[Y]$, y hacemos

$$b(Y) = b_0 + b_1 Y + b_2 Y^2 + \cdots$$
$$a(Y) + B(Y) = c_0 + c_1 Y + c_2 Y^2 + \cdots ,$$

tendremos que

$$1 = pb_0 + (c_0 + pb_1)Y + (c_1 + pb_2)Y^2 + \cdots ,$$

lo que implica que $1 = pb_0$, $0 = c_0 + pb_1 = c_1 + pb_2 + \cdots$ Pero esto es absurdo, pues p, por ser irreducible, no es una unidad. Entonces

Proposición 2. *Si A es un dominio factorial, en el dominio factorial $A[Y]$ existen elementos $a(Y)$ y $b(Y)$ que satisfacen (a) pero no (c).*

Como consecuencia tenemos el siguiente resultado, muy conocido:

Corolario 3. *Los anillos factoriales $\mathbb{Z}[Y]$ y $K[X,Y]$, donde K es un cuerpo conmutativo, no son principales.*

Demostración. Si estos anillos fuesen principales, tendríamos, en virtud del corolario 1, que $(a) \Longleftrightarrow (c)$, lo cual es contradictorio. □

Nota. Naturalmente, la conclusión del corolario 2 se extiende a $K[X_1, X_2, ..., X_n]$. Cabe anotar que la imposibilidad de $(*)$ en $A[Y]$, cuando A es factorial, implica que no siempre es posible expresar el máximo común divisor de dos de sus elementos como una combinación lineal de los mismos. En [6, págs. 325 ss.], por ejemplo, se demuestra este hecho para $K[X,Y]$, pero también allí se establece que si se multiplica el máximo común divisor $d(Y,Y)$ de dos polinomios $f(X,Y)$ y $g(X,Y)$ por un polinomio conveniente R que contenga solamente una de las indeterminadas X, Y, es posible escribir

$$R \cdot d(X,Y) = a(X,Y)f(X,Y) + b(X,Y)g(X,Y),$$

donde $a(X,Y), b(X,Y) \in K[X,Y]$. El polinomio R está íntimamente ligado con la *resultante* de los polinomios $f(X,Y)$ y $g(X,Y)$ y, por ende, con la *teoría de la eliminación.*

Para completar el estudio de las posibles equivalencias de las caracterizaciones que hemos considerado en esta nota, daremos un ejemplo de un dominio A en el cual (a) no implica (b). Es claro que un tal dominio no puede ser factorial (ni, por consiguiente, euclídeo o principal). Este, muy conocido, es el dominio $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} : x, y \in \mathbb{Z}\}$. En él, los números 2 y $1 + \sqrt{-5}$ son irreducibles distintos y, por lo tanto, no tienen divisores comunes. Pero, puesto que

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

vemos que $(1+\sqrt{-5}) \mid 6$. Sin embargo, $(1+\sqrt{-5}) \nmid 3$. En efecto, en caso contrario,

$$\begin{aligned} 3 &= (1+\sqrt{-5})(a+b\sqrt{-5}) \\ &= (a-5b)+(a+b)\sqrt{-5}, \end{aligned}$$

donde $a, b \in \mathbb{Z}$. Pero esto implica que $3 = a - 5b,\ 0 = a + b$, y, por consiguiente, que $6a = 3$. Esto es absurdo, pues esta ecuación no tiene soluciones enteras.

Agradecimientos. El autor agradece al profesor VÍCTOR S. ALBIS el haberle sugerido el tema de este trabajo. Le agradece también sus valiosas sugerencias durante el desarrollo del mismo y el haberle suministrado las referencias bibliográficas que lo hicieron posible. Extendemos nuestros agradecimientos al revisor por su contribución a la mejor presentación de esta nota.

REFERENCIAS

1. J. BARSHAY, *Topics in Ring Theory*, Benjamin, New York, 1969.
2. P. DUBREIL & M. L. DUBREIL-JACOTIN, *Leçons d'algèbre moderne*, Dunod, Paris, 1961.
3. H. HASSE, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, J. für r. und a. Math. **159** (1926), 3–12.
4. P. JAFFARD, *Les systémes d'idéaux*, Dunod, Paris, 1960.
5. B. W. JONES, *An introduction to Modern Algebra*, MacMillan, New York, 1975.
6. F. SEVERI, *Lecciones de Análisis*, Tomo I, Labor, Barcelona, 1960.

RICARDO PALACIOS
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD NACIONAL DE COLOMBIA
BOGOTÁ, COLOMBIA