Métodos de Factorización de números naturales*

Geovany Sanabria Brenes

Resumen

Se abordan varios métodos de factorización prima, los cuales se justifican y clasifican. Para ello, se realiza una presentación didáctica y formal de algunos tópicos de Teoría de Números. Además se brindan los aspectos más relevantes de la vida de Euler y Fermat, junto con su aporte a la factorización prima.

Palabras claves: teoría de números, factorización prima, didáctica.

Contenidos

1 Introducción y Justificación **2**

2 Un vistazo a la historia: Fermat y Euler. **3**
2.1 Fermat: su vida y obra 3
2.2 Euler: su vida y obra. 4

3 Preliminares: Tópicos Elementales de la Teoría de Números. **5**
3.1 Definiciones y resultados básicos 5
3.2 Ejercicios. 10

4 Métodos de Factorización prima. **10**
4.1 Métodos de factorización por factores primos. 11
4.1.1 Método de ensayo y error. 11
4.1.2 Método por reglas de divisibilidad. 12
4.1.3 Desventajas de los métodos por factores primos. 14
4.2 Métodos de factorización por factores compuestos. 15
4.2.1 Método de factorización de Fermat 16
4.2.2 Método de Factorización de Euler 19

5 Algunas respuestas **24**

*Fecha de recepción del artículo: Febrero, 2005. Fecha de aceptación: Junio, 2005.

6 Los números primos menores que 200 **25**

7 Conclusión **25**

8 Bibliografía **26**

1 Introducción y Justificación

La enseñanza matemática secundaria dedica poco tiempo al estudio de los números naturales. Sobre este tema, en los programas de estudio de secundaria, se evidencia una enseñanza muy algoritmizada y sintáctica, en la cual, los estudiantes deben memorizar algorítmos que carecen de justificación teórica, como por ejemplo: algoritmos de factorización de un número y el algoritmo para calcular el máximo común divisor y el mínimo común múltiplo.
Dentro de los tópicos más importantes en el estudio de los números naturales están los métodos de factorización prima, pues son utilizados, por ejemplo, en la obtención del máximo común divisor y el mínimo común múltiplo, en operaciones con fracciones y en la factorización de polinomios. Sin embargo, en secundaria, se suele usar un método muy ineficiente, lo que provoca que se trabaje con números pequeños, y en consecuencia, la mayoría de problemas sean descontextualizados.
En el presente trabajo, se brinda una presentación a un nivel elemental y completo de los métodos de factorización, específicamente el método de Fermat y el método de Euler. En la primera parte, se incluye una breve biografía de ambos, ya que son considerados los que mayores aportes han hecho en lo que respecta al tema. En cada una se resaltan algunas de sus contribuciones al desarrollo de la teoría de números. En la segunda parte, se brinda un tratamiento sencillo y didáctico de algunos tópicos de la teoría de números. Finalmente, en la tercera parte, se logra realizar una clasificación de algunos métodos de factorización prima, de los cuales se brinda su algoritmo, entre ellos, los propuestos por Fermat y Euler.
Este material está dirigido a docentes de secundaria y se espera que encuentren en él algunas ideas para introducir ciertos tópicos de Teoría de Números.

2 Un vistazo a la historia: Fermat y Euler.

2.1 Fermat: su vida y obra

Pierre Fermat (1601-1665) es un matemático francés, nacido en Beaumont-de-Lomagne en 1601. En su juventud, con su amigo el científico y filósofo Blaise Pascal, realizó una serie de investigaciones sobre las propiedades de los números, las cuales nunca quizo publicar, incluso, llegó a escribir a Pascal:

"No quiero que aparezca mi nombre en ninguno de los trabajos considerados dignos de exposición pública"

En 1631 fue nombrado concejal en el parlamento de Toulouse, su trabajo consistía en servir de enlace entre los ciudadanos y el gobierno y el rey.
Aunque Fermat disfrutaba de la literatura y escribió muchos versos, lo que realmente amaba era las matemáticas. Este matemático contribuyó notablemente a la Teoría de la Probabilidad, al Cálculo y a la Teoría de Números.
Fermat, en Cálculo, introduce el concepto de diferencial con base en las rectas tangentes y el concepto de integral como el cálculo numérico de áreas. Se ha descubierto que Newton utilizó para el desarrollo del Cálculo, el método de trazar tangentes de Fermat, de ahí que algunos matemáticos consideran a Fermat el padre del Cálculo.

Sin embargo, la pasión de Fermat en matemáticas fue indudablemente en teoría de números. Algunas de sus contribuciones en este campo son:

a) Hallar la segunda pareja de números amigos. Dos números naturales n y m son amigos si la suma de de los divisores de n es igual a m y la suma de de los divisores de m es igual a n. Los pitagóricos descubren la primer pareja: 220 y 284. Fermat, descubre la segunda 17296 y 18416, además halla una regla general (conocida por ibn Qurra):

"Si $q = 3 \cdot 2^{p-1} - 1$, $r = 3 \cdot 2^p - 1$, $s = 9 \cdot 2^{2p-1} - 1$ son números primos, entonces $n = 2pqr$ y $m = 2ps$ son números amigos".

b) **Método de Factorización de Fermat**. Este método es encontrado en una carta aproximadamente en 1643, dirigida probablemente a Mersenne (1588-1648), un padre franciscano, filósofo y matemático, amigo de Descartes. Este método será expuesto con detalle más adelante.

c) **Teorema pequeño de Fermat**: si a es un número natural cualquiera y p un número primo que no es divisor de a, entonces p es divisor exacto de $a^{p-1} - 1$. Por ejemplo $2^{5-1} - 1 = 15$ es divisible por 5.

d) Último Teorema de Fermat: las ecuaciones del tipo: $x^n + y^n = z^n$, para el entero $n \geq 3$, no tiene solución, en el campo de los números enteros. Fermat supuestamente escribió en los márgenes de un libro que había descubierto una maravillosa demostración de este teorema, pero que no le cabía en ese espacio. Falleció sin haber hecho pública nunca la solución. El 23 de junio de 1993, Andrew Wiles, presentó una demostración de este teorema, sin embargo, Nick Katz encontró en septiembre de ese año, que el trabajo de Wiles presentaba un error que invalidaba la demostración. Tras un año de esfuerzo, Wiles, el 25 de octubre de 1994, presentó en dos manuscritos - unas 130 páginas en total - la demostración de dicho teorema.

2.2 Euler: su vida y obra.

Leonhard Euler (1707-1783), nació en Basilea- Suiza y estudió en su Universidad con el matemático suizo Jean Bernoulli, obteniendo la licenciatura a los 16 años. Además de contribuir en casi todas las ramas de la matemática tenía amplios conocimientos en otras disciplinas como la medicina, la geografía y las lenguas modernas entre otras.
En 1727, fue miembro del profesorado de la Academia de Ciencias de San Petersburgo, luego, en 1741 fue profesor de matemáticas en la Academia de Ciencias de Berlín y en 1766, regresó a San Petersburgo , donde permaneció hasta su muerte.
Las malas condiciones de trabajo y el esfuerzo realizado provocó la pérdida de la visión de un ojo, hasta quedar totalmente ciego en 1766.
Sus principales tratados fueron "Introductio in Analysis Infinitorum" (1748); "Institutiones Calculi Differentialis" (1975) e "Institutiones Calculi Integralis" (1768-1794). En "Introductio in Analysis Infinitorum"(1748). Realiza el primer tratamiento analítico completo del Ágebra, la Teoría de Ecuaciones, la Trigonometría y la Geometría Analítica. Además, introduce la notación $f(x)$ para una función de x y el símbolo $\sum$ para representar una suma. También estableció la relación $e^{\pi i} + 1 = 0$ y la generaliza dando una relación entre las funciones trigonométricas y la exponencial por medio de $e^{i\theta} = \cos\theta + isen\theta$

En ecuaciones diferenciales, propuso los métodos: reducción del orden, un factor integrante y soluciones por series de potencias. En geometría propone el siguiente teorema: "En un poliedro simple, el número de caras sumado al número de vértices es igual al número de aristas aumentado en dos".
Algunas de sus contribuciones a la Teoría de Números son:

a) La función φ de Euler. Esta se denota por $\phi(n)$, e indica el número de enteros positivos menores o iguales que n. Euler demostró que si $\prod_{i=1}^{k} p_i^{a_i}$ representa la factorización prima de n, entonces $\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

b) Teorema de Euler (Generalización del Teorema pequeño de Fermat): Si a y m son dos números naturales primos relativos entonces $a^{\phi(m)} - 1$ es divisible por m

c) Teorema de Euclides-Euler (recíproco del teorema de Euclides sobre números perfectos). Un número n es perfecto si la suma de sus divisores es igual a $2n$, por ejemplo 6 es un número perfecto, pues $1 + 2 + 3 + 6 = 2 \cdot 6$. El Teorema de Euclides-Euler señala que: Si n es un número perfecto y par, entonces $n = 2^{k-1}(2^k - 1)$, donde $2^k - 1$ es un número primo

d) Los números amigos. Euler ofrece otras 58 parejas de númeroso amigos.

e) Método de factorización de Euler. Aunque la cocepción de este método es atribuido a Frénicle de Berry (1605-1675) y a Mersenne (1588-1648), es Euler el primero en hacerlo explícito. Este método será expuesto con detalle más adelante.

3 Preliminares: Tópicos Elementales de la Teoría de Números.

3.1 Definiciones y resultados básicos

Seguidamente se presentarán algunas definiciones y resultados elementales de la Teoría de Números, que permitirán posteriormente la introducción de los métodos de factorización.

Definición 1

Dado dos números naturales n y m, se dice que m es un **factor o divisor** de n si existe un número natural k tal que: $n = mk$. Se dice que n es un múltiplo de m y de k.

Ejemplo 1. El número 4 es divisor de 12 pues $12 = 4 \cdot 3$, en este caso se toma k igual a 3.

A continuación se enumeran algunos resultados consecuencia de la primer definición.

Grupo de Resultados A

1. Si m es factor de n entonces $\dfrac{n}{m}$ es factor de n
2. Para todo número natural n, se tiene que 1 y n son divisores de n.
3. Si l es divisor de m y m es divisor de n entonces l es divisor n

Justificación de los resultados A.

1. Si m es un factor de n entonces existe $k \in \mathbb{N}$ tal que $n = mk$, por lo que $\frac{n}{m} = k$, y en consecuencia k es un factor de n, pues $n = km$. Este resultado señala que si $n = mk$ entonces tanto m como k son factores de n.
2. Dado que $n = n \cdot 1$, entonces por el resultado anterior, n y 1 son divisores de n.
3. Se tiene que existen dos naturales, j y k que cumplen: $m = lj$ y $n = mk$ entonces $n = l\,(kj)$. Por lo tanto l es divisor de n.

Se entenderá por factorizar un número n como el proceso mediante el cual se expresa n como una multiplicación de dos o más factores diferentes de 1.

Ejemplo 2. Las posibles factorizaciones de 8 son: $2 \cdot 4$ y $2 \cdot 2 \cdot 2$.

Definición 2.

Se define A_n como el conjunto de divisores de n.

Ejemplo 3. $A_6 = \{1, 2, 3, 6\}\,, A_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

A continuación se enumeran algunos propiedades del conjunto A_n.

Grupo de Resultados B.

1. Para todo n, A_n no es vacío.
2. Si n es divisor de m entonces $A_n \subset A_m$.
3. El máximo elemento de A_n es n.
4. Para cualesquiera números naturales n y m, se tiene que $A_n \cap A_m$ es diferente del conjunto *vacío*.

Justificación de los resultados B.

1. Por el resultado $A2$ se tiene que $1 \in A_n$. Además $n \in A_n$
2. Sea $k \in A_n$, entonces k es divisor de n y como n es divisor de m, por el resultado $A3$, se tiene que k es factor de m. Por lo tanto $k \in A_m$.
3. Sea $k \in A_n$, entonces existe $j \in A_n$, tal que $kj = n$, por lo tanto $k \leq kj = n$.

4. De la justificación del resultado $B1$, se tiene que $1 \in A_n$ y $1 \in A_m$, para cualesquiera naturales n y m.

El conjunto $A_n \cap A_m$ es llamado el **conjunto de los divisores comunes** de m y n.

Definición 3.

Se define el **máximo común divisor** de los números naturales m y n como el máximo del conjunto formado por los divisores comunes de m y n. Se denota por (m, n) :

$$(m, n) = \max (A_n \cap A_m)$$

El máximo común divisor esta bien definido debido que $A_n \cap A_m$ es diferente de vacío (resultado $B4$) y es acotado, pues A_n y A_m son acotados (resultado $B3$), por lo tanto $A_n \cap A_m$ es un conjunto infinito no vacío.

Ejemplo 4. Determine $(30, 48)$

Solución. Note que $A_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$, $A_{48} = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$, entonces $A_{30} \cap A_{48} = \{1, 2, 3, 6\}$. Por lo tanto $(30, 48) = 6$.

Más adelante veremos un algoritmo que permite hallar el máximo común divisor de una manera más rápida.

Definición 4.

Se define el conjunto B_n como el conjunto formado por todos los múltiplos de n.

Ejemplo 5. El con junto B_2 es el conjunto de los números pares. Por otro lado, $B_3 = \{3, 6, 9, 12, 15, ...\}$

Algunas de las propiedades del conjunto B_n se muestran a continuación.

Grupo de Resultados C.

1. Para todo n, B_n es diferente del vacío
2. Si n es divisor de m entonces $B_m \subset B_n$.
3. El mínimo valor de B_n es n.

4. B_n no posee un elemento máximo.
5. Para cualesquiera números naturales n y m, se tiene que $B_n \cap B_m$ es diferente del conjunto *vacío*.

Justificación de los resultados C.

1. Como n es múltiplo de n entonces $n \in B_n$.
2. Sea $k \in B_m$, entonces m es divisor de k y como n es divisor de m, por el resultado $A3$, se concluye que k es múltiplo de n.
3. Si $k \in B_n$, entonces existe un número natural j tal que $jn = k$, por lo tanto, $n \leq nj = k$.
4. Si m es el máximo de B_n, entonces $mn \in B_n$, pues mn es un múltiplo de n, así se llega a una contradicción.
5. Note que nm es múltiplo de n y de m, por lo tanto $mn \in B_n \cap B_m$

El conjunto $B_n \cap B_m$ suele ser llamado como el **conjunto de los múltiplos comunes** de n y m.

Definición 5.

Se define el **mínimo común múltiplo** de los números naturales m y n como el mínimo valor del conjunto formado por los múltiplos comunes de m y n, se denota por $[m, n]$. Es decir

$$[m, n] = \min (B_n \cap B_m)$$

Al igual que el máximo común divisor, el mínimo común múltiplo esta definido debido que $B_n \cap B_m$ es diferente de vacío (resultado $C5$) y además $B_n \cap B_m \subset \mathbb{N}$

Ejemplo 6. Determine el mínimo común múltiplo de $[30, 48]$

Solución. Se tiene que $B_{30} = \{30, 60, 90, 120, 150, 180, 210, 240...\}$ y $B_{48} = \{48, 96, 144, 192, 240, ..\}$ por lo tanto $[30, 48] = \min (B_{30} \cap B_{48}) = 240$.

Note que calcular un mínimo común múltiplo utilizando la definición no es un algoritmo muy eficiente, más adelante se brinda una manera más eficiente de calcularlo.

Definición 6

Se dice que un número natural p es **primo** si tiene solamente dos divisores, es decir $A_p = \{1, p\}$. Si un número tiene más de dos divisores se dice que es **compuesto**.

Ejemplo 7. Los números: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 son los primeros diez primos.

Uno de los resultados más importantes en Teoría de Números es el **Teorema Fundamental de la Aritmética**:"Todo número natural puede expresarse como una multiplicación de números primos". Más aun, si dichos factores se ordenan de manera ascendente, la forma de expresar el número n es única, o sea n puede escribirse de manera única así:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}, \text{ donde } p_1, p_2, ...y\ p_k \text{ son primos y además } p_1 < p_2 < .. < p_k. \quad (1)$$

La demostración de este teorema se puede consultar en casi cualquier libro de Teoría de Números.

Ejemplo 8. $30 = 2 \cdot 3 \cdot 5\ y\ 144 = 2^4 \cdot 3^2$. ■

Se entenderá por factorización prima de n, la expresión de n de la forma dada en (1). Como consecuencia de este teorema, se obtiene un resultado que simplifica el cálculo del máximo común divisor y el mínimo común múltiplo:

Teorema. Sea $q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot ... \cdot q_k^{\alpha_k}$ y $s_1^{\beta_1} \cdot s_2^{\beta_2} \cdot ... \cdot s_j^{\beta_j}$ la factorización prima de n y m respectivamente.

a) Tomemos todos los primos involucrados en la factorización prima de n y m : $q_1, q_2, ..., q_k$, $s_1, s_2, ..., s_j$; y reordenémonos de menor a mayor, entonces, n y m se pueden escribir de la siguiente manera:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}, \text{ donde si } p_i \notin A_n \text{ se define } \alpha_i = 0,$$
$$m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r} \text{ donde si } p_i \notin A_m \text{ se define } \beta_i = 0.$$

b) Utilizando la notación de m y n dada por la parte a, se tiene que:

$$(n,m) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot ... \cdot p_r^{\min(\alpha_r,\beta_r)},$$
$$[n,m] = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot ... \cdot p_r^{\max(\alpha_r,\beta_r)}.$$

Ejemplo 9. Determine $(28, 30)$ y $[28, 30]$

Solución. La factorización de 28 y 30 es respectivamente $2^2 \cdot 7$ y $2 \cdot 3 \cdot 5$. Así, estos números se puede escribir como $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1$ y $30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0$. Por lo tanto $(28, 30) = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 2$ y $[28, 30] = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 420$.

En la practica, el lector puede apreciar que se puede omitir la notación dada en el teorema anterior. A raíz del Teorema Fundamental de la Aritmética surgen varios métodos para hallar la factorización prima de un número natural, que se estudiarán en la siguiente sección, los cuales permitirán de acuerdo al teorema anterior, hallar de una manera más ágil el máximo común divisor y el mínimo común múltiplo.

3.2 Ejercicios.

1. Demuestre que el (a, b) es un factor de a y de b.
2. Pruebe que los números a y b son factores de $[a, b]$.
3. Determine por extensión el conjunto $A_n \cap B_n$.
4. Pruebe que si n es divisor de m entonces $A_n \cup B_m \subset A_m \cup B_n$
5. Pruebe que $A_n \cap B_m \neq \phi$ entonces m es divisor de n.
6. ¿Por qué no tiene sentido hablar del máximo común múltiplo y del mínimo común divisor?

4 Métodos de Factorización prima.

Los métodos de factorización prima son algoritmos que permiten hallar los factores primos de un número. Dichos algoritmos se puede clasificar en: factorización por factores primos y

por factores compuestos. Para el desarrollo de estos algoritmos es indispensable identificar los números primos, por ello, al final del presente trabajo se brinda una tabla con los números primos menores que 200. Seguidamente se explican cada una de estos tipos de métodos de factorización prima.

4.1 Métodos de factorización por factores primos.

Estos métodos son la aplicación directa del teorema de factorización prima, pues da un número natural n consisten en hallar de manera ascendente cada uno de los factores primos de n. En forma general estos algoritmos siguen los siguientes pasos:

Paso 1. $k = 1$, $n_k = n$

Paso 2. Determinar el número primo más pequeño que divide a n_k. Este sera llamado p_k.

Paso 3. Se define $n_{k+1} = \dfrac{n_k}{p_k}$.

Paso 4. Si n_{k+1} es primo entonces finaliza el procedimiento y se obtiene que

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k \cdot n_{k+1},$$

donde $p_1, p_2, ... p_k$ y n_{k+1} son primos y además $p_1 \leq p_2 \leq ... \leq p_k \leq n_{k+1}$. Si no se pasa al paso 5

Paso 5. Incrementar k en una unidad y pasar al paso 2.

Básicamente, estos métodos siguen un procedimiento de búsquedad lineal, es decir no se puede determinar el k-ésimo primo, p_k, si no se han determinado todos los anteriores: $p_1, p_2, ..., p_{k-1}$, lo que provoca que estos métodos sea muy ineficientes para números grandes. A continuación se presentan los dos métodos que obedecen este procedimiento.

4.1.1 Método de ensayo y error.

En este método, para el paso 2 se procede realizando la división de n_k entre $2, 3, 5, 7, 11, ...$ hasta obtener el primer primo divisor de n_k, veamos el siguiente ejemplo.

Ejemplo 1. Determine la factorización prima de 1638.

Solución. Los resultados del método ensayo y error se presentan en la siguiente tabla

k	n_k	Residuo de la división de n_k entre:				p_k
		2	3	5	7	
1	1638	0				2
2	$\frac{1638}{2} = 819$	1	0			3
3	$\frac{819}{3} = 273$	1	0			3
4	$\frac{273}{3} = 91$	1	1	1	0	7
5	$\frac{91}{7} = 13$					

Así, en este caso se obtiene que $n = 1638 = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot n_5 = 2 \cdot 9 \cdot 7 \cdot 13$

4.1.2 Método por reglas de divisibilidad.

Este método es una variación del anterior y consiste en sustituir algunas de las divisiones por reglas de divisibilidad. Para efectos de dicha presentación se enumeran seguidamente.
Dado un número n, se dice que

1. n es divisible entre 2 si su último digito es $0, 2, 4, 6$ *o* 8
2. n es divisible entre 3 si la suma de sus dígitos es múltiplo de 3.
3. n es divisible entre 5 si su último digito es 0 *o* 5
4. n es divisible entre 7 si el número que queda suprimiendo el dígito de de las unidades, disminuido en el doble de las unidades es 0 o múltiplo de 7.
5. n es divisible entre 11, si la suma de los dígitos de las posiciones pares menos la suma de los dígitos de las posiciones impares es 0 o múltiplo de 11.

Ejemplo 2. Determine la factorización prima de 45 885.

Solución. Los resultados del método por reglas de divisibilidad se observan en la siguiente tabla.

k	n_k	Es divisible n_k entre					Residuode n_k entre:			p_k
		2	3	5	7	11	13	17	19	
1	45885	no	si							3
2	$\frac{45885}{3} = 15\,295$	no	no	si						5
3	$\frac{15295}{5} = 3059$	no	no	no	si					7
4	$\frac{3059}{7} = 437$	no	no	no	no	no	8	12	0	19
5	$\frac{437}{19} = 23$									

Por lo tanto se realiza $45\,885 = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot n_5 = 3 \cdot 5 \cdot 7 \cdot 19 \cdot 23$. ■

Nota: Esta tabla como la del ejemplo anterior, es una manera de exhibir los resultados del método posterior a su aplicación, pues una vez aplicado el método, se sabe cuantas columnas se requieren.
Si bien este método es más eficiente que el anterior, se puede mejorar. En efecto, la idea consiste en romper el orden de menor a mayor de los primos y verificar primero si el n_k es divisible por 5 y luego por 2, que es fácil de comprobarlo. Esto permitirá obtener luego un n_k más cómodo para determinar si es divisible por $3, 7, 11, 13...$

Hasta el momento se han presentado en los ejemplos, unas tablas que ilustran muy bien el procedimiento de los algoritmos utilizados. Sin embargo, en secundaria se utiliza una tabla donde se suele omitir el paso 2 de los algoritmos, las cuales tienen la ventaja de que se puede utilizar para ir presentado los datos conforme el método avanza, y no como en las anteriores, en donde no se podía construir la tabla hasta que el algoritmo finalice. El docente puede optar en un primer momento, por utilizar tablas similares a las expuestas en los ejemplos, permitiendo que los alumnos se familiaricen con los algoritmos, y posteriormente, utilizar la tradicional tabla que se expone en el siguiente ejemplo.

Ejemplo 3. Determine la factorización prima de $40\,950$.

Solución. Aplicando el algoritmo se tiene que

n_k	p_k
40950	5
$\frac{40950}{5} = 8190$	5
$\frac{8190}{5} = 1638$	2
$\frac{1638}{2} = 819$	3
$\frac{819}{3} = 273$	3
$\frac{273}{3} = 91$	7
$\frac{91}{7} = 13$	

Por lo tanto $40950 = 2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13$. ■

4.1.3 Desventajas de los métodos por factores primos.

Como se han mencionado anteriormente, una de las mayores desventajas de estos métodos de factorización de un número natural n es que utilizan un procedimiento de búsquedad lineal para hallar los factores primos de n. Otras desventajas que tienen estos métodos son:

1. Funcionan sólo para números "pequeños". Para números muy grandes estos algoritmos requieren mucho tiempo.

2. Se cuenta con pocas reglas de divisibilidad. Estás son sólo para los primeros primos.

3. Es complicado saber si un número mayor que 100 es primo. La mayoría de personas conocen a lo sumo los veinte primeros números. Esto provoca que si n esta compuesto con primos mayores que 100, se une al algoritmo la dificultad de tener que ir determinando los primos en el orden que se sigue.

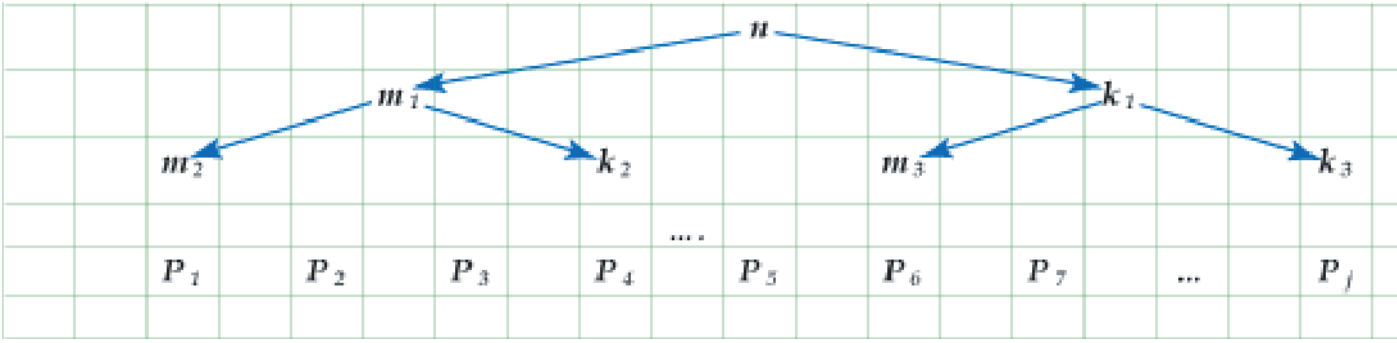
4.2 Métodos de factorización por factores compuestos.

Estos métodos consisten en, dado un número natural n, hallar dos números m y k (no necesariamente primos) que cumplan $n = mk$. De manera general, estos algoritmos siguen los siguientes pasos para la factorización de n:

Paso 1. Hallar dos números naturales m y k que cumplan que $mk = n$.

Paso 2. Factorizar m y k utilizando algunos de los métodos de factorización.

Si se continúa aplicando este mismo tipo de método, se puede apreciar que se sigue un procedimiento de búsqueda de árbol, pues se va simultáneamente hallando los factores primos de n :



Veamos el siguiente ejemplo.

Ejemplo 4. Determine la factorización prima de 6400.

Solución. Se tiene que $6400 = 64 \cdot 100$ y como $64 = 8^2 = 2^6$ y $100 = 10^2 = 2^2 5^2$, entonces $6400 = 2^8 5^2$.

No siempre es tan fácil determinar para un número natural n dos números que multiplicados entre sí den como resultado n. Es fácil cuando el número es divisible por 2, 3 o 5. Por lo tanto, en los métodos que presentaremos en las secciones siguientes se asumirá que el número n a factorizar es impar y no es divisible por 3 ni por 5, pues, en caso contrario, es mejor

aplicar inicialmente algunos de los métodos vistos, hasta obtener factores (un valor n_k) que cumplan dicho supuesto.

4.2.1 Método de factorización de Fermat

Sea n un número natural impar, se quiere hallar dos naturales m y k que cumplan

$$n = mk$$

Como n es impar entonces tanto m como k son impares y suponiendo sin pérdida de generalidad que $m \geq k$ entonces, $\dfrac{m-k}{2}$ y $\dfrac{m+k}{2}$ son números naturales. Tómese

$$x = \frac{m+k}{2} \in \mathbb{N}, \quad y = \frac{m-k}{2} \in \mathbb{N}$$

Note que $x + y = m \quad$ y $\quad x - y = k$, por lo tanto

$$n = mk = (x+y)(x-y) = x^2 - y^2. \qquad (*)$$

Así, nuestro problema se reduce ha hallar dos números naturales x, y que cumplan $n = x^2 - y^2$.

Note que de $(*)$ se tiene que $x^2 = n + y^2$, entonces $x^2 \geq n$ y se sigue que

$$x \geq n \qquad (1)$$

Por otro lado, de $(*)$ se deduce que $x^2 - n$ debe ser un cuadrado perfecto, que se denotará por $\Delta(x)$, por lo tanto

$$\Delta(x) = x^2 - n \text{ debe ser un cuadrado perfecto} \qquad (2).$$

En resumen a partir de (1) y (2), el Método de Fermat sigue los siguientes pasos, para determinar los factores m y k de un número natural n:

Paso 1. Si $\sqrt{n} \in \mathbb{N}$ tome $m = k = \sqrt{n}$ y finaliza el algoritmo. Sino pase al paso 2

Paso 2. Sea k el número natural entre $\sqrt{n}$ y $\sqrt{n} + 1$, pase al paso siguiente

Paso 3. Si $\Delta(k)$ es cuadrado perfecto tome $x = k$, $y = \sqrt{\Delta(x)}$, $m = x + y$, $k = x - y$, y finaliza el algoritmo. Si no, pase al paso siguiente.

Paso 4. Incremente k en una unidad y pase al paso anterior.

Ejemplo 5. Determine la factorización prima de 14 647.

Solución. En este caso se tiene que $\sqrt{n} = \sqrt{14647} = 121.02$ por lo tanto se debe buscar un número $x \geq 122$ que cumpla: $\Delta(x)$ se un cuadrado perfecto. Por lo tanto se procede de manera inductiva sobre k a partir de $k = 122$ hasta obtener que $\Delta(k)$ sea un cuadrado perfecto:

k	$\Delta(k)$	$\sqrt{\Delta(k)}$
122	237	$15,39480432$
123	482	$21,9544984$
124	729	27

Por lo tanto $x = 124$, $y = 27$, y se obtiene que el número $n = 14647$ puede ser factorizado por

$$14647 = (124 + 27)(124 - 27) = 151 \cdot 97.$$

Como 151 y 97 son primos, entonces dicha factorización es la factorización prima de 14647.

Ahora bien, este método se puede mejorar si se halla una fórmula recursiva para $\Delta(k)$. En efecto, note que

$$\Delta(k+1) = (k+1)^2 - n = k^2 + 2k + 1 - n = \Delta(k) + 2k + 1.$$

Dicha fórmula facilita el cálculo de $\Delta(k)$.

El siguiente ejemplo muestra que a pesar de que el Método de Fermat requiere menos tiempo que los anteriores, no es tan rápido.

Ejemplo 6. Determine la factorización prima de $31 \cdot 19 \cdot 101 \cdot 107 \cdot 5 = 31\,826\,615$

Solución. Note que este número es divisible entre 5, por lo tanto nos interesa factorizar $\frac{31\,826\,615}{5} = 6365\,323$. Sea $n = 6365\,323$, se tiene que $\sqrt{n} = 2522,959175$. Por lo tanto, se obtiene que

k	$\Delta(k)$	$\sqrt{\Delta(k)}$
2523	206	$14,35270009$
2524	5253	$72,47758274$
2525	10302	$101,4987685$
$\vdots$	$\vdots$	$\vdots$
2581	296238	$544,2775028$
2582	301401	549

Así, $x_1 = 2582$, $y_1 = 549$, $m_1 = x_1 + y_1 = 3131$ y $k_1 = x_1 - y_1 = 2033$, por lo tanto

$$6365\,323 = 3131 \cdot 2033 \qquad (1)$$

Ahora, factoricemos 3131, note que

$$3131 = 31 \cdot 100 + 31 = 31\,(100 + 1) = 31 \cdot 101 \qquad (2)$$

Por otro lado, utilicemos el método de Fermat para factorizar $k = 2033$, donde $\sqrt{2033} = 45.089$. Se sigue que

k	$\Delta(k)$	$\sqrt{\Delta(k)}$
46	83	$9,110433579$
47	176	$13,26649916$
48	271	$16,46207763$
$\vdots$	$\vdots$	$\vdots$
62	1811	$42,55584566$
63	1936	44

Así, se obtiene que $x_2 = 63, y_2 = 44$, $m_2 = x_2 + y_2 = 107$ y $k_2 = x_2 - y_2 = 19$, entonces

$$2033 = 107 \cdot 19 \qquad (3)$$

Por (1) , (2) y (3) , se concluye que

$$31\,826\,615 = 5 \cdot 6365\,323 = 5 \cdot 31 \cdot 19 \cdot 101 \cdot 107.$$

Ejercicios

1. Utilice el Método de Fermat para hallar la factorización prima de

a)	4757	*f*)	2873	*k*)	20 449
b)	893	*g*)	77 653	*l*)	532 627
c)	689	*h*)	19 109	*m*)	114 433
d)	6161	*i*)	2431	*o*)	79 007
e)	15 553	*j*)	12 827	*p*)	3127

2. Utilice los métodos de factorización vistos para halla la factorización prima de

a)	342	*d*)	190 045	*g*)	64 989
b)	5885	*e*)	33 441	*h*)	31 976 175
c)	9776	*f*)	420 042	*i*)	6374 680

3. A partir del método de factorización utilizado para factorizar 3131 (en el ejemplo 4.2.1), deduzca **una factorización** de los siguientes tipos de números escritos en base 10 :

a)	$(ababab)$	*d*)	$(a0a0a0a)$
b)	$(abcabc)$	*e*)	$(abc000abc)$
c)	$(ab0ab)$	*f*)	$(ab00ab00ab)$

4.2.2 Método de Factorización de Euler

Suponga que el número impar n a factorizar puede ser representado en dos formas distintas, como la suma de dos cuadrados perfectos:

$$n = a^2 + b^2 = c^2 + d^2, \text{ con } a, b, c, d \in \mathbb{N}$$

Como n es impar, entonces solo puede ser expresado como la suma de un impar y un par, por lo tanto, supongamos sin perdida de generalidad que a y c son números impares, en tanto, b

y d son pares, y además $a > c$, por lo tanto $b < d$. Debido a esto, note que a^2 es de la forma $4m$, mientras b^2 es de la forma $4m+1$, por lo tanto, n es de la forma $4m+1$.

Por otro lado, de (1) se tiene que $d^2 - b^2 = a^2 - c^2$, y se sigue que

$$(d-b)(d+b) = (a+c)(a-c) \qquad (2)$$

Sea $m = (a-c, d-b)$, por lo tanto existen dos números naturales l y k que cumplen:

$$a - c = km, \quad d - b = lm \quad y \quad (k,l) = 1. \qquad (3)$$

Note que m es par, pues $a-c$ y $d-b$ son pares. Sustituyendo (3) en (2) se obtiene que

$$l(d+b) = k(a+c) \qquad (4)$$

Como $(l,k) = 1$ entonces l es divisor de $(a+c)$, y entonces existe un número natural j que cumple

$$a + c = lj \qquad (5)$$

Sustituyendo (5) en (4) se sigue

$$d + b = kj \qquad (6)$$

Debido a (5), (6) y $(l,k) = 1$, se obtiene que $j = (a+c, b+d)$, y como $a+c$ y $b+d$ son pares se concluye que j es par.

Dado que m y j son números pares, verifiquemos que una factorización de n está dada por

$$\left[\left(\frac{m}{2}\right)^2 + \left(\frac{j}{2}\right)^2\right]\left[(l)^2 + (k)^2\right] \qquad (7)$$

En efecto, expandiendo (7) se obtiene que

$$\left[\left(\frac{m}{2}\right)^2 + \left(\frac{j}{2}\right)^2\right]\left[(l)^2 + (k)^2\right] = \frac{(lm)^2 + (km)^2 + (lj)^2 + (kj)^2}{4},$$

aplicando $(3), (5)$ y (6) se deduce que (7) es equivalente a

$$\frac{(d-b)^2+(a-c)^2+(a+c)^2+(d+b)^2}{4} = \frac{2\left(a^2+b^2+c^2+d^2\right)}{4} = n.$$

Lo anterior justifica el Método de Euler que se enuncia en las siguientes líneas.

En resumen, para poder factorizar un número impar n con el Método de Euler, este debe cumplir:

1. Es de la forma $4m+1$.

2. Se puede representar como la suma de dos cuadrados perfectos: $n = a^2 + b^2$, con a impar y b par.

3. Posee otra representación como la suma de dos cuadrados perfectos: $n = c^2 + d^2$, con c impar y d par.

Así para un n que cumple con las reglas anteriores, se puede factorizar siguiendo los siguientes pasos:

Paso 1. Calcular $m = (a-c, d-b)$

Paso 2. Hallar $k = \dfrac{a-c}{m}, \quad l = \dfrac{d-b}{m}$

Paso 3. Determinar $j = \dfrac{a+c}{l}$

Paso 4. La factorización de n esta dada por $\left[\left(\dfrac{m}{2}\right)^2 + \left(\dfrac{j}{2}\right)^2\right]\left[(l)^2+(k)^2\right]$.

Ejemplo 7. Determine la factorización prima de 901

Solución. Dado que $901 = 30^2 + 1^2 = 15^2 + 26^2$, se tiene que

$$\begin{array}{llll} a = & 15 & m = & (14,4) = 2 \\ b = & 26 & k = & 7 \\ c = & 1 & l = & 2 \\ d = & 30 & j = & 8 \end{array}$$

Por lo tanto,

$$n = \left[1^2 + 4^2\right]\left[2^2 + 7^2\right] = 17 \cdot 53.$$

El principal inconveniente de este método es la determinación de 2 representaciones del número n a factorizar como la suma de dos cuadrados. Sin embargo, al igual que en el Método de Fermat, se puede buscar por medio de una tabla, dos valores enteros de x entre 1 y $\sqrt{n}$, para los cuales $T(x) = n - x^2$ es un cuadrado perfecto. En caso de que existan dichos valores de x, digamos x_0 y x_1, se obtiene que n tiene 2 representaciones como la suma de dos cuadrados:

$$n = x_0^2 + \left(\sqrt{T(x_0)}\right)^2 = x_1^2 + \left(\sqrt{T(x_1)}\right)^2.$$

Además, se puede establecer una fórmula recursiva para $T(x)$:

$$T(x+1) = n - (x+1)^2 = T(x) - 2x - 1.$$

Ejemplo 8. Determine la factorización prima de 10001.

Solución. En la siguiente tabla se aprecian los valores de x y $\sqrt{T(x)}$:

x	$T(x)$	$\sqrt{T(x)}$
1	10000	100
2	9997	99, 98499887
⋮	⋮	⋮
76	4225	65

Así, se tiene que $a = 65, b = 76, c = 1$ y $d = 100$, además $m = (a - c, d - b) = (64, 24) = \left(2^6, 2^3 \cdot 3\right) = 2^3 = 8$, con estos valores se obtiene: $k = \dfrac{a-c}{m} = 8, \quad l = \dfrac{d-b}{m} = 3$ y $j = \dfrac{a+c}{l} = \dfrac{66}{3} = 22$. Por lo tanto, la factorización prima de 10001 es

$$10001 = \left[\left(\frac{m}{2}\right)^2 + \left(\frac{j}{2}\right)^2\right]\left[(l)^2 + (k)^2\right] = \left(4^2 + 11^2\right)\left(3^2 + 8^2\right) = 137 \cdot 73.$$

Ejemplo 9. Determine la factorización prima de 6970697

Solución. Note que $6970697 = 697 + 10000 \cdot 697 = 697 \cdot 10001$, y por el ejercicio anterior se sabe que la factorización prima de $10001 = 137 \cdot 73$, por lo que solo resta factorizar $n = 697$, para el cual se tiene los siguientes valores de x y $T(x)$:

x	$T(x)$	$\sqrt{T(x)}$
1	696	26, 38181192
2	693	26, 32489316
⋮	⋮	⋮
11	576	24
⋮	⋮	⋮
16	441	21

Así, se obtiene que

$$\begin{array}{llll} a = & 21 & m = & (10, 8) = 2 \\ b = & 16 & k = & 5 \\ c = & 11 & l = & 4 \\ d = & 24 & j = & 8 \end{array}$$

Por lo tanto $697 = \left(1 + 4^2\right)\left(4^2 + 5^2\right) = 17 \cdot 41$. Se concluye que la factorización prima de 6970697 es

$$6970697 = 17 \cdot 41 \cdot 73 \cdot 137$$

Con este ejemplo se finaliza esta presentación, esperamos que esta sea de utilidad al lector.

Ejercicios.

1. Utilice el Método de Euler para hallar la factorización prima de

$a)$	221	$f)$	2813	$k)$	35 657
$b)$	1073	$g)$	4453	$l)$	33 389
$c)$	2501	$h)$	10 961	$m)$	4901
$d)$	11 461	$i)$	5459	$o)$	6409
$e)$	3293	$j)$	2929	$p)$	38077

2. Utilice los métodos de factorización vistos para halla la factorización prima de

$a)$	43 018	$d)$	793 793
$b)$	190 105	$e)$	7280 728
$c)$	79 566	$f)$	6630 663

5 Algunas respuestas

Ejercicios de la sección 4.2.1

1.

$a)$	$67 \cdot 71$	$f)$	$13^2 \cdot 17$	$k)$	$11^2 \cdot 13^2$
$b)$	$19 \cdot 47$	$g)$	$19 \cdot 61 \cdot 67$	$l)$	$17^2 \cdot 19 \cdot 97$
$c)$	$53 \cdot 13$	$h)$	$197 \cdot 97$	$m)$	$101 \cdot 11 \cdot 103$
$d)$	$101 \cdot 61$	$i)$	$11 \cdot 13 \cdot 17$	$o)$	$47 \cdot 41^2$
$e)$	$103 \cdot 151$	$j)$	$127 \cdot 101$	$p)$	$59 \cdot 53$

2.

$a)$	$2 \cdot 3^2 \cdot 19$	$d)$	$5 \cdot 191 \cdot 199$	$g)$	$3^3 \cdot 29 \cdot 83$
$b)$	$5 \cdot 11 \cdot 107$	$e)$	$3 \cdot 157 \cdot 71$	$h)$	$3 \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 113$
$c)$	$2^4 \cdot 13 \cdot 47$	$f)$	$2 \cdot 3 \cdot 7 \cdot 73 \cdot 137$	$i)$	$2^3 \cdot 5 \cdot 13^2 \cdot 23 \cdot 41$

3.

$a)$	$(ab) \cdot (10101)$	$d)$	$(a) \cdot (1010101)$
$b)$	$(abc) \cdot (1001)$	$e)$	$(abc) \cdot (1000001)$
$c)$	$(ab)\,(1001)$	$f)$	$(ab) \cdot (100010001)$

Ejercicios de la sección 4.2.2

1.

$a)$	$13 \cdot 17$	$f)$	$97 \cdot 29$	$k)$	$181 \cdot 197$
$b)$	$29 \cdot 37$	$g)$	$61 \cdot 73$	$l)$	$173 \cdot 193$
$c)$	$41 \cdot 61$	$h)$	$113 \cdot 97$	$m)$	$13^2 \cdot 29$
$d)$	$73 \cdot 157$	$i)$	$103 \cdot 53$	$o)$	$13 \cdot 17 \cdot 29$
$e)$	$37 \cdot 89$	$j)$	$29 \cdot 101$	$p)$	$13 \cdot 29 \cdot 101$

2.

$a)$	$2 \cdot 137 \cdot 157$	$d)$	$7 \cdot 11 \cdot 13^2 \cdot 61$
$b)$	$5 \cdot 193 \cdot 197$	$e)$	$13 \cdot 56 \cdot 137 \cdot 73$
$c)$	$3 \cdot 2 \cdot 149 \cdot 89$	$f)$	$3 \cdot 17 \cdot 13 \cdot 137 \cdot 73$

6 Los números primos menores que 200

2	23	59	97	137	179
3	29	61	101	139	181
5	31	67	103	149	191
7	37	71	107	151	193
11	41	73	109	157	197
13	43	79	113	163	199
17	47	83	127	167	
19	53	89	131	173	

7 Conclusión

Este material está dirigido a docentes o futuros docentes de secundaria. En él se realizaron de manera sencilla justificaciones a diversos tópicos de la Teoría de Números. Muchos de estos son actualmente abordados en la enseñanza secundaria, y la forma en que fueron presentados junto con la astucia del docente puede ser combinadas para favorecer la comprensión de tales tópicos en su salón de clase.

Por otro lado, se realizó una clasificación de los principales métodos de factorización prima, introduciendo métodos no tradicionales en la enseñanza secundaria, en especial los métodos de Fermat y Euler. Se hizo hincapié en la justificación y descripción paso a paso de la aplicación de cada uno de estos métodos.

En el caso especificó de los métodos de Fermat y Euler, se propone a los docentes adaptar sus justificaciones a la enseñanza secundaria con el fin de que los estudiantes observen métodos más eficientes para la factorización prima de números grandes, los comprendan y los apliquen.

Esto sin caer en el error de pretender que tengan que memorizarlos.

Se espera que esta presentación sea de utilidad al lector.

8 Bibliografía

1. Andrews G. 1994. Number Theory. Editorial Dover Piblications, New York.
2. Jones, B. (1969). Teoría de los Números. Editorial F. Trillas, S.A., Mexico.
3. Koblitz, N. 1987. A course in Number Theory and Cryptography. Springer-Verlag, New York.
4. Ore, O. Number Theory and its History.
5. Pettofrezzo, A; Byrkit, D. 1972. Introducción a la Teoría de los Números (Traducción por Pomareda Rolando). Editorial Prentice/Hall International.
6. Vinogradov, I. 1977. Fundamentos de la Teoría de Números. Editorial Mir, Moscú.
7. Vorobiov, N. 1984. Criterios de Divisivibilidad. Lecciones populares de matemática. Editorial Mir, Moscú.

Sitios web visitados:
http://platea.pntic.mec.es/˜aperez4/numeroshtml/numeros.htm
http://www.diribera.com/mates/historia.htm
http://www.terra.es/personal/jftjft/Historia/Biografias/Euler.htm
http://thales.cica.es/rd/Recursos/rd97/Biografias/28-2-B-E.html