Miscelánea Matemática **61** (2015) 1-9 SMM

El algoritmo de Euclides con residuos de menor valor absoluto

Jesús Efrén Pérez Terrazas, Luis Felipe Solís Sansores, Emmanuel Vázquez Cetina

Facultad de Matemáticas
Universidad Autónoma de Yucatán
jperezt@correo.uady.mx

Resumen

En este trabajo se analiza el número de pasos que requiere el algoritmo de Euclides con residuos de menor valor absoluto, mostrando la relación que la velocidad de convergencia del algoritmo tiene con la sucesión de Pell y el llamado número de plata.

1. Introducción

El algoritmo de Euclides es una herramienta muy importante en teoría de números, así como una idea fundamental que se retoma en álgebra abstracta y en temas actuales de investigación en matemáticas. En particular es conocido que calcula el máximo común divisor de dos enteros distintos de cero, y es muy natural preguntarse por la cantidad de pasos que requiere para llegar a ese resultado.

Tenemos la impresión de que no es tan sencillo, como sería de esperarse, encontrar referencias acerca de la mejor cota para determinar la velocidad de convergencia del algoritmo euclidiano cuando se consideran los residuos con menor valor absoluto (ver, por ejemplo, la bibliografía al final del escrito), por lo que hemos consideramos que vale la pena publicar algunos artículos al respecto.

En la sección 2 se explica a qué nos referimos con algoritmo euclidiano con residuos de mínimo valor absoluto, así como qué queremos decir con la cantidad de pasos que requiere dicho algoritmo, además de una primera cota superior para dicho número de pasos, cota que está asociada con la menor norma euclidiana que se le puede asociar a

$\mathbb{Z}$, (véase [4]). Sin embargo, el mencionado algoritmo es aún más rápido, lo que se muestra en la tercera sección, donde se da una cota superior usando las propiedades de la sucesión de Pell, lo que muestra que la velocidad de convergencia del algoritmo euclidiano está relacionada con el logaritmo en base $1 + \sqrt{2}$.

2. Dos versiones del algoritmo euclidiano

Recordemos que el algoritmo de la división nos asegura, para un par de enteros a, b no negativos con $b \neq 0$, que existen enteros q y r únicos tales que $a = bq + r$, donde $0 \leq r < b$.

No es difícil verificar, usando lo anterior, que si a y b son enteros, con b distinto de cero, entonces existen enteros q y r, no necesariamente únicos, tales que $a = bq + r$, con $0 \leq \mid r \mid \leq \frac{|b|}{2}$. En este caso decimos que r es un residuo de mínimo valor absoluto.

Por ejemplo, si consideramos $a = 10$ y $b = 6$, la primera versión del algoritmo de la división nos indica la identidad $a = b(1) + 4$, mientras que la versión con residuos de mínimo valor absoluto nos lleva a la identidad $a = b(2) - 2$.

De manera un tanto coloquial se puede decir que el algoritmo de Euclides, dados los enteros positivos a y b, consiste en repetir el algoritmo de la división hasta que se obtiene un residuo que divide al residuo previo:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ &\vdots \quad \vdots \quad \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \end{aligned}$$

donde $r_{n-1} = r_n q_{n+1}$.

Es conocido que r_n es un divisor de a y de b, así como que si d es un divisor común de a y de b entonces divide a r_n: en este sentido es que r_n es un *máximo común divisor* de a y b, pues la relación *divide a* casi es un orden parcial en $\mathbb{Z}$.

El algoritmo de Euclides tiene que terminar en un número finito de pasos, pues en la versión en que solo se permiten residuos positivos se cumple que $0 < r_n < r_{n-1} < \ldots < r_1 < b$, mientras que en la versión con residuos de mínimo valor absoluto tenemos que $|r_i| \leq \frac{|b|}{2^i}$.

Ahora acordemos qué significa, en este escrito, la cantidad de pasos que requiere el algoritmo euclidiano: en general supondremos que $|a| \geq |b|$, y además consideraremos que el algoritmo termina al obtenerse r_n, es decir, no contaremos como un paso verificar que r_n divide a r_{n-1}.

Con esta convención obtenemos, por ejemplo, que si b es un divisor de a entonces el algoritmo euclidiano requirió cero pasos.

Nótese que como r_i es un entero y $|r_i| \leq \frac{|b|}{2^i}$, si se cumple la desigualdad $\frac{|b|}{2^i} < 2$ entonces $r_i \in \{-1, 0, 1\}$, por lo que el algoritmo euclidiano con residuos de mínimo valor absoluto tendría que haber concluido, así que dicho algoritmo a lo más requeriría n pasos, donde n es el primer entero tal que $|b| < 2^{n+1}$.

Recordemos que la *función piso*, denotada por $\lfloor \quad \rfloor$, se define para cada real r como el mayor entero que es menor o igual a r.

Luego tenemos una cota superior para el número de pasos de la segunda versión del algoritmo euclidiano, dada por $\lfloor \log_2 (| \, b \, |) \rfloor$.

3. La sucesión de Pell

Definición 3.1. Una sucesión recurrente de orden k, con $k \in \mathbb{N}$,

$$u_1, u_2, \ldots, u_n, \ldots$$

es una sucesión de números complejos determinada por los términos $u_1, u_2, \ldots, u_k$ llamados *términos de arranque*, los complejos fijos $a_0, a_1, \ldots, a_{k-1}$ y una relación de recurrencia

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + \ldots + a_{k-1} u_{n+k-1}.$$

Ejemplos clásicos de estas sucesiones son la muy conocida sucesión de Fibonacci, así como la sucesión de Pell, dada por la relación de recurrencia $P_{m+2} = 2P_{m+1} + P_m$, donde los términos de arranque son $P_1 = 1$ y $P_2 = 2$, por lo que la sucesión es

$$1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, \ldots$$

De manera similar a como ocurre en la sucesión de Fibonacci, podemos deducir una fórmula para calcular cada término de la sucesión de Pell.

Teorema 3.2. *Para cada m natural se cumple que:*

$$P_m = \frac{1}{2\sqrt{2}} \left[\left(1 + \sqrt{2}\right)^m - \left(1 - \sqrt{2}\right)^m \right].$$

Demostración. El argumento es análogo al que se usa para deducir la fórmula de Binet para la sucesión de Fibonacci.

Así que comenzamos observando que las únicas soluciones complejas de la ecuación $x^2 = 2x + 1$ son $1 + \sqrt{2}$ y $1 - \sqrt{2}$.

Luego, para los complejos arbitrarios c y d, y los números $Q_m = c\left(1+\sqrt{2}\right)^m + d\left(1-\sqrt{2}\right)^m$, tenemos las identidades:

$$\begin{aligned} Q_{m+2} &= c\left(1+\sqrt{2}\right)^{m+2} + d\left(1-\sqrt{2}\right)^{m+2} \\ &= c\left[2\left(1+\sqrt{2}\right)^{m+1} + \left(1+\sqrt{2}\right)^m\right] + d\left[2\left(1-\sqrt{2}\right)^{m+1} \right. \\ &\quad \left. + \left(1-\sqrt{2}\right)^m\right] \\ &= 2\left[c\left(1+\sqrt{2}\right)^{m+1} + d\left(1-\sqrt{2}\right)^{m+1}\right] + \left[c\left(1+\sqrt{2}\right)^m \right. \\ &\quad \left. + d\left(1-\sqrt{2}\right)^m\right] \\ &= 2Q_{m+1} + Q_m, \end{aligned}$$

así que se cumple la relación de recurrencia de la sucesión de Pell.

Ahora, eligiendo complejos arbitrarios u y v tenemos que la ecuación

$$\begin{pmatrix} 1+\sqrt{2} & 1-\sqrt{2} \\ \left(1+\sqrt{2}\right)^2 & \left(1-\sqrt{2}\right)^2 \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$$

tiene una única solución, pues el determinante de la matriz es $2\sqrt{2}$, y la mencionada solución es $c = \frac{\left(1-\sqrt{2}\right)^2 u + \left(\sqrt{2}-1\right)v}{2\sqrt{2}}$ y $d = \frac{-\left(1+\sqrt{2}\right)^2 u + \left(\sqrt{2}+1\right)v}{2\sqrt{2}}$.

Entonces, para el caso específico en que $Q_1 = P_1 = 1$ y $Q_2 = P_2 = 2$, obtenemos que $c = \frac{1}{2\sqrt{2}}$ y $d = \frac{-1}{2\sqrt{2}}$. Como la sucesión Q_m cumple la fórmula de recurrencia y coincide en los términos de arranque con la de Pell, entonces es igual a la sucesión de Pell, lo que demuestra el enunciado. □

Observación 3.3. La sucesión en la demostración del teorema 3.2 exhibe una interesante propiedad: si el complejo c es diferente de cero entonces

$$\lim_{m\to\infty} \frac{Q_{m+1}}{Q_m} = \lim_{m\to\infty} \frac{c\left(1+\sqrt{2}\right)^{m+1} + d\left(1-\sqrt{2}\right)^{m+1}}{c\left(1+\sqrt{2}\right)^m + d\left(1-\sqrt{2}\right)^m} = 1+\sqrt{2},$$

valor que recibe el nombre de *número de plata*.

Observación 3.4. Consideremos la sucesión de Pell y observemos que la identidad $P_3 = 2P_2 + P_1$ tiene residuo con mínimo valor absoluto posible. Más aún, no es difícil verificar para $m > 1$, dado que tenemos las identidades $P_{m+2} = 2P_{m+1} + P_m$ y $P_{m+2} = 3P_{m+1} + (P_m - P_{m+1}) = 3P_{m+1} + (-P_m - P_{m-1})$, que el residuo de mínimo valor absoluto que queda al aplicar el algoritmo de la división a P_{m+2} y P_{m+1} es P_m, así que

tenemos el siguiente algoritmo euclidiano de residuos con mínimos valores absolutos:

$$\begin{aligned} P_{n+1} &= 2P_n + P_{n-1}, \\ P_n &= 2P_{n-1} + P_{n-2}, \\ \vdots &\ \vdots\ \vdots \\ P_3 &= 2P_2 + P_1, \end{aligned}$$

el cual tiene exactamente $n-1$ pasos. Como $P_1 = 1$, también se muestra que P_{n+1} es primo relativo con P_n.

El siguiente resultado nos permite observar que éste es el peor caso posible, es decir, que la sucesión de Pell nos proporciona parejas de enteros con los cuales el algoritmo euclidiano «tarda más».

Teorema 3.5. *Consideremos los enteros a y b tales que $|a| > |b| > 0$, y sea*

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ \vdots &\ \vdots\ \vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \\ r_{n-1} &= r_nq_{n+1}, \end{aligned}$$

un algoritmo de Euclides con residuos de mínimo valor absoluto. Entonces, para cada $m \in \{1, \ldots, n\}$ se cumple que $|r_m| \leq \frac{|b|}{P_{m+1}}$.

Demostración. Procederemos por inducción sobre m.

Primero notemos que para r_1 tenemos que $|r_1| \leq \frac{|b|}{2} = \frac{|b|}{P_2}$.

Ahora recordemos la definición de la función signo, es decir que $\operatorname{sgn} : \mathbb{Z} - \{0\} \to \{-1, 1\}$ es tal que $\operatorname{sgn}(a) = -1$ si y solo si $a < 0$.

Para ver qué sucede si $m = 2$ consideraremos dos casos:

- **Caso 1:** $|r_1| \leq \frac{2|b|}{5}$. Como estamos considerando residuos de mínimo valor absoluto tenemos que $|r_2| \leq \frac{|r_1|}{2} \leq \frac{|b|}{5} = \frac{|b|}{P_3}$.
- **Caso 2:** $\frac{2|b|}{5} \leq |r_1| < \frac{|b|}{2}$ (si $|r_1| = \frac{|b|}{2}$ entonces, por cómo se estableció el último residuo del algoritmo euclidiano, no existe r_2.)

  Para verificar que se cumple $|b - 2\operatorname{sgn}(b)\operatorname{sgn}(r_1)\, r_1| \leq \frac{|b|}{5}$ analizamos cada caso:
  - Si $b, r_1 > 0$ entonces $|b - 2\operatorname{sgn}(b)\operatorname{sgn}(r_1)\, r_1| = b - 2r_1 \leq b - \frac{4b}{5} = \frac{b}{5}$.
  - Si $b, r_1 < 0$ entonces $|b - 2\operatorname{sgn}(b)\operatorname{sgn}(r_1)\, r_1| = |b - 2r_1| = -b + 2r_1 \leq -b + \frac{4b}{5} = -\frac{b}{5}$.
  - Si $b < 0$ y $r_1 > 0$ entonces $|b - 2\operatorname{sgn}(b)\operatorname{sgn}(r_1)\, r_1| = |b + 2r_1| = -b - 2r_1 \leq -b + \frac{4b}{5} = -\frac{b}{5}$.

– Si $b > 0$ y $r_1 < 0$ entonces $|b-2\operatorname{sgn}(b)\operatorname{sgn}(r_1)\, r_1| = |b+2r_1| = b + 2r_1 \leq b - \frac{4b}{5} = \frac{b}{5}$.

Así $|r_2| \leq \frac{|b|}{5} = \frac{|b|}{P_3}$.

Ahora supongamos que el enunciado se cumple para cualquier algoritmo de Euclides, con residuos de mínimo valor absoluto, para los primeros m residuos, y consideremos dos casos para analizar el siguiente valor:

- **Caso 1:** $|r_1| \leq \frac{|b|P_{m+1}}{P_{m+2}}$.

  Es claro que

$$\begin{aligned} b &= r_1 q_2 + r_2, \\ &\vdots \quad \vdots \quad \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

  es un algoritmo de Euclides con residuos de mínimo valor absoluto, así que por hipótesis de inducción $|r_{m+1}| \leq \frac{|r_1|}{P_{m+1}}$, luego

$$|r_{m+1}| \leq \frac{|b|P_{m+1}}{P_{m+1}P_{m+2}} = \frac{|b|}{P_{m+2}}.$$

- **Caso 2:** $\frac{|b|P_{m+1}}{P_{m+2}} \leq |r_1| < \frac{|b|}{2}$.

  En este caso tenemos

$$|r_2| \leq |b - 2\operatorname{sgn}(b)\operatorname{sgn}(r_1) r_1| \leq \left| b - 2\frac{bP_{m+1}}{P_{m+2}} \right| = \left| \frac{bP_m}{P_{m+2}} \right|.$$

  Como

$$\begin{aligned} r_1 &= r_2 q_3 + r_3, \\ &\vdots \quad \vdots \quad \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

  es un algoritmo de Euclides con residuos de valores absolutos mínimos, por la hipótesis de inducción tenemos $|r_{m+1}| \leq \frac{|r_2|}{P_m}$, luego

$$|r_{m+1}| \leq \frac{|b|P_m}{P_m P_{m+2}} = \frac{|b|}{P_{m+2}}.$$ □

Corolario 3.6. *Sean $a, b \in \mathbb{Z}$ tales que $0 < |b| \leq |a|$. Entonces, para el algoritmo de Euclides con residuos de mínimo valor absoluto y $|r_n| = (a, b)$ se tiene que*

$$n \leq \left\lfloor \frac{\log_{10}\left(\sqrt{2} \mid b \mid + \frac{1}{5}\right)}{\log_{10}\left(1+\sqrt{2}\right)} \right\rfloor.$$

Es decir, si definimos $\delta = 1+\sqrt{2}$, *entonces* $n \leq \left\lfloor \log_\delta \left(\sqrt{2}|b| + \frac{1}{5}\right)\right\rfloor$.

Demostración. Como el valor mínimo para (a,b) es 1 afirmamos, por el teorema 3.5, que si $\frac{|b|}{P_{m+1}} < 2$ entonces $n \leq m$. Así, por la fórmula para el $(m+1)-$ésimo término de la sucesión de Pell, se está considerando la desigualdad

$$\frac{|b|}{\frac{1}{2\sqrt{2}}\left[\left(1+\sqrt{2}\right)^{m+1} - \left(1-\sqrt{2}\right)^{m+1}\right]} < 2 \qquad (*)$$

de donde obtenemos $\sqrt{2}|b| < \left(1+\sqrt{2}\right)^{m+1} - \left(1-\sqrt{2}\right)^{m+1}$. Además, ya que $\left(1-\sqrt{2}\right)^{m+1} < \left(1-\sqrt{2}\right)^{2} < \frac{1}{5}$, tenemos entonces $\left(1+\sqrt{2}\right)^{m+1} - \frac{1}{5} < \left(1+\sqrt{2}\right)^{m+1} - \left(1-\sqrt{2}\right)^{m+1}$, por lo que si $\sqrt{2}|b| \leq \left(1+\sqrt{2}\right)^{m+1} - \frac{1}{5}$ entonces se cumple la desigualdad $(*)$. Despejando obtenemos $\log_\delta\left(\sqrt{2} \mid b \mid + \frac{1}{5}\right) - 1 \leq m$, así que el primer entero para el que se cumple esta desigualdad es $\left\lfloor \log_\delta\left(\sqrt{2} \mid b \mid + \frac{1}{5}\right)\right\rfloor$, de lo que se sigue la afirmación. □

Notemos que el resultado del corolario 3.6 es el mismo que el del teorema 4.2 de [2], pues $\log_\delta\left(\sqrt{2} \mid b \mid + \frac{1}{5}\right)$ no es un número entero.

Observemos que esta cota no puede ser mejorada significativamente y que el peor caso ocurre cuando a y b son números consecutivos de la sucesión de Pell: no es difícil verificar, para $a > b = P_n$, que la fórmula previa indica que el máximo común divisor se obtendrá a lo más en $n-1$ pasos, justo los que vimos en la observación 3.4 que se requieren cuando, adicionalmente, $a = P_{n+1}$.

Para tener otra forma de comparar las cotas obtenidas en la sección 2 y en la sección 3, sean r un real tal que $2^r = \mid b \mid$ y s un real tal que $\delta^s = \sqrt{2} \mid b \mid + \frac{1}{5}$. Por otra parte, sea e tal que $2^e = \delta$, entonces tenemos que $2^{es} = \delta^s = \sqrt{2} \mid b \mid + \frac{1}{5} \approx \left(\sqrt{2}\right) 2^r = 2^{r+0.5}$, luego $s \approx \frac{r+0.5}{e} \approx 0.786439701\,(r+0.5)$.

Además, puesto que $log_\delta(10) \approx 2.6125$, podemos decir, a grosso modo, que el algoritmo de Euclides con residuos de mínimo valor absoluto requiere, en pasos, menos de 3 veces la cantidad de dígitos de b, lo que es mucho mejor que lo que requiere el algoritmo usual de Euclides (véase [2]).

4. Apéndice

Hay resultados que se cumplen en sucesiones recurrentes, y queremos mostrar algunas propiedades que la sucesión de Pell tiene en común

con la sucesión de Fibonacci. El lector puede encontrar una discusión un poco más general en [6].

Proposición 4.1. *Para t natural y s entero mayor o igual a 2 se tiene que $P_{s+t} = P_s P_{t+1} + P_{s-1} P_t$, identidad que es conocida como propiedad de desplazamiento.*

Demostración. La prueba se realizará por inducción sobre s, es decir que se supone fijo el valor de t y se realiza inducción para $s \in \mathbb{N} - \{1\}$.

Los casos base son simples, pues para $s = 2$ tenemos que por definición $P_{t+2} = 2P_{t+1} + P_t$, y $P_2 = 2$ y $P_1 = 1$, mientras que para $s = 3$ tenemos que $P_{t+3} = 2P_{t+2} + P_{t+1} = 2(2P_{t+1} + P_t) + P_{t+1} = 5P_{t+1} + 2P_t = P_3 P_{t+1} + P_2 P_t$.

Ahora supongamos cierto el enunciado para $s \in \{2, \ldots, k\}$, con $k \geq 3$, y demostrémoslo para $s = k + 1$:

$$\begin{aligned} P_{t+k+1} &= 2P_{t+k} + P_{t+k-1} \\ &= 2(P_k P_{t+1} + P_{k-1} P_t) + (P_{k-1} P_{t+1} + P_{k-2} P_t) \\ &= (2P_k + P_{k-1}) P_{t+1} + (2P_{k-1} + P_{k-2}) P_t \\ &= P_{k+1} P_{t+1} + P_k P_t. \end{aligned}$$

□

Proposición 4.2. Sean a y b enteros positivos tales que $a|b$, entonces P_a divide a P_b.

Demostración. Sean a y b enteros positivos para los cuales existe un entero positivo q tal que $b = aq$.

Primero notemos que si $a = 1$ tenemos $P_a = 1$ y así $P_a | P_b$.

A continuación consideremos a fija con $a \geq 2$ y procedamos por inducción sobre q.

El caso base $q = 1$ es trivial.

Ahora supongamos cierto el enunciado para $q = k$ y veamos que se cumple para $q = k + 1$.

De la identidad $b = ak + a$ y la propiedad de desplazamiento tenemos que $P_b = P_a P_{ak+1} + P_{a-1} P_{ak}$, y por la hipótesis de inducción $P_a | P_{ak}$, luego $P_a | P_b$. □

Proposición 4.3. *Dados los enteros positivos a y b, con b menor o igual que a, es decir que $a = bq + r$ con r entero no negativo y $r < a$, se cumple que $(P_a, P_b) = (P_r, P_b)$.*

Demostración. Si $r = 0$ entonces $b|a$ y la afirmación se sigue de la proposición 4.2.

En otro caso, aplicando la propiedad de desplazamiento obtenemos $P_a = P_{bq} P_{r+1} + P_{bq-1} P_r$, y por la proposición 4.2 sabemos que P_b divide a P_{bq}, luego $(P_a, P_b) = (P_{bq-1} P_r, P_b)$. Aplicando el algoritmo euclidiano como en la sección 3 se verifica que $(P_b, P_{bq-1}) = 1$, por lo tanto $(P_{bq-1} P_r, P_b) = (P_r, P_b)$. □

Corolario 4.4. *Sean a y b enteros positivos, entonces $(P_a, P_b) = P_{(a,b)}$. En particular, $a|b$ si y solo si $P_a|P_b$.*

Demostración. La primera afirmación se sigue de aplicar el algoritmo euclidiano y la proposición 4.3. □

Finalmente queremos agradecer a los árbitros anónimos por sus valiosos comentarios que mejoraron este escrito.

Bibliografía

[1] E. Bach y J. Shallit, *Algorithmic Number Theory*, Efficient Algorithms, vol. 1, The MIT Press, 1996.
[2] C. Garza, E. Pérez y L. Solís, «El algoritmo de Euclides», *Eureka*, vol. 30, 2013, 5–21.
[3] D. E. Knuth, *The Art of Computer Programming*, 3.ª ed., Seminumerical Algorithms, vol. 2, Addison Wesley Longman, 1998.
[4] J. Lara, E. Pérez y L. Solís, «La menor norma euclidiana», *Eureka*, vol. 33, 2014, 6–12.
[5] A. I. Markushévich, *Sucesiones Recurrentes, Lecciones populares de Matemáticas*, Editorial Mir, Moscú, 1974.
[6] E. Pérez, L. Solís y E. Vázquez, «Algunas propiedades de algunas sucesiones recurrentes», *Abstraction & Application*, vol. 11, 2014, 29–34.
[7] J. V. Uspensky y M. A. Heaslet, *Elementary Number Theory*, McGraw Hill, 1939.