VII Festival Internacional de Matemática

15, 16, 17 de abril de 2010

San Carlos

Criterios de divisibilidad

Prof. Manuel Murillo
ITCR-UNED

0.1 Definiciones básicas

Se dice que un número entero n es **par** si $\exists k$, $k \in \mathbb{Z}$, tal que $n = 2k$. Se llama número **impar** si $\exists k$, $k \in \mathbb{Z}$, tal que $n = 2k + 1$.

Ejemplo 1. *Como* $12 = 2 \cdot 6$*, es claro que* 12 *es par y como* $17 = 2 \cdot 8 + 1$*, se tiene que* 17 *es impar.* ■

Ejemplo 2. *Aunque* $7^{100} + 3$ *es un número de muchos dígitos en su forma expandida, se puede concluir que es par, pues* 7^{100} *es divisible solamente por las potencias de* 7*, que no son pares, por lo que* 7^{100} *es impar, además,* 3 *es impar, y sabemos que la suma de dos números impares es par.* ■

Se dice que un número natural n, $n \geq 2$, es un número **primo** si los únicos divisores positivos de n son 1 y n. Si no es primo, se llama número **compuesto**.

Ejemplo 3. *Los únicos divisores positivos de* 17 *son el* 1 *y el* 17*, por lo que* 17 *es primo. Como* 2 *divide a* 24*, es claro que* 24 *es compuesto* ■

Para a y b enteros, decimos que **a divide a b** si existe $k \in \mathbb{Z}$ tal que $b = ak$, en este caso escribimos $\boldsymbol{a|b}$, además, esto dice que b es divisible por a o que a es un **factor** de b. Si a no divide a b escribimos $\boldsymbol{a \nmid b}$.

Ejemplo 4. *Es claro que* $7|42$ *pues con* $k = 6$ *se tiene* $42 = 7 \cdot 6$*. También es claro que* $5 \nmid 18$ *pues no existe* k *entero de manera que se cumpla* $18 = 5 \cdot k$*.* ■

Teorema 1. *Si* a*,* b*,* c *son enteros arbitrarios, entonces se cumple:*

1. $a|a$*,* $1|a$ *y* $a|0$
2. *Si* $a|b$ *y* $b|a$*, entonces* $|a| = |b|$
3. *Si* $a|b$ *y* $b|c$*, entonces* $a|c$
4. *Si* $a|b$ *y* $a|c$*, entonces* $a|(mb + nc)$ *para todo* $m, n \in \mathbb{Z}$
5. *Si* $a|b$*, entonces* $(ac)|(bc)$ *para todo* $c \in \mathbb{Z}$

6. *Si* $0|a$*, entonces* $a = 0$
7. *Si* $a|b$*, entonces* $|a| \leq |b|$
8. *Si* $(ac)|(bc)$ *con* $c \neq 0$*, entonces* $a|b$

Ejemplo 5. *Los únicos factores primos de* 75 *son el* 3 *y el* 5*, y por lo tanto, es claro que* $75 = 3 \cdot 5^2$. ■

Ejemplo 6. *Determine todos los divisores positivos de* 75*.*

Solución. Como $75 = 3 \cdot 5^2$, los divisores de él serán todos aquellos números que contengan algún factor de 75, así, los seis divisores de 75 son 1, 3, 5, 15, 25, 75. ■

Ejemplo 7. *Determine todos los divisores positivos de* 33075*.*

Solución. Como $33075 = 3^3 \cdot 5^2 \cdot 7^2$, los divisores de él son: 1, 3, 9, 27, 7, 21, 63, 189, 49, 147, 343, 441, 5, 15, 45, 135, 35, 105, 315, 945, 245, 735, 6615, 25, 75, 225, 675, 2025, 175, 525, 1575, 4725, 1225, 3675, 11025, 33075. ■

Teorema 2. *Si* n *es un entero compuesto, entonces* n *tiene un factor primo que no excede a* $\sqrt{n}$*.*

Demostración. Como n es compuesto, existen a, b, mayores que 1 y menores que n, de manera que $n = ab$, supongamos sin perder generalidad que $a \leq b$. Debemos probar que $a \leq \sqrt{n}$, supongamos que esto no ocurre. En este caso se tiene que $b \geq a > \sqrt{n}$, por lo tanto $ab > \sqrt{n}\sqrt{n} = n$, que contradice nuestro supuesto, así, se ha probado que el factor a debe ser menor o igual que $\sqrt{n}$. Como $a > 1$, por el teorema fundamental de la aritmética, debe contener un factor primo p que será también factor de n y cumple que $p \leq \sqrt{n}$. □

El teorema anterior garantiza que si un número es compuesto, necesariamente tendrá un factor primo que será menor que $\sqrt{n}$, es decir, para comprobar que un número es primo basta verificar que p no es divisible por todos los primos menores que $\sqrt{n}$.

Ejemplo 8. *Determine si* 103 *es primo.*

Solución. Los números primos menores que $\sqrt{103}$ son 2, 3, 5, 7 y al efectuar la división de 103 por cada uno de ellos se obtiene un residuo no nulo, por lo que 103 es primo. ■

Teorema 3. *Sean a y b enteros no nulos, entonces existen s y t enteros tales que* $\mathrm{mcd}(a, b) = as + bt$.

Demostración. Ver [8]. □

Corolario 1. *Si a y b son enteros, primos entre sí, entonces existen s y t enteros tales que* $1 = as + bt$.

En realidad el recíproco de este corolario también es verdadero, pues básicamente, el $\mathrm{mcd}(a, b)$ es el menor entero positivo que se puede obtener de las posibles combinaciones lineales de la forma $as + bt$ con s y t enteros. Con lo cual se puede escribir el siguiente teorema.

Teorema 4. *Los enteros a y b, no ambos nulos, son coprimos si y solo si existen s y t enteros tales que* $1 = as + bt$.

El teorema siguiente, conocido como el lema de Euclides, garantiza que si un número divide al producto de dos números y es coprimo con uno de ellos, entonces necesariamente debe dividir al otro número.

Teorema 5. (Lema de Euclides). *Sean a, b, c números enteros, si $a|bc$ y* $\mathrm{mcd}(a, b) = 1$, *entonces* $a|c$.

Demostración. Como $a|bc$, existe k entero tal que $ak = bc$, además, como $\mathrm{mcd}(a, b) = 1$, aplicando el teorema 4, existen s y t enteros tales que $1 = as + bt$, al multiplicar por c, se obtiene

$$c = acs + bct = acs + akt = a(cs + kt)$$

con lo cual, se concluye que $a|c$. □

Corolario 2. *Si p es primo y $p|ab$, entonces $p|a$ ó $p|b$.*

Demostración. Si $p \nmid a$ entonces $\mathrm{mcd}(p, a) = 1$ y por el teorema anterior se tiene que $p|b$. □

0.2 Criterios de divisibilidad

Una *regla* o criterio de divisibilidad es un algoritmo o procedimiento por medio del cual, es posible determinar si un entero es divisible por otro de una manera rápida y eficiente, es decir, las reglas o criterios nos ayudan a decidir sin necesidad de efectuar la división e incluso sin necesidad de calculadora. Como ejemplo inicial, sabemos que un número es divisible por 2 si y solo si el dígito de las unidades es un número par, así, con solo observar que $n = 72359038$ termina en 8 y 8 es par, se concluye que n es divisible por 2.

> Sea m un entero mayor que 1, llamamos los **residuos potenciales** de t módulo m a los residuos que dejan las potencias sucesivas de t al dividirlas por m.

Por supuesto que nos interesará, principalmente, los residuos potenciales cuando $t = 10$, ya que usualmente utilizamos la notación en base 10 de los números.

Ejemplo 9. *Los residuos potenciales de* 10 *módulo* 2*, son*

$$1,\ 0,\ 0,\ 0, \ldots$$

ya que cualquier potencia de 10 *es divisible por* 2*, salvo* $10^0 = 1$ *cuyo residuo es* 1. ■

Ejemplo 10. *Los residuos potenciales de* 10 *módulo* 11*, son*

$$1,\ 10,\ 1,\ 10, \ldots$$

ya que, al dividir cualquier potencia par de 10 *por* 11 *el residuo es* 1*, mientras que cualquier potencia impar el residuo es* 10. ■

Teorema 6. *Un número es divisible por* 11 *si y solo si la diferencia entre la suma de los dígitos de lugar par y la suma de sus dígitos de lugar impar es divisible por* 11.

Demostración. Observe que un número n, con $d+1$ dígitos, se puede expresar en base 10 como

$$n = a_d 10^d + a_{d-1} 10^{d-1} + \cdots + a_1 10 + a_0$$

Supongamos ahora, sin perder generalidad, que d es impar, así, $d = 2k+1$. Si ahora se divide n por 11, utilizando el resultado del ejemplo anterior, obtenemos como residuo r la expresión

$$\begin{aligned} r &= a_{2k+1} 10 + a_{2k} + \cdots + a_2 + a_1 10 + a_0 \\ &= (a_{2k} + \cdots + a_2 + a_0) + 10(a_{2k+1} + \cdots + a_1) \end{aligned}$$

claro que como $10 = 11 - 1$, el residuo se puede reescribir como

$$11(a_{2k+1} + \cdots + a_1) + [(a_{2k} + \cdots + a_2 + a_0) - (a_{2k+1} + \cdots + a_1)]$$

y n será divisible por 11 si la expresión

$$(a_{2k} + \cdots + a_2 + a_0) - (a_{2k+1} + \cdots + a_1)$$

es un múltiplo de 11, como se quería demostrar. □

Ejemplo 11. *Utilice la regla de divisibilidad por* 11 *para verificar que* 11 *divide a* 98 172 614 232.

Solución. Al sumar los dígitos que se encuentran en posiciones pares, contadas de derecha a izquierda, obtenemos $2 + 2 + 1 + 2 + 1 + 9 = 17$ y la suma de los dígitos en posiciones impares obtenemos $3 + 4 + 6 + 7 + 8 = 28$, al efectuar la resta de ambos números obtenemos $28 - 17 = 11$, que como es un múltiplo de 11 prueba que el número dado es divisible por 11 ■

A partir de los dos ejemplos anteriores podemos deducir los siguientes teoremas, con un razonamiento análogo al de la prueba del teorema 6.

Ejemplo 12. *Los residuos potenciales de* 10 *módulo* 3*, son*

$$1,\ 1,\ 1,\ 1, \ldots$$

ya que, al dividir cualquier potencia de 10 *por* 3 *el residuo es* 1. ■

Teorema 7. *Un número es divisible por* 3 *si y solo si la suma de todos los dígitos es divisible por* 3.

Ejemplo 13. *Los residuos potenciales de* 10 *módulo* 5*, son*

$$1,\ 0,\ 0,\ 0, \ldots$$

ya que, al dividir cualquier potencia de 10 *por* 5 *el residuo es* 0*, salvo* $10^0 = 1$ *cuyo residuo es* 1. ■

Teorema 8. *Un número es divisible por* 5 *si y solo si el dígito de las unidades es divisible por* 5.

Ejemplo 14. *Utilice las reglas para verificar que* 16 261 190 995 *es divisible por* 33.
Solución. Al sumar los dígitos que se encuentran en posiciones pares, contadas de derecha a izquierda, obtenemos

$$5 + 9 + 9 + 6 + 6 = 35$$

y la suma de los dígitos en posiciones impares obtenemos

$$9 + 0 + 1 + 2 + 1 = 13$$

al efectuar la resta de ambos números obtenemos $35-13 = 22$, que como es un múltiplo de 11 prueba que el número dado es divisible por 11, además, al sumar todos los dígitos obtenemos

$$1 + 6 + 2 + 6 + 1 + 9 + 0 + 9 + 9 + 5 = 48$$

y $4 + 8 = 12$ que al ser múltiplo de 3 prueba que el número dado es divisible por 3. Como 3 y 11 son primos relativos entonces el número dado es divisible por el producto de ellos $3 \cdot 11 = 33$. ■

Teorema 9. *Sea n un número entero, si definimos $S = S_1 + 3S_2 + 2S_3$ donde S_1 es la suma de los dígitos (alternando el signo) que están en las posiciones* 0, 3, 6,. . . ; *donde S_2 es la suma de los dígitos (alternando el signo) que están en las posiciones* 1, 4, 7,. . . ; *y S_3 es la suma de los dígitos (alternando el signo) que están en las posiciones* 2, 5, 8,. . . . *Entonces, n es divisible por* 7 *si y solo si S es divisible por* 7.
Demostración. Los residuos potenciales de 10 módulo 7 son:

$$1,\ 3,\ 2,\ 6,\ 4,\ 5,\ 1,\ 3,\ 2,\ 6, \ldots$$

Por ser la divisibilidad por 7, podemos reescribir $6 = 7 - 1$, $4 = 7 - 3$, $5 = 7 - 2$, así, los residuos se reescriben

$$1,\ 3,\ 2,\ -1,\ -3,\ -2,\ 1,\ 3,\ 2,\ -1, \ldots$$

de esta manera, el número n, se puede expresar en base 10 como:

$$n = a_d 10^d + a_{d-1}10^{d-1} + \cdots + a_1 10 + a_0$$

Si ahora se divide n por 7, utilizando los residuos dados, obtenemos como residuo r la expresión:

$$\begin{aligned} r &= a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 \cdots \\ &= (a_0 - a_3 + a_6 - \cdots) + 3(a_1 - a_4 + a_7 - \cdots) + 2(a_2 - a_5 + \cdots) \\ &= S_1 + 3S_2 + 2S_3 \end{aligned}$$

Con lo cual, es claro que n será divisible por 7 si y solo si $S_1 + 3S_2 + 2S_3$ es divisible por 7, como se quería demostrar. □

De la misma demostración del teorema anterior, es evidente que si n es un entero y definimos $S = S_1 + 3S_2 + 2S_3 + 6S_4 + 4S_5 + 5S_6$ donde S_1 es la suma de los dígitos que están en las posiciones 0, 6, 12, ...; con S_2 la suma de los que están en las posiciones 1, 7, 13, ...; con S_3 la suma de los que están en las posiciones 2, 8, 14, ...; análogamente para S_4 en las posiciones 3, 9, ...; S_5, en las posiciones 4, 10, ... y S_6 en las 5, 11, ... Entonces, n es divisible por 7 si y solo si S es divisible por 7. Sin embargo esta regla de divisibilidad por 7 es menos eficiente que la dada en el teorema anterior.

Teorema 10. *Un número es divisible por 7 si y solo si al restar el doble de las unidades al número que se obtiene de suprimir el dígito de las unidades, el resultado es divisible por 7.*

Demostración. Sea $n = 10a + u$ con u el dígito de las unidades donde $0 \leq u < 10$. Es claro que a es el número que se obtiene de suprimir a n el dígito de las unidades.

"$\Rightarrow$" Suponiendo que $7|n$ y como se sabe que $7|7a$, utilizando la propiedad de la linealidad, dada en el teorema 1, parte 4, página 2, se concluye que:

$$7|(-2(10a + u) + 3 \cdot 7a)$$

es decir, $7|(a - 2u)$, como se quería demostrar.

"$\Leftarrow$" Suponiendo ahora que $7|(a - 2u)$, y como $a - 2u = -2(10a + u) + 3 \cdot 7a$, se tiene que $7|(-2(10a + u) + 3 \cdot 7a)$, como además es claro que $7|(3 \cdot 7a)$, se debe tener que $7|(-2(10a + u))$. Finalmente, utilizando el lema de Euclides, tenemos que $7|(10a + u)$ como se debía demostrar.

Como se quería demostrar. □

Corolario 3. *Un número es divisible por 7 si y solo si al sumar el quíntuplo de las unidades al número que se obtiene de suprimir el dígito de las unidades, el resultado es divisible por 7.*

Demostración. $7|(a - 2u) \Leftrightarrow 7|(a - 2u + 7u) \Leftrightarrow 7|(a + 5u)$. □

Este nuevo criterio es menos eficiente que el dado en el teorema pues al restar el número resultante pierde dígitos. Por otro lado, si el número n es muy grande, es posible repetir la regla dada en el teorema anterior las veces que sea necesario. Veamos el siguiente ejemplo, que aunque se puede realizar de rápidamente al obtener 0 como residuo al efectuar la división, lo haremos utilizando los criterios de divisibilidad por 7 que hemos visto y demostrado en los teoremas 9 y 10.

Ejemplo 15. *Determine si* 204673 *es divisible por* 7*.*

Solución. Procedemos a realizarlo de dos formas:

- Hacemos $S = S_1 + 3S_2 + 2S_3 = (3 - 4) + 3(7 - 0) + 2(6 - 2) = 28$, y como claramente $7|28$, por el teorema 9, se concluye que $7|204673$.

- El dígito de las unidades es 3, así, formamos el nuevo número $20467 - 6 = 20461$, ahora repetimos el criterioy como el dígito de las unidades es 1, formamos el nuevo número $2046 - 2 = 2044$, ahora el dígito de las unidades es 4, formamos de nuevo el número $204 - 8 = 196$, ahora el dígito de las unidades es 6, formamos de nuevo el número $19 - 12 = 7$ que claramente es divisible por 7, por el teorema 10 se concluye que $7|204673$.

■

Ejercicios (sección 0.2)

1. Utilice las reglas de divisibilidad para verificar que:

   (a) 7 divide a 2208178336.

   (b) 33 divide a 175128261.

   (c) 165 divide a 960833280.

2. Sea n un número entero, si definimos $S = S_1 + 10S_2 + 9S_3$ donde S_1 es la suma (alternando el signo) de los dígitos que están, iniciando a la derecha, en las posiciones 0, 3, 6,...; donde S_2 es la suma (alternando el signo) de los dígitos que están en las posiciones 1, 4, 7,...; y S_3 es suma (alternando el signo) de los dígitos que están en las posiciones 2, 5, 8,.... Demuestre que, n es divisible por 13 si y solo si S es divisible por 13. ($S = S_1 + 10S_2 + 9S_3 + 12S_4 + 3S_5 + 4S_6$)

3. Utilice la regla dada en el ejercicio anterior para verificar que

   (a) 4663802 es divisible por 13.

   (b) 333936395 es divisible por 13.

4. Demuestre la validez de la siguiente regla de divisibilidad por 13: *Borre el último dígito del número n, luego, sustraiga* 9 *veces este dígito al número resultante. Si este número es divisible por* 13 *el número original n lo será también.*

5. Utilice la regla dada en el ejercicio anterior para verificar que
   (a) 208403 es divisible por 13.
   (b) 54094369875 es divisible por 13.
6. Sabemos que un úmero es divisible por 6 si lo es por 2 y por 3. Determine otra regla de divisibilidad por 6 y utilice esta regla para verificar que 82356710982 es divisible por 6.
7. Determine una regla de divisibilidad por 37. Utilice esta regla para verificar que 2586418969134 es divisible por 37.
8. Determine una regla de divisibilidad por 19. Utilice esta regla para verificar que 380280869970 es divisible por 19.
9. Determine una regla de divisibilidad por 3 para un número dado en base 5. Utilice esta regla para decidir si $(23142013232)_5$ es o no divisible por 3.
10. Determine una regla de divisibilidad por 4 para un número dado en base 7. Utilice esta regla para decidir si $(62650503123)_7$ es o no divisible por 4.

0.3 Fracciones continuas

En esta sección haremos una breve introducción al tema de las fracciones continuas. Esta forma de expresar una fracción racional, será de utilidad para determinar las soluciones enteras de una ecuación lineal con coeficientes enteros.

Si desea profundizar en este tema, se recomienda consultar [1], [9].

En general, una **fracción continua**, se define como una expresión de la forma

$$a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cdots}}$$

$$\cdots + \cfrac{b_{n-2}}{a_{n-1} + \cfrac{b_{n-1}}{a_n}}$$

donde los a_i y b_i son números reales o complejos.

Ejemplo 16. *Calculemos la fracción racional asociada a la fracción continua*

$$\begin{aligned} 3+\cfrac{3}{-2+\cfrac{5}{3+\cfrac{2}{5}}} &= 3+\cfrac{3}{-2+\cfrac{5}{\cfrac{17}{5}}} \\ &= 3+\cfrac{3}{-2+\cfrac{25}{17}} \\ &= 3+\frac{-17}{3}=\frac{-8}{3} \end{aligned}$$

■

En el caso particular de las fracciones continuas en donde cada $b_i = 1$, y todos los a_i son números enteros y para $i \geq 2$ los a_i son positivos (a_1 puede ser negativo), la fracción se llamará **fracción continua simple** y en este caso se denotará por

$$[a_1, a_2, a_3, \ldots, a_n] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots \atop \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

Los valores a_i se conocen como los **términos** de la fracción continua. En particular se tiene que $[a_1] = a_1$. Decimos que la fracción continua es finita o infinita si la cantidad de términos es finita o infinita, respectivamente.

Como veremos, todos los números racionales tienen representación en fracción continua simple finita y algunos irracionales en forma de fracción continua simple infinita. Observe cómo, en los siguientes ejemplos, se encuentran las fracciones continuas simples asociadas con números racionales y el proceso inverso, es decir, dada la fracción continua se encuentra el racional que esta representa, tanto para racionales positivos y negativos. Luego trabajaremos con algunos irracionales cuadráticos.

Ejemplo 17. *Encuentre la fracción racional asociada a la fracción continua simple* $[1, 3, 3, 2]$.

Solución.

$$\mathbf{1}+\cfrac{1}{\mathbf{3}+\cfrac{1}{\mathbf{3}+\cfrac{1}{\mathbf{2}}}}=1+\cfrac{1}{3+\cfrac{1}{\frac{7}{2}}}=1+\frac{1}{3+\frac{2}{7}}=1+\frac{1}{\frac{23}{7}}=\frac{30}{23}$$

por lo que $[1,3,3,2]=\frac{30}{23}$. ∎

Ejemplo 18. *Encuentre la fracción continua simple asociada a* $\frac{418}{131}$.

Solución.

$$\begin{aligned}\frac{418}{131}=3+\frac{25}{131}=3+\cfrac{1}{\cfrac{131}{25}} &= 3+\cfrac{1}{5+\cfrac{6}{25}}\\ &= 3+\cfrac{1}{5+\frac{1}{\cfrac{25}{6}}}\\ &= \mathbf{3}+\cfrac{1}{\mathbf{5}+\cfrac{1}{\mathbf{4}+\cfrac{1}{\mathbf{6}}}}\end{aligned}$$

por lo que $\frac{418}{131}=[3,5,4,6]$. ∎

Ejemplo 19. *Exprese* $\frac{19}{11}$ *como una fracción continua simple.*

Solución.

$$\frac{19}{11}=\mathbf{1}+\cfrac{1}{\mathbf{1}+\cfrac{1}{\mathbf{2}+\cfrac{1}{\mathbf{1}+\cfrac{1}{\mathbf{2}}}}}$$

por lo que $\frac{19}{11}=[1,1,2,1,2]$. ∎

Ejemplo 20. *Encuentre la fracción continua simple asociada a* $-\frac{120}{47}$.

Solución.

$$-\frac{120}{47}=-3+\frac{21}{47}=-\mathbf{3}+\cfrac{1}{\mathbf{2}+\cfrac{1}{\mathbf{4}+\cfrac{1}{\mathbf{5}}}}$$

por lo que $-\frac{120}{47}=[-3,2,4,5]$. ∎

Teorema 11. *Si x es un número racional, x se puede representar como una fracción continua simple finita.*

Demostración. Sea $x = \frac{p}{q}$ con $q > 0$, por el algoritmo de la división existen a_1, r_1 tal que $\frac{p}{q} = a_1 + \frac{r_1}{q}$ con $0 < r_1 < q$, además, $a_1 + \frac{r_1}{q} = a_1 + \frac{1}{\frac{q}{r_1}}$, de nuevo, existen a_2, r_2 tales que $\frac{q}{r_1} = a_2 + \frac{r_2}{r_1}$ con $0 < r_2 < r_1$, al seguir este proceso, se obtiene una sucesión de residuos r_i tales que $r_{i+1} < r_i$, y como son positivos, por el principio de buen ordenamiento, se concluye que este proceso es finito, con lo cual se determina la fracción continua $\frac{p}{q} = [a_1, a_2, \ldots, a_n]$, cuando $r_{n-1} = 1$. $\square$

Corolario 4. *Toda fracción continua simple infinita representa a un número irracional.*

Demostración. Se sigue del teorema anterior al aplicar la contrapositiva de la implicación. $\square$

Se definen los **convergentes c_k** de la fracción continua simple $[a_1, a_2, a_3, \ldots]$, finita o infinita, como las fracciones finitas

$$\begin{aligned} c_1 &= [a_1] \\ c_2 &= [a_1, a_2] \\ \vdots & \quad \vdots \\ c_k &= [a_1, a_2, a_3, \ldots, a_k] \end{aligned}$$

Ejemplo 21. *Calcule los convergentes de la fracción continua $[2, 3, 2, 5]$.*

Solución. De acuerdo a la definición, se tiene que $c_1 = [2] = 2$, $c_2 = [2, 3] = 2 + \frac{1}{3} = \frac{7}{3}$, $c_3 = [2, 3, 2] = 2 + \frac{1}{3+\frac{1}{2}} = \frac{16}{7}$. Por último, $c_4 = [2, 3, 2, 5] = 2 + \frac{1}{3+\frac{1}{2+\frac{1}{5}}} = \frac{87}{38}$. $\blacksquare$

Ejemplo 22. *Calcule los primeros cuatro convergentes de la fracción continua infinita $\left[4, \overline{3, 2}\right]$.*

Solución. En este caso, se tiene que $c_1 = [4] = 4$, $c_2 = [4, 3] = 4 + \frac{1}{3} = \frac{13}{3}$, $c_3 = [4, 3, 2] = 4 + \frac{1}{3+\frac{1}{2}} = \frac{30}{7}$ y por último, $c_4 = [4, 3, 2, 3] = 4 + \frac{1}{3+\frac{1}{2+\frac{1}{3}}} = \frac{103}{24}$. $\blacksquare$

Teorema 12. *Si el n-ésimo convergente asociado a la fracción continua simple $[a_1, a_2, a_3, \ldots]$ es $c_n = \frac{p_n}{q_n}$, entonces $\forall n \geq 2$ se cumple que*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n \tag{0.1}$$

Demostración. Véase [8]. □

En ocasiones es útil recurrir al concepto de determinante para recordar el resultado del teorema anterior, sobre los convergentes sucesivos, de esta forma (0.1) se reescribe como:

$$\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = (-1)^n \tag{0.2}$$

Este resultado lo utilizaremos en la sección 0.4 para resolver ecuaciones diofánticas y en la sección 0.5 para encontrar algunos criterios de divisibilidad.

0.4 Ecuaciones diofánticas

Recordemos que para $n \in \mathbb{Z}$,

$$x = x_0 - bn, \qquad y = y_0 + an$$

es la forma general de todas las soluciones de la ecuación diofántica $ax + by = c$, a partir de una solución particular que denotamos por (x_0, y_0). Se puede utilizar el algoritmo de la división para encontrar esta solución particular, véase [8]. En los siguientes ejemplos utilizaremos un procedimiento que involucra a los convergentes de las fracciones continuas.

Específicamente, calculamos la fracción continua asociada a $\frac{a}{b}$, donde a y b son los coeficientes de la ecuación diofántica. Sabemos que si $\frac{a}{b} = [a_1, a_2, \ldots, a_n]$, para los convergentes $c_k = \frac{p_k}{q_k}$ se tiene que $c_n = \frac{a}{b}$, aplicando el resultado (0.1) dado en la página 13 se tiene

$$aq_{n-1} - p_{n-1}b = (-1)^n$$

por lo que simplemente basta mutltiplicar por $(-1)^n c$ para obtener una solución particular de la forma

$$a\left[q_{n-1}(-1)^n c\right] + b\left[-p_{n-1}(-1)^n c\right] = c$$

Ejemplo 23. *Utilice el método de las fracciones continuas para resolver la ecuación diofántica* $61x + 18y = 8$.

Solución. Como $\operatorname{mcd}(61, 18) = 1$, la ecuación tiene solución. Al aplicar las fracciones continuas obtenemos que

$$\frac{61}{18} = 3 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}}$$

es decir, $\frac{61}{18} = [3, 2, 1, 1, 3]$ al eliminar la fracción $\frac{1}{3}$ se obtiene en convergente $[3, 2, 1, 1]$ que equivale a

$$3 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1}}} = \frac{17}{5}$$

utilizando el resultado (0.1), página 13, se obtiene

$$61 \cdot 5 - 17 \cdot 18 = -1$$

al multiplicar la ecuación por -8 y agrupar, obtenemos la ecuación

$$61 \cdot (-40) + 18 \cdot (136) = 8$$

así, una solución particular es $x = -40$ y $y = 136$, de donde la solución general es de la forma $x = -40 - 18n$ y $y = 136 + 61n$ con $n \in \mathbb{Z}$. ■

Ejemplo 24. *Resuelva la ecuación diofántica $8x + 6y = 12$, utilizando el método de las fracciones continuas.*

Solución. La ecuación es equivalente a $4x + 3y = 6$, usando el método de las fracciones continuas, encontramos que $\frac{4}{3} = 1 + \frac{1}{3}$, es decir, $\frac{4}{3} = [1, 3]$ y al eliminar el 3, y utilizar el resultado (0.1), se obtiene la nueva identidad $4 \cdot 1 - 3 \cdot 1 = 1$ la cual al multiplicar por 6 se transforma en

$$4 \cdot 6 + 3 \cdot (-6) = 6$$

así, una solución particular es $x = 6$ y $y = -6$, de donde la solución general es de la forma $x = 6 + 3n$ y $y = -6 - 4n$ con $n \in \mathbb{Z}$. ■

Ejemplo 25. *Resuelva la ecuación diofántica $418x - 131y = 3$, utilizando el método de las fracciones continuas.*

Solución. Primero, encontramos que $\frac{418}{131} = [3, 5, 4, 6]$ y es claro que $c_4 = \frac{418}{131}$ y $c_3 = \frac{67}{21}$, del resultado (0.1), se obtiene la nueva identidad $418 \cdot 21 - 131 \cdot 67 = 1$ la cual al multiplicar por 3 se transforma en

$$418 \cdot 63 - 131 \cdot 201 = 3$$

así, una solución particular es $x = 63$ y $y = 201$, de donde la solución general es de la forma $x = 63 + 131n$ y $y = 201 + 418n$ con $n \in \mathbb{Z}$. ■

0.5 Más sobre criterios de divisibilidad

En la sección 0.2 hemos dado algunos criterios de divisibilidad a partir del desarrollo de los residuos potenciales de t módulo m, principalmente con $t = 10$ por ser la base que utilizamos con mayor frecuencia. Ahora justificamos otros criterios, utilizando las propiedades de las fracciones continuas.

Si n es un natural cualquiera, es claro que en base 10 se puede escribir como $n = 10a + u$ con u el dígito de las unidades donde $0 \leq u < 10$ y donde a es el número que se obtiene de suprimir a n el dígito de las unidades. En el criterio de la divisibilidad por 7, dado en el teorema 10 en la página 8, determinamos que $7 \mid n$ si y solo si $7 \mid (a - 2u)$. En general, trataremos de encontar un criterio de divisibilidad por m de la forma $m \mid n$ si y solo si $m \mid (a + ku)$, para números escritos en base 10.

Supongamos, para iniciar, que $m > 10$, a partir de que $m|n$ y $m|ma$, debemos aplicar la propiedad de linealidad dada en el teorema 1, parte 4, página 2, para que de

$$m|(k \cdot (10a + u) + y \cdot ma)$$

obtengamos que

$$m|((10k + ym)a + ku) \Longleftrightarrow m|(a + ku)$$

es decir, debemos encontrar k entero que satisfaga la ecuación diofántica

$$10k + my = 1 \tag{0.3}$$

Para que (0.3) tenga solución se debe cumplir que $\text{mcd}(10, m) = 1$. Si $[a_1, a_2, a_3, \ldots, a_n]$ es la fracción continua simple finita de la $\frac{m}{10}$, sabemos que los convergentes $c_k = \frac{p_k}{q_k}$, véase página 13, satisfacen la propiedad:

$$mq_{n-1} - 10p_{n-1} = (-1)^n \tag{0.4}$$

pues en este caso, $c_n = \frac{m}{10}$, el último convergente es $\frac{m}{10}$.

Luego de comparar términos en las ecuaciones (0.3) y (0.4) es claro que si n es par, $k = -p_{n-1}$ y si n es impar, $k = p_{n-1}$. Por último, en el caso de que $m < 10$ el proceso es análogo y se debe desarrollar la fracción continua de $\frac{10}{m}$.

Ejemplo 26. *Determinemos un criterio de divisibilidad por* 13.

Solución. Como $m = 13$, obtenemos que $\frac{13}{10} = [1, 3, 3]$, así $c_2 = [1, 3] = \frac{4}{3}$, por lo que $p_2 = 4$ y dado que n es impar, se obtiene que $k = 4$ y el criterio para $n = 10a + u$, simbólicamente sería

$$13|n \iff 13|(a + 4u)$$

o en palabras: "Borre el último dígito del número n, luego, sume 4 veces este dígito al número resultante. Si este número es divisible por 13 el número original n lo será también". Además, dado que $4 - 13 = -9$, se puede enunciar el criterio como

$$13|n \iff 13|(a - 9u)$$

como se hizo en la página 9. ■

Ejercicios (sección 0.5)

1. Con lo visto en esta sección, determine reglas de:

   (a) Divisibilidad por 17.

   (b) Divisibilidad por 19.

   (c) Divisibilidad por 47.

   (d) Divisibilidad por 67.

2. Determine un criterio de divisibilidad por 37 y compárelo con el dado en la solución del ejercicio 7 de la página 10.

3. Determine un criterio de divisibilidad por 7 y compárelo con el dado en la página 8.

Solución ejercicios Sección 0.2

1c. Al sumar los dígitos que se encuentran en posiciones pares, contadas de derecha a izquierda, obtenemos $9 + 0 + 3 + 2 + 0 = 14$ y la suma de los dígitos en posiciones impares obtenemos $6 + 8 + 3 + 8 = 25$, al efectuar la resta de ambos números obtenemos $14 - 25 = -11$, que como es un múltiplo de 11 prueba que el número dado es divisible por 11, además, al sumar todos los dígitos obtenemos $9 + 6 + 0 + 8 + 3 + 3 + 2 + 8 + 0 = 39$, que al ser múltiplo de 3 prueba que el número dado es divisible por 3. Por otro lado, es claro que es divisible por 5 pues el dígito de la unidades es 0. Como 3, 5 y 11 son todos primos relativos entonces el número dado es divisible por el producto de ellos $3 \cdot 5 \cdot 11 = 165$.

5. Sea $n = 208403$, hacemos $20840 - 9 \cdot 3 = 20813$, de nuevo, $2081 - 9 \cdot 3 = 2054$, de nuevo, $205 - 9 \cdot 4 = 169$ que como es claramente divisible por 13 lo será también 208403.

7. Sea n un número entero, si definimos $S = S_1 + 10S_2 + 26S_3$ donde S_1 es la suma de los dígitos que están en las posiciones 0, 3, 6,...; donde S_2 es la suma de los dígitos que están en las posiciones 1, 4, 7,...; y S_3 es la suma de los dígitos que están en las posiciones 2, 5, 8,.... Entonces, n es divisible por 37 si y solo si S es divisible por 37. Note que otro criterio, igualmente válido, es si cambiamos $S = S_1 + 10S_2 - 11S_3$. Otro criterio de divisibilidad por 37 es el siguiente: Un número es divisible por 37 si y solo si al restar once veces el dígito de las unidades al número que se obtiene de suprimir el dígito de las unidades, el resultado es divisible por 37.

Solución ejercicios Sección 0.5

1b. $19|n \iff 19|(a - 17u)$ ó $19|n \iff 19|(a + 2u)$ que es más fácil de aplicar.

1c. $47|n \iff 47|(a - 14u)$

1d. $67|n \iff 67|(a - 20u)$

2. $37|n \iff 37|(a - 11u)$.

Bibliografía

[1] Beskin, N. *Fracciones maravillosas*, Editorial Mir, Moscú, 1987.

[2] Burde, Klaus. *Numeración fraccionaria*, Revista Investigación y Ciencia, Num. 227, España, 1995.

[3] Corbalán, Fernando. *Galois: Revolución y matemáticas*, Editorial Nivola, España, 2000.

[4] Guelfond, A. *Resolución de ecuaciones en números enteros*, Editorial Mir, Moscú, 1984.

[5] Halmos, Paul. *Problems for Mathematicians, Young and Old*, The Mathematical Association of America, 1991.

[6] Jones, Burton. *Teoría de los Números*, Edit. Trillas, México, 1969.

[7] Koblitz, Neal. *A Course in Number Theory and Cryptography*, Springer Verlag, 1987.

[8] Murillo T. Manuel & González Fabio. , Editorial Tecnológica, Costa Rica, 2006.

[9] Pettofrezzo, A. & Byrkit, D. *Introducción a la Teoría de los Números*. Editorial Prentice Hall, España, 1972.

[10] Vorobiov, N. N. *Criterios de divisibilidad*, Lecciones populares de matemática, Editorial Mir, Moscú, 1984.