Apuntes de
Teoría Elemental de Números

por Enrique Arrondo(*)

Versión del 19 de Enero de 2009

Aunque en orden diverso, estas notas están basadas en el libro "Elementary Number Theory", de David M. Burton, donde el lector puede profundizar en los detalles.

(*) Departamento de Álgebra, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, 28040 Madrid, arrondo@mat.ucm.es

0. Preliminares

Definición. Denotaremos por $\mathbb{Z}$ al conjunto de números enteros. Dado $a \in \mathbb{Z}$, denotaremos por $\mathbb{Z}_{\geq a}$ al conjunto de los números enteros mayores o iguales que a. De esta forma evitaremos polémicas estériles sobre si los números naturales empiezan con el 0 o con el 1, y escribiremos simplemente $\mathbb{Z}_{\geq 0}$ o $\mathbb{Z}_{\geq 1}$ según nos haga falta.

Teorema 0.1 (Principio del buen orden)**.** *Sea a un número entero y sea $S \subset \mathbb{Z}_{\geq a}$ un subconjunto no vacío de $\mathbb{Z}_{\geq a}$. Entonces S tiene un elemento mínimo.*

Demostración: Como S es no vacío, existe $b \in S$. Como $S \subset \mathbb{Z}_{\geq a}$, entonces $a \leq b$. Considerando el conjunto finito $\{a, a+a, \ldots, b-1, b\}$, tomamos c el menor elemento de tal conjunto que esté en S (sabemos que, en el peor de los casos, b lo está). Es claro entonces que c es un elemento mínimo de S. □

Teorema 0.2 (Principio de inducción)**.** *Sea P una propiedad relativa a los números de $\mathbb{Z}_{\geq a}$. Supongamos que se verifica alguna de las dos siguientes hipótesis:*

(i) (Inducción débil)*: P es cierta para el número a y cada vez que P es cierta para cada $n \in \mathbb{Z}_{\geq a}$ entonces P es cierta para $n+1$.*

(ii) (Inducción fuerte)*: P es cierta para el número a y cada vez que P es cierta para todos los números de a a n entonces P es cierta para $n+1$.*

Entonces P es cierta para todo $n \in \mathbb{Z}_{\geq a}$.

Demostración: Sea S el conjunto de enteros mayores o iguales que a que no verifica la propiedad P. Como estamos suponiendo que a verifica P, entonces $a \notin S$. El teorema estará demostrado si demostramos que S es el conjunto vacío. Supongamos entonces, por reducción al absurdo, que S es no vacío. Por el principio del buen orden, el conjunto S tendrá un mínimo m. Esto quiere decir que los números $a, a+1, \ldots, m-1$ no están en S, es decir, verifican la propiedad P. Pero tanto (i) como (ii) aplicadas a $n = m-1$ implican que entonces m también verifica P, lo que contradice que m esté en S. □

Ejercicio 0.3. Se considera la *sucesión de Fibonacci* $\{u_n\}$ de números enteros

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

definida de forma recursiva por $u_1 = u_2 = 1$, $u_n = u_{n-1} + u_{n-2}$. Probar por inducción que $u_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$. Comprobar la fórmula para $n = 4$.

1. Divisibilidad y factorización en enteros

Definición. Se dice que *un número entero a divide a otro número entero b* y se escribe $a|b$ si existe $c \in \mathbb{Z}$ tal que $b = ac$. En tal caso, diremos que a es un *divisor* de b.

Demostramos a continuación las propiedades básicas de divisibilidad que necesitaremos. Las demostraciones son extremadamente simples, pero vale la pena hacerlas con rigor al menos una vez, ya que veremos enseguida que hay propiedades aparentemente inmediatas (en el sentido de que son propiedades de sobra conocidas) y que, sin embargo, no pueden hacerse a partir de la definición y requieren técnicas más sofisticadas.

Lema 1.1. *Dados enteros a, b, c, se tiene:*

(i) Si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$.

(ii) $c|a$ y $c|b$, entonces $c|ax + by$ para todo $x, y \in \mathbb{Z}$.

(iii) $a|b$ si y sólo si $a|ac + b$.

(iv) Si $c \neq 0$, entonces $a|b$ si y sólo si $ac|bc$.

Demostración: Demostremos primero (i). Si $a|b$, entonces existe un entero c tal que $b = ac$. Tomando valores absolutos, se tiene $|b| = |a||c|$. Como $b \neq 0$, se tiene $c \neq 0$, luego $|c| \geq 1$. Por tanto, $|b| \geq |a|$.

Para demostrar (ii), vemos que $c|a$ y $c|b$ implica que existen enteros a', b' tales que $a = a'c$ y $b = b'c$. Por tanto, $ax + by = a'cx + b'cy = (a'x + b'y)c$, por lo que $c|ax + by$.

La parte (iii) es consecuencia de (ii). En efecto, si $a|b$, como obviamente $a|a$, se tiene $a|ac + b \cdot 1 = ac + b$. Recíprocamente, si $a|ac + b$, de nuevo por (ii) se tiene $a|(ac + b) \cdot 1 + a(-c) = b$.

Finalmente, para ver (iv), por definición tenemos que $a|b$ si y sólo si existe un entero d tal que $b = ad$. Como $c \neq 0$, esto es equivalente a $bc = acd$, que de nuevo equivale, por definición, a $ac|bc$. □

Definición. Un *número primo* es un entero $p > 1$ cuyos únicos divisores positivos son 1 y p. Por el contrario, un *número compuesto* es un número entero $n > 1$ con algún divisor positivo $n_1 \neq 1, n$, y por tanto $n = n_1 n_2$, con $n_1, n_2 > 1$.

Empezamos con una aplicación del principio de inducción fuerte:

Teorema 1.2 (Fundamental de la aritmética: existencia)**.** *Todo número entero $n \geq 2$ se puede escribir como producto finito de números primos.*

Demostración: Lo demostraremos por inducción sobre $n \in \mathbb{Z}_{\geq 2}$. Claramente 2 es primo, luego el teorema se verifica trivialmente para $n = 2$. Supongamos ahora que tenemos

demostrado el teorema para todos los números $2, 3, \ldots, n$ y veamos que también es cierto para $n+1$. Si $n+1$ fuera un número primo, de nuevo el resultado sería trivial. Queda entonces demostrarlo en el caso en que $n+1$ no es primo. En tal caso, $n+1$ tendría un divisor positivo a distinto de 1 y $n+1$. Es decir, existe $b \in \mathbb{Z}$ tal que $n+1 = ab$. Como $n+1$ y a son positivos, también lo es b. Además, como $a \neq 1, n+1$, también se tiene $b \neq 1, n+1$. De aquí se deduce, junto al Lema 1.1(i), que a y b están en el conjunto $\{2, 3, \ldots, n\}$ en que sabemos que es cierto el teorema. Por tanto, a y b se escriben como producto finito de números primos, de lo que se sigue que también $n+1 = ab$ es producto finito de números primos, como queríamos demostrar. □

Observación 1.3. Obsérvese que de momento no se puede demostrar que la descomposición en primos sea única. En efecto, si tenemos que $n = p_1 \ldots p_r = p'_1 \ldots p'_s$, no podemos demostrar con la mera definición de número primo que las dos factorizaciones son iguales (salvo el orden de los factores). La estrategia sería decir que, por ejemplo, p'_1 divide a n, es decir al producto $p_1 \ldots p_r$. Pero, aunque nos hayan enseñado que si un número primo p'_1 divide a un producto de números $p_1 \ldots p_r$ entonces divide a alguno de los factores, no podemos usarlo porque de momento sólo podemos usar la definición de número primo, que no implica nada de esto de forma inmediata. Sólo más adelante, cuando demostremos el Lema de Euclides (Teorema 1.13) podremos demostrar la unicidad. De momento, usemos la existencia para demostrar otro resultado importante debido a Euclides:

Teorema 1.4 (Euclides)**.** *Existen infinitos números primos.*

Demostración: Supongamos, por reducción al absurdo, que el conjunto de números primos es un conjunto finito $\{p_1, p_2, \ldots, p_r\}$. Sea el número $n = p_1 p_2 \ldots p_r + 1$. Claramente $n \geq 2$ (ya que algún p_i es 2), por lo que el Teorema 1.2 implica que n se escribe como producto de números primos. En particular, n tiene algún factor primo, que necesariamente será de la forma p_i, para algún $i = 1, 2, \ldots, r$. Es decir, $p_i | n = p_1 p_2 \ldots p_r + 1$. Por el Lema 1.1(iii), $p_i | 1$, lo que es absurdo. □

Definición. Se llama *máximo común divisor de dos números* $a, b \in \mathbb{Z}$ (y lo denotaremos por $\mathrm{mcd}(a, b)$) al mayor divisor positivo de a y b. Dado que esta definición no tiene sentido si $a = b = 0$ (ya que cualquier número positivo divide a 0), se puede convenir en escribir $\mathrm{mcd}(0, 0) = 0$, puesto que $\mathrm{mcd}(a, 0) = a$ para cualquier $a \neq 0$. Si $(a, b) \neq (0, 0)$, entonces es claro que $\mathrm{mcd}(a, b) \geq 1$ (por tanto, siempre que demos por descontado que el máximo común divisor de dos números es distinto de cero es porque excluimos el caso trivial en que ambos números son cero). Diremos que dos números a y b son *primos entre sí* o *coprimos* si $\mathrm{mcd}(a, b) = 1$.

Como ya hemos observado, con la mera definición de primos y divisibilidad no se puede andar muy lejos. Para el caso del máximo común divisor, sin saber que la descomposición en producto de números primos es única, no habría siquiera en principio un modo de calcularlo. Enunciamos en primer lugar los resultados que sí pueden hacerse sin más que la propia definición.

Proposición 1.5. *El máximo común divisor verifica las siguientes propiedades:*

(i) $\mathrm{mcd}(a, an+b) = \mathrm{mcd}(a,b)$ *para cualquier* $n \in \mathbb{Z}$.

(ii) Si $d = \mathrm{mcd}(a,b)$, *entonces* $\mathrm{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$.

(iii) Dado un número primo p *y un entero cualquiera* a, *entonces o bien* $p|a$ *o bien* $\mathrm{mcd}(a,p) = 1$.

Demostración: Para demostrar la parte (i) bastará que los divisores comunes de a y $an+b$ son lo divisores comunes de a y b. Tomemos entonces un divisor $d|a$ y veamos que $d|an+b$ si y sólo si $d|b$. En efecto, como $d|a$, podremos escribir $a = da'$. El Lema 1.1(iii) nos dice ahora que d divide a $an+b = d(a'n)+b$ si y sólo si d divide a b.

Para la parte (ii), si fuera $c = \mathrm{mcd}(\frac{a}{d}, \frac{b}{d}) > 1$, entonces, como $c|\frac{a}{d}$ y $c|\frac{b}{d}$, se seguiría $cd|a$ y $cd|b$. Como $cd > d$, se llega a contradicción.

La parte (iii) es inmediata de la definición de número primo, ya que, por ser $\mathrm{mcd}(a,p)$ un divisor de p, se tiene que o bien $\mathrm{mcd}(a,p) = 1$ o bien $\mathrm{mcd}(a,p) = p$ (en cuyo caso $p|a$). □

El primer resultado importante es el siguiente:

Teorema 1.6 (Algoritmo de división)**.** *Dados* $a, b \in \mathbb{Z}$ *con* $b > 0$, *existen* $q, r \in \mathbb{Z}$ *únicos tales que* $a = qb + r$ *y* $0 \leq r < b$.

Demostración: Consideremos el conjunto $S = \{a - xb \mid x \in \mathbb{Z},\ a - xb \geq 0\}$. Como para $x = -|a|$ se tiene $a - xb = a + |a|b \geq a + |a| \geq 0$, el conjunto S es no vacío. Por el Principio del Buen Orden (usando $S \subset \mathbb{Z}_{\geq 0}$) se deduce que S tiene un elemento mínimo $r = a - qb$. Por definición, $r \geq 0$. Veamos que también $r < b$. En efecto, si fuera $r \geq b$, entonces tendríamos $0 \leq r - b = a - (q+1)b$, luego $r - b$ sería un elemento de S menor que r, lo que es absurdo. Esto demuestra la existencia de la división.

Para ver la unicidad, supongamos que tenemos dos divisiones distintas $qb + r = a = q'b + r'$ con $0 \leq r, r' < b$. Entonces se tendría $(q - q')b = r' - r$, es decir, $b|r' - r$. Ahora bien, $r' - r < b - 0 = b$ y $r - r' < b - 0 = b$, por lo que $|r' - r| < b = |b|$. El Lema 1.1(i) implica entonces $r' - r = 0$, de donde se deduce $r = r'$ y $q = q'$. □

Observación 1.7. El resultado anterior nos permite clasificar los números según el resto que den al dividir por un número dado. Por ejemplo, dividiendo por 4, es claro que todo entero es de alguna de las siguientes formas: $4k$, $4k+1$, $4k+2$, $4k+3$. Claramente, los números de la forma $4k$ nunca serán primos, y el único número primo de la forma $4k+2$ es $p=2$. Por tanto, según el Teorema 1.4, habrá infinitos primos de la forma $4k+1$ o de la forma $4k+3$ (veremos más adelante que hay infinitos de cualquiera de las dos formas). Veamos de momento que existen infinitos números primos de la forma $4k+3$ (más en general, un teorema de Dirichlet asegura que, dados enteros a, b con $\mathrm{mcd}(a,b)=1$, existen infinitos números primos de la forma $ak+b$; la demostración de este teorema requiere técnicas mucho más avanzadas que las presentes en estas notas, por lo que sólo demostraremos casos muy particulares). El lector reconocerá aquí (y en demostraciones de resultados parecidos) la técnica de la demostración de Euclides para la existencia de infinitos números primos (Teorema 1.4). Si suponemos que $p_1, p_2, \ldots, p_r$ son todos los números primos de la forma $4k+3$, consideramos el número $n = 4p_1p_2\ldots p_r - 1$. Como al menos algún p_i es 3, se tiene $n \geq 2$. Por el Teorema Fundamental de la Aritmética (Teorema 1.2), n será producto finito de números primos (necesariamente distintos de 2, porque n es impar). No pueden ser todos de la forma $4k+1$, porque entonces su producto n sería también de la forma $4k+1$, mientras que n es de la forma $4k+3$. Por tanto, n es divisible por algún número primo de la forma $4k+3$, es decir, es divisible por algún p_i. Por el Lema 1.1(i), $p_i | -1$, lo que es absurdo.

Teorema 1.8 (Bézout)**.** *Dados $a, b \in \mathbb{Z}$, entonces el conjunto $\{ax+by \in \mathbb{Z} \mid x, y \in \mathbb{Z}\}$ es el conjunto de los múltiplos de $d = \mathrm{mcd}(a,b)$. En particular,* $\mathrm{mcd}(a,b) = 1$ *si y sólo si existen $x, y \in \mathbb{Z}$ tales que $ax+by=1$.*

Demostración: Podemos suponer que a y b son distintos de cero, ya que en caso contrario el resultado es inmediato. Obsérvese que, como $d|a, b$, entonces el Lema 1.1(ii) implica $d|ax+by$ para todo $x, y \in \mathbb{Z}$. Basta entonces demostrar que cualquier múltiplo de d se escribe de la forma $ax+by$, para lo cual es suficiente verlo para d.

Consideramos el conjunto $S = \{ax+by \mid x, y \in \mathbb{Z},\ ax+by \geq 1\}$. Como $a^2+b^2 > 0$, se tiene que S es no vacío, ya que contiene al menos a a^2+b^2. Por el Principio del Buen Orden (viendo S como subconjunto de $\mathbb{Z}_{\geq 1}$), se sigue que S tiene un elemento mínimo, que será de la forma $d' = ax+by$. Queremos ver que $d' = d$, lo que terminaría la demostración.

Veamos primero que $d'|a$. Para ello efectuamos la división euclídea y tendremos $a = qd' + r$, con $0 \leq r < d'$. Escribimos entonces

$$r = a - qd' = a - q(ax+by) = a(1-q) + b(-qy).$$

Como $r < d'$ y d' es mínimo en S, no puede ser que r esté en S, por lo que la igualdad anterior implica $r \leq 0$, luego $r = 0$ y por tanto $d'|a$. De forma análoga se demuestra $d'|b$.

Basta ver, por la definición de máximo común múltiplo, que cualquier divisor común positivo de a y b es menor o igual que d'. Sea entonces $c > 0$ tal que $c|a$ y $c|b$. Se tiene entonces, por el Lema 1.1(ii) que $c|ax + by = d'$, luego por el Lema 1.1(i) $c \leq d'$, como queríamos. □

El resultado anterior nos permite obtener un gran número de propiedades de la divisibilidad que serían obvias usando factorización en primos pero que no son obvias usando sólo la definición de divisibilidad.

Proposición 1.9. *Dados números enteros no nulos a_1, a_2, b, se tiene que* $\mcd(a_1a_2, b) = 1$ *si y sólo si* $\mcd(a_1, b) = 1$ *y* $\mcd(a_2, b) = 1$.

Demostración: Es claro, usando sólo divisibilidad, que si $\mcd(a_1a_2, b) = 1$, entonces a_1 y b no pueden tener un divisor común mayor de uno (porque sería un divisor común de a_1a_2 y b), ni tampoco a_2 y B pueden tenerlo, por lo que $\mcd(a_1, b) = 1$ y $\mcd(a_2, b) = 1$.

Recíprocamente, si $\mcd(a_1, b) = 1$ y $\mcd(a_2, b) = 1$, por el Teorema 1.8 se sigue que existen $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ tales que

$$a_1x_1 + by_1 = 1$$

$$a_2x_2 + by_2 = 1.$$

Multiplicando ambas expresiones, se obtiene

$$a_1a_2x_1x_2 + b(a_1x_1y_2 + a_2x_2y_1 + by_1y_2) = 1,$$

lo que implica, de nuevo por el Teorema 1.8, $\mcd(a_1a_2, b) = 1$. □

Muchas veces que tengamos un resultado como el anterior, válido para dos elementos a_1, a_2, será válido también para un número finito de elementos, demostrándose este hecho por recurrencia (que en esencia es lo mismo que la inducción débil). Para ilustrar este hecho, demostramos a continuación la generalización de la Proposición 1.9 a r factores con el lenguaje de la inducción, mientras que en el Corolario 1.12 haremos lo mismo a partir de la Proposición 1.11, usando en ese caso el método de inducción. Queda al lector el convencerse de que en realidad ambos métodos son equivalentes, y escoger cuál de los dos le resulta más convincente para aplicarlo en casos sucesivos (ya que a partir de ahora enunciaremos sin demostrar resultados de este tipo).

Corolario 1.10. $\mcd(a_1a_2 \dots a_r, b) = 1$ *si y sólo si* $\mcd(a_i, b) = 1$ *para todo* $i = 1, 2, \dots, r$.

Demostración: Si agrupamos $a_1a_2 \dots a_r = (a_1a_2 \dots a_{r-1})a_r$, por la Proposición 1.9 tendremos que $\mcd(a_1a_2 \dots a_r, b) = 1$ si y sólo si $\mcd(a_1a_2 \dots a_{r-1}, b) = 1$ y $\mcd(a_r, b) = 1$.

Repetimos lo mismo para $a_1a_2\dots a_{r-1}$ y tendremos ahora que $\mathrm{mcd}(a_1a_2\dots a_{r-1},b)=1$ si y sólo si $\mathrm{mcd}(a_1a_2\dots a_{r-2},b)=1$ y $\mathrm{mcd}(a_{r-1},b)=1$. Por tanto, $\mathrm{mcd}(a_1a_2\dots a_r,b)=1$ si y sólo si $\mathrm{mcd}(a_1a_2\dots a_{r-2},b)=1$, $\mathrm{mcd}(a_{r-1},b)=1$ y $\mathrm{mcd}(a_r,b)=1$. Está claro que, reiterando el procedimiento, se llega al enunciado. □

Proposición 1.11. *Dados $a,b,n\in\mathbb{Z}$ tales que $\mathrm{mcd}(a,b)=1$ y $a|n$, $b|n$, se tiene que entonces $ab|n$.*

Demostración: De la hipótesis $a|n$, $b|n$ podemos escribir $n=ar=bs$, con $r,s\in\mathbb{Z}$. Por otra parte, como $\mathrm{mcd}(a,b)=1$, el Teorema 1.8 implica que existen $x,y\in\mathbb{Z}$ tales que $ax+by=1$. Tenemos entonces

$$n=n\cdot 1=n(ax+by)=nax+nby=(bs)ax+(ar)by=ab(sx+ry),$$

por lo que $ab|n$. □

Corolario 1.12. *Sean $a_1,a_2,\dots,a_r$ números enteros tales que $\mathrm{mcd}(a_i,a_j)=1$ si $i\neq j$. Entonces, dado un número entero n tal que $a_i|n$ para cada $i=1,2,\dots,r$, se tiene que $a_1a_2\dots a_r|n$.*

Demostración: Lo demostramos por inducción sobre el número de factores r. Si $r=2$, entonces es la Proposición 1.11. Supongamos entonces, por hipótesis de inducción, que sabemos que, si r números coprimos dos a dos dividen a un entero, entonces el producto también divide a ese número. Veámoslo ahora para $r+1$ números coprimos entre sí.

Suponemos entonces que tenemos $a_1,a_2,\dots,a_{r+1}$ tales que $\mathrm{mcd}(a_i,a_j)=1$ si $i\neq j$ y supongamos $a_i|n$ para cada $i=1,2,\dots,r+1$. Por hipótesis de inducción, como en particular $a_i|n$ para cada $i=1,2,\dots,r$, se tiene $a_1a_2\dots a_r|n$. Además, por el Corolario 1.10, se tiene $\mathrm{mcd}(a_1a_2\dots a_r,a_{r+1})=1$, luego aplicando la Proposición 1.11 con $a=a_1a_2\dots a_r$ y $b=a_{r+1}$, se tiene $a_1a_2\dots a_ra_{r+1}|n$, como queríamos. □

Teorema 1.13 (Lema de Euclides)**.** *Dados $a,b,c\in\mathbb{Z}$ tales que $a|bc$ y $\mathrm{mcd}(a,b)=1$, se tiene que entonces $a|c$.*

Demostración: Como $\mathrm{mcd}(a,b)=1$, por el Teorema 1.8 existen $x,y\in\mathbb{Z}$ tales que $ax+by=1$. Por tanto

$$c=c\cdot 1=c(ax+by)=a(cx)+(bc)y.$$

Como $a|bc$, se sigue que a divide a los dos sumandos de la derecha, luego $a|c$. □

Este resultado nos permite demostrar ya la propiedad clave que todos conocemos de los números primos.

Corolario 1.14. *Sea p un número primo. Si $a_1, a_2, \ldots, a_r$ son números enteros tales que $p|a_1a_2\ldots a_r$, entonces existe $i = 1, 2, \ldots, r$ tal que $p|a_i$.*

Demostración: Supongamos, por reducción al absurdo, que, para cada $i = 1, 2, \ldots, r$, ocurriera $p \not| a_i$. Por el Lema 1.5(iii), se tendría $\text{mcd}(p, a_i) = 1$, luego, por el Corolario 1.10, $\text{mcd}(p, a_1a_2, \ldots, a_r) = 1$. Aplicando el Lema de Euclides con $a = p$, $b = a_1a_2\ldots a_r$ y $c = 1$, se llegaría a $p|1$, lo que es absurdo. □

Con esta propiedad podemos demostrar finalmente por completo el teorema fundamental de la aritmética (ver Observación 1.3).

Teorema 1.15. (Fundamental de la aritmética). *Todo número entero $n \geq 2$ se puede escribir de forma única (salvo el orden de los factores) como producto finito de números primos.*

Demostración: La existencia ya la demostramos en el Teorema 1.2, así que sólo hay que demostrar la unicidad de la descomposición. Supongamos que tenemos dos descomposiciones $n = p_1p_2\ldots p_r = p'_1p'_2\ldots p'_s$ de n en producto de números primos. Como $p'_s|p'_1p'_2\ldots p'_s = p_1p_2\ldots p_r$, el Corolario 1.14 implica que p_s divide a algún p_i. Reordenando los primos $p_1, p_2, \ldots, p_r$, podemos suponer $p'_s|p_r$. Como p_r es primo, se sigue $p_r = p'_s$. Por tanto, cancelando este factor en la igualdad anterior, tendremos $p'_s|p'_1p'_2\ldots p'_{s-1} = p_1p_2\ldots p_{r-1}$. Podemos reiterar el proceso demostrando que cada p'_j es un p_i y cancelándolos en la igualdad. Nótese que no puede ocurrir que se acaben primero los p'_j (es decir $r > s$), ya que entonces llegaríamos a una igualdad $p_1p_2\ldots p_{r-s} = 1$, lo que es imposible. De la misma forma, no se pueden acabar primero los p_i (es decir $r < s$) ya que en tal caso se llegaría al absurdo $p'_1p'_2\ldots p'_{s-r} = 1$. Por tanto, el número de factores es el mismo, y éstos coinciden salvo el orden (además cada factor primo aparece el mismo número de veces). □

Notación. En general, agruparemos los números primos que se repitan en la descomposición y escribiremos $n = p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$, con $p_1, p_2, \ldots, p_r$ todos distintos entre sí. De hecho, mientras no especifiquemos lo contrario, siempre que digamos que $n = p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$ es la factorización en primos de n, se entenderá que $p_1, p_2, \ldots, p_r$ todos distintos entre sí.

Con los resultados vistos hasta ahora podemos recuperar los métodos ya conocidos de calcular el máximo común divisor.

Proposición 1.16. *Sea $a = p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$ la descomposición de un entero $a \geq 2$ en producto de números primos. Entonces los divisores positivos de a son los números de la forma $p_1^{c_1}p_2^{c_2}\ldots p_r^{c_r}$, con $0 \leq c_i \leq a_i$ para cada $i = 1, 2, \ldots, r$. Por tanto, si $b = p_1^{b_1}p_2^{b_2}\ldots p_r^{b_r}$, se tendrá $\text{mcd}(a, b) = p_1^{c_1}p_2^{c_2}\ldots p_r^{c_r}$, con $c_i = \min\{a_i, b_i\}$ para cada $i = 1, 2, \ldots, r$.*

Demostración: Es claro que los números de la forma $p_1^{c_1}p_2^{c_2}\dots p_r^{c_r}$, con $0 \le c_i \le a_i$, son divisores positivos de a. Recíprocamente, sea d un divisor positivo de a. Existirá por tanto otro entero q, también positivo, tal que $a = qd$. Si $q = 1$ o $d = 1$ el resultado es trivial, así que supondremos $q, d \ge 2$. Por el Teorema Fundamental de la Aritmética podremos escribir $q = {p'_1}^{a'_1}{p'_2}^{a'_2}\dots {p'_s}^{a'_s}$ y $d = {p''_1}^{a''_1}{p''_2}^{a''_2}\dots {p''_t}^{a''_t}$. Por tanto, $a = {p'_1}^{a'_1}{p'_2}^{a'_2}\dots {p'_s}^{a'_s}{p''_1}^{a''_1}{p''_2}^{a''_2}\dots {p''_t}^{a''_t}$ es una descomposición de a en factores primos (en que puede haber primos repetidos). Por la unicidad demostrada en el Teorema 1.15, necesariamente los factores de ${p''_1}^{a''_1}{p''_2}^{a''_2}\dots {p''_t}^{a''_t}$ son parte de los factores de $p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$. Esto quiere decir que ${p''_1}^{a''_1}{p''_2}^{a''_2}\dots {p''_t}^{a''_t} = p_1^{c_1}p_2^{c_2}\dots p_r^{c_r}$, con $0 \le c_i \le a_i$, lo que demuestra el resultado. □

Corolario 1.17. *Sean a, b enteros positivos tales que $\mathrm{mcd}(a, b) = 1$. Entonces:*

(i) Los divisores positivos de ab son los productos de la forma dd', con $d|a$ y $d'|b$ y $d, d' > 0$.

(ii) Si $ab = c^n$ para algún $c \in \mathbb{Z}_{\ge 1}$, entonces $a = u^n$ y $b = v^n$ para ciertos $u, v \in \mathbb{Z}$.

Demostración: Como $\mathrm{mcd}(a, b) = 1$, en las factorizaciones en factores primos

$$a = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$$

$$b = q_1^{l_1}q_2^{l_2}\dots q_s^{l_s}$$

se tiene $p_i \ne q_j$ para todo $i = 1, 2, \dots, r$ y $j, 1, 2, \dots, s$. Por tanto, la factorización en factores primos de ab es

$$ab = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}q_1^{l_1}q_2^{l_2}\dots q_s^{l_s},$$

luego los divisores positivos de ab son, por la Proposición 1.16, los números de la forma $p_1^{k'_1}p_2^{k'_2}\dots p_r^{k'_r}q_1^{l'_1}q_2^{l'_2}\dots q_s^{l'_s}$, con $0 \le k'_i \le k_i$ y $0 \le l'_j \le l_j$, es decir, el producto de un divisor positivo de a y un otro de b. Esto demuestra (i).

Para la parte (ii), sea p un primo que divide a c. En particular, $p|c^n = ab = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}q_1^{l_1}q_2^{l_2}\dots q_s^{l_s}$. Por el Corolario 1.14, se sigue que p es un p_i o un q_j, luego la factorización en primos de c se escribe de la forma $c = p_1^{k'_1}p_2^{k'_2}\dots p_r^{k'_r}q_1^{l'_1}q_2^{l'_2}\dots q_s^{l'_s}$. Por tanto, $p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}q_1^{l_1}q_2^{l_2}\dots q_s^{l_s} = ab = c^n = p_1^{nk'_1}p_2^{nk'_2}\dots p_r^{nk'_r}q_1^{nl'_1}q_2^{nl'_2}\dots q_s^{nl'_s}$. Por la unicidad del Teorema 1.15, se sigue que $k_i = nk'_i$ para $i = 1, 2, \dots, r$ y $l_j = nl'_j$ para $j = 1, 2, \dots, s$. Por tanto $a = (p_1^{k'_1}p_2^{k'_2}\dots p_r^{k'_r})^n$ y $b = (q_1^{l'_1}q_2^{l'_2}\dots q_s^{l'_s})^n$. □

Teorema 1.18. *Sean a, b, c enteros positivos tales que $a^n = b^n c$ para algún entero positivo n. Entonces $c = d^n$ para algún $d \in \mathbb{Z}$. En particular, si c no es la potencia n-ésima de un número entero, entonces $\sqrt[n]{c}$ no es un número racional.*

Demostración: Si $a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ es la descomposición de a en factores primos, entonces la descomposición de a^n en factores primos será

$$a^n = p_1^{nk_1} p_2^{nk_2} \dots p_r^{nk_r}.$$

Como $b|a^n$, entonces, por la Proposición 1.16, la descomposición de b en factores primos será de la forma

$$b = p_1^{k_1'} p_2^{k_2'} \dots p_r^{k_r'}$$

con $0 \leq k_i' \leq nk_i$ para $i = 1, 2, \dots, r$. De la misma forma, tendremos

$$c = p_1^{k_1''} p_2^{k_2''} \dots p_r^{k_r''}$$

con $0 \leq k_i'' \leq nk_i$ para $i = 1, 2, \dots, r$. Por tanto,

$$a^n = b^n c = p_1^{nk_1'+k_1''} p_2^{nk_2'+k_2''} \dots p_r^{nk_r'+k_r''}$$

y, por la unicidad de la descomposición en primos, para cada $i = 1, 2 \dots, r$ tendremos $nk_i = nk_i' + k_i''$. Por tanto, $k_i'' = n(k_i - k_i') \geq 0$, es decir, $k_i - k_i'' \geq 0$. Luego el número $d = p_1^{k_1-k_1'} p_2^{k_2-k_2'} \dots p_r^{k_r-k_r'}$ es un entero positivo que verifica $d^n = c$.

Para la última parte, si $\sqrt[n]{c}$ fuera racional, se podía escribir $\sqrt[n]{c} = \frac{a}{b}$, con a, b enteros positivos. Por tanto, $a^n = b^n c$, y por la parte ya demostrada llegaríamos a la contradicción que c debe ser una potencia n-ésima de un número entero. □

Para el cálculo del máximo común divisor no siempre es práctico usar la Proposición 1.16 (que requiere, por ejemplo, saber factorizar los números en cuestión). Usaremos en cambio muchas veces el método más clásico:

Teorema 1.19 (Algoritmo de Euclides)**.** *Sean a, b números enteros con $b > 0$. Definimos por recurrencia $r_{-1} = a$, $r_0 = b$ y, supuestos definidos r_{k-1}, r_k con $r_k \neq 0$, definimos r_{k+1} como el resto de la división euclídea de de r_{k-1} entre r_k. Entonces, existe algún n tal que $r_n = 0$, y se verifica además que $r_{n-1} = \mathrm{mcd}(a, b)$.*

Demostración: De la definición por recurrencia se sigue que $0 \leq r_{k+1} < r_k$ para todo $k \geq 0$. Por tanto $r_0, r_1, \dots$ forma una sucesión estrictamente decreciente de enteros no negativos, por lo que tiene que ocurrir $r_n = 0$ para algún miembro de la sucesión. Por otra parte, si para cada $k = 0, \dots, n$ escribimos la división $r_{k-1} = q_k r_k + r_{k+1}$, por la Proposición 1.5(i) se tendrá $\mathrm{mcd}(r_{k-1}, r_k) = \mathrm{mcd}(q_k r_k + r_{k+1}, r_k) = \mathrm{mcd}(r_{k+1}, r_k)$. Por tanto:

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(r_{-1}, r_0) = \mathrm{mcd}(r_0, r_1) = \dots = \mathrm{mcd}(r_{n-1}, r_n) = \mathrm{mcd}(r_{n-1}, 0) = r_{n-1}.$$

□

Ejemplo 1.20. Veamos cómo el algoritmo de Euclides sirve no sólo para calcular el máximo común divisor de dos números, sino también para obtenerlo como combinación lineal de ellos, como indica el Teorema 1.8. por ejemplo, supongamos que queremos calcular $\mathrm{mcd}(28, 72)$ y escribirlo en función de 28 y 72. Efectuamos para ellos las sucesivas divisiones euclídeas:

$$72 = 2 \cdot 28 + 16$$

$$28 = 1 \cdot 16 + 12$$

$$16 = 1 \cdot 12 + 4$$

$$12 = 3 \cdot 4 + 0.$$

Hemos llegado por tanto a un resto 0, luego el máximo común divisor de 72 y 28 es el resto anterior, que es 4 (que es, por supuesto, el máximo común divisor obtenido a partir de la descomposición de $72, 28$ en factores primos). Si vamos despejando este 4 desde la penúltima división hacia arriba obtendremos:

$$4 = 16 - 1 \cdot 12 = 16 - 1 \cdot (28 - 1 \cdot 16) = 2 \cdot 16 - 28 = 2(72 - 2 \cdot 28) - 28 = 2 \cdot 72 - 5 \cdot 28,$$

lo que nos da la expresión de 4 como combinación de 72 y 28, confirmando por tanto el Teorema de Bézout.

Teorema 1.21. *Dados $a, b, c \in \mathbb{Z}$ y $d = \mathrm{mcd}(a, b)$, la ecuación $ax + by = c$ tiene solución si y sólo si $d|c$. Además, si x_0, y_0 es una solución de la ecuación y , b no son simultáneamente nulos, el conjunto de soluciones se puede escribir como*

$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ y = y_0 - \dfrac{a}{d}t \end{cases}$$

con $t \in \mathbb{Z}$.

Demostración: Que la ecuación tenga solución si y sólo si $d|c$ (es decir, c es un múltiplo de d) es una mera reformulación del Teorema 1.8. Por otra parte, supongamos que tenemos una solución fija x_0, y_0, es decir, $c = ax_0 + by_0$. El hecho de que a, b no son simultáneamente cero quiere decir que $d \neq 0$, por lo que podemos dividir por d. Es claro entonces que los pares de la forma $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ son solución de la ecuación.

Recíprocamente, si x, y es una solución de la ecuación, entonces $ax + by = ax_0 + by_0$, que es equivalente a $a(x - x_0) = b(y_0 - y)$ o también $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$, por lo que

$\frac{a}{d}|\frac{b}{d}(y_0 - y)$. Por la Proposición 1.5(ii) se tiene $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$, luego por el Lema de Euclides (Teorema 1.13) se tiene $\frac{a}{d}|y_0 - y$, luego existe $t \in \mathbb{Z}$ tal que $y_0 - y = \frac{a}{d}t$, es decir, $y = y_0 - \frac{a}{d}t$. Sustituyendo y por este valor en $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$ se obtiene $x = x_0 + \frac{b}{d}t$, luego todas las soluciones son de la forma del enunciado. □

Ejemplo 1.22. Retomemos el Ejemplo 1.20 para ver cómo resolver de forma práctica una ecuación como la del teorema anterior. Nos planteamos resolver la ecuación $72x + 28y = 8$. Como $\text{mcd}(72, 28) = 4$ y $4|8$, la ecuación tiene solución. Además, vimos que podemos escribir $4 = 2 \cdot 72 - 5 \cdot 28$, por lo que multiplicando por 2 obtenemos que $x_0 = 4,\ y_0 = -10$ es una solución. Las soluciones de la ecuación serán, por tanto, de la forma

$$\begin{cases} x = \quad 4 + 7t \\ y = -10 - 18t \end{cases}$$

con $t \in \mathbb{Z}$. Obsérvese que este proceso puede interpretarse como encontrar todos los puntos de la recta $72x + 28y = 8$ del plano afín que tienen sus dos coordenadas enteras. El Teorema 1.21 nos da una caracterización de cuándo una recta afín dada por una ecuación implícita con coeficientes enteros tiene puntos con coordenadas enteras. Además, en caso afirmativo, los puntos de coordenadas enteras se pueden obtener dando valores enteros a una ecuación paramétrica (con coeficientes enteros) de la recta.

2. Teoría de congruencias

Definición. Fijado un número entero positivo n y dados números enteros a, b, diremos que *a es congruente con b módulo n*, y lo denotaremos con $a \equiv b \pmod{n}$, si $n|a-b$.

Proposición 2.1. *Fijado un entero $n > 0$ y dados números enteros a, b, c, d, se tiene:*

(i) $a \equiv a \pmod{n}$.

(ii) $a \equiv b \pmod{n}$ *si y sólo si* $b \equiv a \pmod{n}$.

(iii) Si $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$, *entonces* $a \equiv c \pmod{n}$.

(iv) Si $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$, *entonces y* $a + c \equiv b + d \pmod{n}$.

(v) Si $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$,, *entonces* $ac \equiv bd \pmod{n}$.

(vi) Si $ac \equiv bc \pmod{n}$, *entonces* $a \equiv b \pmod{\frac{n}{d}}$, *donde* $d = \mathrm{mcd}(c, n)$. *En particular, si* $\mathrm{mcd}(c, n) = 1$, *entonces* $ac \equiv bc \pmod{n}$ *si y sólo si* $a \equiv b \pmod{n}$.

Demostración: Es un simple ejercicio que se deja al lector. Hagamos al menos la demostración de la parte (vi). Por definición, $ac \equiv bc \pmod{n}$ quiere decir $n|ac-bc = (a-b)c$. Dividiendo por d tendremos $\frac{n}{d}|(a-b)\frac{c}{d}$. Como $\mathrm{mcd}(\frac{n}{d}, \frac{c}{d}) = 1$ (ver Proposición 1.5(ii)), por el Lema de Euclides (Teorema 1.13) se sigue $\frac{n}{d}|(a-b)$, es decir, $a \equiv b \pmod{\frac{n}{d}}$. □

Observación 2.2. En lenguaje más matemático, obsérvese que las tres primeras propiedades de la Proposición 2.1 están diciendo que la relación $\equiv \pmod{n}$ es una relación de equivalencia ((i) es la propiedad reflexiva, (ii) es la simétrica y (iii) es la transitiva). El cociente por esta relación es lo que en Álgebra Básica se denota por $\mathbb{Z}_n$, y las propiedades (iv) y (v) nos dicen que tal cociente tiene estructura de anillo. Nótese que, por la propiedad (ii), el orden de los elementos en la congruencia es indistinto, por lo que se puede hablar de que a y b son *congruentes entre sí* o no.

Una pregunta natural es si todos los enteros son congruentes a números sencillos. El siguiente resultado da una respuesta satisfactoria a dicha pregunta:

Proposición 2.3. *Dado n un número entero positivo, cada número entero a es congruente módulo n con uno y sólo uno de los elementos del conjunto $\{0, 1, \ldots, n-1\}$, precisamente al resto de la división euclídea de a entre n. En particular, dos enteros a, b son congruentes módulo n si y sólo si a y b tienen el mismo resto al dividir entre n.*

Demostración: Sea $a = qn + r$ la división euclídea de a entre n. Es claro que $n|a-r$, por lo que $a \equiv r \pmod{n}$. Por otra parte, si $a \equiv s \pmod{n}$ para algún $s \in \{0, 1, \ldots, n-1\}$, entonces $n|a-s$, luego se podría escribir $a = cn + s$, para algún $c \in \mathbb{Z}$. Como $0 \leq s < n$,

la unicidad de la división euclídea (Teorema 1.6) implica que $a = cn + s$ es precisamente la división euclídea de a , por lo que $s = r$. □

De hecho, la proposición anterior no hace sino decir en otro lenguaje un resultado que ya conocíamos: que, fijado n, cada número entero se puede escribir de una sola de las formas $nk + r$, con $r \in \{0, 1, \ldots, n-1\}$. Si cambiamos el conjunto $\{0, 1, \ldots, n-1\}$, tendremos la siguiente definición.

Definición. Se llama *sistema completo de restos módulo n* a un conjunto R de números enteros tales que cada $a \in \mathbb{Z}$ es congruente módulo n a un elemento de R y sólo a uno.

Por ejemplo, $\{8, -3, 6, -1\}$ sería un sistema completo de restos módulo 4, ya que $8 \equiv 0 \pmod 4$, $-3 \equiv 1 \pmod 4$, $6 \equiv 2 \pmod 4$ y $-1 \equiv 3 \pmod 4$. En otras palabras, comparando con la Observación 1.7, estamos diciendo que cada número entero es de una y sólo una de las formas $4k + 8, 4k - 3, 4k + 6, 4k - 1$. Una partición así puede parecer arbitraria, pero por ejemplo el lector puede darse cuenta ahora de que nuestra demostración de la existencia de infinitos números primos de la forma $4k + 3$ utilizaba en realidad los números de la forma $4k - 1$.

Damos a continuación un método útil para caracterizar sistemas completos de restos módulo un número n (que da en particular, como condición necesaria, que deben ser conjuntos de n elementos).

Lema 2.4. *Sea n un número entero positivo y sea $R = \{r_1, r_2, \ldots, r_m\}$ un conjunto de números enteros. Sean $r'_1, r'_2, \ldots, r'_m$ respectivamente los restos de la división euclídea entre n de $r_1, r_2, \ldots, r_m$. Entonces son equivalentes:*

(i) R es un sistema completo de restos módulo n.

(ii) $m \geq n$ y para cada $i \neq j$ se tiene $r_i \not\equiv r_j \pmod n$.

(iii) Los números $r'_1, r'_2, \ldots, r'_m$ coinciden, en cierto orden, con $0, 1, \ldots, n-1$.

Demostración: Haremos la demostración de forma cíclica.

(i)⇒(ii): Como cada uno de los números $0, 1, \ldots, n-1$ son congruentes módulo n a algún elemento de R y dos de ellos no son congruentes entre sí, necesariamente R debe contener al menos n elementos, es decir, $m \geq n$.

Además, si para algún $i \neq j$ fuera $r_i \equiv r_j \pmod n$, entonces el número r_i sería simultáneamente congruente módulo n con r_i y r_j, contrario a la definición de sistema completo.

(ii)⇒(iii): Si $i \neq j$, tenemos por hipótesis $r_i \not\equiv r_j \pmod n$, luego, por la Proposición 2.3, se tendrá $r'_i \neq r'_j$. Por tanto, los números $r'_1, r'_2, \ldots, r'_m$ son m números distintos entre los n números $0, 1, \ldots, n-1$. Como $m \geq n$, ambos sistemas de números deben coincidir.

(iii)⇒(i): Por la Proposición 2.3, cada número entero es congruente con uno y sólo uno de los números $0, 1, \ldots, n-1$, que por hipótesis son los números $r'_1, r'_2, \ldots, r'_m$. Como, de nuevo por la Proposición 2.3, un número es congruente con r'_i si y sólo si es congruente con r_i, se concluye que cada número entero es congruente con uno y sólo uno de los números $r_1, r_2, \ldots, r_m$, es decir, R es un sistema completo de restos módulo n. □

A partir del lema, podemos ya dar muchas formas de construir sistemas completos de restos módulo n:

Proposición 2.5. *Dado un entero positivo n, los siguientes conjuntos son sistemas completos de restos módulo n:*

(i) Cualquier conjunto de n enteros consecutivos.

(ii) $\{ar_1 + b, ar_2 + b, \ldots, ar_n + b\}$, donde $\{r_1, r_2, \ldots, r_n\}$ es un sistema completo de restos módulo n, a es un entero tal que $\mathrm{mcd}(a, n) = 1$ y b es un entero cualquiera.

(iii) $\{b, a + b, 2a + b, \ldots, (n-1)a + b\}$, donde a es un entero tal que $\mathrm{mcd}(a, n) = 1$ y b es un entero cualquiera.

Demostración: Es todo consecuencia del Lema 2.4(ii). Para el conjunto (i) usamos que tiene n elementos y que claramente no hay dos elementos que sean congruentes entre sí. Para el conjunto (ii), usamos que, por ser $\{r_1, r_2, \ldots, r_n\}$ es un sistema completo de restos módulo n, si $i \neq j$ entonces $r_i \not\equiv r_j \pmod{n}$. Como $\mathrm{mcd}(a, n) = 1$, se sigue de la Proposición 2.1 que $ar_i \not\equiv ar_j \pmod{n}$ y $ar_i + b \not\equiv ar_j + b \pmod{n}$. El Lema 2.4(ii) implica entonces que $\{ar_1 + b, ar_2 + b, \ldots, ar_n + b\}$ es un sistema completo de restos módulo n. Finalmente, (iii) es el caso particular de (ii) en que tomamos $\{r_1, r_2, \ldots, r_n\} = \{0, 1, \ldots, n-1\}$. □

Ejemplo 2.6. Se pueden usar las congruencias para dar criterios de divisibilidad. Recordemos que un número con expresión decimal $a_r a_{r-1} \ldots a_1 a_0$ quiere decir el número $n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_1 \cdot 10 + a_0$. Entonces, por ejemplo:

–Como $10 \equiv 1 \pmod{3}$, se sigue de las propiedades del Lema 2.1 que $n \equiv a_r + a_{r-1} + \ldots + a_1 + a_0 \pmod{3}$. En particular se obtiene el resultado conocido: *un número es divisible por* 3 *si y sólo si la suma de sus cifras es divisible por* 3.

–Como también $10 \equiv 1 \pmod{9}$, se obtiene del mismo modo que *un número es divisible por* 9 *si y sólo si la suma de sus cifras es divisible por* 9. Más aún, de la congruencia $n \equiv a_r + a_{r-1} + \ldots + a_1 + a_0 \pmod{3}$ se sigue la clásica *prueba del nueve*. Por ejemplo, si queremos multiplicar 53914 por 13518, usamos que

$$161277 \equiv 1 + 6 + 1 + 2 + 7 + 7 = 24 \equiv 2 + 4 = 6 \pmod{9}$$

$$140263 \equiv 1+4+0+2+6+3 = 16 \equiv 1+6 = 7 \pmod{9}$$

por lo que debe ser

$$161277 \cdot 140263 \equiv 6 \cdot 7 = 42 \equiv 4+2 = 6 \pmod{9}.$$

Por tanto, una forma de comprobar que el producto está bien calculado es comprobar del mismo modo que es congruente con 6 módulo 9. Y, en efecto, tenemos:

$$22621195851 \equiv 2+2+6+2+1+1+9+5+8+5+1 = 42 \equiv 4+2 = 6 \pmod{9}.$$

Obviamente, si la prueba no sale es que la operación está mal hecha, pero el que salga bien la prueba no implica que la operación esté bien hecha (por ejemplo, 22531195851 hubiera dado el mismo resultado módulo 9).

–Si usamos ahora $10 \equiv -1 \pmod{11}$, obtenemos el criterio que *un número es divisible por* 11 *si y sólo si la suma con signo alternado de sus cifras es divisible por* 11, ya que $n \equiv (-1)^r a_r + (-1)^{r-1} a_{r-1} + \ldots - a_1 + a_0 \pmod{11}$. De hecho, este hecho nos permite inventarnos una "prueba del once". Siguiendo con el ejmplo anterior, tendremos:

$$161277 \equiv -1+6-1+2-7+7 = 6 \pmod{11}$$

$$140263 \equiv -1+4-0+2-6+3 = 2 \pmod{11}$$

por lo que debe ser

$$161277 \cdot 140263 \equiv 6 \cdot 2 = 12 \equiv -1+2 = 1 \pmod{11}.$$

En efecto, tenemos

$$22621195851 \equiv 2-2+6-2+1-1+9-5+8-5+1 = 12 \equiv -1+2 = 1 \pmod{11}.$$

Obsérvese que esta nueva prueba serviría para reforzar la prueba del nueve, ya que ahora $22531195851 \equiv 2-2+5-3+1-1+9-5+8-5+1 = 10 \not\equiv 1 \pmod{11}$, lo que indica que 22531195851 no puede ser el producto.

Muchas veces es más sencillo reducir una congruencia módulo un entero n a congruencias con módulos más pequeños que n. El siguiente resultado explica cómo:

Proposición 2.7. *Sean $n_1, n_2, \ldots, n_r$ números naturales tales que $\mathrm{mcd}(n_i, n_j) = 1$ si $i \neq j$. Entonces, para cada par de enteros a, b se tiene que $a \equiv b \pmod{n_1 n_2 \ldots n_r}$ si y sólo si $a \equiv b \pmod{n_1}$, $a \equiv b \pmod{n_2}, \ldots, a \equiv b \pmod{n_r}$.*

Demostración: Por definición, $a \equiv b \pmod{n_1 n_2 \ldots n_r}$ si y sólo si $n_1 n_2 \ldots n_r | a-b$. Como $\mathrm{mcd}(n_i, n_j) = 1$ si $i \neq j$, el Corolario 1.12 implica que $n_1 n_2 \ldots n_r | a-b$ es equivalente a que, para cada $i = 1, 2, \ldots, r$, se tenga $n_i | a-b$, es decir, $a \equiv b \pmod{n_i}$. □

Si en cambio queremos pasar de una congruencia módulo n a congruencias módulo un único divisor de n, entonces el resultado es más complicado:

Proposición 2.8. *Si $d|n$ entonces $a \equiv b \pmod{\frac{n}{d}}$ si y sólo si $a \equiv b + i\frac{n}{d} \pmod{n}$ para algún $i \in \{0, 1, \ldots, d-1\}$. Además, los números $b, b + \frac{n}{d}, \ldots, b + (d-1)\frac{n}{d}$ son dos a dos incongruentes módulo n.*

Demostración: Por una parte, es claro que, si $a \equiv b + i\frac{n}{d} \pmod{n}$, entonces existe $c \in \mathbb{Z}$ tal que $a - b - i\frac{n}{d} = cn$. Por tanto, $a = b + \frac{n}{d}(i + cd)$, luego $a \equiv b \pmod{\frac{n}{d}}$.

Recíprocamente, si $a \equiv b \pmod{\frac{n}{d}}$, existe $t \in \mathbb{Z}$ tal que $a = b + \frac{n}{d}t$. Consideramos la división euclídea de t entre d:

$$t = qd + r$$

con $0 \leq r < d$. Por tanto, podremos escribir

$$a = b + \frac{n}{d}t = b + \frac{n}{d}(qd + r) = b + nq + r\frac{n}{d}.$$

De aquí se deduce $a \equiv b + r\frac{n}{d} \pmod{n}$ y, como $0 \leq r < d$, es una de las d congruencias que queríamos.

Finalmente, los números $b, b + \frac{n}{d}, \ldots, b + (d-1)\frac{n}{d}$ son dos a dos incongruentes módulo n porque son un subconjunto de los números $b, b + 1, \ldots, b + (n-1)$, que es un sistema completo de restos módulo n (Proposición 2.5(i)). □

Con el lenguaje de congruencias, podemos reinterpretar el Teorema 1.21 del siguiente modo:

Proposición 2.9. *Sean a, b, n numeros enteros con $n > 0$ y $a \neq 0$, y sea $d = \mathrm{mcd}(a, n)$. Entonces la congruencia $ax \equiv b \pmod{n}$ tiene solución si y sólo si $d|b$. Además, en este caso hay exactamente d soluciones módulo n.*

Demostración: La congruencia tiene solución si y sólo si existe $x \in \mathbb{Z}$ tal que $n|b - ax$, es decir, si y sólo si existen $x, y \in \mathbb{Z}$ tales que $b - ax = ny$. Como el Teorema 1.21 afirma que la ecuación $ax + ny = b$ tiene solución si y sólo si $d|b$, la primera parte queda demostrada. Además, el mismo Teorema 1.21 dice que las soluciones de la ecuación dependen de un parámetro t y son de la forma

$$\begin{cases} x = x_0 + \dfrac{n}{d}t \\ y = y_0 - \dfrac{a}{d}t. \end{cases}$$

Entonces las soluciones de la congruencia son los enteros x de la forma $x \equiv x_0 \pmod{\frac{n}{d}}$ que, por la Proposición 2.8, da d soluciones módulo n. □

Ejemplo 2.10. Consideremos la congruencia lineal $72x \equiv 8 \pmod{28}$. Como indica la demostración de la Proposición 2.9, para resolverla, debemos resolver primero la ecuación

$72x + 28y = 8$, que ya resolvimos en el Ejemplo 1.22, y cuya solución era

$$\begin{cases} x = \quad 4 + 7t \\ y = -10 - 18t. \end{cases}$$

Por tanto, la solución a nuestra congruencia es $x = 4+7t$, es decir $x \equiv 4 \pmod{7}$ o, escrito módulo 28, $x \equiv 4, 11, 18, 25 \pmod{28}$.

La Proposición 2.9 nos dice que toda congruencia de la forma $ax \equiv b \pmod{n}$ es equivalente a varias congruencias de la forma $x \equiv x_0 \pmod{n}$ (o en realidad a una congruencia de la forma $x \equiv x_0 \pmod{\frac{n}{d}}$). Por tanto, si queremos resolver varias congruencias lineales al mismo tiempo basta resolver un sistema de congruencias todas del tipo $x \equiv x_0 \pmod{n}$. El siguiente teorema nos dice cómo resolver tales sistemas. El interés del resultado no será sólo el enunciado teórico (existencia de solución bajo ciertas hipótesis), sino también la demostración, que da un método efectivo de resolución.

Teorema 2.11 (chino del resto)**.** *Sean $n_1, n_2, \ldots, n_r$ números enteros positivos tales que $\mathrm{mcd}(n_i, n_j) = 1$ si $i \neq j$. Entonces cualquier sistema de congruencias*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

tiene solución, que además es única módulo $n_1 n_2 \ldots n_r$.

Demostración: Para cada $i = 1, 2, \ldots, r$ definimos

$$N_i = \frac{n_1 n_2 \ldots n_r}{n_i} = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_r.$$

Por el Corolario 1.10 se tendrá $\mathrm{mcd}(n_i, N_i) = 1$, ya que $\mathrm{mcd}(n_i, n_j) = 1$ para cada factor n_j de N_i. Por tanto, por la Proposición 2.9, existe $x_i \in \mathbb{Z}$ tal que $N_i x_i \equiv a_i \pmod{n_i}$, ya que obviamente $\mathrm{mcd}(n_i, N_i) | a_i$. Veamos que

$$x_0 = N_1 x_1 + N_2 x_2 + \ldots + N_r x_r$$

es una solución del sistema de congruencias. En efecto, para cada $i = 1, 2, \ldots, r$ se tiene $N_j \equiv 0 \pmod{n_i}$ si $i \neq j$, luego $x_0 \equiv N_i x_i \equiv a_i \pmod{n_i}$.

Para la unicidad, observemos en primer lugar que, si $x \equiv x_0 \pmod{n_1 n_2 \ldots n_r}$, es claro que x es también solución del sistema de congruencias. Recíprocamente, sea x una

solución del sistema. Entonces $x \equiv x_0 \pmod{n_i}$ para cada $i = 1, 2, \ldots, r$, luego, por la Proposición 2.7, $x \equiv x_0 \pmod{n_1 n_2 \ldots n_r}$. □

Ejemplo 2.12. Veamos que el resultado anterior se puede usar incluso si los n_i no son todos primos entre sí (con la diferencia de que entonces puede ocurrir que el sistema de congruencias no tenga solución). Supongamos por ejemplo que queremos resolver el sistema de congruencias

$$\begin{cases} x \equiv 5 \pmod{24} \\ x \equiv 1 \pmod{28} \\ x \equiv -4 \pmod{15} \end{cases}$$

Evidentemente, no estamos en las condiciones del Teorema Chino del Resto, ya que, por ejemplo, $\mcd(24, 28) = 4$. Sin embargo, podemos usar la Proposición 2.7 para sustituir nuestro sistema por el sistema equivalente:

$$\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 5 \pmod{3} \\ x \equiv 1 \pmod{4} \\ x \equiv 1 \pmod{7} \\ x \equiv -4 \pmod{3} \\ x \equiv -4 \pmod{5}. \end{cases}$$

Por supuesto, seguimos sin estar en las hipótesis del Teorema Chino del Resto, pero ahora vamos a poder quitar las congruencias que nos sobran. En primer lugar, tenemos las congruencias $x \equiv 5 \pmod{3}$ y $x \equiv -4 \pmod{3}$, que son equivalentes, ya que $5 \equiv -4 \pmod{3}$, así que podemos eliminar una de ellas. Aún tenemos el par de congruencias $x \equiv 5 \pmod{8}$ y $x \equiv 1 \pmod{4}$ que no nos permiten aplicar el Teorema Chino del Resto. En este caso, observamos que $x \equiv 5 \pmod{8}$ implica obviamente $x \equiv 5 \pmod{4}$, que es equivalente a $x \equiv 1 \pmod{4}$, porque $5 \equiv 1 \pmod{4}$. Así pues, podemos eliminar la congruencia $x \equiv 1 \pmod{4}$ y tenemos ya el sistema equivalente de congruencias:

$$\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 5 \pmod{3} \\ x \equiv 1 \pmod{7} \\ x \equiv -4 \pmod{5} \end{cases}$$

que ya está en las hipótesis del Teorema Chino del Resto, luego ya sabemos que tiene solución (vale la pena hacer aquí una pausa para observar que podría haber ocurrido que,

en lugar de encontrar congruencias equivalentes módulo 4, hubiéramos encontrado congruencias incompatibles; esto hubiera querido decir que el sistema de partida es incompatible y no tiene solución). Aplicamos ahora el método de resolución que nos da el Teorema Chino del Resto, es decir, resolvemos primero (con el método explicado en el Ejemplo 2.10) las congruencias:

- $105x \equiv 5 (\text{mod } 8)$, que tiene como solución $x \equiv 5 (\text{mod } 8)$.
- $280x \equiv 5 (\text{mod } 3)$, que tiene como solución $x \equiv 2 \ (\text{mod } 3)$.
- $120x \equiv 1 (\text{mod } 7)$, que tiene como solución $x \equiv 1 \ (\text{mod } 7)$.
- $168x \equiv -4 (\text{mod } 5)$, que tiene como solución $x \equiv 2 \ (\text{mod } 5)$.

La solución final queda, por tanto

$$x \equiv 105 \cdot 5 + 280 \cdot 2 + 120 \cdot 1 + 168 \cdot 2 = 1541 \equiv 701 \ (\text{mod } 840).$$

Como nos indica el ejemplo anterior, para estudiar congruencias, basta estudiar congruencias módulo la potencia de un primo. El caso más simple es el de congruencias módulo un primo, sobre el que se pueden demostrar toda una serie de resultados. El primero de todos es el siguiente:

Teorema 2.13 (Fermat)**.** *Sea p un número primo. Entonces, para cada $a \in \mathbb{Z}$ no divisible por p se tiene $a^{p-1} \equiv 1 \ (\text{mod } p)$. Como consecuencia, $a^p \equiv a \ (\text{mod } p)$ para cualquier $a \in \mathbb{Z}$.*

Demostración: Por la Proposición 2.5(iii), sabemos que, si $\text{mcd}(a, p) = 1$, los números $0, a, 2a, \ldots, (p-1)a$ forman un sistema completo de restos módulo p. Por el Lema 2.4, esto quiere decir que sus restos al dividir por p son, en cierto orden, $0, 1, 2, \ldots, p-1$. Como obviamente el cero del primer conjunto se corresponde con el cero del segundo, se tiene que los números $a, 2a, \ldots, (p-1)a$ son congruentes módulo p, en cierto orden, con $1, 2, \ldots, p-1$. Multiplicando todas las congruencias tendremos $(p-1)!a^{p-1} \equiv (p-1)! \ (\text{mod } p)$. Además, como p es un número primo, es coprimo con todos los factores $1, 2, \ldots, p-1$ de $(p-1)!$, luego (Corolario 1.10) $\text{mcd}((p-1)!, p) = 1$. Se sigue entonces de la Proposición 2.1(vi) que $a^{p-1} \equiv 1 \ (\text{mod } p)$.

La congruencia anterior implica automáticamente $a^p \equiv a \ (\text{mod } p)$, siempre bajo la hipótesis $\text{mcd}(a, p) = 1$. Si en cambio $p|a$, entonces tanto a^p como a son congruentes con cero módulo p, luego la congruencia $a^p \equiv a \ (\text{mod } p)$ es también válida en este caso. □

La propiedad del Teorema de Fermat no es característica de los números primos, ya que hay números compuestos que satisfacen lo mismo.

Definición. Se llama *número pseudoprimo en base a* a un número compuesto n tal que $a^n \equiv a \pmod{n}$. Se llama simplemente *número pseudoprimo* a un número compuesto n tal que $2^n \equiv 2 \pmod{n}$. Finalmente, se llama *pseudoprimo absoluto* o *número de Carmichael* a un número compuesto n tal que $a^n \equiv a \pmod{n}$ para cualquier número entero a.

Obviamente son mucho más interesantes (y más difíciles de encontrar) los números de Carmichael que los pseudoprimos (aunque los matemáticos chinos de hace 25 siglos pensaban que no había números pseudoprimos). De ambos se sabe que hay infinitos de ellos. En el caso de pseudoprimos, no cuesta mucho ver que, dado un número pseudoprimo impar n, entonces $2^n - 1$ es también un número pseudoprimo, lo que permite construir infinitos pseudoprimos (basta empezar por $341 = 11 \cdot 31$, que es el primer número pseudoprimo). Para números de Carmichael, nos limitaremos a dar el siguiente resultado:

Proposición 2.14. *Sea $n = p_1 p_2 \dots p_r$ un producto de r primos distintos, con $r > 1$. Si para cada $i = 1, 2, \dots, r$ se tiene $p_i - 1 | n - 1$, entonces n es un número de Carmichael.*

Demostración: Claramente n es compuesto, porque $r > 1$, así que hay que demostrar que $a^n \equiv a \pmod{p_1 p_2 \dots p_r}$ para todo entero a. Por la Proposición 2.7, hay que demostrar que, para cada $i = 1, 2, \dots, r$, se tiene $a^n \equiv a \pmod{p_i}$. Obviamente esto es cierto si $p_i | a$, así que podemos suponer $\mcd(a, p_i) = 1$. En tal caso, por el Teorema de Fermat se tendrá $a^{p_i - 1} \equiv 1 \pmod{p_i}$ y, como por hipótesis $p_i - 1 | n - 1$, se tendrá también $a^{n-1} \equiv 1 \pmod{p_i}$, lo que implica $a^n \equiv a \pmod{p_i}$. □

Ejemplo 2.15. Con la proposición anterior, se demuestra que $561 = 3 \cdot 11 \cdot 17$ es un número de Carmichael (de hecho es el primero de todos). Otros ejemplos obtenidos de este modo son los números $1729 = 7 \cdot 13 \cdot 19$, $6601 = 7 \cdot 23 \cdot 41$ y $10585 = 5 \cdot 29 \cdot 73$. Aunque no verifiquen el critero de la proposición anterior, también son números de Carmichael $1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot 13 \cdot 31$, $15841 = 7 \cdot 31 \cdot 73$ y $16046641 = 13 \cdot 37 \cdot 73 \cdot 457$ (uno de los pocos conocidos con cuatro factores, descubierto por el propio Carmichael). Sólo en 1994 se demostró que existen infinitos números de Carmichael. Son tan escasos que sólo hay 43 de ellos menores que un millón.

Ejemplo 2.16. Si consideramos el conjunto de restos módulo 11, observamos que tenemos los pares disjuntos $\{2, 6\}$, $\{3, 4\}$, $\{5, 9\}$, $\{7, 8\}$ con la propiedad de que el producto de los elementos de un par es congruente con 1 módulo 11. Además, la unión de todos los pares da el conjunto $\{2, 3, 4, 5, 6, 7, 8, 9\}$, por lo que tendremos

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \equiv 1 \pmod{11}.$$

Esto no es casualidad, y para cada número primo tenemos la misma situación, lo que nos permite demostrar el siguiente teorema.

Teorema 2.17 (Wilson)**.** *Si p es un número primo, entonces* $(p-1)! \equiv -1 \pmod{p}$.

Demostración: Suponemos $p > 3$, ya que los casos $p = 2, 3$ se pueden comprobar trivialmente a mano. Para cada $a = 1, 2 \ldots, p-1$, consideramos la congruencia $ax \equiv 1 \pmod{p}$ que, por la Proposición 2.9 tendrá exactamente una solución módulo p, luego se podrá representar exactamente por un número $a' \in \{1, 2, \ldots, p-1\}$ (claramente, no puede ser $a' = 0$). Por tanto, tenemos una aplicación $\{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}$ que asocia a cada a el elemento a'. Tal aplicación es necesariamente biyectiva, al tener ambos conjuntos el mismo número de elementos. Obsérvese que, si $a' = a$, entonces $a^2 \equiv 1 \pmod{p}$, es decir $p | a^2 - 1 = (a+1)(a-1)$. Por el Corolario 1.14, se tiene $p | a+1$ o bien $p | a-1$. Como $a \in \{1, 2, \ldots, p-1\}$, se sigue $a = 1$ o bien $a = p-1$. Por tanto, el conjunto $\{2, 3, \ldots, p-2\}$ se descompone, como en el Ejemplo 2.16, en pares $\{a, a'\}$ con la propiedad $aa' \equiv 1 \pmod{p}$. Agrupando según estos pares el producto de todos los elementos de $\{2, 3, \ldots, p-2\}$, se llega a $2 \cdot 3 \ldots (p-2) \equiv 1 \pmod{p}$ y, por tanto, $(p-1)! = 1 \cdot (2 \cdot 3 \ldots (p-2))(p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$, como queríamos. □

Observación 2.18. Nótese que, al contrario que pasa con el teorema de Fermat, la propiedad anterior sí que caracteriza a los números primos. En efecto, dado un número compuesto n, si $d \neq 1, n$ es un divisor suyo, se tendrá que d es uno de los factores de $(n-1)!$, por lo que $(n-1)! \equiv 0 \pmod{d}$. Por tanto, no puede ser $(n-1)! \equiv -1 \pmod{n}$. En realidad, no es difícil demostrar que, si $n > 4$ es un número compuesto, entonces $(n-1)! \equiv 0 \pmod{n}$.

El Teorema de Wilson tiene el siguiente corolario inesperado:

Teorema 2.19. *Si p es primo, la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y sólo si $p = 2$ o bien $p \equiv 1 \pmod{4}$.*

Demostración: Supongamos primero que la congruencia tiene una solución, que llamaremos a. Obviamente, a no puede ser divisible por p, porque en tal caso $a^2 \equiv 0 \pmod{p}$. Para ver que $p = 2$ o bien $p \equiv 1 \pmod{4}$ basta demostrar que $p \not\equiv 3 \pmod{4}$. En efecto, si fuera $p \equiv 3 \pmod{4}$, entonces $\frac{p-1}{2}$ sería un número impar, y como $a^2 \equiv -1 \pmod{p}$, entonces

$$a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p} = -1 \pmod{p},$$

mientras que el Teorema de Fermat (Teorema 2.13), implica $a^{p-1} \equiv 1 \pmod{p}$, lo que da una contradicción.

Recíprocamente, supongamos $p = 2$ o bien $p \equiv 1 \pmod{4}$ y veamos que la congruencia tiene solución. Es claro que $x^2 \equiv -1 \pmod{2}$ tiene solución (de hecho, cualquier x impar

lo es), así que podemos limitarnos al caso $p \equiv 1 \pmod 4$. En tal caso, tenemos que $\frac{p-1}{2}$ es un número par. Esto quiere decir que el número de congruencias (triviales)

$$1 \equiv -(p-1) \pmod p$$

$$2 \equiv -(p-2) \pmod p$$

$$\vdots$$

$$\frac{p-1}{2} \equiv -\frac{p+1}{2} \pmod p$$

es par. Por tanto, multiplicándolas todas tendremos

$$(\frac{p-1}{2})! \equiv (p-1)(p-2)\dots\frac{p+1}{2} \pmod p$$

de donde se deduce, usando el Teorema de Wilson para la última congruencia,

$$\big((\frac{p-1}{2})!\big)^2 \equiv (p-1)(p-2)\dots\frac{p+1}{2}(\frac{p-1}{2})! = (p-1)! \equiv -1 \pmod p.$$

Por tanto, $x = (\frac{p-1}{2})!$ es una solución de $x^2 \equiv -1 \pmod p$.

□

Corolario 2.20. *Existen infinitos números primos de la forma* $4k+1$.

Demostración: Como siempre, supongamos por reducción al absurdo que $p_1, p_2, \dots, p_r$ sean todos los números primos de la forma $4k+1$. Consideramos entonces el número $a = (2p_1p_2\dots p_r)^2 + 1$ y sea p un divisor primo de a (que obviamente existe, por ser $a > 4$. Entonces, $2p_1p_2\dots p_r$ es una solución de la congruencia $x^2 \equiv -1 \pmod p$, por lo que el Teorema 2.19 implica que $p = 2$ o bien p es de la forma $4k+1$, es decir, es uno de los $p_1, p_2, \dots, p_r$. Como claramente ni 2 ni $p_1, p_2, \dots, p_r$ son divisores de a, se llega la contradicción buscada. □

Podemos mejorar el resultado anterior de la misma forma que hicimos en la Observación 1.7 con el Teorema de Euclides:

Corolario 2.21. *Existen infinitos números primos de la forma* $8k+5$.

Demostración: Supongamos que $p_1, p_2, \dots, p_r$ sean todos los números primos de la forma $8k+5$, y consideramos de nuevo $a = (2p_1p_2\dots p_r)^2 + 1$. Ya hemos observado en la demostración anterior que los divisores primos de a son de la forma $4k+1$. Por tanto, son de la forma $8k+1$ o bien $8k+5$. Ahora bien, como cada $(p_1p_2\dots p_r)^2$ es impar, es decir, de la forma $2k+1$, entonces $a = 4(p_1p_2\dots p_r)^2 + 1$ es de la forma $8k+5$. Por tanto, no todos los divisores primos de a son de la forma $8k+1$, por lo que a es divisible por algún primo de la forma $8k+5$, es decir, por algún p_i, lo que es imposible. □

3. Funciones aritméticas

Vamos a intentar extender ahora el Teorema de Fermat (Teorema 2.13) cuando el exponente es un número arbitrario n no necesariamente primo. Mirando a la demostración, vamos a necesitar multiplicar sólo los restos módulo n que sean coprimos con n (pues si no, no podríamos cancelarlos luego). Ahora bien, ¿cuántos restos hay coprimos con n? Claramente, esto dependerá de n, es decir, será una función, a la que de momento damos un nombre (nuestro objetivo en este capítulo será estudiar funciones de este tipo):

Definición. Se llama *función ϕ de Euler* a la función $\phi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ que asocia a cada entero $n \geq 1$ el número $\phi(n)$ de enteros $r \in \{1, 2, \ldots, n\}$ tales que $\mathrm{mcd}(r, n) = 1$. Nótese que, como ni $r = 0$ ni $r = n$ verifican $\mathrm{mcd}(r, n) = 1$, se puede definir también $\phi(n)$ como el número de enteros $r \in \{0, 1, \ldots, n-1\}$ tales que $\mathrm{mcd}(r, n) = 1$.

Con esta definición, la generalización del Lema 2.4 (en realidad sólo la implicación que nos intereresa) es la siguiente:

Lema 3.1. *Sea n un número entero positivo y sean $r_1, r_2, \ldots, r_m$ números enteros enteros tales que, $m \geq \phi(n)$, para todo $i = 1, 2, \ldots, m$ se tiene $\mathrm{mcd}(r_i, n) = 1$ y $\mathrm{mcd}(r_i, r_j) = 1$ si $j \neq i$. Entonces, los restos de la división euclídea de $r_1, r_2, \ldots, r_m$ entre n son todos distintos y coinciden, en cierto orden, con los números entre 0 y n que son coprimos con n.*

Demostración: Consideramos en primer lugar los números $s_1, s_2, \ldots, s_r \in \{0, 1, \ldots, n-1\}$ tales que $\mathrm{mcd}(s_j, n) \neq 1$ para $j = 1, 2, \ldots, r$. Obsérvese que, por definición, $r = n - \phi(n)$. Como $s_1, s_2, \ldots, s_r$ forman parte de un sistema completo de restos módulo n, son incongruentes dos a dos módulo n. Además, ningún r_i es congruente módulo n con ningún s_j, ya que eso querría decir que $\mathrm{mcd}(r_i, n) = \mathrm{mcd}(s_j, n)$, contra nuestra hipótesis. Por tanto, por el Lema 2.4, como $m + r = m + n - \phi(m) \geq n$, se tiene que los restos de la división de $r_1, r_2, \ldots, r_m, s_1, s_2, \ldots, s_r$ entre n son todos distintos y coinciden, en cierto orden con $0, 1, \ldots, n-1$. Como los restos de $s_1, s_2, \ldots, s_r$ son ellos mismos, el resultado queda demostrado. □

Con estas herramientas, podemos proceder ya a generalizar el Teorema de Fermat:

Teorema 3.2 (Euler)**.** *Dado un número entero $n \geq 2$, entonces para cada número entero a tal que $\mathrm{mcd}(a, n) = 1$ se tiene $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Demostración: Sean $r_1, \ldots, r_{\phi(n)}$ los enteros positivos menores que n tales que $\mathrm{mcd}(r_i, n) = 1$. Como $\mathrm{mcd}(a, n) = 1$, la Proposición 1.9 implica que $\mathrm{mcd}(ar_i, n) = 1$ para todo $i = 1, 2, \ldots, \phi(n)$ y, si $j \neq i$, la Proposición 2.1(vi) implica $ar_i \not\equiv ar_j \pmod{n}$. Por el Lema

3.1, los números $ar_1, \ldots, ar_{\phi(n)}$ son congruentes, en algún orden, con $r_1, \ldots, r_{\phi(n)}$ módulo n. Por tanto, haciendo el producto de todos ellos tendremos

$$a^{\phi(n)} r_1 \ldots r_{\phi(n)} \equiv r_1 \ldots r_{\phi(n)} \pmod{n}.$$

Como $\mcd(r_1 \ldots r_{\phi(n)}, n) = 1$ (por la Proposición 1.9), la Proposición 2.1(vi) implica $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Como consecuencia, obtenemos un método práctico para resolver una congruencia lineal:

Corolario 3.3. *Si* $\mcd(a, n) = 1$, *la congruencia lineal* $ax \equiv b \pmod{n}$ *es equivalente a* $x \equiv a^{\phi(n)-1} b \pmod{n}$.

Demostración: Por la Proposición 2.9), la congruencia tiene una única solución, así que basta ver que $a^{\phi(n)-1}b$ es una solución. Pero esto es inmediato, ya que $a(a^{\phi(n)-1}b) = a^{\phi(n)}b$ es, por el Teorema de Euler, congruente con b módulo n. □

Observación 3.4. Claramente, el Teorema de Euler es una generalización del pequeño teorema de Fermat, ya que si p es un número primo es claro que $\phi(p) = p - 1$ (puesto que $1, 2, \ldots, p-1$ son los números coprimos con p y menores que él). Más en general, si $n = p^k$, con p número primo, es claro que los enteros positivos menores o iguales que n que no son primos con n son los múltiplos de p, es decir, $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. Como hay p^{k-1} de ellos, se sigue entonces que

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - \frac{1}{p}).$$

Calcular $\phi(n)$ para un n arbitrario no parece a priori fácil. Sin embargo, tenemos la siguiente propiedad que resuelve el problema.

Teorema 3.5. *Si* $\mcd(m, n) = 1$, *entonces* $\phi(mn) = \phi(m)\phi(n)$.

Demostración: Escribimos los primeros mn números en forma de rectángulo $n \times m$:

$$\begin{array}{ccccccc}
1 & 2 & \ldots & i & \ldots & m-1 & m \\
m+1 & m+2 & \ldots & m+i & \ldots & 2m-1 & 2m \\
\vdots & \vdots & & \vdots & & \vdots & \vdots \\
jm+1 & jm+2 & \ldots & jm+i & \ldots & jm+m-i & (j+1)m \\
\vdots & \vdots & & \vdots & & \vdots & \vdots \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+i & \ldots & mn-1 & mn
\end{array}$$

es decir, escribimos cada número como $jm+i$, con $i = 1, 2, \ldots, m$ y $j = 0, 1, \ldots, n-1$. Por la Proposición 1.9, un número es primo con mn si y sólo si es primo con m y con n, luego $\phi(mn)$ será el número de elementos $jm + i$ que son primos con m y con n. La primera observación es que (por la Proposición 1.5(i)) $\mathrm{mcd}(jm + i, m) = \mathrm{mcd}(i, m)$, luego el que un número $jm+i$ sea primo con m depende sólo de la columna i-ésima en que está. Por la propia definición de ϕ, tendremos exactamente $\phi(m)$ valores de i tales que $\mathrm{mcd}(i, m) = 1$, es decir, que los elementos de la tabla que son primos con m son los elementos de $\phi(m)$ columnas.

Queda entonces ver cuántos elementos en cada columna de las $\phi(n)$ anteriores son además primos con n. De hecho, el teorema quedará demostrado si vemos que cada una de esas columnas tiene exactamente $\phi(n)$ elementos primos con n. De hecho, cualquier columna de la matriz tiene exactamente $\phi(n)$ elementos primos con n. En efecto, los elementos de una columna son de la forma $i, m + i, 2m + i, \ldots (n - 1)m + i$ que, por la Proposición 2.5(iii), forman un sistema completo de restos módulo n. Por tanto, son congruentes, aunque posiblemente en otro orden, a $0, 1, 2, \ldots, n-1$, por lo que hay exactamente $\phi(n)$ que sean coprimos con n. □

Corolario 3.6. *Si $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ es la descomposición de n en factores primos, entonces $\phi(n) = p_1^{k_1-1} p_2^{k_2-1} \ldots p_r^{k_r-1}(p_1-1)(p_2-1)\ldots(p_r-1) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_r})$.*

Demostración: Es consecuencia inmediata de que, aplicando reiteradamente el Teorema 3.5, se tiene $\phi(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = \phi(p_1^{k_1})\phi(p_2^{k_2})\ldots\phi(p_r^{k_r})$, y por otra parte, como vimos en la Observación 3.4, para cada $i = 1, 2, \ldots, r$ se tiene $\phi(p_i^{k_i}) = p_i^{k_i-1}(p_i - 1)$. □

Ejemplo 3.7. Aunque el teorema de Euler sea una generalización del de Fermat, normalmente con este último se puedun obtener resultados mejores. Por ejemplo, para estudiar cuándo una potencia es congruente con 1 módulo 35, el teorema de Euler diría que, como

$$\phi(35) = \phi(5 \cdot 7) = \phi(5)\phi(7) = (5 - 1)(7 - 1) = 24,$$

entonces $a^{24} \equiv 1 \pmod{35}$ si $\mathrm{mcd}(a, 35) = 1$. Sin embargo, como $\mathrm{mcd}(a, 35) = 1$ es equivalente a $\mathrm{mcd}(a, 5) = 1 = \mathrm{mcd}(a, 7)$ (ver Proposición 1.9), por el teorema de Fermat se tiene

$$a^4 \equiv 1 \pmod{5}$$

y

$$a^6 \equiv 1 \pmod{7}.$$

Elevando respectivamente al cubo y al cuadrado se tendrá

$$a^{12} \equiv 1 \pmod{5}$$

y

$$a^{12} \equiv 1 \pmod{7},$$

de donde se deduce $a^{12} \equiv 1 \pmod{35}$.

Definición. Una *función aritmética* es una función $f : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$. Se dice además que es *multiplicativa* si $f(mn) = f(m)f(n)$ cuando $\text{mcd}(m, n) = 1$.

Ejemplo 3.8. De forma trivial se pueden construir varias funciones aritméticas multiplicativas:

1) La función idénticamente cero es claramente multiplicativa.

2) Si una función multiplicativa f no es idénticamente cero, existe $n \in \mathbb{Z}_{\geq 1}$ tal que $f(n) \neq 0$. Como se tiene $f(n) = f(n \cdot 1) = f(n)f(1)$, se sigue entonces $f(1) = 1$. Esto sugiere otro segundo ejemplo trivial de función aritmética multiplicativa:

$$f(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

3) De la misma forma, la función idénticamente uno es claramente multiplicativa.

4) La función identidad $id(n) = n$ es también claramente multiplicativa.

5) Más en general, aunque no vayamos a usarla, para cada $k \geq 0$, la función $f(n) = n^k$ es multiplicativa.

Todos los ejemplos anteriores son "mucho más multiplicativos" que la función ϕ, ya que $f(mn) = f(m)f(n)$ independientemente de que m y n tengan factores en común o no. El siguiente resultado nos dará un modo de calcular funciones multiplicativas "más serias" a partir de otras funciones multiplicativas, aunque sean triviales:

Teorema 3.9. *Si f es una función aritmética multiplicativa, entonces la función*

$$F(n) = \sum_{d|n} f(d)$$

es también una función multiplicativa.

Demostración: Sean $m, n \in \mathbb{Z}_{\geq 1}$ tales que $\text{mcd}(m, n) = 1$. Por el Corolario 1.17(i), cada divisor positivo de mn se puede escribir como dd' con $d|m$ y $d'|n$. Podemos entonces escribir

$$F(mn) = \sum_{d|m, d'|n} f(dd') = \sum_{d|m, d'|n} f(d)f(d') = \big(\sum_{d|m} f(d)\big)\big(\sum_{d'|n} f(d')\big) = F(m)F(n).$$

□

Ejemplo 3.10. Apliquemos la construcción anterior a los ejemplos que tenemos de funciones multiplicativas.

1) Evidentemente, si f es idénticamente cero, entonces F también lo es.

2) Si f vale cero para todo n, excepto para $f(1) = 1$, es claro que entonces F es constantemente 1.

3) Cuando f es la función constante 1, se suele escribir τ para la función F correspondiente, y se tiene que $\tau(n)$ es el número de divisores positivos de n.

4) Cuando $f = id$, la función F se suele denotar σ, y se tiene que $\sigma(n)$ es la suma de los divisores positivos de n.

5) Cuando $f = \phi$, en principio no es fácil deducir quién es F. La ventaja es que sabemos que F es multiplicativa, por lo que basta calcularla para potencias de primos. Usando que los divisores de una potencia de un primo p son las potencias menores de p, tendremos, por la Observación 3.4:

$$F(p^k) = \phi(1) + \phi(p) + \phi(p^2) + \ldots + \phi(p^{k-1}) + \phi(p^k) =$$

$$= 1 + (p-1) + (p^2 - p) + \ldots + (p^{k-1} - p^{k-2}) + (p^k - p^{k-1}) = p^k.$$

Por tanto, F es la identidad en potencias de primos, y por ser multiplicativa se tendrá $F = id$. En otras palabras, hemos demostrado que para todo $n \in \mathbb{Z}_{\geq 1}$ se verifica:

$$\sum_{d|n} \phi(d) = n$$

Observación 3.11. El hecho de que las funciones τ y σ anteriores son multiplicativas se puede deducir directamente de su propia definición. En efecto, dado un número $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, con $p_1, \ldots, p_r$ primos distintos, sus divisores son (por la Proposición 1.16) los números de la forma $p_1^{a_1} \ldots p_r^{a_r}$ con $0 \leq a_i \leq k_i$, es decir, los sumandos de

$$(1 + p_1 + p_1^2 + \ldots + p_1^{k_1})(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}) \ldots (1 + p_r + p_r^2 + \ldots + p_r^{k_r}).$$

Claramente hay $(k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$ sumandos por lo que

$$\tau(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$$

y

$$\sigma(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = (1 + p_1 + p_1^2 + \ldots + p_1^{k_1})(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}) \ldots (1 + p_r + p_r^2 + \ldots + p_r^{k_r})$$

o equivalentemente

$$\sigma(p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}) = \frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2 1+1}-1}{p_2-1}\dots\frac{p_r^{k_r+1}-1}{p_r-1}.$$

Con estas descripciones, si $\mathrm{mcd}(m,n)=1$, eso quiere decir que sus factorizaciones son, como en la demostración del Teorema 3.9, de la forma $m = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ y $n = q_1^{l_1}q_2^{l_2}\dots q_s^{l_s}$, con $p_i \neq q_j$ para todo $i = 1, 2, \dots, r$ y $j, 1, 2, \dots, s$. Por tanto, mn factoriza como $mn = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}q_1^{l_1}q_2^{l_2}\dots q_s^{l_s}$, y se tiene

$$\tau(mn) = (k_1+1)(k_2+1)\dots(k_r+1)(l_1+1)(l_2+1)\dots(l_s+1) = \tau(m)\tau(n)$$

y

$$\sigma(mn) = \frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2 1+1}-1}{p_2-1}\dots\frac{p_r^{k_r+1}-1}{p_r-1}\frac{q_1^{l_1+1}-1}{q_1-1}\frac{q_2^{l_2 1+1}-1}{q_2-1}\dots\frac{q_r^{l_s+1}-1}{q_s-1} = \sigma(m)\sigma(n)$$

En el Ejemplo 3.10 hemos visto que, aplicando la construcción del Teorema 3.9, el ejemplo 2 genera el 3 y que el 3 genera la función τ, mientras que el ejemplo 4 genera la función σ y está generado por la función ϕ. Cabe preguntarse, por tanto, si el ejemplo 2 está generado a partir de alguna función aritmética. El siguiente resultado nos da la respuesta:

Proposición 3.12. *Sea $\mu : \mathbb{Z}_{\geq 1} \to \{-1, 0, 1\}$ la función definida por:*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si existe un primo } p \text{ tal que } p^2|n \\ (-1)^r & \text{si } n = p_1p_2\dots p_r \text{ con } p_1, p_2, \dots, p_r \text{ primos distintos} \end{cases}$$

Entonces

(i) μ es multiplicativa.

(ii) $\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1. \end{cases}$

Demostración: Veamos primero la parte (i). Sean por tanto $m, n \in \mathbb{Z}_{\geq 1}$ con $\mathrm{mcd}(m,n) = 1$. Distinguimos tres casos:

–Si $m = 1$ o $n = 1$, es evidente que $\mu(mn) = \mu(m)\mu(n)$, ya que $\mu(1) = 1$.

–Si existe un primo p cuyo cuadrado divide a m (resp. n), entonces su cuadrado divide también a mn, luego $\mu(mn) = 0$, que conicide con $\mu(m)\mu(n)$ ya que $\mu(m)$ (resp. $\mu(n)$) es cero.

–Finalmente si ni m ni n son divisibles por cuadrados de primos, se podrá escribir $m = p_1 \dots p_r$ y $q_1 \dots q_s$, con $p_1, \dots, p_r, q_1, \dots, q_s$ primos distintos. Por tanto, $mn = p_1 \dots p_r q_1 \dots q_s$ y se tendrá

$$\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n).$$

Para la parte (ii), definimos $F(n) = \sum_{d|n} \mu(d)$, que será multiplicativa por (i) y el Teorema 3.9. Por tanto, basta comprobar que $F(1) = 1$ (lo que es evidente, ya que $F(1) = \mu(1) = 1$) y que si p es un número primo y $k > 0$ entonces $F(p^k) = 0$. Esto último sigue de que los divisores de p^k son $1, p, p^2, \dots, p^k$, y que por definición $\mu(p^j) = 0$ si $j \geq 2$, por lo que

$$F(p^k) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k) = 1 + (-1)^1 + 0 + \ldots + 0 = 0.$$

□

Definición. La función μ definida en el teorema anterior se llama *función de Möbius*.

Teorema 3.13. *Sea f una función aritmética (no necesariamente multiplicativa) y sea F la función definida por $F(n) = \sum_{d|n} f(d)$. Entonces:*

(i) (Fórmula de inversión de Möbius) $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})F(d)$.

(ii) $\sum_{i=1}^{n} F(i) = \sum_{k=1}^{n} \left[\frac{n}{k}\right] f(k)$.

Demostración: Es claro que, en (i), las dos expresiones para $f(n)$ son iguales, así que basta demostrarlo para la primera expresión. Tendremos entonces:

$$\sum_{d|n} \mu(d)F(\frac{n}{d}) = \sum_{d|n} \mu(d)\big(\sum_{c|\frac{n}{d}} f(c)\big) = \sum_{d|n, c|\frac{n}{d}} \mu(d)f(c).$$

La primera observación ahora es que el conjunto de pares (d, c) tales que $d|n$ y $c|\frac{n}{d}$ es igual al conjunto de pares (d, c) tales que $c|n$ y $d|\frac{n}{c}$. Por tanto, la igualdad anterior prosigue como

$$\sum_{d|n} \mu(d)F(\frac{n}{d}) = \sum_{c|n, d|\frac{n}{c}} \mu(d)f(c) = \sum_{c|n} f(c)\big(\sum_{d|\frac{n}{c}} \mu(d)\big).$$

Ahora bien, por la Proposición 3.12 sabemos que

$$\sum_{d|\frac{n}{c}} \mu(d) = \begin{cases} 1 & \text{si } \frac{n}{c} = 1 \\ 0 & \text{si } \frac{n}{c} > 1, \end{cases}$$

por lo que $\sum_{c|n} f(c)\big(\sum_{d|\frac{n}{c}} \mu(d)\big) = f(n)$.

Para demostrar (ii), tenemos que

$$\sum_{i=1}^{n} F(i) = \sum_{i=1}^{n} \big(\sum_{d|i} f(d) \big) = \sum_{i=1}^{n} \sum_{d|i} f(d).$$

La observación central es que basta demostrar que, para cada $k = 1, \ldots, n$, $f(k)$ aparece $\left[\frac{n}{k}\right]$ veces en la suma anterior. Y en efecto, k aparecerá tantas veces como k sea un divisor de un número $i \in \{1, 2, \ldots, n\}$. Como k es divisor de $1 \cdot k, 2 \cdot k, \ldots, \left[\frac{n}{k}\right]k$, el resultado sigue inmediatamente. □

Ejemplo 3.14. Aplicando el resultado anterior a los casos 3, 4, y 5 del Ejemplo 3.10, deducimos respectivamente las siguientes fórmulas para todo $n \in \mathbb{Z}_{\geq 1}$:

Si $f = 1$ y $F = \tau$:

$$\sum_{d|n} \mu(\frac{n}{d})\tau(d) = 1$$

$$\sum_{i=1}^{n} \tau(i) = \sum_{k=1}^{n} \Big[\frac{n}{k}\Big],$$

si $f = id$ y $F = \sigma$:

$$\sum_{d|n} \mu(\frac{n}{d})\sigma(d) = n$$

$$\sum_{i=1}^{n} \sigma(i) = \sum_{k=1}^{n} [\frac{n}{k}]k$$

y si $f = \phi$ y $F = id$:

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \mu(\frac{n}{d})d$$

$$\sum_{i=1}^{n} i = \sum_{k=1}^{n} [\frac{n}{k}]\phi(k)$$

Veamos alguna aplicación de las funciones τ y σ en teoría de números.

Ejemplo 3.15. La primera observación es que es equivalente que un número n sea primo a que $\tau(n) = 2$ o $\sigma(n) = 1 + n$. Las fórmulas anteriores nos dan en realidad una fórmula para calcular estas funciones para un número n del que no sabemos si factoriza. En efecto, la observación es que en general $F(n) = \sum_{i=1}^{n} F(i) - \sum_{i=1}^{n-1} F(i)$, así que, por ejemplo, tendremos la fórmula, para $n > 1$,

$$\tau(n) = \sum_{k=1}^{n} [\frac{n}{k}] - \sum_{k=1}^{n-1} [\frac{n-1}{k}] = 2 + \sum_{k=2}^{n-1} \big([\frac{n}{k}] - [\frac{n-1}{k}] \big).$$

Por ejemplo, para $n = 7$, podemos escribir

$$\tau(7) = 2 + (3-3) + (2-2) + (1-1) + (1-1) + (1-1) = 2,$$

lo que concluye que 7 es primo. En realidad, el resultado no es sorprendente, ya que $n > 1$ es primo si y sólo si no es divisible por ningún $k = 2, \ldots, n-1$, es decir, que $\frac{n}{k}$ no es entero, que es equivalente a $\left[\frac{n}{k}\right] = \left[\frac{n-1}{k}\right]$, es decir $\tau(n) = 2$.

Veamos otra simple aplicación del tipo de ideas anterior para estudiar una clase de números que llamaron la atención a los griegos clásicos:

Definición. Se llama *número perfecto* a un entero positivo que sea igual a la suma de todos sus divisores menores que él. Usando la terminología anterior, la suma de los divisores de n es $\sigma(n)$, por lo que para obtener la suma de los divisores de n menores que n hay que quitar el propio n. Es decir, n es un número perfecto si y sólo si $\sigma(n) - n = n$, i.e. $\sigma(n) = 2n$.

El resultado más importante sobre los números perfectos es el siguiente:

Teorema 3.16. *Un número par n es un número perfecto si y sólo si se puede escribir como $n = 2^{k-1}(2^k - 1)$, siendo $k \geq 2$ y $2^k - 1$ un número primo.*

Demostración: Supongamos en primer lugar que n es un número perfecto par. Lo escribimos separando los factores primos impares, es decir, de la forma $n = 2^{k-1}m$ con $k \geq 2$ y m impar. La condición de que n sea perfecto es equivalente a $\sigma(n) = 2n$, que usando que σ es multiplicativa y la fórmula de la Observación 3.11 quiere decir:

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Como $\text{mcd}(2^k, 2^k - 1) = 1$, se sigue de que existe $M \in \mathbb{Z}_{\geq 1}$ tal que

$$\begin{cases} m = (2^k - 1)M \\ \sigma(m) = 2^k M \end{cases}$$

En particular, m y M son dos divisores distintos de m, por lo que se tendrá $\sigma(m) \geq m + M$, y de hecho se dará la igualdad si y sólo si m y M son los únicos divisores de m, es decir, m es primo y $M = 1$. Ahora observamos que efectivamente se da la igualdad, ya que se tiene

$$2^k M = \sigma(m) \geq m + M = (2^k - 1)M + M = 2^k M.$$

Por tanto, $m = 2^k - 1$ es un número primo y $n = 2^{k-1}m = 2^{k-1}(2^k - 1)$.

Recíprocamente, si $n = 2^{k-1}(2^k - 1)$, con $k \geq 2$ y $2^k - 1 = p$ primo, entonces, como σ es multiplicativa y usando la fórmula de la Observación 3.11, se tiene

$$\sigma(n) = \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p) = (2^k - 1)(p + 1) = (2^k - 1)2^k = 2n.$$

□

El interés del resultado anterior radica en que no se conocen números perfectos impares, y de hecho todo indica que no existen (por ejemplo, se sabe que un número perfecto impar debería tener al menos 300 cifras). Respecto a la existencia de infinitos números perfectos pares, es también un problema abierto. Por el teorema anterior, bastaría que demostrar que existen infinitos números primos de la forma 2^k-1. Es una simple observación que si 2^k-1 es primo entonces k es primo (ya que, si $r|k =$, entonces $2^s-1|2^k-1$).

Definición. Se llama *número primo de Mersenne* a un número primo de la forma $M_k := 2^k-1$ con k primo (nótese que es equivalente a decir que, en base dos, se escribe sólo con unos).

Por tanto, existen infinitos números perfectos pares si y sólo si existen infinitos números primos de Mersenne (lo que se conjetura que es cierto). Damos a continuación una tabla con los primeros k primos tales que M_k es primo, con el correspondiente número perfecto $n = 2^{k-1}(2^k-1)$.

k	$M_k = 2^k-1$	$n = 2^{k-1}(2^k-1)$
2	3	6
3	7	28
5	31	496
7	127	8128
13	8191	33550336
17	131071	8589869056
19	524287	137438691328
31	2147483647	2305843008139952128
61	2305843009213693951	2658455991569831744654692615953842176

Nótese que $k = 11$ es el primer número primo tal que M_k no es primo ($M_{11} = 2047 = 23\cdot 89$), y a partir de ahí hay muchos k con la misma propiedad. Hasta la fecha, se conocen sólo 43 números primos de Mersenne (el último, obtenido en septiembre de 2008). El mayor número primo de Mersenne que se conoce (encontrado en agosto de este año) es para $k = 43112609$, y el número de cifras de M_k es 12978189 (casi trece millones). El primo M_{31} ya era conocido por Euler en 1772.

4. Órdenes, raíces primitivas e índices

El Ejemplo 3.7 muestra que, dado $n \in \mathbb{Z}_{\geq 1}$, no siempre $\phi(n)$ es la menor potencia a la que debemos elevar un número para que nos dé 1 módulo n. En este capítulo, pretendemos estudiar en qué condiciones $\phi(n)$ es dicho menor exponente. Las definiciones naturales de partida son las siguientes:

Definición. Fijado un entero positivo n, para cada $a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a, n) = 1$ se llama *orden del elemento a módulo n* al menor entero positivo k tal que $a^k \equiv 1 \pmod{n}$. Del teorema de Euler sigue $k \leq \phi(n)$, y diremos que a es una *raíz primitiva (de la unidad) módulo n* si su orden es $k = \phi(n)$.

Ejemplo 4.1. Estudiemos el caso $n = 11$. Si tomamos $a = 2$, es un simple cálculo observar que las potencias $2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}$ son respectivamente congruentes con $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$ módulo 11. Por tanto, 2 tiene orden 10 módulo 11, y por tanto es una raíz primitiva. Obsérvese que las distintas potencias nos han dado precisamente todos los restos $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$, aunque en orden distinto. Ya veremos más adelante que esto no es una coincidencia. Si en cambio tomamos $a = 3$, las potencias $3^1, 3^2, 3^3, 3^4, 3^5$ son respectivamente congruentes con $3, 9, 5, 4, 1$ módulo 11, por lo que 3 tiene orden 5 módulo 11 y no es una raíz primitiva. Tampoco es casualidad que el orden de 3 sea un divisor de $\phi(11) = 10$.

No tienen por qué existir siempre raíces primitivas (de hecho, es lo menos frecuente). Por ejemplo, el Ejemplo 3.7 indica que 35 no tiene raíces primitivas. Más aún, indica que el problema es que 35 factoriza en dos números primos entre sí, 7 y 5, cuyos valores de ϕ no son primos entre sí, ya que son ambos pares. El siguiente resultado indica que esta situación se repetirá muchas veces.

Lema 4.2. *Si $n > 2$, $\phi(n)$ es par.*

Demostración: Si n contiene algún divisor primo impar p, entonces el resultado es evidente, ya que se podrá escribir $n = p^k m$ con $\mathrm{mcd}(m, p) = 1$ y $k \geq 1$. Entonces $\phi(n) = \phi(p^k)\phi(m)$, y $\phi(p^k)$ es par, ya que por la Observación 3.4 se tiene $\phi(p^k) = p^{k-1}(p-1)$ y $p - 1$ es par.

Queda por tanto estudiar el caso en que n no tiene factores impares, es decir, es de la forma $n = 2^k$. En tal caso, $\phi(2^k) = 2^{k-1}$, que es también par por ser $k > 1$ (puesto que $n > 2$). □

Del lema sacamos ya muchos casos en que no hay raíces primitivas.

Proposición 4.3. *Si $\mathrm{mcd}(m, n) > 1$ y $m, n > 2$, entonces mn no tiene raíces primitivas.*

Demostración: Sea $a \in \mathbb{Z}$ tal que $\text{mcd}(a, mn) = 1$, es decir, $\text{mcd}(a, m) = 1$ y $\text{mcd}(a, n) = 1$ (ver Proposición 1.9). Si aplicamos el Teorema de Euler separadamente a m y n, tendremos que $a^{\phi(m)} \equiv 1 \pmod{m}$ y $a^{\phi(n)} \equiv 1 \pmod{n}$. Elevando respectivamente a $\frac{\phi(n)}{2}$ y $\frac{\phi(m)}{2}$ (que son enteros, ya que por el lema $\phi(m)$ y $\phi(n)$ son pares) obtenemos que $a^{\frac{\phi(m)\phi(n)}{2}}$ es congruente con 1 módulo m y n, luego también módulo mn. Por tanto, el orden de a módulo mn es a lo sumo $\frac{\phi(m)\phi(n)}{2}$. Como $\phi(mn) = \phi(m)\phi(n)$ al ser $\text{mcd}(m, n) = 1$, se tiene que ningún a tiene orden $\phi(mn)$. □

Como consecuencia, los únicos números que pueden tener raíces primitivas son los de la forma p^k o $2p^k$ (con $p \neq 2$ en el segundo caso). El caso de las potencias de 2 queda excluido (salvo para las dos primeras potencias) por el siguiente resultado.

Proposición 4.4. *Para todo número impar a y para cada entero $k \geq 3$, se tiene que $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Por tanto, 2^k no tiene raíces primitivas.*

Demostración: Si demostramos la primera parte, como $\phi(2^k) = 2^{k-1}$ por la Observación 3.4, se sigue que 2^k no tiene raíces primitivas. Basta entonces demostrar la primera parte, es decir, $2^k | a^{2^{k-2}} - 1$ si $k \geq 3$. Lo demostraremos por inducción sobre k. Si $k = 3$, entonces tenemos $a^2 - 1 = (a + 1)(a - 1)$. Como $a - 1$ y $a + 1$ son dos pares consecutivos, uno de ellos es necesariamente múltiplo de 4, con el producto de ambos es divisible por 8.

Supongamos ahora que lo tenemos demostrado para k y queremos demostrarlo para $k + 1$. Entonces escribimos $a^{2^{k-1}} - 1 = (a^{2^{k-2}} + 1)(a^{2^{k-2}} - 1)$. El primer factor es par, mientras que el segundo, por hipótesis de inducción, es divisible por 2^k, así que el producto de ambos factores es divisible por 2^{k+1}, como queríamos demostrar. □

El resultado final, que demostraremos algo más adelante, cuando dispongamos de las técnicas necesarias, es el siguiente:

Teorema 4.5. *Un número natural $n > 1$ posee raíces primitivas si y sólo si es $n = 2$, $n = 4$, $n = p^k$ o $n = 2p^k$ donde p es un primo impar y $k \geq 1$.*

Por las Proposiciones 4.3 y 4.4, tenemos que los únicos casos posibles son los del enunciado. Por otra parte, es evidente que 3 es una raíz primitiva módulo 2 y módulo 4. Por tanto, basta ver que los números de la forma p^k o $2p^k$ tienen raíces primitivas. Eso lo demostraremos en el Teorema 4.12.

Dado que debemos estudiar la existencia de elementos de orden $\phi(n)$, parece razonable estudiar primero propiedades de los órdenes de los elementos.

Proposición 4.6. *Sea a un elemento de orden k módulo n. Entonces:*

(i) $a^h \equiv 1 \pmod{n}$ *si y sólo si* $k|h$.

(ii) k *es un divisor de* $\phi(n)$.

(iii) $a^i \equiv a^j \pmod{n}$ *si y sólo si* $i \equiv j \pmod{k}$.

(iv) Los elementos $a, a^2, \ldots, a^{k-1}, a^k$ *son incongruentes módulo* n.

(v) Si $h > 0$, *entonces* a^h *tiene orden* $\frac{k}{\text{mcd}(h,k)}$ *módulo* n.

Demostración: Para la parte (i), sea $h = qk + r$ la división euclídea de h entre k, por lo que $0 \leq r < k$. Se tendrá entonces

$$a^h = a^{qk+r} = (a^k)^r a^r \equiv 1^k a^r = a^r \pmod{n}.$$

Por tanto, $a^h \equiv 1 \pmod{n}$ si y sólo si $a^r \equiv 1 \pmod{n}$. Como $r < n$ y, por definición de orden, k es el menor entero positivo tal que $a^k \equiv 1 \pmod{n}$, se sigue que $a^r \equiv 1 \pmod{n}$ si y sólo si $r \leq 0$, es decir, si y sólo si $r = 0$ (ya que $r \geq 0$). Como esto es equivalente a decir $k|h$, queda demostrado (i).

La parte (ii) es una consecuencia de (i), ya que, por el Teorema de Euler, se tiene $a^{\phi(n)} \equiv 1 \pmod{n}$.

Para (iii), podemos suponer $i \leq j$. Entonces $a^i(a^{j-i} - 1) \equiv 0 \pmod{n}$, es decir, $n|a^i(a^{j-i} - 1)$. Como $\text{mcd}(a, n) = 1$, se sigue que $n|a^{j-i} - 1$, es decir, $a^{j-i} \equiv 1 \pmod{n}$. Por (i), $k|j - i$, o lo que es lo mismo $i \equiv j \pmod{k}$.

La parte (iv) es una consecuencia de (iii), ya que, si $i, j \in \{1, 2, \ldots, k\}$, la condición $a^i \equiv a^j \pmod{n}$ es equivalente a $i \equiv j \pmod{k}$, que a su vez es equivalente a $i = j$, por ser $\{1, 2, \ldots, k\}$ un sistema completo de restos módulo k (Proposición 2.5(i)).

Finalmente, para demostrar la parte (v), observamos que $(a^h)^j \equiv 1 \pmod{n}$ si y sólo si $a^{hj} \equiv 1 \pmod{n}$, que por (i), es equivalente a $k|hj$. Por el Lema 1.1(iv), esto equivale a $\frac{k}{\text{mcd}(h,k)} | \frac{h}{\text{mcd}(h,k)} j$. Como, por la Proposición 1.5(ii), $\frac{k}{\text{mcd}(h,k)}$ y $\frac{h}{\text{mcd}(h,k)}$ son primos entre sí, el Lema de Euclides implica que la condición anterior es equivalente también a $\frac{k}{\text{mcd}(h,k)} | j$. En otras palabras, las potencias de a^h que son congruentes con 1 módulo n son precisamente los múltiplos de $\frac{k}{\text{mcd}(h,k)}$, lo que implica que $\frac{k}{\text{mcd}(h,k)}$ es precisamente el orden de a^h módulo n. □

La observación principal a la hora de buscar raíces primitivas es que éstas son las soluciones de la congruencia $x^{\phi(n)} \equiv 1 \pmod{n}$ que no son solución solución de ninguna congruencia de la forma $x^d \equiv 1 \pmod{n}$ con $d|\phi(n)$. En los casos que hemos visto en que n no tiene raíces primitivas ocurre que existe $d < \phi(n)$ tal que la congruencia $x^d \equiv 1 \pmod{n}$ tiene $\phi(n)$ soluciones módulo n (como en el Ejemplo 3.7, en que la

congruencia $x^{12} \equiv 1 \pmod{35}$ tiene 24 soluciones). Este tipo de anomalías (tener más soluciones que el grado de la congruencia) no se dan en el caso en que n es un número primo (ni para congruencias de grado uno, como indica la Proposición 2.9), y de hecho se tiene el siguiente resultado, que será clave para demostrar el Teorema 4.5:

Teorema 4.7 (Lagrange)**.** *Sea p un número primo y $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$ un polinomio con algún a_i no divisible por p. Entonces existen como mucho d soluciones distintas módulo p de la congruencia $f(x) \equiv 0 \pmod{p}$.*

Demostración: Lo hacemos por inducción sobre d. Si $d = 0$, entonces $f(x)$ es una constante a_0 no divisible por p, por lo que $f(x) \equiv 0 \pmod{p}$ no tiene solución. Supongamos entonces que tenemos el resultado demostrado para polinomios no nulos de grado menor o igual que d y demostrémoslo para polinomios de grado $d+1$. Tomemos por tanto un polinomio $f(x) = a_{d+1}x^{d+1} + a_d x^d + \ldots + a_1 x + a_0$ con algún a_i no divisible por p. Distinguimos dos casos:

–Si $p | a_{d+1}$, entonces algún a_i, con $i = 0, 1, \ldots, d$, no es divisible por p. Además, las soluciones de $f(x) \equiv 0 \pmod{p}$ son las soluciones de $a_d x^d + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$, que, por hipótesis de inducción, son al máximo d distintas módulo p. Por tanto, en este caso hay incluso menos de $d+1$ soluciones módulo p.

–Si en cambio $p \not| a_{d+1}$, demostraremos por reducción al absurdo que $f(x) \equiv 0 \pmod{p}$ no puede tener más de $d+1$ soluciones módulo p. En efecto, supongamos que tuviera $d+2$ soluciones distintas, que denotamos por $x \equiv x_1, x_2 \ldots, x_{d+1}, x_{d+2} \pmod{p}$. Consideramos el polinomio

$$g(x) = f(x) - a_{d+1}(x - x_1) \ldots (x - x_{d+1}),$$

que claramente tiene grado como mucho d (ya que el coeficiente de x^{d+1} es cero). Además, no todos sus coeficientes son divisibles por p, ya que $g(x_{d+2}) = -a_{d+1}(x_{d+2} - x_1) \ldots (x_{d+2} - x_{d+1}) \not\equiv 0 \pmod{p}$ porque es el producto de números no divisibles por p (Corolario 1.14). Por tanto, por hipótesis de inducción la congruencia $g(x) \equiv 0 \pmod{p}$ tiene a lo sumo d soluciones distintas módulo p, mientras que claramente $x \equiv x_1, x_2 \ldots, x_{d+1} \pmod{p}$ son soluciones, lo que nos da la contradicción que buscábamos. □

Definición. Dado un polinomio $f(x)$ con coeficientes enteros, llamaremos *raíces del polinomio módulo p* a las soluciones de la congruencia $f(x) \equiv 0 \pmod{p}$.

Un ejemplo típico del resultado anterior es el polinomio $x^{p-1} - 1$, que por el pequeño Teorema de Fermat tiene exactamente $p-1$ raíces módulo p. Entre este hecho y el teorema podemos demostrar el siguiente resultado fundamental:

Proposición 4.8. *Para cada $d|p-1$, la congruencia $x^d-1 \equiv 0 \pmod{p}$ tiene exactamente d soluciones módulo p.*

Demostración: Si escribimos $p-1=dk$, entonces podemos escribir

$$x^{p-1}-1=(x^d)^k-1=(x^d-1)\big((x^d)^{k-1}+(x^d)^{k-2}+\ldots+x^d+1\big)=(x^d-1)f(x)$$

donde $f(x)$ está definido como el segundo factor, y en particular tiene grado $dk-d=p-1-d$. Como, por el pequeño teorema de Fermat cada a primo con a es raíz módulo p de $x^{p-1}-1$, entonces también es raíz de x^d-1 o de $f(x)$. Como por el Teorema de Lagrange x^d-1 tiene como mucho d raíces módulo p y $f(x)$ tiene como mucho $p-1-d$, se sigue que se da la igualdad en ambos casos, es decir, x^d-1 tiene exactamente d raíces módulo p. □

Podemos demostrar ya el resultado principal que nos da los elementos que tenemos de cada orden, y en particular la existencia de raíces primitivas módulo p:

Teorema 4.9. *Para cada $d|p-1$, existen exactamente $\phi(d)$ enteros incongruentes de orden d módulo p.*

Demostración: Llamamos $\psi(d)$ al número de enteros incongruentes módulo p de orden d. Como el orden de un elemento módulo p es un divisor de $\phi(p)=p-1$, se tendrá

$$\sum_{d|p-1}\psi(d)=p-1.$$

Por otra parte, como vimos en la parte 5 del Ejemplo 3.10,

$$\sum_{d|p-1}\phi(d)=p-1,$$

por lo que bastará ver que $\psi(d)\leq\phi(d)$ para cada $d|p-1$. Sea entonces $d|p-1$. Si $\psi(d)=0$, entonces no hay nada que demostrar, así que podemos suponer que existe un elemento a de orden d módulo p. Entonces, los elementos $a,a^2,\ldots,a^d$ son todos incongruentes módulo p por la Proposición 4.6(iv), luego son las d soluciones de $x^d-1\equiv 0 \pmod{p}$ de la proposición anterior. Por tanto, los elementos de orden d son de la forma a^i, y por la Proposición 4.6(v), un elemento a^i tiene orden d si y sólo si $\mathrm{mcd}(i,d)=1$, es decir, hay exactamente $\phi(d)$ elementos incongruentes de orden d, lo que demuestra el resultado. □

Corolario 4.10. *Cualquier número primo tiene raíces primitivas.*

Demostración: Es consecuencia del teorema, tomando $d=p-1$. De hecho, podemos precisar que hay exactamente $\phi(p-1)$ elementos incongruentes entre sí de orden $p-1$ módulo p, es decir, raíces primitivas módulo p. □

Pasar de raíces primitivas módulo un número primo a una potencia suya se basa en la siguiente observación:

Lema 4.11. *Sea r una raíz primitiva módulo un número primo p. Entonces, para cualquier $k \geq 2$, el orden de r módulo p^k es de la forma $(p-1)p^j$, con $j \leq k-1$. En particular, r es una raíz primitiva módulo p^k si y sólo si p^k no divide a $r^{p^{k-2}(p-1)} - 1$.*

Demostración: Sea m el orden de r módulo p^k. Se tendrá, en particular, $a^m \equiv 1 \pmod{p^k}$, y en particular $a^m \equiv 1 \pmod{p}$. Por el Lema 4.6(i), se tendrá $p-1|m$, ya que $p-1$ es el orden de r módulo p (por ser r raíz primitiva). Además, por el Lema 4.6(ii) aplicado ahora a $n = p^k$, se tendrá $m|\phi(p^k) = p^{k-1}(p-1)$. De estas dos condiciones sobre m se deduce que es de la forma $m = (p-1)p^j$, con $j \leq k-1$.

Para demostrar la segunda parte, es claro ahora que r no es una raíz primitiva módulo p^k si y sólo si tiene orden $m = (p-1)p^j$, con $j \leq k-2$, es decir si y sólo si su orden m divide a $(p-1)p^{k-2}$. Por el Lema 4.6(i), esta condición es equivalente a $r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$, es decir, a $p^k | r^{p^{k-2}(p-1)} - 1$. □

Este resultado nos permite finalmente terminar de demostrar el Teorema 4.5:

Teorema 4.12. *Si p es un número primo impar, p^k y $2p^k$ tienen raíces primitivas para cada $k \geq 1$.*

Demostración: Ya hemos visto en el Corolario 4.10 que existen raíces primitivas módulo p. Demostremos en primer lugar una raíz primitiva módulo p^2. Para ello, fijaremos una raíz primitiva r módulo p, y veamos que, si r no es una raíz primitiva módulo p^2, entonces $r+p$ lo es (en realidad valdría cualquier $r+ip$ con $\mathrm{mcd}(i,p) = 1$).

En efecto, si r no es una raíz primitiva módulo p^2, por el Lema 4.11 sabemos que p^2 divide a $r^{p-1} - 1$. Por tanto, módulo p^2 tendremos

$$(r+p)^{p-1} - 1 \equiv r^{p-1} + (p-1)r^{p-2}p - 1 \equiv (p-1)r^{p-2}p \pmod{p^2}.$$

Como $(p-1)r^{p-2}$ no es divisible por p, entonces $(p-1)r^{p-2}p$ no es divisible por p^2, luego $(r+p)^{p-1} - 1$ tampoco lo es, lo que implica por Lema 4.11 que $r+p$ es una raíz primitiva módulo p^2.

Construida pues una raíz primitiva r módulo p^2, veamos que, por ser p impar, r es también una raíz primitiva módulo p^k para cualquier $k \geq 2$. Por el Lema 4.11, tenemos que demostrar que, si p^2 no divide a $r^{p-1} - 1$, entonces p^k no divide a $r^{p^{k-2}(p-1)} - 1$. Lo demostraremos por inducción sobre k, siendo el resultado trivial para $k = 2$. Supongamos ahora cierto el resultado para k y vamos a demostrarlo para $k+1$. Por el Teorema de

Euler para p^{k-1}, sabemos que $r^{p^{k-2}(p-1)} - 1$ es divisible por p^{k-1}, y nuestra hipótesis de inducción indica que no es divisible por p^k. En otras palabras, podemos escribir

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$$

con a no divisible por p. Elevando a p, tendremos

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p = 1 + ap^k + \binom{p}{2} a^2 p^{2k-2} + \dots$$

Como $p > 2$ (es aquí donde usamos que p sea impar), $\binom{p}{2}$ es divisible por p, luego el sumando $\binom{p}{2} a^2 p^{2k-2}$ es divisible por p^{2k-1} y $2k - 1 \geq k + 1$ por ser $k \geq 2$. El resto de sumandos en los puntos suspensivos son divisibles por $p^{i(k-1)}$ con $i \geq 3$, y como $i(k-1) \geq 3k-3 \geq k+1$ son también divisible por p^{k+1}. Se concluye así que

$$r^{p^{k-1}(p-1)} \equiv 1 + ap^k \pmod{p^{k+1}}$$

y como ap^k no es divisible por p^{k+1}, entonces $r^{p^{k-1}(p-1)} - 1$ tampoco lo es.

Finalmente, dada una raíz primitiva módulo p^k, si es par le añadimos p^k y seguirá siendo una raíz primitiva módulo p^k, pero ahora impar. Por tanto, existe r impar que es una raíz primitiva módulo p^k. Veamos que es también raíz primitiva módulo $2p^k$. En efecto, en primer lugar es evidente que $\mcd(r, 2p^k) = 1$, ya que $\mcd(r, 2) = 1$ y $\mcd(r, p^k) = 1$. Por otra parte $\phi(2p^k) = (2-1)p^{k-1}(p-1) = p^{k-1}(p-1) = \phi(p^k)$, luego $r^{\phi(2p^k)} \equiv 1 \pmod{2p^k}$ y no existe $a < \phi(2p^k)$ tal que $r^a \equiv 1 \pmod{2p^k}$, por lo que r tiene orden $\phi(2p^k)$ módulo p^k. □

Ejemplo 4.13. El resultado anterior es constructivo. Por ejemplo, vamos a buscar una raíz primitiva módulo $242 = 2 \cdot 11^2$. Ya sabemos, por el Ejemplo 4.1, que 2 es una raíz primitiva módulo 11. Nos preguntamos si será también una raíz primitiva módulo 11^2, para lo que usaremos el Lema 4.11. Como $2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$ no es divisible por 11^2, se sigue que 2 es, en efecto, una raíz primitiva módulo 11^2 (nótese que, si hubiéramos obtenido que no lo era, la demostración del Teorema 4.12(ii) nos diría automáticamente que $2 + 11$ es una raíz primitiva). Finalmente, por la demostración de la parte (iv) del Teorema 4.12, tenemos que $2 + 11^2 = 123$ es una raíz primitiva módulo $2 \cdot 11^2$.

Ahora que sabemos qué números tienen raíz primitiva, veamos en qué podemos usarlo. Obsérvese en primer lugar que, si r es una raíz primitiva módulo n, entonces por la Proposición 4.6(iv) los elementos $r, r^2, \dots, r^{\phi(n)}$ son todos no congruentes dos a dos, luego, por el Lema 3.1, son congruentes módulo n, en algún orden, a los números $1, 2, \dots, n$ que

son primos con n. Por tanto, cualquier $a \in \mathbb{Z}$ con $\text{mcd}(a, n) = 1$ es congruente a un único r^i con $i \in \{1, 2, \ldots, \phi(n)\}$. Recordando la definición de logaritmo, damos la siguiente:

Definición. Dado un número n con raíz primitiva r, se llama índice de a relativo a r al menor entero positivo k tal que $a \equiv r^k \pmod{n}$ y escribiremos $k = \text{ind}_r(a)$.

Ejemplo 4.14. Si $n = 11$, sabemos por el Ejemplo 4.1 que $r = 2$ es una raíz primitiva módulo 11. Además, $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ son, respectivamente, congruentes módulo 11 con $2^{10}, 2^1, 2^8, 2^2, 2^4, 2^9, 2^7, 2^3, 2^6, 2^5$, por lo que sus índices relativos a 2 son, respectivamente, $10, 1, 8, 2, 4, 9, 7, 3, 6, 5$

El índice funciona, en efecto, como un logaritmo en base r, y de hecho se tienen las siguientes propiedades:

Proposición 4.15. *Si r es una raíz primitiva módulo n, se verifica:*

(i) $r^k \equiv a \pmod{n}$ *si y sólo si* $k \equiv \text{ind}_r(a) \pmod{\phi(n)}$.

(ii) $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\phi(n)}$.

(iii) $\text{ind}_r(a^k) \equiv k\text{ind}_r(a) \pmod{\phi(n)}$.

(iv) $\text{ind}_r(1) \equiv 0 \pmod{\phi(n)}$ *(y de hecho* $\text{ind}_r(1) = \phi(n)$*).*

(v) $\text{ind}_r(r) = 1$.

Demostración: Veamos primero (i). Como por definición $r^{\text{ind}_r(a)} \equiv a \pmod{n}$, entonces $r^k \equiv r^{\text{ind}_r(a)} \pmod{n}$, y por la Proposición 4.6(iii) se sigue $k \equiv \text{ind}_r(a) \pmod{\phi(n)}$ (recuérdese que el hecho de que r sea raíz primitiva módulo n se traduce en que el orden de r módulo n es $\phi(n)$).

El resto de los apartados se demuestra inmediatamente a partir de (i). Haremos sólo, a modo de ejemplo, (ii). Como se tiene

$$r^{\text{ind}_r(a)+\text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \pmod{n}$$

la parte (i) implica $\text{ind}_r(a) + \text{ind}_r(b) \equiv \text{ind}_r(ab) \pmod{\phi(n)}$. □

La teoría de índices se usa para resolver cierto tipo de congruencias no lineales, pasando de congruencias módulo n a congruencias módulo $\phi(n)$. Antes de ver el resultado preciso, hagamos un ejemplo.

Ejemplo 4.16. Consideremos la congruencia $x^6 \equiv 3 \pmod{11}$. Evidentemente, cualquier solución verifica $\text{mcd}(x, 11) = 11$. Por tanto, como 2 es una raíz primitiva módulo 11 ver Ejemplo 4.1), se podrá se podrá escribir $x \equiv 2^y \pmod{11}$. Además, sabemos que $3 \equiv 2^8 \pmod{11}$, por lo que nuestra congruencia es equivalente a $2^{6y} \equiv 2^8 \pmod{11}$.

Por la Proposición 4.6(iii), esta congruencia es equivalente a $6y \equiv 8 \pmod{10}$. Aplicando ahora la Proposición 2.9, sabemos que esta congruencia tiene dos soluciones, precisamente $y \equiv 3, 8 \pmod{10}$. De nuevo por la Proposición 4.6(iii), estas soluciones son equivalentes a $2^y \equiv 2^3, 2^8 \pmod{11}$, es decir, $x \equiv 8, 3 \pmod{11}$.

Teorema 4.17. *Sea n un entero con una raíz primitiva r, y sean $k \geq 2$ y $d = \mathrm{mcd}(k, \phi(n))$. Si $a \in \mathbb{Z}$ verifica $\mathrm{mcd}(a, n) = 1$, y por tanto $a \equiv r^b \pmod{n}$ para algún $b \in \mathbb{Z}_{\geq 1}$, entonces son equivalentes:*

(i) La congruencia $x^k \equiv a \pmod{n}$ tiene solución.

(ii) $d|b$.

(iii) $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$.

Además, en tal caso, la congruencia tiene exactamente d soluciones módulo n

Demostración: Evidentemente, las soluciones de $x^k \equiv a \pmod{n}$ verifican $\mathrm{mcd}(x, n) = 1$, por lo que se podrá escribir $x \equiv r^y \pmod{n}$ para algún $y \in \mathbb{Z}$. En otras palabras, la congruencia tendrá solución si y sólo si tiene solución la congruencia

$$r^{ky} \equiv r^b \pmod{n}$$

que, por la Proposición 4.6(iii), es equivalente a

$$ky \equiv b \pmod{\phi(n)}.$$

Por la Proposición 2.9, tal congruencia tiene solución si y sólo si $d|b$, y además en tal caso el número de soluciones módulo $\phi(n)$ es d. Esto da la equivalencia de (i) y (ii), y además tomando potencias de r nos dice que el número de soluciones de nuestra congruencia módulo n es d.

Finalmente, $d|b$ es equivalente a $\phi(n)|b\frac{\phi(n)}{d}$, que por la Proposición 4.6(i), es equivalente a $r^{b\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$, es decir, $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$, lo que demuestra que (ii) y (iii) son equivalentes. □

El resultado anterior nos permite generalizar el Teorema 2.19:

Teorema 4.18. *Sea p un número primo impar, y sea $m \geq 1$. Entonces la congruencia $x^{2^m} \equiv -1 \pmod{p}$ tiene solución si y sólo si $p \equiv 1 \pmod{2^{m+1}}$.*

Demostración: Si escribimos $p - 1 = 2^n a$ con a impar, entonces es evidente que $d = \mathrm{mcd}(2^m, p-1) = 2^{\min\{n,m\}}$ y por tanto $\frac{p-1}{d} = 2^{\max\{0,n-m\}}a$. Por la parte (iii) del teorema (que podemos usar ya que p tiene raíces primitivas), la congruencia tendrá solución si y sólo si $(-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, es decir, si y sólo si $\frac{p-1}{d}$ es par, si y sólo si $n > m$, si y sólo si $2^{m+1}|p-1$, si y sólo si $p \equiv 1 \pmod{2^{m+1}}$. □

Podemos por tanto generalizar el Corolario 2.20:

Teorema 4.19. *Para cada $m \geq 1$, existen infinitos número primos de la forma $2^m k + 1$.*

Demostración: Si $p_1, p_2, \ldots, p_r$ fueran los únicos primos de la forma $2^m k+1$, consideramos el número $n = (2p_1 p_2 \ldots p_r)^{2^{m-1}} + 1$. Claramente, n es impar, luego sus posibles divisores primos son impares. Si p es un divisor primo impar de n, entonces $2p_1 p_2 \ldots p_r$ es una solución de la congruencia $x^{2^{m-1}} \equiv -1 \pmod{p}$. Por el Teorema 4.18, $p \equiv 1 \pmod{2^m}$, es decir, p es de la forma $2^m k + 1$. Por tanto p tiene que ser alguno de los $p_1, p_2, \ldots, p_r$, lo que es absurdo. □

Ejercicio 4.20. Demostrar que, para cada $m \geq 2$, existen infinitos número primos de la forma $2^m k + 2^{m-1} + 1$.

5. Congruencias cuadráticas

En el Teorema 4.17 hemos visto que el Teorema 4.12 parece funcionar particularmente bien para ciertas congruencias de grado 2^k. En este capítulo vamos a centrarnos en las congruencias de grado dos. Obsérvese en primer lugar que cualquier congruencia módulo un entero n se puede descomponer en congruencias módulo las potencias de primos que dividen a n. Podemos usar por tanto que, con la excepción de las potencias de dos, las potencias de un primo tienen raíces primitivas. De todas formas, vamos a iniciar nuestro estudio con congruencias cuadráticas módulo un número primo. Podemos suponer que el primo es impar, ya que $x^2 \equiv x \pmod 2$, luego las congruencias cuadráticas módulo dos son equivalentes a congruencias lineales.

El primer resultado nos da la clásica resolución de una ecuación de grado dos, pero ahora en el lenguaje de congruencias.

Proposición 5.1. *Sea p un número primo impar y sean $a, b, c \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, p) = 1$. Entonces la congruencia $ax^2 + bx + c \equiv 0 \pmod p$ tiene solución si y sólo si la congruencia $x^2 \equiv b^2 - 4ac \pmod p$ tiene solución. Además, las soluciones de $ax^2 + bx + c \equiv 0 \pmod p$ son exactamente las soluciones de $2ax \equiv -b + d \pmod p$ y $2ax \equiv -b - d \pmod p$, donde d es una solución de $x^2 \equiv b^2 - 4ac \pmod p$.*

Demostración: Como $\mathrm{mcd}(4a, p) = 1$, la congruencia $ax^2 + bx + c \equiv 0 \pmod p$ es equivalente a $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod p$, es decir,

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod p.$$

Por tanto, si nuestra congruencia original tiene solución, entonces $b^2 - 4ac$ es un cuadrado módulo p. Recíprocamente, si $d^2 \equiv b^2 - 4ac \pmod p$, entonces la congruencia anterior es equivalente a $p|(2ax + b)^2 - d^2$, es decir $p|(2ax + b + d)(2ax + b - d)$, que es a su vez equivalente a $2ax \equiv -b + d \pmod p$ o $2ax \equiv -b - d \pmod p$, y ambas tienen solución única porque $\mathrm{mcd}(2a, p) = 1$ (ver Proposición 2.9). □

El resultado anterior indica que para saber resolver ecuaciones cuadráticas módulo un número primo basta saber decidir cuándo un número es un cuadrado módulo dicho número primo. Por supuesto, si el número es divisible por el número primo, es congruente con el cuadrado de cero, y es la única solución. En caso contrario, podemos usar el Teorema 4.17 para dar una respuesta:

Teorema 5.2 (Criterio de Euler**).** *Sea p un número primo impar y sea $a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a, p) = 1$. Entonces la congruencia $x^2 \equiv a \pmod p$ tiene solución si y sólo si $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Además, si la congruencia no tiene solución se verifica $a^{\frac{p-1}{2}} \equiv -1 \pmod p$*

Demostración: Como $\phi(p) = p - 1$ es par, se tiene que $\mathrm{mcd}(2, \phi(p)) = 2$, luego por el Teorema 4.17 la congruencia $x^2 \equiv a \pmod{p}$ tiene solución si y sólo si $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Por otra parte, por el Teorema de Euler se tiene $a^{p-1} \equiv 1 \pmod{p}$, es decir,

$$p | a^{p-1} - 1 = (a^{\frac{p-1}{2}})^2 - 1 = (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1)$$

lo que implica que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ o $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Definición. Si $\mathrm{mcd}(a, p) = 1$, se dice que a es un *resto cuadrático módulo* p si la congruencia $x^2 \equiv a \pmod{p}$ tiene solución. Se llama *símbolo de Legendre* al número

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si es un resto cuadrático módulo } p \\ -1 & \text{si } a \text{ no es un resto cuadrático módulo } p \end{cases}$$

Para $p = 2$, se tiene obviamente $\left(\frac{a}{2}\right) = 1$ para cualquier a impar. Si p es un número primo impar, por el Teorema 5.2, se tiene

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Proposición 5.3. *El símbolo de Legendre verifica las siguientes propiedades:*

(i) *Si* $a \equiv b \pmod{p}$ *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) $\left(\frac{a^2}{p}\right) = 1$, *y en particular* $\left(\frac{1}{p}\right) = 1$

(iv) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *si* p *es impar.*

Demostración: La parte (i) es trivial. La parte (ii) (si p es impar, ya que el caso $p = 2$ es trivial) se sigue de que

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

lo que implica la igualdad de $\left(\frac{ab}{p}\right)$ y $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, ya que ambos valen 1 o -1. La parte (iii) es (ii) cuando $a = b$, y la parte (iv) es el criterio de Euler (nótese que es también equivalente al Teorema 2.19). □

Observación 5.4. La parte (ii) es mucho más potente de lo que aparenta. Por ejemplo, podría parecer que no sirve para calcular $\left(\frac{23}{31}\right)$, pero basta por ejemplo escribir

$$\left(\frac{23}{31}\right) = \left(\frac{-8}{31}\right) = \left(\frac{(-1)2^3}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right)^3.$$

Por (iv), tenemos $\left(\frac{-1}{31}\right) = -1$, mientras que por (iii) tenemos $\left(\frac{2}{31}\right)^3 = \left(\frac{2}{31}\right)$, por lo que finalmente tenemos $\left(\frac{23}{31}\right) = -\left(\frac{2}{31}\right)$, que es más fácil de calcular. En efecto, basta utilizar el criterio de Euler, y observar que

$$2^{\frac{31-1}{2}} = 2^{15} = (2^5)^3 = 32^3 \equiv 1^3 = 1 \pmod{31}$$

por lo que $\left(\frac{2}{31}\right) = 1$ y por tanto $\left(\frac{23}{31}\right) = -1$.

Teorema 5.5. *Sea p un número primo impar y sea $a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a,p) = 1$. Para cada $k = 1, 2, \ldots, \frac{p-1}{2}$, sea $ka = q_k p + r_k$ la división de ka entre p. Separamos los restos $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ de la forma*

$$\{r_1, \ldots, r_{\frac{p-1}{2}}\} = \{r'_1, \ldots, r'_m\} \cup \{r''_1, \ldots, r''_n\}$$

donde $r'_1, \ldots, r'_m$ son los restos menores que $\frac{p}{2}$ y $r''_1, \ldots, r''_n$ son los restos mayores que $\frac{p}{2}$. Entonces:

(i) $\{1, 2 \ldots, \frac{p-1}{2}\} = \{r'_1, \ldots, r'_m\} \cup \{p - r''_1, \ldots, p - r''_n\}$

(ii) (Lema de Gauss) $\left(\frac{a}{p}\right) = (-1)^n$, *donde n es como antes, es decir, el número de elementos de $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ cuyo resto al dividir por p es mayor que $\frac{p}{2}$.*

Demostración: Usaremos repetidamente la Proposición 2.5. Como el conjunto

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}$$

está formado por p números consecutivos, es un sistema completo de restos módulo p. Por tanto, también los números

$$-\frac{p-1}{2}a, -\frac{p-3}{2}a, \ldots, -a, 0, a, \ldots, \frac{p-1}{2}a$$

forma un sistema completo de restos módulo p. Como los números $a, \ldots, \frac{p-1}{2}a$ son congruentes módulo p (en algún orden), a $r_1, \ldots, r_{\frac{p-1}{2}}$, es decir, a $r'_1, \ldots, r'_m, r''_1, \ldots, r''_n$, se tendrá que los números

$$-r'_1, \ldots, -r'_m, -r''_1, \ldots, -r''_n, 0, r'_1, \ldots, r'_m, r''_1, \ldots, r''_n$$

forman un sistema completo de restos módulo p. Esto implica en particular que los números $r'_1, \ldots, r'_m, -r''_1, \ldots, -r''_n$ son incongruentes módulo p cuando se toman dos a dos, y lo mismo es cierto con los números $r'_1, \ldots, r'_m, p - r''_1, \ldots, p - r''_n$, que serán por tanto distintos. Como hay $m + n = \frac{p+1}{2}$ de estos números, y todos ellos están en el conjunto $\{1, 2 \ldots, \frac{p-1}{2}\}$, se sigue inmediatamente la parte (i).

Multiplicando entonces todos estos números, se obtiene:

$$\left(\frac{p-1}{2}\right)! = r'_1 \dots r'_m (p - r''_1) \dots (p - r''_n) \equiv (-1)^n r'_1 \dots r'_m r''_1 \dots r''_n \pmod{p}.$$

y, como por otra parte,

$$r'_1 \dots r'_m r''_1 \dots r''_n \equiv a(2a)(3a) \dots (\frac{p-1}{2}a) = \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \pmod{p},$$

juntando ambas congruencias, se sigue $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$, lo que prueba (ii). □

Teorema 5.6. *Si p es un primo impar, entonces*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 8 \text{ o } p \equiv 7 \pmod 8 \\ -1 & \text{si } p \equiv 3 \pmod 8 \text{ o } p \equiv 5 \pmod 8 \end{cases}$$

Demostración: Usamos el lema de Gauss, y tenemos que ver cuántos de los $\frac{p-1}{2}$ números $2, 4, \dots, p-1$ son mayores que $\frac{p}{2}$. Lo haremos analizando separadamente todos los posibles restos de p módulo 8:

–Si $p = 8k+1$, entonces el conjunto $2, 4, \dots, p-1 = 8k$ tiene tenemos $4k$ elementos, de los que los menores de $\frac{p}{2} = 4k+\frac{1}{2}$ son $2, 4, \dots, 4k$, es decir, $2k$. Por tanto, $n = 4k-2k = 2k$, que es par, luego $\left(\frac{2}{p}\right) = 1$.

–Si $p = 8k+3$, entonces el conjunto $2, 4, \dots, p-1 = 8k+2$ tiene tenemos $4k+1$ elementos, de los que los menores de $\frac{p}{2} = 4k+\frac{3}{2}$ son $2, 4, \dots, 4k$, es decir, $2k$. Por tanto, $n = (4k+1) - 2k = 2k+1$, que es impar, luego $\left(\frac{2}{p}\right) = -1$.

–Si $p = 8k+5$, entonces el conjunto $2, 4, \dots, p-1 = 8k+4$ tiene tenemos $4k+2$ elementos, de los que los menores de $\frac{p}{2} = 4k+\frac{5}{2}$ son $2, 4, \dots, 4k+2$, es decir, $2k+1$. Por tanto, $n = (4k+2) - (2k+1) = 2k+1$, que es impar, luego $\left(\frac{2}{p}\right) = -1$.

–Si $p = 8k+7$, entonces el conjunto $2, 4, \dots, p-1 = 8k+6$ tiene tenemos $4k+3$ elementos, de los que los menores de $\frac{p}{2} = 4k+\frac{7}{2}$ son $2, 4, \dots, 4k+2$, es decir, $2k+1$. Por tanto, $n = (4k+3) - (2k+1) = 2k+2$, que es par, luego $\left(\frac{2}{p}\right) = 1$. □

Corolario 5.7. *Existen infinitos números primos de la forma $8k+7$.*

Demostración: Si $p_1, p_2, \dots, p_r$ fueran todos los números primos de la forma $8k+7$, consideramos el número $a = 8(p_1 p_2 \dots p_r)^2 - 1$. Sea p un divisor primo de a (necesariamente p será impar). Entonces, $(4p_1 p_2 \dots p_r)^2 \equiv 2 \pmod{p}$, por lo que, por el Teorema 5.6, se tiene $p \equiv 1 \pmod 8$ o $p \equiv 7 \pmod 8$. Como $a \equiv 7 \pmod 8$, no todos los divisores de a

pueden ser de la forma $8k+1$. Por tanto, a es divisible por algún primo de la forma $8k+7$, es decir, por algún p_i, lo que es absurdo. □

Teorema 5.8. *Si p es un primo impar, entonces*

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 8 \text{ o } p \equiv 3 \pmod 8 \\ -1 & \text{si } p \equiv 5 \pmod 8 \text{ o } p \equiv 7 \pmod 8 \end{cases}$$

Demostración: Basta combinar el Teorema 5.6 con las partes (iii) y (iv) de la Proposición 5.3. Lo hacemos según el resto de p módulo 8:

–Si $p \equiv 1 \pmod 8$, entonces por el Teorema 5.6, $\left(\frac{2}{p}\right) = 1$, mientras que por otra parte $p \equiv 1 \pmod 4$ luego por la Proposición 5.3(iv) se tiene $\left(\frac{-1}{p}\right) = 1$. Por tanto, de la Proposición 5.3(iv) se sigue $\left(\frac{-2}{p}\right) = 1$.

–Si $p \equiv 3 \pmod 8$, entonces por el Teorema 5.6, $\left(\frac{2}{p}\right) = -1$, mientras que por otra parte $p \equiv 3 \pmod 4$ luego por la Proposición 5.3(iv) se tiene $\left(\frac{-1}{p}\right) = -1$. Por tanto, de la Proposición 5.3(iv) se sigue $\left(\frac{-2}{p}\right) = 1$.

–Si $p \equiv 5 \pmod 8$, entonces por el Teorema 5.6, $\left(\frac{2}{p}\right) = -1$, mientras que por otra parte $p \equiv 1 \pmod 4$ luego por la Proposición 5.3(iv) se tiene $\left(\frac{-1}{p}\right) = 1$. Por tanto, de la Proposición 5.3(iv) se sigue $\left(\frac{-2}{p}\right) = -1$.

–Si $p \equiv 7 \pmod 8$, entonces por el Teorema 5.6, $\left(\frac{2}{p}\right) = 1$, mientras que por otra parte $p \equiv 3 \pmod 4$ luego por la Proposición 5.3(iv) se tiene $\left(\frac{-1}{p}\right) = -1$. Por tanto, de la Proposición 5.3(iv) se sigue $\left(\frac{-2}{p}\right) = -1$. □

Corolario 5.9. *Existen infinitos números primos de la forma $8k+3$.*

Demostración: Como siempre, supogamos que $p_1, p_2, \ldots, p_r$ son todos los números primos de la forma $8k+3$. Consideramos el número $a = (p_1 p_2 \ldots p_r)^2 + 2$. Entonces, si p es un divisor primo de a (necesariamente impar), se tendrá que $(p_1 p_2 \ldots p_r)^2 \equiv -2 \pmod p$, y por el Teorema 5.8 se tendrá que p es congruente con 1 o 3 módulo 8. Como a es de la forma $8k+3$ (ya que el cuadrado de cada p_i es de la forma $8k+1$), no todos los divisores de a son de la forma $8k+1$. Por tanto, a es divisible por algún número primo de la forma $8k+3$, es decir, por algún p_i; lo que es imposible. □

Damos a continuación un modo práctico de calcular los símbolos de Legendre:

Lema 5.10. *Si p es un primo impar, $a \in \mathbb{Z}$ es impar y* $\mathrm{mcd}(a,p)=1$, *entonces*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}.$$

Demostración: Usando las notaciones del Teorema 5.5, tenemos que demostrar, por la parte (ii) de dicho teorema, que n y $\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$ tienen la misma paridad. Como a y p son impares, y tomando congruencias módulo 2, tendremos:

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] \equiv p \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] = p \sum_{k=1}^{\frac{p-1}{2}} q_k = \sum_{k=1}^{\frac{p-1}{2}} (ka - r_k) = \sum_{k=1}^{\frac{p-1}{2}} ka - (r'_1 + \ldots + r'_m) - (r''_1 + \ldots + r''_n) \equiv$$

$$\equiv \sum_{k=1}^{\frac{p-1}{2}} k - (r'_1 + \ldots + r'_m) - (r''_1 + \ldots + r''_n) \pmod 2.$$

Por el Teorema 5.5(i), $\{r'_1, \ldots, r'_m, p - r''_1, \ldots, p - r''_n\} = \{1, 2, \ldots, \frac{p-1}{2}\}$, y por tanto

$$(r'_1 + \ldots + r'_m) + ((p - r''_1) + \ldots + (p - r''_n)) = \sum_{k=1}^{\frac{p-1}{2}} k.$$

Sustituyendo en la congruencia anterior, obtenemos

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] \equiv ((p - r''_1) + \ldots + (p - r''_n)) - (r''_1 + \ldots + r''_n) = pn - 2(r''_1 + \ldots + r''_n) \equiv n \pmod 2$$

que es lo que queríamos demostrar. □

El resultado anterior nos permite demostrar el siguiente resultado fundamental, que servirá para calcular cualquier símbolo de Legendre:

Teorema 5.11 (Ley de reciprocidad cuadrática)**.** *Si p, q son primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Demostración: Consideramos el conjunto de pares de la forma (k,l), con $k \in \{1, 2, \ldots, \frac{p-1}{2}\}$ y $l \in \{1, 2, \ldots, \frac{q-1}{2}\}$. Evidentemente, hay $\frac{p-1}{2}\frac{q-1}{2}$ de dichos pares. Dividimos ahora el mencionado conjunto en dos subconjuntos:

–En primer lugar, consideramos los pares (k,l) tales que $kq \leq lp$. Para cada $l \in \{1, 2, \ldots, \frac{q-1}{2}\}$ los posibles valores de k son $1, 2, \ldots, \left[\frac{lp}{q}\right]$. Por tanto, el número de pares de esta forma es $\sum_{l=1}^{\frac{q-1}{2}} \left[\frac{lp}{q}\right]$.

–Consideramos por otra parte los pares (k,l) tales que $kq \geq lp$. Para cada $k \in \{1,2,\ldots,\frac{p-1}{2}\}$ los posibles valores de l son $1,2,\ldots,\left[\frac{kq}{p}\right]$. Por tanto, el número de pares de esta forma es $\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]$.

Observemos que no hay pares que estén en ambos subconjuntos, ya que por ejemplo p no divide a ningún kq. Por tanto, el número total de pares es igual, por una parte a $\frac{p-1}{2}\frac{q-1}{2}$, y por otra parte a $\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right]$. Tomando potencias de -1 y usando el Lema 5.10, tenemos

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]+\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right]}=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]}(-1)^{\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right]}=\left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

□

Observación 5.12. La ley de reciprocidad cuadrática es el resultado del que más demostraciones se conocen. En http://www.rzuser.uni-heidelberg.de/∼hb3/fchrono.html hay una lista de ellas, y hasta el año 2007 se llevan contabilizadas 224 distintas.

Corolario 5.13. *Sea $p>3$ un número primo. Entonces:*

(i) $\left(\frac{3}{p}\right)=\begin{cases}1 & \text{si } p\equiv 1 \pmod{12} \text{ o } p\equiv 11 \pmod{12}\\ -1 & \text{si } p\equiv 5 \pmod{12} \text{ o } p\equiv 7 \pmod{12}\end{cases}$

(ii) $\left(\frac{-3}{p}\right)=\begin{cases}1 & \text{si } p\equiv 1 \pmod{3}\\ -1 & \text{si } p\equiv 2 \pmod{3}\end{cases}$

Demostración: Por la ley de reciprocidad cuadrática, tenemos $\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$. Por otra parte, por la Proposición 5.3(iv), tenemos $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. Por tanto, $\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)$, que claramente viene dado por la fórmula de (ii). La parte (i) se demuestra como el Corolario 5.8 a partir de (i). □

Corolario 5.14. *Existen infinitos números primos de la forma $12k+11$.*

Demostración: Supongamos en primer lugar que $p_1,\ldots,p_r$ sean todos los números primos de la forma $12k+11$. Consideramos $a=12(p_1\ldots p_r)^2-1$. Entonces, si p es un divisor primo de a (necesariamente $p>3$), se tiene que $6p_1\ldots p_r$ es una solución de $x^2\equiv 3 \pmod{p}$. El Corolario 5.13(i) implica entonces que p es de la forma $12k+1$ o $12k+11$. Como a es de la forma $12k+11$, necesariamente tendrá algún divisor primo de la forma $12k+11$, es decir, algún p_i, lo que es absurdo. □

Ejercicio 5.15. Demostrar que existen infinitos números primos de la forma $3k+1$. Más aún, demostrar que existen infinitos números primos de la forma $12k+7$.

Ejemplo 5.16. Veamos en un ejemplo práctico cómo la Ley de Reciprocidad Cuadrática permite calcular cualquier símbolo de Legendre. Supongamos que queremos calcular $\left(\frac{17}{41}\right)$. Por la Ley de Reciprocidad Cuadrática, podremos escribir $\left(\frac{17}{41}\right) = \left(\frac{41}{17}\right)$ y, como se tiene $41 \equiv 7 \pmod{17}$, también tendremos $\left(\frac{41}{17}\right) = \left(\frac{7}{17}\right)$. Por tanto, hemos reducido calcular un símbolo $\left(\frac{17}{41}\right)$ a calcular $\left(\frac{7}{17}\right)$, que involucra números más pequeños. Es claro que podemos seguir el proceso, escribiendo ahora $\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right)$, que es igual a -1 por el Corolario 5.13. Por tanto, $\left(\frac{17}{41}\right) = -1$.

Aprovechamos para hacer el mismo cálculo con un truco distinto. Podemos escribir

$$\left(\frac{17}{41}\right) = \left(\frac{-24}{41}\right) = \left(\frac{-2 \cdot 2^2 \cdot 3}{41}\right) = \left(\frac{-2}{41}\right)\left(\frac{2^2}{41}\right)\left(\frac{3}{41}\right) = 1 \cdot 1 \cdot (-1) = -1$$

donde los tres últimos símbolos han sido calculados respectivamente con el Teorema 5.6, la Proposición 5.3(iii) y el Corolario 5.13(i).

Veamos, para terminar el capítulo, que el símbolo de Legendre también mide cuándo un número es un resto cuadrático módulo la potencia de un primo:

Teorema 5.17. *Si p es un primo impar, $k \geq 1$, y $\mathrm{mcd}(a,p) = 1$, entonces la congruencia $x^2 \equiv a \pmod{p^k}$ tiene solución si y sólo si $\left(\frac{a}{p}\right) = 1$. Además, en tal caso, el número de soluciones módulo p^k es dos.*

Demostración: Obviamente, si $x^2 \equiv a \pmod{p^k}$ tiene solución, también la tiene $x^2 \equiv a \pmod{p}$, por lo que $\left(\frac{a}{p}\right) = 1$. Hay que demostrar entonces el recíproco, que si $\left(\frac{a}{p}\right) = 1$ entonces $x^2 \equiv a \pmod{p^k}$ tiene solución. Lo haremos por inducción sobre k, siendo trivial el caso $k = 1$.

Supongamos entonces que $x^2 \equiv a \pmod{p^k}$ tiene solución x_0 y encontremos una solución de $x^2 \equiv a \pmod{p^{k+1}}$. Como las soluciones de esta segunda congruencia son soluciones de la primera, en realidad buscamos enteros de la forma $x_0 + yp^k$ que sean solución de la segunda congruencia.

Que x_0 sea solución de la primera congruencia quiere decir que se puede escribir $x_0^2 = a + bp^k$, para algún $b \in \mathbb{Z}$. Por tanto, tendremos

$$(x_0 + yp^k)^2 = x_0^2 + 2x_0yp^k + y^2p^{2k} = a + (2x_0y + b)p^k + p^{2k}$$

de donde se deduce que $(x_0 + yp^k)^2 \equiv a \pmod{p^{k+1}}$ si y sólo si $p | 2x_0y + b$. Como $\mathrm{mcd}(2,p) = 1$, la congruencia $2x_0y + b \equiv 0 \pmod{p}$ tiene solución, y tomando una solución y se tiene que $x_0 + yp^k$ es una solución de $x^2 \equiv a \pmod{p^{k+1}}$.

El hecho de que haya exactamente dos soluciones módulo p^k es consecuencia del Teorema 4.17, ya que p^k tiene raíces primitivas. Puede hacerse también directamente, ya que, si x_0 es una solución, entonces cualquier otra solución x verifica $x^2 \equiv x_0^2 \pmod{p^k}$, es decir, $p^k | x^2 - x_0^2 = (x+x_0)(x-x_0)$. No puede ocurrir simultáneamente $p|x+x_0$ y $p|x-x_0$, ya que entonces $p|(x+x_0)-(x-x_0) = 2x_0$ y, como p es un primo impar, $p|x_0$, lo que contradice que $x_0^2 \equiv 1 \pmod{p^k}$. Por tanto $\mcd(p^k, x+x_0) = 1$ o bien $\mcd(p^k, x-x_0) = 1$, por lo que $p^k | x-x_0$ o bien $p^k | x+x_0$. Por tanto, $x \equiv x_0 \pmod{p^k}$ o bien $x \equiv -x_0 \pmod{p^k}$, y éstas son las únicas soluciones. □

Ejemplo 5.18. Veamos cómo se puede seguir la demostración anterior para resolver congruencias cuadráticas. Por ejemplo, como $\left(\frac{3}{13}\right) = 1$ (por el Corolario 5.13(i)), entonces la ecuación $x^2 \equiv 3 \pmod{13^2}$ tendrá dos soluciones módulo 13^2. En primer lugar, debemos resolver la ecuación $x^2 \equiv 3 \pmod{13}$, y se ve a ojo que $x \equiv \pm 4 \pmod{13}$ son las soluciones. Trabajamos por elemplo con la solución $x_0 = 4$, y tenemos que buscar ahora los valores de y para los que $4 + 13y$ es solución de $x^2 \equiv 3 \pmod{13^2}$. Operando (mejor así que intentar aprenderse de memoria la fórmula) queremos $16 + 104y + 13^2 y^2 \equiv 3 \pmod{13^2}$, es decir, $13(1+8y) \equiv 0 \pmod{13^2}$, que es equivalente a $1 + 8y \equiv 0 \pmod{13}$. Congruencias lineales de este tipo ya aprendimos a resolverlas en el Capítulo 2, y se comprueba fácilmente que $y \equiv 8 \pmod{13}$ es la solución. Por tanto, $x \equiv 4 + 13 \cdot 8 = 108 \pmod{13^2}$ es una solución. Para calcular la segunda solución no hace falta empezar con $x_0 = -4$, ya que necesariamente $x \equiv -108 \equiv 61 \pmod{13^2}$ es la otra solución.

Nos queda ver el caso de restos cuadráticos módulo una potencia de 2, que estudiamos a continuación:

Teorema 5.19. *Sea a un número impar. Entonces:*

(i) La congruencia $x^2 \equiv a \pmod{2}$ tiene siempre solución.

(ii) La congruencia $x^2 \equiv a \pmod{4}$ tiene solución si y sólo si $a \equiv 1 \pmod{4}$.

(iii) Si $k \geq 3$, la congruencia $x^2 \equiv a \pmod{2^k}$ tiene solución si y sólo si $a \equiv 1 \pmod{8}$. Además, en este caso, la congruencia tiene exactamente dos soluciones módulo 2^{k-1}

Demostración: La parte (i) es obvia, y la parte (ii) sigue del hecho de que el cuadrado de cualquier número impar es de la forma $4k+1$. Para parte (iii) observamos que, como el cuadrado de un número impar es siempre de la forma $8k+1$, entonces si la congruencia $x^2 \equiv a \pmod{2^k}$ tiene solución, entonces $a \equiv 1 \pmod{8}$. Demostraremos el recíproco por inducción sobre k, siendo el caso $k = 3$ trivial (las soluciones módulo 4 son 1 y 3). Supongamos entonces que $x^2 \equiv a \pmod{2^k}$ tiene solución, es decir, que existe $x_0 \in \mathbb{Z}$ tal

que $x_0^2 = a + 2^k b$ para algún $b \in \mathbb{Z}$. Veamos que existe una solución de $x^2 \equiv a \pmod{2^{k+1}}$ de la forma $x = x_0 + 2^{k-1}y$. En efecto, como

$$(x_0 + 2^{k-1}y)^2 = x_0^2 + 2^k x_0 y + 2^{2k-2}y^2 = a + 2^k(b + x_0 y) + 2^{2k-2}y^2$$

y x_0 es impar, si tomamos y de la misma paridad que b tendremos que $x_0 + 2^{k-1}y$ es solución de $x^2 \equiv a \pmod{2^{k+1}}$.

Además, si x_0 es una solución de $x^2 \equiv a \pmod{2^k}$, entonces para cualquier otra solución x se verifica

$$2^k | x^2 - x_0^2 = (x + x_0)(x - x_0)$$

y, como el máximo común divisor de $x + x_0$ y $x - x_0$ es divisible por 2 pero no por 4, se sigue que $x \equiv -x_0 \pmod{2^{k-1}}$ o $x \equiv x_0 \pmod{2^{k-1}}$. □

6. Ecuaciones diofánticas

Se llama *ecuación diofántica* a una ecuación cuyas variables son números enteros. La más conocida es la llamada *ecuación de Fermat*, que es $x^n + y^n = z^n$. Fermat aseguró que, si $n \geq 3$, las únicas posibles soluciones son aquéllas en que alguno de los x, y, z es cero. Este resultado, conocido como *Último Teorema de Fermat*, ha sido demostrado sólo recientemente por Wiles. En esta sección estudiaremos los casos más sencillos de esta ecuación, así como otras ecuaciones diofánticas similares.

Empezamos con el caso $n = 2$, que no entra dentro del Último Teorema de Fermat, ya que en este caso sí que existe solución, y de hecho infinitas, como demostraremos enseguida, viendo qué estructura tienen.

Definición. Se llama *terna pitagórica* al conjunto de tres enteros x, y, z tales que $x^2 + y^2 = z^2$. El nombre viene dado porque, si $x, y, z > 0$ forman una terna pitagórica, por el teorema de Pitágoras existe un triángulo rectángulo que tiene a x e y como longitudes de sus catetos y a z como longitud de la hipotenusa. Un triángulo así (es decir, rectángulo con las longitudes de los lados enteras) se llama *triángulo pitagórico*.

Lema 6.1. *Sea x, y, z una terna pitagórica y $d = \mcd(x, y, z)$. Entonces:*

(i) $d = \mcd(x, y) = \mcd(x, z) = \mcd(y, z)$.

(ii) Si escribimos $x = dx'$, $y = dy'$, $z = dz'$, entonces x', y', z' es una terna pitagórica.

Demostración: De (i) demostraremos sólo $d = \mcd(x, y)$, siendo idénticas las demostraciones de las otras igualdades. Sea $d = \mcd(x, y)$. Es evidente que $\mcd(x, y, z)$ divide a d, por lo que basta demostrar que d divide a $\mcd(x, y, z)$. Para ello, observamos que $d|x$ y $d|y$ implica $d^2|x^2$ y $d^2|y^2$. Por tanto, $d^2|x^2 + y^2 = z^2$, de donde se deduce $d|z$ (por el Teorema 1.18). De aquí se concluye $d|\mcd(x, y, z)$.

La parte (ii) es inmediata. □

Definición. Una terna pitagórica se dice que es primitiva si $\mcd(x, y, z) = 1$, o equivalentemente cualquiera de los $\mcd(x, y)$, $\mcd(x, z)$, $\mcd(y, z)$ es 1.

Lema 6.2. *Sea x, y, z una terna pitagórica primitiva. Entonces entre x, y, z hay exactamente un número par, que es o bien x o bien y.*

Demostración: Es evidente que entre x, y, z hay exactamente un número par. Si fuera z, entonces xx, y serían impares, luego $x^2, y^2 \equiv 1 \pmod 8$, luego $z^2 = x^2 + y^2 \equiv 2 \pmod 8$, lo que es absurdo, porque z^2 debe ser divisible por 4. □

Teorema 6.3. *Sea x, y, z una terna pitagórica primitiva con $x, y, z > 0$ y x par. Entonces existen $s, t \in \mathbb{Z}$ tales que $0 < t < s$, $\mathrm{mcd}(s, t) = 1$, $s \not\equiv t \pmod 2$ y*

$$\begin{cases} x = 2st \\ y = s^2 - t^2 \\ z = s^2 + t^2 \end{cases}$$

Demostración: Observamos en primer lugar que $\mathrm{mcd}(z+y, z-y) = 2$. En efecto, cualquier divisor común de $z + y$ y $z - y$ lo es también de su suma y su diferencia, es decir, de $2z$ y $2y$ Como $\mathrm{mcd}(y, z) = 1$, se sigue el único posible divisor común de $z + y$ y $z - y$ es 2, que efectivamente es un divisor, ya que y, z son impares. Podemos escribir entonces $z + y = 2a$ y $z - y = 2b$, con a, b enteros tales que $\mathrm{mcd}(a, b) = 1$. Por tanto

$$\begin{cases} y = a - b \\ z = a + b \end{cases}$$

Obsérvese que, como $y < \sqrt{x^2 + y^2} = z$, entonces $b > 0$ y, como $y > 0$, también $a > b$. Por otra parte, como x es par, podemos escribir $x = 2c$. De la igualdad $x^2 = z^2 - y^2 = (z + y)(z - y)$ se deduce entonces $c^2 = ab$, luego, por el Corolario 1.17(ii), existen enteros positivos s, t tales que $a = s^2$ y $b = t^2$ (y por tanto $x = 2st$, $y = s^2 - t^2$ y $z = s^2 + t^2$). Como $\mathrm{mcd}(a, b) = 1$, necesariamente $\mathrm{mcd}(s, t) = 1$ y, como $a > b$, será $s > t$. Finalmente,como ni y ni z son pares, necesariamente s y t tienen distinta paridad. □

Teorema 6.4. *La ecuación $x^4 + y^4 = z^2$ no tiene solución entera positiva.*

Demostración: Sea S el conjunto de los enteros positivos z para los que existen $x, y > 0$ tales que $z^2 = x^4 + y^4$. Supongamos, por reducción al absurdo, que la ecuación $x^4 + y^4 = z^2$ tiene solución entera positiva. Esto quiere decir que el conjunto S es no vacío, y por el principio del buen orden existirá un elemento mínimo de S. Sea pues una solución x, y, z con S mínimo en S. Los enteros x^2, y^2, z forman entonces una terna pitagórica, que veremos a continuación que es primitiva. En efecto, si $\mathrm{mcd}(x^2, y^2) \neq 1$, entonces $\mathrm{mcd}(x, y) = d > 1$. Si escribimos $x = dx'$, $y = dy'$, entonces $d^4 | x^4 + y^4 = z^2$, luego $d^2 | z$ y podremos escribir $z = d^2 z'$, con $z' \in \mathbb{Z}_{\geq 1}$. Entonces, haciendo esas sustituciones en la igualdad $x^4 + y^4 = z^2$ queda $d^4 x'^4 + d^4 y'^4 = d^4 z'^2$, de donde se deduce $x'^4 + y'^4 = z'^2$. Por tanto, $z' \in S$, lo que es imposible porque $z' < dz' = z$ y z era mínimo en S.

Sin pérdida de generalidad, podemos suponer que x^2 es par e y^2, z impares. Por el Teoorema 6.3, se tendrá que existen s, t enteros positivos primos entre sí y de distinta paridad tales que

$$\begin{cases} x^2 = 2st \\ y^2 = s^2 - t^2 \\ z = s^2 + t^2 \end{cases}$$

En particular, $t^2+y^2=s^2$, luego t, y, s es también una terna pitagórica primitiva y además necesariamente s es impar y t es par. Usando de nuevo el Teorema 6.3, concluimos que podemos encontrar u, v primos entre sí y de distinta paridad tales que

$$\begin{cases} t = 2uv \\ y = u^2 - v^2 \\ s = u^2 + v^2 \end{cases}$$

Como s es impar, $\text{mcd}(2t, s) = 1$, luego de la igualdad $x^2 = (2t)s$ y del Corolario 1.17(ii) deducimos que existen $t', s' \in \mathbb{Z}_{\geq 1}$ tales que

$$\begin{cases} 2t = (2t')^2 \\ s = s'^2 \end{cases}$$

Finalmente, haciendo la sustitución $t = 2t'^2$ en la igualdad $t = 2uv$ llegamos a $t'^2 = uv$, y usando de nuevo el Corolario 1.17(ii) y $\text{mcd}(u, v) = 1$, obtenemos que existen $u', v' \in \mathbb{Z}_{\geq 1}$ tales que

$$\begin{cases} u = u'^2 \\ v = v'^2 \end{cases}$$

Por tanto, la igualdad $s = u^2 + v^2$ se convierte en $s'^2 = u'^4 + v'^4$, luego $s' \in S$. La desigualdad

$$s' \leq s'^2 = s \leq s^2 < s^2 + t^2 = z$$

produce entonces una contradicción con el hecho de que z era mínimo en S. □

Corolario 6.5. *El Último Teorema de Fermat es cierto para $n = 4$.*

Demostración: En efecto, si la ecuación $x^4 + y^4 = z^4$ tuviera una solución entera $x = a, y = b, z = c$ con $abc \neq 0$, entonces $x = |a|, y = |b|, z = c^2$ sería una solución entera positiva de $x^4 + y^4 = z^2$, lo que es imposible por el Teorema 6.4. □

Observación 6.6. El corolario anterior reduce el Último Teorema de Fermat al caso en que el exponente n es un número primo. En efecto, supongamos demostrado el Último Teorema de Fermat para exponentes primos. Entonces, para cada $n > 2$, o bien n tiene un divisor primo impar o es una potencia de 2. En el primer caso, si $n = pk$, con $p > 2$ primo, entonces la ecuación de Fermat se puede escribir como $(x^k)^p + (y^k)^p = (z^k)^p$, que no tiene solución no trivial, porque por hipótesis $x^p + y^p = z^p$ no la tiene. Si, en cambio, n es una potencia de 2, como $n > 2$, necesariamente se puede escribir $n = 4k$ (además, k sería una potencia de 2, aunque esto no nos interesa). En este caso, se puede escribir la ecuación como $(x^k)^4 + (y^k)^4 = (z^k)^4$, pero el Corolario 6.5 implica que entonces $x^k y^k z^k = 0$, es decir, $xyz = 0$.

Veamos otra ecuación diofántica más restrictiva que la de Fermat de grado cuatro:

Teorema 6.7. *La ecuación $x^4 + y^2 = z^4$ no tiene solución entera positiva.*

Demostración: Como en el Teorema 6.4, suponemos por reducción al absurdo que exista solución y tomamos aquélla con z mínimo, lo que implicará en particular que x^2, y, z^2 es una terna pitagórica primitiva. Tenemos que distinguir ahora dos casos según la paridad de x e y.

Si x es impar e y es par se tendrá, por el Teorema 6.3, que existen $s, t \in \mathbb{Z}$ tales que

$$\begin{cases} x^2 = s^2 - t^2 \\ y = 2st \\ z^2 = s^2 + t^2 \end{cases}$$

y, multiplicando la primera y última igualdad se obtiene $x^2z^2 = (s^2 - t^2)(s^2 + t^2) = s^4 - t^4$, y en particular $t^4 + (xz)^2 = s^4$. Como $s^2 < s^2 + t^2 = z^2$, se concluye que $s < z$, lo que contradice la minimalidad de z.

Nos queda entonces el caso en que x^2 es par e y impar. Por el Teorema 6.3, se tendrá que existen s, t enteros positivos primos entre sí y de distinta paridad tales que

$$\begin{cases} x^2 = 2st \\ z^2 = s^2 + t^2 \end{cases}$$

donde no decimos si $y = s^2 - t^2$ o $y = t^2 - s^2$; por tanto, s y t juegan un papel simétrico, y podemos suponer que s es par y t impar. Como la igualdad $s^2 + t^2 = z^2$ nos dice que s, t, z es una terna pitagórica (primitiva porque $\mathrm{mcd}(s, t) = 1$), por el Teorema 6.3, podemos encontrar u, v primos entre sí y de distinta paridad tales que

$$\begin{cases} s = 2uv \\ t = u^2 - v^2 \\ z = u^2 + v^2 \end{cases}$$

Como t es impar, $\mathrm{mcd}(2s, t) = 1$, luego de la igualdad $x^2 = (2s)t$ y del Corolario 1.17(ii) deducimos que existen $s', t' \in \mathbb{Z}_{\geq 1}$ tales que

$$\begin{cases} 2s = (2s')^2 \\ t = t'^2 \end{cases}$$

Finalmente, haciendo la sustitución $s = 2s'^2$ en la igualdad $s = 2uv$ llegamos a $s'^2 = uv$, y usando de nuevo el Corolario 1.17(ii) y $\mathrm{mcd}(u, v) = 1$, obtenemos que existen $u', v' \in \mathbb{Z}_{\geq 1}$ tales que

$$\begin{cases} u = u'^2 \\ v = v'^2 \end{cases}$$

Por tanto, la igualdad $t = u^2 - v^2$ se convierte en $v'^4 + t'^2 = u'^4$, y claramente

$$u' \leq u'^2 = u \leq u^2 < u^2 + v^2 = z$$

lo que contradice la minimalidad de z. □

Corolario 6.8. *El área de un triángulo pitagórico no puede ser un cuadrado perfecto.*

Demostración: Si x, y, z son las longitudes de los lados de un triángulo pitagórico, el área del mismo es $\frac{1}{2}xy$, luego si es un cuadrado perfecto existirá $u \in \mathbb{Z}_{\geq 1}$ tal que $xy = 2u^2$. Por tanto tendremos

$$(x+y)^2 = x^2 + 2xy + y^2 = z^2 + 4u^2$$
$$(x-y)^2 = x^2 - 2xy + y^2 = z^2 - 4u^2$$

y multiplicando llegamos a

$$(x^2 - y^2)^2 = z^4 - (2u)^4$$

que contradice el Teorema 6.7. □

Observación 6.9. No podemos seguir poniendo más restricciones a la ecuación de Fermat de grado cuatro sin llegar ya a soluciones no triviales. Obsérvese que en los Teoremas 6.4 y 6.7 hemos cambiado un exponente 4 por un 2. Si cambiáramos dos exponentes 4 por un 2, es decir, si consideráramos las ecuaciones $x^2 + y^4 = z^2$ y $x^2 + y^2 = z^4$, ya tendríamos infinitas soluciones. Basta mirar en la expresión de las ternas pitagóricas primitivas dada en el Teorema 6.3 para ver que se obtienen infinitas soluciones de $x^2 + y^4 = z^2$ si existen infinitas soluciones de

$$\begin{cases} x = 2st \\ y^2 = s^2 - t^2 \\ z = s^2 + t^2 \end{cases}$$

lo que es cierto porque existen infinitas soluciones de $y^2 = s^2 - t^2$. De la misma forma, existirán infinitas soluciones de $x^2 + y^2 = z^4$ si existen infinitas soluciones de

$$\begin{cases} x = 2st \\ y = s^2 - t^2 \\ z^2 = s^2 + t^2 \end{cases}$$

lo que vuelve a ser cierto, porque basta encontrar infinitas soluciones de $z^2 = s^2 + t^2$.

Las soluciones de la ecuación $x^2 + y^2 = z^2$ se pueden interpretar desde otro punto de vista: ¿cuándo un cuadrado perfecto z^2 se puede escribir como suma de dos cuadrados

x^2+y^2? O bien, ¿cuándo un cuadrado perfecto x^2 se puede escribir como diferencia de dos cuadrados z^2-y^2? A continuación queremos estudiar un problema más general: ¿cuándo un número se puede escribir como suma o diferencia de dos cuadrados?. Empezamos con el caso de la diferencia de cuadrados, que resulta sorprendentemente fácil:

Teorema 6.10. *Un número $n \in \mathbb{Z}$ se puede escribir como $n = x^2 - y^2$ si y sólo si $n \not\equiv 2 \pmod 4$.*

Demostración: Supongamos primero que $n = x^2 - y^2$. Como $x^2, y^2 \equiv 0, 1 \pmod 4$, se sigue que $n = x^2 - y^2 \equiv 0, 1, 3 \pmod 4$. Recíprocamente, supongamos que $n \not\equiv 2 \pmod 4$. Distinguimos dos casos:

-Si n es impar, entonces escribimos $n = (\frac{n+1}{2})^2 - (\frac{n-1}{2})^2$.

-Si n es par, entonces es múltiplo de 4, y podemos escribir $n = (\frac{n+4}{4})^2 - (\frac{n-4}{4})^2$. □

El caso de la suma de dos cuadrados es más complicado. Empezamos con una observación que será muy útil:

Lema 6.11. *El producto de dos sumas de dos cuadrados es también una suma de dos cuadrados.*

Demostración: En efecto, basta observar que $(x^2+y^2)(z^2+w^2) = (xz+yw)^2+(xw-yz)^2$. □

A la vista del resultado anterior, parece lógico estudiar primero qué números primos son sumas de dos cuadrados. En este caso, tenemos el siguiente primer resultado:

Proposición 6.12. *Si p es un número primo y $x, y \in \mathbb{Z}$, entonces:*

(i) $p = x^2 + y^2$ si y sólo si $p|x^2 + x^2$ y $0 < |x|, |y| < \sqrt{p}$.

(ii) Si $p = x^2+y^2 = z^2+w^2$, entonces o bien $|x| = |z|$, $|y| = |w|$ o bien $|x| = |w|$, $|y| = |z|$.

Demostración: Para demostrar (i), supongamos primero $p = x^2 + y^2$, de donde se deduce inmediatamente $p|x^2 + x^2$. Además, no puede ser $x = 0$, ya que entonces $p = y^2$, y no podría ser un número primo. De la misma forma, $y \neq 0$, por lo que $|x|, |y| > 0$. De aquí se deduce también $x^2 < x^2 + y^2 = p$, luego $|x| < \sqrt{p}$ y, análogamente, $|y| < \sqrt{p}$.

Recíprocamente, supongamos $p|x^2+x^2$ y $0 < |x|, |y| < \sqrt{p}$. En particular, $x^2+y^2 = np$ para algún $n > 0$. Por otra parte, $np = x^2 + y^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = p + p = 2p$, luego $n < 2$, es decir, $n = 1$ y $x^2 + y^2 = p$.

Para demostrar (ii), es claro que basta suponer $x, y, z, w > 0$. Tenemos entonces

$$(xz-yw)(xw-yz) = x^2zw-xyz^2-xyw^2+y^2zw = (x^2+y^2)zw-xy(z^2+w^2) = p(zw-xy).$$

Como p es primo, entonces $p|xz-yw$ o $p|xw-yz$. Por otra parte, por (i), $x,y,z,w<\sqrt{p}$, luego $|xz-yw|,|xw-yz|<p$, por lo que decir que $xz-yw$ o $xw-yz$ son divisibles por p es lo mismo que decir que $xw-yz$ o $xw-yz$ son cero y, en cualquiera de los caso, se tendrá también $zw-xy=0$. Supongamos por ejemplo $xw-yz=0$. Entonces

$$zw^2=w(zw)=w(xy)=y(xw)=y(yz)=y^2z$$

de donde se sigue $y^2=w^2$ y por tanto $x^2=w^2$, es decir, $y=w$ y $x=z$. Cuando $xw-yz=0$, el mismo argumento demuestro $x=w$, $y=z$. □

A la vista de la parte (i) del resultado anterior, empezamos viendo cuándo una suma de dos cuadrados es divisible por un número primo.

Lema 6.13. *Sea p un número primo y sean x,y números enteros no divisibles por p. Sea $a\in\mathbb{Z}$ tal que $ax\equiv y \pmod{p}$. Entonces $p|x^2+y^2$ si y sólo si $a^2\equiv -1 \pmod{p}$. En particular, un número primo $p\equiv 3 \pmod{4}$ no puede dividir a la suma de dos cuadrados no divisibles por p.*

Demostración: Para la primera parte, basta observar que $x^2\equiv -y^2\equiv -a^2x^2 \pmod{p}$. Como $\mcd(x,p)=1$, por la Proposición 2.1(vi) la congruencia anterior es equivalente a $a^2\equiv -1 \pmod{p}$.

Para la segunda parte, supongamos por reducción al absurdo que $p\equiv 3 \pmod{4}$ y $p|x^2+y^2$ con x,y no divisibles por p. Como $\mcd(x,p)=1$, por la Proposición 2.9, existirá $a\in\mathbb{Z}$ tal que $ax\equiv y \pmod{p}$. El Lema 6.13 implica entonces $a^2\equiv -1 \pmod{p}$, y por el Teorema 2.19 no puede ser $p\equiv 3 \pmod{4}$. □

El resultado anterior y la Proposición 6.12(i) sugieren que necesitaremos el siguiente:

Lema 6.14 (Thue)**.** *Sea p un número primo y $a\in\mathbb{Z}$ con $\mcd(a,p)=1$. Entonces existen $x,y\in\mathbb{Z}$ tales que $ax\equiv y \pmod{p}$ y $0<|x|,|y|<\sqrt{p}$.*

Demostración: Consideramos el conjunto de expresiones de la forma $ax-y$ con $0\leq x,y\leq \sqrt{p}$. Como tenemos $([\sqrt{p}]+1)^2>p$ posibilidades para los pares x,y, necesariamente tendremos dos pares distintos x_1,y_1 y x_2,y_2 en esas condiciones tales que $ax_1-y_1\equiv ax_2-y_2 \pmod{p}$. Por tanto, $x=x_1-x_2$, $y=y_1-y_2$ es la solución buscada. □

Teorema 6.15. *Un número primo p se puede expresar como suma de dos cuadrados si y sólo si $p=2$ o $p\equiv 1 \pmod{4}$.*

Demostración: Suponemos en primer lugar que podemos escribir $p=x^2+y^2$. Por la Proposición 6.12(i), $0<|x|,|y|<p$, luego x,y no son divisibles por p. El Lema 6.13 implica entonces que p no es congruente con 3 módulo 4, luego $p=2$ o $p\equiv 1 \pmod{4}$.

Recíprocamente, si $p = 2$ o $p \equiv 1 \pmod 4$, el Teorema 2.19 implica que existe $a \in \mathbb{Z}$ tal que $p|a^2 + 1$. Evidentemente, $\text{mcd}(a, p) = 1$, por lo que por el Lema de Thue existen $x, y \in \mathbb{Z}$ tales que $ax \equiv y \pmod p$ y $0 < |x|, |y| < \sqrt{p}$. La condición $ax \equiv y \pmod p$ implica, por el Lema 6.13, que $p|x^2 + y^2$, y entonces la condición $0 < |x|, |y| < \sqrt{p}$ implica, por el Lema 6.13, $p = x^2 + y^2$, como queríamos. □

Podemos caracterizar finalmente los enteros que son sumas de dos cuadrados:

Teorema 6.16. *Un número positivo es suma de dos cuadrados si y sólo si, en su descomposición en factores primos, todos los factores primos de la forma $4k + 3$ aparecen con exponente par.*

Demostración: Sea $n = x^2 + y^2$ y llamemos $d = \text{mcd}(x, y)$. Podemos entonces escribir $x = dx'$ y $y = dy'$ con $\text{mcd}(x', y') = 1$. Entonces $n = d^2(x'^2 + y'^2)$. Cada factor primo p de $x'^2 + y'^2$, no puede dividir ni a x' ni a y' (si dividiera a uno, dividiría a ambos), luego por la Lema 6.13, no es $p \equiv 3 \pmod 4$. Por tanto, los factores primos de n de la forma $4k + 3$ están todos en d^2, luego aparecen con exponente par.

Recíprocamente, si n tiene todos sus factores primos de la forma $4k+3$ con exponente par, se podrá escribir $n = d^2 p_1 \dots p_r$, donde $p_1, \dots, p_r$ son primos distintos que no son de la forma $4k+3$. Por el Teorema 6.15, cada p_i es suma de dos cuadrados, y por el Lema 6.11 su producto también lo es, es decir, $p_1 \dots p_r = x^2 + y^2$. De aquí se sigue $n = (dx)^2 + (dy)^2$. □

Observación 6.17. Nótese que, si n no es primo, no se tiene la unicidad de la descomposición en suma de dos cuadrados que obtuvimos en la Proposición 6.12(ii). En efecto, consideremos $n = 65 = 5 \cdot 13$. Tenemos entonces $5 = 2^2 + 1^2$ y $13 = 3^2 + 2^2$. Aplicando el Lema 6.11 con $x = 2, y = 1, z = 3, w = 2$, obtenemos $65 = 8^2 + 1^2$, mientras que, si aplicamos el Lema 6.11 con $x = 2, y = 1, z = 2, w = 3$, obtendremos $65 = 7^2 + 4^2$.

Ya que hay muchos números positivos que no se pueden escribir como suma de dos cuadrados, cabe plantearse ahora al pregunta: ¿podrá escribirse todo número positivo como suma de tres cuadrados? Inmediatamente encontramos una respuesta negativa:

Teorema 6.18. *Ningún número de la forma $4^n(8k + 7)$ se puede escribir como suma de tres cuadrados.*

Demostración: Lo demostramos por inducción sobre n. Si $n = 0$, tenemos que ver que no se puede escribir $8k+7 = x^2+y^2+z^2$. Esto es evidente, ya que $x^2, y^2, z^2 \equiv 0, 1, 4 \pmod 8$.

Supongamos ahora demostrado el resultado para n y veamos que es cierto para $n+1$. Supongamos, por reducción al absurdo, que podemos escribir $4^{n+1}(8k+7) = x^2+y^2+z^2$. Como $4^{n+1} \equiv 0 \pmod 4$ y $x^2, y^2, z^2 \equiv 0, 1 \pmod 4$, se sigue que necesariamente $a^2, b^2, c^2 \equiv 0 \pmod 4$, es decir, x, y, z son pares. Escribimos entonces $x = 2x'$, $y = 2y'$ y $z = 2z'$, por lo que se tendrá $4^n(8k+7) = x'^2 + y'^2 + z'^2$, lo que contradice la hipótesis de inducción. □

Observación 6.19. En realidad, se puede demostrar que el teorema anterior caracteriza a los números que no son sumas de tres cuadrados. Sin embargo, la demostración no es fácil (por lo que no la haremos). Esto se debe a que, contrariamente a lo que ocurre para la suma de dos cuadrados (ver el Lema 6.11) el hecho de ser suma de tres cuadrados no se respeta por productos. Por ejemplo, $14 = 3^2 + 2^2 + 1^2$ y $18 = 4^2 + 1^2 + 1^2$, mientras que $14 \cdot 18 = 4(8 \cdot 7 + 7)$ no es suma de tres cuadrados por el Teorema 6.18.

Ya que con tres cuadrados no se puede, podemos seguir preguntándonos ahora: ¿Y será cierto que todo número entero positivo se puede escribir como suma de cuatro cuadrados? La respuesta ahora será positiva, y se basa en que, en este caso ya es cierto el análogo del Lema 6.11, que es una simple cuenta que dejamos como ejercicio:

Ejercicio 6.20. Comprobar que se verifica la igualdad

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = r^2+s^2+t^2+u^2$$

donde

$$\begin{cases} r = ax + by + cz + dw \\ s = bx - ay + dz - cw \\ t = cx - dy - az + bw \\ u = dx + cy - bz - aw \end{cases}$$

A la vista de este resultado, bastará ver que todo número primo es suma de cuatro cuadrados. Como en el caso de dos cuadrados, empezamos de momento con propiedades sobre los divisores de distintas sumas de cuadrados:

Lema 6.21. *Si $p \equiv 3 \pmod 4$ es un número primo, entonces existen $x, y \in \mathbb{Z}$ tales que $p | x^2 + y^2 + 1$.*

Demostración: Por las partes (iii) y (iv) de la Proposición 5.3, tenemos respectivamente $\left(\frac{1}{p}\right) = 1$ y $\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = -1$. Podremos encontrar entonces $a \in \{2, 3, \ldots, p-1\}$ tal que $\left(\frac{a-1}{p}\right) = 1$ y $\left(\frac{a}{p}\right) = -1$ y, en particular,

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)(-1) = 1.$$

Por tanto, existen $a-1$ y $-a$ son restos cuadráticos módulo p, es decir, existen $x, y \in \mathbb{Z}$ tales que $x^2 \equiv a-1 \pmod{p}$ y $y^2 \equiv -a \pmod{p}$. Sumando, tendremos

$$x^2 + y^2 \equiv (a-1) + (-a) = -1 \pmod{p},$$

es decir, $p | x^2 + y^2 + 1$. □

Lema 6.22. *Sea m un divisor impar de una suma $x^2 + y^2 + z^2 + w^2$. Entonces existen $a, b, c, d \in \mathbb{Z}$ tales que*

$$\begin{cases} x \equiv a \pmod{m} \\ y \equiv b \pmod{m} \\ z \equiv c \pmod{m} \\ w \equiv d \pmod{m} \end{cases}$$

y $a^2 + b^2 + c^2 + d^2 = mm'$, con $m' < m$.

Demostración: Sea r el resto de la división de x entre m. Si $r < \frac{m}{2}$ tomamos $a = r$, y si $r > \frac{m}{2}$ tomamos $a = r - m$ (hace falta que m sea impar para que no se pueda dar el caso $r = \frac{m}{2}$. Entonces $x \equiv a \pmod{m}$ y $|a| < \frac{m}{2}$. Construimos de la misma forma b, c, d, es decir, congruentes respectivamente con y, z, w módulo m y de valor absoluto menor que $\frac{m}{2}$. Por tanto, tendremos

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m}$$

luego existirá $m' \in \mathbb{Z}$ tal que $a^2 + b^2 + c^2 + d^2 = mm'$. Además,

$$mm' = a^2 + b^2 + c^2 + d^2 < \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = m^2$$

por lo que $m' < m$. □

Finalmente, podemos demostrar ya el resultado que buscábamos:

Teorema 6.23. *Todo número natural se puede escribir como suma de cuatro cuadrados (no necesariamente distintos de cero).*

Demostración: Por el Ejercicio 6.20, basta demostrar que cada número primo p es suma de cuatro cuadrados. Si $p = 2$ o $p \equiv 1 \pmod{4}$ ya sabemos que p se escribe como suma de incluso sólo dos cuadrados, así que basta demostrar el caso $p \equiv 3 \pmod{4}$. Por el Lema 6.21, sabemos que p divide a la suma de tres cuadrados de enteros no todos nulos, luego en particular un múltiplo de p se puede poner como la suma de cuatro cuadrados de enteros no todos nulos. Sea kp el múltiplo más pequeño de p que se puede escribir como suma de

cuatro cuadrados de enteros positivos no todos nulos. Por el Lema 6.22 tomando $m = p$, se tiene $k < p$, y lo que queremos ver es $k = 1$.

Veamos primero que k es impar. Escribimos

$$kp = x^2 + y^2 + z^2 + w^2.$$

Si k fuera par, entonces entre x, y, z, w hay una cantidad par de números pares y una cantidad par de impares. En cualquier caso, reordenándolos, podemos suponer que x e y tienen la misma paridad y que z y w tienen la misma paridad. Entonces tendremos

$$\frac{k}{2}p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2,$$

lo que contradice la minimalidad de k, lo que implica que k es impar.

Supongamos, por reducción al absurdo, que $k > 1$. Aplicando ahora el Lema 6.22 tomando $m = k$, existirán $a, b, c, d \in \mathbb{Z}$ tales que

$$\begin{cases} x \equiv a \pmod{k} \\ y \equiv b \pmod{k} \\ z \equiv c \pmod{k} \\ w \equiv d \pmod{k} \end{cases}$$

y $a^2 + b^2 + c^2 + d^2 = nk$ con $n < k$. Si fuera $n = 0$, entonces $a = b = c = d = 0$, luego k dividiría a x, y, z, w, así que k^2 dividiría a $x^2 + y^2 + z^2 + w^2 = kp$, es decir, k dividiría a p, lo que contradice el hecho de que $1 < k < p$. Por tanto, $0 < n < k$. Usando la igualdad del Ejercicio 6.20 tendremos

$$k^2np = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) = r^2 + s^2 + t^2 + u^2$$

donde

$$\begin{cases} r = ax + by + cz + dw \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k} \\ s = bx - ay + dz - cw \equiv ba - ab + dc - cd = 0 \pmod{k} \\ t = cx - dy - az + bw \equiv ca - db - ac + bd = 0 \pmod{k} \\ u = dx + cy - bz - aw \equiv da + cb - bc - ad = 0 \pmod{k} \end{cases}$$

es decir, r, s, t, u son divisibles por k. Se tiene entonces

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2,$$

lo que de nuevo contradice la minimalidad de k, ya que $n < k$. Por tanto, $k = 1$, como queríamos. □

Observación 6.24. Para sumas de potencias superiores, se tiene el llamado *problema de Waring*. En concreto, fijado $n \in \mathbb{Z}_{\geq 1}$, ¿cuál es el mínimo número $g(n)$ tal que cada número entero positivo es suma de $g(n)$ potencias n-ésimas de números enteros? En este contexto, el Teorema 6.18 indica que $g(2) \geq 4$ y el Teorema 6.23 indica que $g(2) \leq 4$, por lo que $g(2) = 4$. Para $n \geq 3$ el problema es mucho más complicado, ya que no ocurre que el producto sumas de g potencias n-ésimas sea una suma de g potencias n-ésimas (como ocurre para $n = 2$ con $g = 2$ y $g = 4$). Hay además una situación nueva. Por ejemplo, para $n = 3$ no es difícil ver que $23 = 2^3 + 2^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3$ es la menor descomposición en suma de cubos de 23, por lo que $g(3) \geq 9$. Por otra parte, ha logrado demostrarse (por L. Dickson) que cualquier entero positivo distinto de 23 y 239 puede escribirse como suma de como mucho ocho cubos, y de la misma forma se sabe (por un resultado debido a Linnik) que salvo una cantidad finita de casos, todo entero positivo es suma de a lo sumo de siete cubos. Esto da lugar a otro problema, llamado el *gran problema de Waring* (al anterior se le suele llamar por contraposición *pequeño problema de Waring*): ¿cuál es el mínimo número $G(n)$ tal que cada número entero positivo, salvo una cantidad finita de casos, es suma de $G(n)$ potencias n-ésimas de números enteros? Mientras que para $n = 2$ sigue siendo $g(2) = G(2) = 4$, lo anterior para $n = 3$ se traduce en $g(3) = 9$, $G(3) \leq 7$. Es un problema abierto cuál es el valor de $G(3)$ (se sospecha $G(3) = 4$, pero sólo se sabe $4 \leq G(3) \leq 7$) y en general de $G(n)$ para $n \geq 3$. Respecto a $g(n)$, se ha demostrado recientemente que $g(4) = 19$, $g(5) = 37$ y $g(n) = [(\frac{3}{2})^n] + 2^n - 2$ si $n \geq 6$ salvo quizá una cantidad finita de valores de n.

Los Teoremas 6.10 y 6.16 pueden interpretarse como haber estudiado cuándo las ecuaciones de la forma $x^2 - y^2 = n$ o $x^2 + y^2 = n$ tienen solución entera. El caso más sencillo ha sido el de diferencia de dos cuadrados. Podemos complicar la ecuación un poco más y poner coeficientes a la x y a la y, en cuyo caso las cosas se complican muchísimo. El primer caso, aparentemente sencillo, sería la ecuación $x^2 - dy^2 = 1$ con d entero positivo que no sea un cuadrado perfecto. Esta ecuación (llamada *ecuación de Pell*, aunque en realidad se debería atribuir a Fermat), no es fácil en absoluto, aunque al menos se puede decir que sus soluciones (caso de existir) tienen una buena estructura:

Teorema 6.25. *Sea d un entero positivo que no sea un cuadrado perfecto y consideremos la ecuación $x^2 - dy^2 = 1$.*

(i) Si x', y' y x'', y'' son soluciones enteras de la ecuación, entonces $x'x'' + dy'y'', x'y'' + x''y'$ es también solución de la ecuación.

(ii) Si existe una solución entera positiva x_1, y_1 tal que $x_1 + y_1\sqrt{d}$ es mínimo entre todas las soluciones enteras positivas de la ecuación, entonces las soluciones enteras positivas de la ecuación son los pares de la forma x_n, y_n donde $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.

Demostración: Obsérvese que

$$(x' + y'\sqrt{d})(x'' + y''\sqrt{d}) = (x'x'' + dy'y'') + (x'y'' + x''y')\sqrt{d}$$

$$(x' - y'\sqrt{d})(x'' - y''\sqrt{d}) = (x'x'' + dy'y'') - (x'y'' + x''y')\sqrt{d}$$

Como las soluciones de la ecuación son los enteros que verifican $(x + y\sqrt{d})(x - y\sqrt{d}) = 1$, multiplicando las dos igualdades anteriores se obtiene (i). De la misma forma se obtiene que los pares x_n, y_n de (ii) son solución. Lo que falta ver es que son las únicas soluciones.

Supongamos, por reducción al absurdo, que tenemos otra solución entera positiva x', y' que no es ninguna de las x_n, y_n. Por la minimalidad de x_1, y_1, se tendrá $x_1 + y_1\sqrt{d} < x' + y'\sqrt{d}$. Además como la sucesión $(x_1 + y_1\sqrt{d})^n$ es monótona creciente con límite infinito se tendrá que existe $n \in \mathbb{Z}_{\geq 1}$ tal que

$$(x_1 + y_1\sqrt{d})^n < x' + y'\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}.$$

Multiplicando por $(x_1 - y_1\sqrt{d})^n$ (que es positivo porque su producto con $(x_1 + y_1\sqrt{d})^n$ es 1) se tiene

$$1 < (x' + y'\sqrt{d})(x_1 - y_1\sqrt{d})^n < x_1 + y_1\sqrt{d}.$$

Ahora bien, por (i), si escribimos

$$(x' + y'\sqrt{d})(x_1 - y_1\sqrt{d})^n = (x' + y'\sqrt{d})(x_n - y_n\sqrt{d}) = x'' + y''\sqrt{d}$$

se tiene que x'', y'' es una solución de la ecuación. Para encontrar el absurdo que buscamos basta ver que esta última solución es positiva. Ahora bien, como $x'' + y''\sqrt{d} > 1$ y $(x'' + y''\sqrt{d})(x'' - y''\sqrt{d}) = 1$, entonces $0 < x'' - y''\sqrt{d} < 1$. Por tanto,

$$2x'' = (x'' + y''\sqrt{d}) + (x'' - y''\sqrt{d}) > 1 + 0 > 0$$

$$2y''\sqrt{d} = (x'' + y''\sqrt{d}) - (x'' - y''\sqrt{d}) > 1 - 1 > 0$$

lo que termina la demostración. □

Esta demostración indica lo que es una de las técnicas fundamentales de la Teoría Algebraica de Números: ampliar el conjunto de los enteros a expresiones, por ejemplo, de la forma $a + b\sqrt{d}$. El problema principal de esta técnica es que, salvo para valores muy concretos de d, no se verifica la factorización única que tenemos para los enteros (y cuando se verifica no es de forma tan fácil). Para terminar de estudiar la ecuación de Pell (y en particular la existencia de la solución x_1, y_1 que necesita el teorema anterior) desarrollaremos en la siguiente sección toda una técnica nueva, la de las fracciones continuas.

7. Fracciones continuas

Cuando pasamos de los números enteros a los racionales, la escritura que solemos hacer de ellos, aparte de como fracciones, es a partir de su notación decimal. Esta escritura decimal presenta dos inconvenientes. Uno es que depende de una elección de escritura en base 10, que a priori es arbitraria. El segundo inconveniente es que las expresiones con decimales suelen ser infinitas, aunque al menos son periódicas y se pueden representar de forma finita.

Ejemplo 7.1. Veamos una tercera representación de un número racional a partir del algoritmo de Euclides. Si tenemos el número $\frac{a}{b}$, escribimos

$$\begin{array}{ll} a = ba_0 + r_1 & 0 < r_1 < b \\ b = r_1a_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2a_2 + r_3 & 0 < r_3 < r_2 \\ \vdots & \\ r_{n-2} = r_{n-1}a_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_na_n & \end{array}$$

donde $r_n = \mathrm{mcd}(a, b)$. Además, $a_1, \ldots, a_r > 0$ porque son cocientes de números positivos uno mayor que el otro. Podemos entonces escribir:

$$\frac{a}{b} = a_0 + \frac{r_1}{b}$$

$$\frac{b}{r_1} = a_1 + \frac{r_2}{r_1}$$

$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2}$$

$$\vdots$$

$$\frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{r_n}{r_{n-1}}$$

$$\frac{r_{n-1}}{r_n} = a_n$$

(es decir, $a_0, a_1, \ldots, a_r$ son las partes enteras de $\frac{a}{b}, \frac{b}{r_1}, \ldots, \frac{r_{n-1}}{r_n}$) y, poniendo todo junto,

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} = \ldots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}}$$

Ejemplo 7.2. Podríamos intentar ahora repetir un proceso parecido para cualquier número: dado un número real $\alpha \neq 0$, vamos escribiendo

$$\alpha_0 := \alpha = [\alpha_0] + (\alpha_0 - [\alpha_0]) = a_0 + (\alpha_0 - a_0)$$

$$\alpha_1 := \frac{1}{\alpha_0 - a_0} = [\alpha_1] + (\alpha_1 - [\alpha_1]) = a_1 + (\alpha_1 - a_1)$$

$$\vdots$$

es decir, definimos por recurrencia, a partir de $\alpha_0 = \alpha$, los números a_k y α_k mediante:

$$a_k = [\alpha_k]$$

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}.$$

Tendremos entonces

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{k-1} + \cfrac{1}{a_k + \cfrac{1}{\alpha_{k+1}}}}}}}.$$

Obsérvese que, como $a_k \leq \alpha_k < a_k + 1$, necesariamente $0 \leq \alpha_k - a_k < 1$, por lo que, si $\alpha_k \neq a_k$ (es decir, si α_k no es entero), se tendrá $\alpha_{k+1} > 1$, por lo que $a_k \geq 1$ si $k \geq 1$ (aunque a_0 puede ser cero o incluso negativo). Si α es racional, el Ejemplo 7.1 indica que el proceso termina (lo que ocurre cuando llegamos a algún α_k entero y, por tanto $a_k = \alpha_k$), mientras que si α es irracional, entonces cada α_k es también irracional, y por tanto el proceso no termina nunca. Por ejemplo, si tomamos $\alpha\sqrt{2}$, tendremos entonces

$$\alpha_0 = \sqrt{2} = 1'414213562\ldots = 1 + 0'414213562\ldots = 1 + (\sqrt{2} - 1)$$

$$\alpha_1 = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = 2'414213562\ldots = 2 + 0'414213562\ldots = 2 + (\sqrt{2} - 1)$$

y, a partir de aquí, $\alpha_1 = \alpha_2 = \ldots = \sqrt{2} + 1$, y por tanto $a_1 = a_2 = \ldots = 1$, mientras $a_0 = 1$. Parecería entonces natural escribir

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ldots}}}}$$

Definición. Se llama *fracción continua* a una expresión del tipo

$$[a_0; a_1, a_2, \ldots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ldots}}}}$$

donde los números $a_1, a_2, \ldots$ (que pueden ser una cantidad finita o infinita) son estrictamente positivos. Se llama *fracción continua asociada a un número real* α a la fracción continua $[a_0; a_1, a_2, \ldots]$ definida como en el Ejemplo 7.2. Se dice que una fracción continua es *simple* si $a_0, a_1, \ldots$ son números enteros (y por tanto $a_1, a_2, \ldots \geq 1$). Usaremos también la notación $[a_0; a_1, \ldots, a_r, \overline{a_{r+1}, \ldots, a_{r+s}}]$ para indicar la fracción continua infinita periódica $[a_0; a_1, \ldots, a_r, a_{r+1}, \ldots, a_{r+s}, a_{r+1}, \ldots, a_{r+s}, a_{r+1}, \ldots, a_{r+s}, \ldots]$.

Por lo que hemos visto, un número racional se expresa siempre como una fracción continua simple finita, y es obvio que las fracciones continuas simples finitas representan números racionales. Por otra parte, el método anterior sugiere que los números irracionales tienen asociada una fracción continua infinita. Para dar sentido a dicha expresión infinita, habrá que verla como límite de sus subfracciones infinitas. Más precisamente:

Definición. Se llama *convergente k-ésimo* de una fracción continua simple $[a_0; a_1, a_2, \ldots]$ (finita o infinita) a $C_k = [a_0; a_1, a_2, \ldots, a_k]$.

Teorema 7.3. *Sea* $[a_0; a_1, a_2, \ldots]$ *una fracción continua (no necesariamente simple o finita). Definimos recursivamente dos sucesiones de números* p_k *y* q_k *con* $k \geq -2$ *mediante*

$$\begin{cases} p_{-2} = 0 \\ p_{-1} = 1 \\ p_k = a_k p_{k-1} + p_{k-2} \end{cases} \qquad \begin{cases} q_{-2} = 1 \\ q_{-1} = 0 \\ q_k = a_k q_{k-1} + q_{k-2} \end{cases}$$

Entonces:

(i) Para cada $k \geq 0$ *se tiene* $C_k = \frac{p_k}{q_k}$.

(ii) Para cada $k \geq -2$ *se tiene* $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$.

Demostración: Demostraremos (i) por inducción sobre k. Para $k = 0$, se tiene $p_0 = a_0$, $q_0 = 1$, luego $\frac{p_0}{q_0} = a_0 = [a_0] = C_0$.

Supongamos ahora que sabemos que la fórmula es cierta para convergentes k-ésimos y veamos que es cierta para los $(k+1)$-ésimos. Para ello consideramos la fracción continua

$$[a_0'; a_1', a_2', \ldots, a_k'] := [a_0; a_1, a_2, \ldots, a_k + \frac{1}{a_{k+1}}],$$

que claramente coincide con C_{k+1}. Por otra parte, es claro que si $i \leq k-1$ entonces $p_i' = p_i$ y $q_i' = q_i$, mientras que para $i = k$ se tiene

$$p_k' = a_k' p_{k-1}' + p_{k-2}' = (a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2} = a_k p_{k-1} + p_{k-2} + \frac{p_{k-1}}{a_{k+1}} = p_k + \frac{p_{k-1}}{a_{k+1}}$$

$$q_k' = a_k' q_{k-1}' + q_{k-2}' = (a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2} = a_k q_{k-1} + q_{k-2} + \frac{q_{k-1}}{a_{k+1}} = q_k + \frac{q_{k-1}}{a_{k+1}}$$

luego, por hipótesis de inducción,

$$C_{k+1} = C'_k = \frac{p'_k}{q'_k} = \frac{p_k + \frac{p_{k-1}}{a_{k+1}}}{q_k + \frac{q_{k-1}}{a_{k+1}}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

Demostramos (ii) también por inducción sobre k, siendo trivial el caso $k = -2$. Supuesta cierta la fórmula para k, se tiene

$$p_{k+2}q_{k+1} - p_{k+1}q_{k+2} = (a_{k+2}p_{k+1} + p_k)q_{k+1} - p_{k+1}(a_{k+2}q_{k+1} + q_k) = p_kq_{k+1} - p_{k+1}q_k =$$

$$= -(p_{k+1}q_k - p_kq_{k+1}) = -(-1)^k = (-1)^{(k+1)}.$$

□

Ejemplo 7.4. La parte (ii) del teorema anterior implica, si la fracción continua es simple, que p_k, q_k son enteros primos entre sí (usando por ejemplo el Teorema 1.8). De hecho, puede usarse esta parte para obtener explícitamente una combinación lineal de dos enteros que dé su máximo común divisor. Por ejemplo, consideremos los enteros $a = 34, b = 14$. Si aplicamos el algoritmo de Euclides podremos escribir

$$34 = 2 \cdot 14 + 6$$

$$14 = 2 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

de donde sacamos

$$\frac{34}{14} = [2; 2, 3].$$

Las sucesiones p_k, q_k valen entonces

$$p_0 = 2,\ p_1 = 5,\ p_2 = 17$$

$$q_0 = 1,\ q_1 = 2,\ q_2 = 7$$

lo que nos da $\frac{34}{14} = C_2 = \frac{17}{7}$. Esto indica, por una parte, que $\mathrm{mcd}(34, 14) = 2$, y por otra parte nos da la relación

$$2 \cdot 17 - 5 \cdot 7 = -1,$$

que, cambiando de signo y multiplicada por el máximo común divisor nos da

$$5 \cdot 14 - 2 \cdot 34 = 2$$

Lema 7.5. *Dada una fracción continua, se tiene, para todo $k \geq 0$,:*

(i) $C_{k+1} - C_k = \frac{(-1)^k}{q_{k+1}q_k}$.

(ii) $C_{k+2} - C_k = \frac{(-1)^k}{q_{k+1}}(\frac{1}{q_k} - \frac{1}{q_{k+2}})$.

(iii) Si la fracción es simple, $0 < q_1 < q_2 < \ldots$.

Demostración: Por el Teorema 7.3, tenemos

$$C_{k+1} - C_k = \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{p_{k+1}q_k - p_k q_{k+1}}{q_{k+1}q_k} = \frac{(-1)^k}{q_{k+1}q_k},$$

lo que demuestra (i). Utilizando dos veces (i) tendremos

$$C_{k+2} - C_k = (C_{k+2} - C_{k+1}) + (C_{k+1} - C_k) = \frac{(-1)^{k+1}}{q_{k+2}q_{k+1}} + \frac{(-1)^k}{q_{k+1}q_k} = \frac{(-1)^k}{q_{k+1}}\left(\frac{1}{q_k} - \frac{1}{q_{k+2}}\right),$$

lo que demuestra (ii).

Para la parte (iii), se tiene $q_1 = a_1 > 0$, luego basta demostrar $q_{k-1} < q_k$ para todo $k \geq 2$. Lo hacemos por inducción sobre k. Si $k = 2$, tenemos $q_2 = a_2q_1 + q_0 = a_2q_1 + 1 > a_2q_1$. Como $a_2 \geq 1$ (ya que $a_2 > 0$ y a_2 es entero por ser la fracción simple), se sigue $q_2 > q_1$. El paso de inducción sigue los mismos pasos. Si suponemos que se verifica $q_1 < q_2 < \ldots < q_{k-1} < q_k$, entonces en particular $q_{k-1}, q_k > 0$. Como de nuevo se tiene $a_{k+1} \geq 1$ por ser la fracción simple, se sigue:

$$q_{k+1} = a_{k+1}q_k + q_{k-1} \geq q_k + q_{k-1} > q_k. \qquad \square$$

Teorema 7.6. *Dada una fracción continua simple, se tiene, para todo $k \geq 0$,*

$$C_0 < C_2 < C_4 < \ldots < C_{2k} < C_{2k+1} < \ldots < C_3 < C_1.$$

Además, si la fracción continua es infinita, existe el límite de la sucesión $\{C_k\}$, que es un número irracional α que verifica $C_{2k} < \alpha < C_{2k+1}$ para todo k.

Demostración: Por el Lema 7.5, se tiene $C_{k+2} - C_k = \frac{(-1)^k}{q_{k+1}}(\frac{1}{q_k} - \frac{1}{q_{k+2}})$ y además $q_{k+1} > 0$ y $q_k < q_{k+2}$, luego $C_{k+2} - C_k$ es positivo si k es par y negativo si k es impar, por lo que los convergentes pares son crecientes y los impares son decrecientes. Además $C_{k+1} - C_k = \frac{(-1)^k}{q_{k+1}q_k}$, que es positivo si k es par y negativo si k es impar. Por tanto, un convergente impar es siempre mayor que su convergente anterior par.

Tenemos entonces la sucesión creciente $C_0 < C_2 < C_4 < \ldots$, que está acotada, luego tiene un límite α, y la sucesión decreciente $C_1 > C_3 > C_5 > \ldots$, que también está acotada, luego tiene límite $\alpha' \geq \alpha$. Además, para todo k se tiene

$$\alpha' - \alpha < C_{2k+1} - C_{2k} = \frac{(-1)^{2k}}{q_{2k+1}q_{2k}},$$

que es un valor que tiende a cero (por ser q_k una sucesión creciente de números enteros), luego $\alpha = \alpha'$.

Veamos finalmente que α es irracional. Supongamos, por reducción al absurdo, que fuera $\alpha = \frac{a}{b}$, con a, b enteros (y $b > 0$). Entonces, como para cada k se tiene que α está entre C_k y C_{k+1} (quién sea el mayor de los dos depende de la paridad de k), se tiene

$$0 < |\frac{a}{b} - C_k| < |C_{k+1} - C_k| = \frac{1}{q_{k+1}q_k}.$$

Multiplicando por bq_k, se obtiene

$$0 < |aq_k - bp_k| < \frac{b}{q_{k+1}},$$

lo que es absurdo, porque $aq_k - bp_k$ es un entero y si k es suficientemente grande se tendría $\frac{b}{q_{k+1}} < 1$ (ya que q_{k+1} tiende a infinito). □

Definición. Se llama *valos de una fracción continua simple infinita* al límite α dado por el Teorema 7.6.

Ejemplo 7.7. Veamos ahora un ejemplo de cálculo del valor de una fracción continua infinita. Tomemos, por ejemplo, $[1; \bar{1}]$. Las sucesiones p_k, q_k verifican

$$p_{-1} = 1,\ p_0 = 1,\ p_k = p_{k-1} + p_{k-2}$$
$$q_0 = 1,\ q_1 = 1,\ q_k = q_{k-1} + q_{k-2},$$

por lo que $p_k = u_{k+2}$ y $q_k = u_{k+1}$ (donde u_n es el n-ésimo número de Fibonacci; ver Ejercicio 0.3). Se tiene entonces $C_k = \frac{u_{k+2}}{u_{k+1}}$. Usando la fórmula del Ejercicio 0.3 para el n-ésimo número de Fibonacci, es un simple ejercicio de Análisis Matemático demostrar que $\lim \frac{u_{k+2}}{u_{k+1}} = \frac{1}{2} + \frac{\sqrt{5}}{2}$. Sin embargo, para fracciones continuas periódicas, hay un truco más fácil para calcular su valor. Como el Teorema 7.6 nos asegura que $[1; \bar{1}]$ tiene un valor α, se tendrá la relación:

$$\alpha = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1+\dots}}}} = 1 + \frac{1}{\alpha},$$

por lo que debiera ser $\alpha^2 - \alpha - 1 = 0$, es decir, $\alpha = \frac{1}{2} + \frac{\sqrt{5}}{2}$ (obviamente, debemos tomar la solución positiva).

Tenemos entonces un modo de, a partir de un número irracional, conseguir una fracción continua simple infinita; y tenemos también un modo de, a partir de una fracción continua simple infinita, darle un valor irracional. Una pregunta natural es si ambos procesos son inversos el uno del otro. Por ejemplo, se deja como ejercicio al lector comprobar que la fracción continua asociada a $\frac{1}{2} + \frac{\sqrt{5}}{2}$ (ver el Ejemplo 7.7) es precisamente $[1; \bar{1}]$; de la misma forma, el valor de la fracción continua $[1; \bar{2}]$ (ver el Ejemplo 7.2) es $\sqrt{2}$. El resultado (afirmativo) general es el siguiente:

Teorema 7.8. *Cada número irracional α es el valor de una y sólo una fracción continua infinita simple, que es precisamente la fracción continua asociada a α.*

Demostración: Supongamos primero que un número irracional α es el valor de las fracciones continuas simples $[a_0; a_1, a_2, \ldots]$ y $[a'_0; a'_1, a'_2, \ldots]$. Entonces, por el Teorema 7.6, tendremos $C_0 < \alpha < C_1$, es decir $a_0 < \alpha < a_0 + \frac{1}{a_1}$. Como $a_1 \geq 1$, se tiene entonces $a_0 = [\alpha]$, y de la misma forma $a'_0 = [\alpha]$, por lo que $a_0 = a'_0$. Como se tiene

$$a_0 + \frac{1}{[a_1; a_2, a_3, \ldots]} = [a_0; a_1, a_2, \ldots] = [a'_0; a'_1, a'_2, \ldots] = a'_0 + \frac{1}{[a'_1; a'_2, a'_3, \ldots]}$$

se deduce $[a_1; a_2, a_3, \ldots] = [a'_1; a'_2, a'_3, \ldots]$, y por un argumento de recurrencia se sigue $a'_k = a_k$ para todo k.

Recíprocamente, dado un número irracional α, sea $[a_0; a_1, a_2, \ldots]$ su fracción continua asociada (tomaremos la notación del Ejemplo 7.2). Es claro que, para todo k, se tiene $\alpha = [a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}]$. Entonces el convergente $(k+1)$-ésimo de esta fracción continua finita es α, mientras que el convergente k-ésimo es claramente el convergente k-ésimo C_k de $[a_0; a_1, a_2, \ldots]$. Por el Lema 7.5 aplicado a $[a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}]$, se tendrá entonces

$$\alpha - C_k = \frac{(-1)^k}{(\alpha_{k+1} q_k + q_{k-1}) q_k},$$

donde hemos usado el Teorema 7.3 para calcular el denominador del convergente $(k+1)$-ésimo. Usando ahora las desigualdades $\alpha_{k+1} > a_{k+1}$ y $q_{k+1} > q_k$ se tiene

$$|\alpha - C_k| = \frac{1}{(\alpha_{k+1} q_k + q_{k-1}) q_k} < \frac{1}{(a_{k+1} q_k + q_{k-1}) q_k} = \frac{1}{q_{k+1} q_k} < \frac{1}{q_k^2}.$$

Como q_k tiende a infinito, se tiene que $\alpha = \lim C_k$. □

Ejercicio 7.9. Con la ayuda de una calculadora, comprobar la validez de la fórmula (al menos en sus primeros términos):

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

y utilizar la misma para calcular las diez primeras cifras decimales de e.

Observación 7.10. La demostración tanto del Lema 7.5 como del Teorema 7.8 nos da el grado de aproximación de un convergente a un número irracional α, precisamente $|\alpha - \frac{p_k}{q_k}| < \frac{1}{q_{k+1} q_k} < \frac{1}{q_k^2}$. Por otra parte, si una considera una solución positiva $x = p, y = q$

de la ecuación de Pell $x^2 - dy^2 = 1$, se tiene $p^2 = 1 + q^2 d > q^2 d$, de donde se deduce $p > q\sqrt{d}$. Por tanto,

$$|\frac{p}{q} - \sqrt{d}| = \frac{1}{q}(p - q\sqrt{d}) = \frac{1}{q}\frac{(p - q\sqrt{d})(p + q\sqrt{d})}{(p + q\sqrt{d})} = \frac{1}{q(p + q\sqrt{d})} < \frac{1}{2q^2\sqrt{d}} < \frac{1}{2q^2}.$$

Cabe entonces preguntarse, ya que $\frac{p}{q}$ aproxima $\sqrt{d}$ como un convergente (incluso en principio aún más), si eso no implicará que $\frac{p}{q}$ es realmente un convergente. Si miramos por ejemplo el caso $d = 2$ del Ejemplo 7.2, en que demostramos $\sqrt{2} = [1; \bar{2}]$ tenemos los siguientes valores:

$$p_0 = 1,\ p_1 = 3,\ p_2 = 7,\ p_3 = 17, \ldots$$

$$q_0 = 1,\ q_1 = 2,\ q_2 = 5,\ q_3 = 12, \ldots$$

Por tanto (p_0, q_0) y (p_2, q_2) son soluciones de la ecuación $x^2 - 2y^2 = 1$, mientras que (p_1, q_1) y (p_3, q_3) no son soluciones. De hecho, veremos que las soluciones son convergentes, pero no todos los convergentes son soluciones.

Para ver que un número racional que aproxima mucho a un irracional es un convergente necesitaremos el siguiente lema previo.

Lema 7.11. *Sea α un número irracional, sea $\frac{p_k}{q_k}$ el convergente k-ésimo de su fracción continua y sea q un entero positivo tal que $q < q_{k+1}$. Entonces, para todo entero p se tiene $|p_k - q_k\alpha| \leq |p - q\alpha|$.*

Demostración: Observamos en primer lugar que existen $x, y \in \mathbb{Z}$ tales que

$$\begin{cases} p_k x + p_{k+1} y = p \\ q_k x + q_{k+1} y = q. \end{cases}$$

En efecto, el determinante de la matriz de coeficientes es, por el Teorema 7.3(ii),

$$\begin{vmatrix} p_k & p_{k+1} \\ q_k & q_{k+1} \end{vmatrix} = p_k q_{k+1} - p_{k+1} q_k = -(-1)^k = \pm 1$$

luego existe una única solución del sistema anterior, que es además entera.

Observamos también que $x \neq 0$, ya que si fuera $x = 0$, entonces

$$0 = pq - qp = p(yq_{k+1}) - q(yp_{k+1}) = y(pq_{k+1} - qp_{k+1})$$

y como $y \neq 0$ (ya que $q \neq 0$), se sigue $pq_{k+1} = qp_{k+1}$. Ahora bien, $\mathrm{mcd}(p_{k+1}, q_{k+1}) = 1$, luego $q_{k+1}|q$, lo que es absurdo porque $q < q_{k+1}$.

Comparemos ahora los signos de x e y. Si $y < 0$, entonces

$$q_k x = q - q_{k+1} y > 0$$

de donde se sigue $x > 0$. Si en cambio $y > 0$, entonces $y \geq 1$ y se tiene

$$q_k x = q - q_{k+1} y < q_{k+1} - q_{k+1} y = q_{k+1}(1 - y) \leq 0$$

y por tanto $x < 0$.

Usando lo anterior, tenemos

$$|p - q\alpha| = |(p_k x + p_{k+1} y) - (q_k x + q_{k+1} y)\alpha| = |x(p_k - q_k \alpha) + y(p_{k+1} + q_{k+1}\alpha)|.$$

Si supiéramos que $|x(p_k - q_k\alpha) + y(p_{k+1} + q_{k+1}\alpha)| \geq |x(p_k - q_k\alpha)|$, se concluiría inmediatamente, ya que

$$|x(p_k - q_k\alpha)| = |x||p_k - q_k\alpha| \geq |p_k - q_k\alpha|$$

(puesto que $x \neq 0$ y por tanto $|x| \geq 1$). La desigualdad $|x(p_k - q_k\alpha) + y(p_{k+1} + q_{k+1}\alpha)| \geq |x(p_k - q_k\alpha)|$ es inmediata si $y = 0$, mientras que si $y \neq 0$ hay que demostrar que $x(p_k - q_k\alpha)$ e $y(p_{k+1} - q_{k+1}\alpha)$ tienen el mismo signo. Y esto es así ya que, por una parte, hemos visto que x e y tienen signos opuestos cuando $y \neq 0$; y, por otra parte, como α está siempre en medio de dos convergentes consecutivos, los signos de $\frac{p_k}{q_k} - \alpha$ y $\frac{p_{k+1}}{q_{k+1}} - \alpha$ también son opuestos, es decir, $p_k - q_k\alpha$ y $p_{k+1} - q_{k+1}\alpha$ tienen signos opuestos. Por tanto, $x(p_k - q_k\alpha)$ e $y(p_{k+1} - q_{k+1}\alpha)$ tienen el mismo signo, como queríamos. □

Como primer corolario, podemos ver que el convergente k-ésimo es la mejor aproximación de un número irracional mediante un número racional de denominador como mucho q_k:

Corolario 7.12. *Sea α un número irracional y sea $\frac{p_k}{q_k}$ el convergente k-ésimo de su fracción continua. Entonces, si $q \leq q_k$, se tiene $|\frac{p_k}{q_k} - \alpha| \leq |\frac{p}{q} - \alpha|$ para cualquier entero p.*

Demostración: Como $q_k < q_{k+1}$, se tiene, por el Lema 7.11, $|p_k - q_k\alpha| \leq |p - q\alpha|$ y por tanto

$$|\frac{p_k}{q_k} - \alpha| = \frac{|p_k - q_k\alpha|}{q_k} \leq \frac{|p - q\alpha|}{q_k} \leq \frac{|p - q\alpha|}{q} = |\frac{p}{q} - \alpha|.$$

□

Teorema 7.13. *Sea α un número irracional y sea $\frac{p}{q}$ un número racional tal que $q > 0$. Si $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, entonces $\frac{p}{q}$ es un convergente de α.*

Demostración: Como q_k es una sucesión creciente de números enteros, existirá k tal que $q_k \leq q < q_{k+1}$. Veamos entonces que $\frac{p}{q} = \frac{p_k}{q_k}$. Si no fuera así, entonces $pq_k - qp_k \neq 0$, luego $|pq_k - qp_k| \geq 1$. Tendremos entonces, por una parte:

$$\left|\frac{p}{q} - \frac{p_k}{q_k}\right| = \frac{|pq_k - qp_k|}{qq_k} \geq \frac{1}{qq_k}$$

y por otra parte, usando el Lema 7.11:

$$\left|\frac{p}{q} - \frac{p_k}{q_k}\right| \leq \left|\frac{p}{q} - \alpha\right| + \left|\alpha - \frac{p_k}{q_k}\right| = \left|\frac{p}{q} - \alpha\right| + \frac{|p_k - q_k\alpha|}{q_k} \leq \left|\frac{p}{q} - \alpha\right| + \frac{|p - q\alpha|}{q_k} =$$

$$= \left|\frac{p}{q} - \alpha\right| + \frac{q}{q_k}\left|\frac{p}{q} - \alpha\right| < \frac{1}{2q^2} + \frac{q}{q_k}\frac{1}{2q^2} = \frac{1}{2q^2} + \frac{1}{2qq_k}.$$

Poniendo juntas las dos desigualdades se obtiene

$$\frac{1}{qq_k} < \frac{1}{2q^2} + \frac{1}{2qq_k},$$

lo que implica $\frac{1}{2qq_k} < \frac{1}{2q^2}$, que a su vez implica $q < q_k$, lo que es una contradicción con la elección de k. □

Corolario 7.14. *Si p, q es una solución positiva de $x^2 - dy^2 = 1$, entonces $\frac{p}{q}$ es un convergente de $\sqrt{d}$.*

Demostración: Por la Observación 7.10, $|\frac{p}{q} - \sqrt{d}| < \frac{1}{2q^2}$, lo que implica, por el Teorema 7.13, que $\frac{p}{q}$ es un convergente de $\sqrt{d}$. □

Necesitamos ver ahora qué convergentes de $\alpha = \sqrt{d}$ son soluciones de la ecuación de Pell. Por la construcción por recurrencia del Ejemplo 7.2, está claro que cada α_k se puede escribir en función de $\sqrt{d}$. El siguiente resultado nos dará una fórmula precisa, en que lo fundamental es que el coeficiente de $\sqrt{d}$ en el numerador es 1:

Lema 7.15. *Sea $\alpha = \sqrt{d}$ y, para cada $k \geq 0$, sea α_k definido como en el Ejemplo 7.2. Entonces, definiendo por recurrencia $s_0 = 0, t_0 = 1$,*

$$s_{k+1} = a_k t_k - s_k$$

$$t_{k+1} = \frac{d - (a_k t_k - s_k)^2}{t_k} = \frac{d - s_{k+1}^2}{t_k}$$

se puede escribir $\alpha_k = \frac{s_k+\sqrt{d}}{t_k}$, *y además* s_k *y* t_k *son enteros y* $t_k \neq 0$.

Demostración: Lo demostramos por inducción sobre k, siendo claro el caso $k = 0$. Si ahora suponemos $\alpha_k = \frac{s_k+\sqrt{d}}{t_k}$ con s_k y t_k enteros y $t_k \neq 0$, entonces tenemos

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} = \frac{1}{\frac{s_k+\sqrt{d}}{t_k} - a_k} =$$

$$= \frac{t_k}{s_k + \sqrt{d} - a_k t_k} = \frac{t_k(\sqrt{d} - s_k + a_k t_k)}{(\sqrt{d} + s_k - a_k t_k)(\sqrt{d} - s_k + a_k t_k)} =$$

$$= \frac{t_k(a_k t_k - s_k + \sqrt{d})}{d - (a_k t_k - s_k)^2} = \frac{a_k t_k - s_k + \sqrt{d}}{\frac{d-(a_k t_k - s_k)^2}{t_k}} = \frac{s_{k+1} + \sqrt{d}}{t_{k+1}}.$$

Es claro que s_{k+1} es entero por serlo a_k, s_k, t_k. Por otra parte, si escribimos

$$t_{k+1} = \frac{d - s_{k+1}^2}{t_k} = \frac{d - (a_k t_k - s_k)^2}{t_k} = \frac{d - s_k^2}{t_k} - a_k^2 t_k + 2a_k s_k = t_{k-1} - a_k^2 t_k + 2a_k s_k$$

se obtiene que t_{k+1} es entero (en realidad, como estamos usando que t_{k-1} es entero, habría que demostrar también el caso $k = 1$ de la inducción, pero al ser $t_0 = 1$ es evidente que t_1 es entero). □

Proposición 7.16. *Con las notaciones del Lema 7.15, se tiene:*

(i) Si $\frac{p_k}{q_k}$ *es el convergente* k*-ésimo de* $\sqrt{d}$*, entonces* $p_k^2 - dq_k^2 = (-1)^{k+1} t_{k+1}$.

(ii) $t_k > 0$ *para todo* $k \geq 0$.

(iii) Existen enteros t, s *tales que* $t_k = t$ *y* $s_k = s$ *para infinitos valores de* k.

Demostración: Escribiendo $\sqrt{d} = [a_0; a_1, \ldots, a_k, \alpha_{k+1}]$, sabemos que coincide con su convergente $(k+1)$-ésimo, y por el Teorema 7.3 tendremos

$$\sqrt{d} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} = \frac{\frac{s_{k+1}+\sqrt{d}}{t_{k+1}} p_k + p_{k-1}}{\frac{s_{k+1}+\sqrt{d}}{t_{k+1}} q_k + q_{k-1}} = \frac{s_{k+1} p_k + t_{k+1} p_{k-1} + p_k \sqrt{d}}{s_{k+1} q_k + t_{k+1} q_{k-1} + q_k \sqrt{d}}$$

Por tanto

$$(s_{k+1}p_k + t_{k+1}p_{k-1}) + p_k\sqrt{d} = (s_{k+1}q_k + t_{k+1}q_{k-1} + q_k\sqrt{d})\sqrt{d} = dq_k + (s_{k+1}q_k + t_{k+1}q_{k-1})\sqrt{d}$$

lo que implica

$$\begin{cases} p_k = s_{k+1}q_k + t_{k+1}q_{k-1} \\ dq_k = s_{k+1}p_k + t_{k+1}p_{k-1} \end{cases}$$

Usando estas igualdades junto con el Teorema 7.3(ii) tendremos

$$p_k^2 - dq_k^2 = p_k(s_{k+1}q_k + t_{k+1}q_{k-1}) - q_k(s_{k+1}p_k + t_{k+1}p_{k-1}) =$$

$$= t_{k+1}(p_kq_{k-1} - p_{k-1}q_k) = (-1)^{k-1}t_{k+1}$$

lo que prueba (i).

Demostremos (ii) por inducción sobre k. Es evidente para $k = 0$, ya que, por definición, $t_0 = 1$. Supongamos entonces que sabemos $t_k > 0$ y demostremos $t_{k+1} > 0$. Por (i), tendremos

$$\frac{t_{k+1}}{t_k} = -\frac{p_{k+1}^2 - dq_{k+1}^2}{p_k^2 - dq_k^2}.$$

El signo del numerador es igual al signo de

$$\frac{p_{k+1}^2 - dq_{k+1}^2}{q_{k+1}^2} = C_{k+1}^2 - d$$

que es el signo de $C_{k+1} - \sqrt{d}$. Análogamente, el signo del denominador es el signo $C_k - \sqrt{d}$. Como por el Teorema 7.6 los signos de $C_{k+1} - \sqrt{d}$ y $C_k - \sqrt{d}$ son distintos, se sigue que $\frac{t_{k+1}}{t_k}$ tiene signo positivo, y como t_k es positivo entonces también t_{k+1} es positivo. Esto demuestra (ii).

Para demostrar (iii), basta recordar la igualdad $t_kt_{k+1} + s_k^2 = d$ y, al ser $t_k, t_{k+1} > 0$ por (ii), se tendrá $1 \leq t_k \leq d$ y $|s_k| < \sqrt{d}$. Por tanto, hay una cantidad finita de posibles valores para los pares (t_k, s_k), por lo que necesariamente alguno se debe repetir infinitas veces. □

Observación 7.17. Nótese que la parte (i) de la Proposición 7.16 indica que la ecuación de Pell $x^2 - dy^2 = 1$ tiene solución (ya sabemos por el Teorema 7.13 que necesariamente debe ser un convergente $\frac{p_k}{q_k}$) si y sólo si existe algún $k \in \mathbb{Z}$ para el que $t_{k+1} = 1$ (recuérdese que $t_{k+1} > 0$ por la parte (ii)). Esto es equivalente a decir $\alpha_{k+1} = s_{k+1} + \sqrt{d}$, es decir, $a_{k+1} = [\alpha_{k+1}] = s_{k+1} + [\sqrt{d}]$ y $\alpha_{k+2} = \frac{1}{\alpha_{k+1} - a_{k+1}} = \frac{1}{\sqrt{d} - [\sqrt{d}]} = \alpha_1$. Por tanto, los datos de la fracción continua se deben repetir después de $k + 1$ pasos, por lo que debe ser $\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{k+1}}]$.

De momento, la parte (iii) de la Proposición 7.16 garantiza sólo que existen k, l tales que $t_{k+l} = t_k$ y $s_{k+l} = s_k$, y por tanto $\alpha_{k+l} = \alpha_k$. De aquí se deduce que $a_{k'+l} = a_{k'}$ para todo $k' \geq k$, y lo que faltaría ver es que se puede tomar $k = 1$.

Lema 7.18. *Para cada $k \geq 1$, definimos β_k mediante la recurrencia $\beta_1 = a_0 + \sqrt{d}$ y $\beta_{k+1} = a_k + \frac{1}{\beta_k}$. Entonces:*

(i) $\beta_k > 1$ *(y por tanto* $[\beta_{k+1}] = a_k$*).*

(ii) $\beta_k = \frac{t_k}{\sqrt{d}-s_k} = \frac{s_k+\sqrt{d}}{t_{k-1}}$.

Demostración: Para demostrar (i), usamos inducción sobre k, siendo evidente el caso $k = 1$. Si suponemos ahora $\beta_k > 1$, entonces $\frac{1}{\beta_k} > 0$, y como $a_k \geq 1$, de la fórmula de recurrencia $\beta_{k+1} = a_k + \frac{1}{\beta_k}$ se sigue $\beta_{k+1} > 1$.

Para demostrar (ii), observamos primero que, por el Lema 7.15, tenemos:

$$\frac{t_k}{\sqrt{d}-s_k} = \frac{t_k(\sqrt{d}+s_k)}{(\sqrt{d}-s_k)(\sqrt{d}+s_k)} = \frac{t_k(s_k+\sqrt{d})}{d-s_k^2} = \frac{t_k(s_k+\sqrt{d})}{t_k t_{k-1}} = \frac{s_k+\sqrt{d}}{t_{k-1}}$$

por lo que basta ver que β_k coincide con uno cualquiera de los dos valores. Lo demostramos por inducción sobre. Si $k = 1$, recordando del Lema 7.15 las igualdades $s_0 = 0$, $t_0 = 1$ y $s_1 = a_0 t_0 - s_0 = a_0$, tenemos inmediatamente $\beta_1 = a_0 + \sqrt{d} = \frac{s_1+\sqrt{d}}{t_0}$. Supongamos ahora demostrado $\beta_k = \frac{t_k}{\sqrt{d}-s_k}$ y demostremos la fórmula para $k+1$. Para ello, aplicamos de nuevo el Lema 7.15 y tendremos:

$$\beta_{k+1} = a_k + \frac{1}{\beta_k} = a_k + \frac{\sqrt{d}-s_k}{t_k} = \frac{(a_k t_k - s_k)+\sqrt{d}}{t_k} = \frac{s_{k+1}+\sqrt{d}}{t_k}.$$

□

Teorema 7.19. *Si un entero positivo* d *no es un cuadrado perfecto, entonces su fracción continua tiene la forma* $\sqrt{d} = [a_0; \overline{a_1, a_2, a_3 \ldots a_3, a_2, a_1, 2a_0}]$.

Demostración: Como ya vimos en la Observación 7.17, existirán k, l tales que $t_{k+l} = t_k$ y $s_{k+l} = s_k$. Veamos en primer lugar que podemos tomar $k = 1$. En efecto, si $k > 1$, por la parte (ii) del Lema 7.18 tendremos $\beta_{k+l} = \beta_k$, mientras que la parte (i) implica entonces $a_{k+l-1} = [\beta_{k+l}] = [\beta_k] = a_{k-1}$. Como también tenemos

$$\frac{1}{\alpha_{k+l-1} - a_{k+l-1}} = \alpha_{k+l} = \alpha_k = \frac{1}{\alpha_{k-1} - a_{k-1}}$$

se concluye $\alpha_{k+l-1} = \alpha_{k-1}$, es decir, $t_{k+l-1} = t_{k-1}$ y $s_{k+l-1} = s_{k-1}$. Reiterando el proceso, llegaremos a $t_{l+1} = t_1$ y $s_{l+1} = s_1$. Esto quiere decir que $\alpha_{l+1} = \alpha_1$, lo que implica que tendremos

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots a_l}].$$

Por otra parte, podemos escribir:

$$\beta_1 = \beta_{l+1} = a_l + \frac{1}{\beta_l} = a_l + \frac{1}{a_{l-1} + \frac{1}{\beta_{l-1}}} = \ldots = a_l + \cfrac{1}{a_{l-1} + \cfrac{1}{a_{l-2} + \cfrac{1}{\ddots \cfrac{1}{a_2 + \cfrac{1}{a_1 + \frac{1}{\beta_1}}}}}}$$

de donde se deduce $\beta_1 = [\overline{a_l; a_{l-1}, a_{l-2} \ldots, a_1}]$, o equivalentemente

$$\beta_1 = [a_l; \overline{a_{l-1}, a_{l-2} \ldots, a_1, a_l}].$$

Por otra parte tenemos también

$$\beta_1 = a_0 + \sqrt{d} = a_0 + [a_0; \overline{a_1, a_2, \ldots a_l}] = [2a_0; \overline{a_1, a_2, \ldots a_l}].$$

Comparando ambas expresiones se obtiene el resultado. □

En realidad, no nos va a interesar el aspecto simétrico que tiene el periodo, sino simplemente saber que empieza en a_1 y qué longitud tiene.

Definición. Llamaremos *longitud del periodo de* $\sqrt{d}$ al mínimo entero positivo r para el que podemos escribir $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_r}]$.

Teorema 7.20. *Si el periodo de* $\sqrt{d}$ *tiene longitud* r*, entonces* $t_k = 1$ *si y sólo si* $r|k$.

Demostración: Como $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_r}]$, se sigue $\alpha_{ir+1} = \alpha_1$ para todo i, es decir,

$$\frac{1}{\alpha_{ir} - a_{ir}} = \frac{1}{\sqrt{d} - a_0}.$$

De aquí sigue, junto con el Lema 7.15,

$$\sqrt{d} - a_0 = \alpha_{ir} - a_{ir} = \frac{s_{ir} + \sqrt{d}}{t_{ir}} - a_{ir}$$

luego quitando denominadores queda

$$(t_{ir} - 1)\sqrt{d} = s_{ir} - a_{ir}t_{ir} + a_0 t_{ir},$$

de donde deducimos $t_{ir} = 1$ para todo i, es decir, que $t_k = 1$ si $r|k$.

Supongamos ahora $t_k = 1$. Por tanto, por el Lema 7.15 se tendrá $\alpha_k = s_k + \sqrt{d}$, y tomando parte entera se sigue

$$a_k = [\alpha_k] = s_k + [\sqrt{d}] = s_k + a_0.$$

Por tanto,

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} = \frac{1}{(s_k + \sqrt{d}) - (s_k + a_0)} = \frac{1}{\sqrt{d} - a_0} = \alpha_1$$

y por tanto el bloque $a_1, \ldots, a_k$ se repite periódicamente en la fracción continua de $\sqrt{d}$, es decir, $r|k$. □

El resultado final es entonces el siguiente:

Teorema 7.21. *Si el periodo de $\sqrt{d}$ tiene longitud r, entonces las soluciones positivas de la ecuación de Pell $x^2 - dy^2 = 1$ son:*

(i) Si r es par, $x = p_{ir-1}$, $y = q_{ir-1}$.

(ii) Si r es impar, $x = p_{2ir-1}$, $y = q_{2ir-1}$.

Demostración: Por el Corolario 7.14, las posibles soluciones de la ecuación de Pell son de la forma $x = p_k$, $y = q_k$ donde $\frac{p_k}{q_k}$ es un convergente de $\sqrt{d}$. Por la Proposición 7.16, $x^2 - dy^2 = (-1)^{k+1}t_{k+1}$, por lo que debe ser $(-1)^{k+1}t_{k+1} = 1$. Como además t_{k+1} es positivo, $x = p_k$, $y = q_k$ es una solución de la ecuación si y sólo si k impar y $t_{k+1} = 1$. Por el Teorema 7.20, esto es equivalente a que k sea impar y $r|k+1$. Distinguimos ahora dos casos:

–Si r es par, entonces la condición $r|k+1$ ya implica que k es impar, luego $x = p_k$, $y = q_k$ es una solución de la ecuación si y sólo si se puede escribir $k = ir - 1$.

–Si r es impar, la condición $r|k+1$ equivale a que se pueda escribir $k = i'r - 1$, y que k sea impar equivale ahora a que i' es par, luego se puede escribir $k = 2ir - 1$. □