FACTORIZACIÓN DE ENTEROS DEL TIPO $b^n \pm 1$

DIRECTOR DE LA REVISTA

Abstract. Se presentan ejemplos concretos de factorización de enteros del tipo $b^n \pm 1$ y algunas técnicas para su cálculo, con el fin de proporcionar a lectores que enseãn computación consideren su utilidad

1. Introduction

Sea N un número natural, un par de problemas que interesan tanto en matemática pura como aplicada son:

A) Determinar si N es un número primo
B) Cuando N no es un número primo, calcular su factorización en números primos.

La resolución de estos problemas es de actualidad en matemática como por ejemplo lo indica el artílo de libre acceso en

http://www.ams.org

en el journal Bulletin descargar el archivo

Granville, It is easy to determine whether a given integer is prime, Bull. AMS, Vol. 42, No 1, Enero 2005, Pag. 3-39.

y las referencias contenidas en su bibliografía.

El método quizás mas antiguo para determinar cuando un número es primo es utiliza el algoritmo de división del modo siguiente:

Fija un número natural N el cual se desea saber si es primo o compuesto, a continuación

Para cada natural $1 < d < N$ se realiza el siguiente

Procedimiento: calcular el resto r de dividir N por d, si este resto es cero, paramos, pués hemos encontrado que N no es primo, sino es cero continuamos con el siguiente de d

En caso de encontrar un divisor d efectuando la división de N por d obtemos de modo explícito dos divisores de N, a saber, d y N/d.

Ahora calculamos los factores primos de d y N/d y así logramos los factores primos de N.

Una computadora PC con un procesador .....realiza ...operaciones por segundo, por consiguiente, si el número N tiene 500 cifras el tiempo de cómputo para saber si N es primo es aproximadamente .....

Puesto que $N \approx 10^{500}$, de manera que realizamos $10^5 00$ divisiones y 10^{500} restas para calcular el resto, de modo que el tiempo de cálculo es aproximadamente

$$2 * 10^5 00 * ..../60\text{segundos} = \text{minutos}$$

Desde los tiempos del florecimiento de la civilización griega, 300 años antes de cristo, se conoce el siguiente teorema:

Si un número N no es primo, entonces admite un divisor primo (o al menos un divisor) p tal que $1 < p < \sqrt{N}$.

Por lo tanto, si sólo realizamos el procedimiento descripto más arriba para $d = 2, 3, \cdots, floor\{\sqrt{N}\}$ aplicado a un número de aproximadamente 500 cifras, toma

$$2 * 10^{250} * ..../60\text{segundos} = \text{minutos}$$

tiempo mucho menor!

Este ejemplo sencillo muestra que para disminuir costos de cálculo conocer teoremas es de importancia.

Existen otros métodos para determinar cuando un número es primo, invitamos a nuestros lectores a escribir artílos sobre el tema.

Con el programa Maple es muy fácil encontrar la factorización de un número en productos de primos, simplemente debemos escribir en la pantalla

with(numtheory) ifactor(N);

sí sólo se desea saber si N es primo o no, se usa el comando

isprimeN;

La pregunta que uno se hace, es ? como estan hechos esos programos?, si usted habre el help o un manual de dichos programas encontrará indicaciones al respecto.

A continuación presentamos un método para encontrar factorización en números primos para los enteros $b^n \pm 1$ distinto al método rudimentario descripto en los párrafos anteriores.

Se basa en conocer los polinomios ciclotómicos y algunas de sus propiedades.

Para cada natural d se define un polinomio ciclotómico ϕ_d del modo siguiente,

$\phi_1(x) = x - 1, \phi_2(x) = x + 1, \phi_3(x) = x^2 + x + 1,$

$\phi_4(x) = x^2 + 1, \phi_5(x) = x^4 + x^3 + x^2 + x + 1,$

y en general por la fórmula inductiva,

$$\phi_n(x) = \frac{x^n - 1}{\prod_{k/n, k<n} \phi_k(x)} \qquad (cic).$$

Por ejemplo

$$\phi_6(x) = \frac{x^6-1}{\prod_{k/6,k<6}\phi_k(x)} = \frac{x^6-1}{\phi_1(x)\phi_2(x)\phi_3(x)} = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2-x+1$$

$$\phi_7(x) = \frac{x^7-1}{\prod_{k/7,k<7}\phi_k(x)} = \frac{x^7-1}{\phi_1(x)} = \frac{x^7-1}{x-1} = x^6+x^5+x^4+x^3+x^2+x+1$$

Utilizando maple, la instrucción para calcular $\phi_n(x)$ es:
with(numtheory): ¿ cyclotomic(n,x);

En general, como lo hicimos para $p = 7$ se demuestra con un cálculo muy sencillo que para p primo,

$$\phi_p(x) = xp - 1 + \cdots + x + 1.$$

(basta recordar un caso de factoreo!)

Como ejercicio proponemos

a) Mostrar que para n impar se tiene que

$$\phi_{2n}(x) = \phi_n(-x).$$

b) Para p primo que no divide al número n, se tiene que

$$\phi_{pn}(x) = \frac{\phi_n(x^p)}{\phi_n(x)}$$

Un ejercicio más dificil es mostrar que

$$\phi_n(x) = \prod_{d/n}(x^{n/d} - 1)^{\mu(d)} \qquad (1)$$

Donde μ es la función de Möbius definida por

$$\mu(s) = \begin{cases} 0 & \text{si } s \text{ es divisible por } p^2 \text{ para algun primo } p \\ (-1)^r & \text{si } s \text{ es producto de } r \text{ primos distintos} \\ 1 & \text{si } s = 1 \end{cases}$$

Con maple y la instrucción
> with(numtheory):
¿ for n to 7 do print(n, mobius(n)) od;
se obtiene

n, mobius(n)
1, 1
2, -1
3, -1
4, 0
5, -1
6, 1
7, -1

Aplicando la fórmula (1) y la tabla recientemente calculada se obtiene

$$\begin{aligned}\phi_6(x) &= \prod_{d/6}(x^{6/d}-1)^{\mu(d)} \\ &= (x^6-1)^{\mu(1)}(x^3-1)^{\mu(2)}(x^2-1)^{\mu(3)}(x^1-1)^{\mu(6)} \\ &= (x^6-1)^1(x^3-1)^{-1}(x^2-1)^{-1}(x^1-1)^1 = x^2-x+1\end{aligned}$$

Un hecho importante es que los polinomios ciclotómicos son a coeficientes enteros.

Esto se deduce de varias maneras, una, es debido a que los primeros polinomios ciclotómicos poseen coeficientes enteros y son mónicos, por ende al efectuar la división que los define obtenemos un polinomio a coeficientes enteros, otra manera, es observando que en la fórmula (1), estamos multiplicando polinomios a coeficientes enteros.

A continuación explicamos sucintamente como se utilizan los polinomios ciclotómicos para factorizar en primos n úmeros de la forma $b^n \pm 1$.

Por la defínción misma de los polinomos ciclotómicos se tiene la identidad

$$x^n - 1 = \prod_{d/n} \phi_d(x) \quad n \geq 1$$

Por tanto, para cada b natural como $\phi_d(b)$ es un número si tiene la factorización como producto de enteros

$$b^n - 1 = \prod_{d/n} \phi_d(b)$$

Cuando los números $\phi_d(b)$ son números primos para cada d que divide a n obtenemos la factorización en primos de $b^n - 1$. De lo contrario obtenemos una factorización de $b^n - 1$.

Ejemplos

$2^7 - 1 = \phi_1(2)\phi_7(2) = (2-1)(2^6+2^5+2^4+2^3+2^2+2+1) = 1*128$ poco uso....

$2^6-1 = \phi_1(2)\phi_2(2)\phi_3(2)\phi_6(2) = (2-1)(2+1)(2^2+2+1)(2^2-2+1) = 3*7*3$ la desomposición en factores primos!

Nos resta analizar como descomponer b^n+1 para esto utilizamos los casos de factoreo y los llevamos a casos conocidos, como

$$b^{2n} - 1 = (b^n - 1)(b^n + 1)$$

se tiene

$$b^n + 1 = \frac{(b^{2n} - 1)}{(b^n - 1)} = \prod_{d/2n} \phi_d(b) / \prod_{k/n} \phi_d(k).$$

Escribiendo $2n = 2^t m$ con m impar y relacionando los divisores de $2n$ con los de n la fórmula anterior se simplica en

$$b^n + 1 = \prod_{d/n} \phi_{2^t d}(b).$$

Un ejemplo es $n = 78 = 2*39 = 2*3*39$ por ende $2n = 2^2*39$ lo cual origina

$$\begin{aligned} 2^{78} + 1 &= \prod_{d/39} \phi_{4d}(2) = \phi_4(2)\phi_{12}(2)\phi_{52}(2)\phi_{156}(2) \\ &= (5)(13)(53*157*1613)(13*313*1249*3121*21841). \end{aligned}$$

En la bibliografía indicada mas abajo presenta tablas de de factorizaciones, para dar una muestra copiamos...

chichi copiar la fotocopia aqui

Factorizaciones de Aurifeuille

A partir de la fórmula (1) hemos obtenido factorizaciones de números naturales, es posible generar identidades polinómicas a partir de los polinomios ciclotótomicos de manera de generar otras factorizaciones del número en cuestion. Estas factorizaciones se las obtiene al observar que en ciertas identidades aparecen diferencias de cuadrados. A continuación presentamos algunas debidas a Aurifeuille.

En la identidad,

$$x^2 + 1 = \phi_2(x^2) = (x+1)^2 - 2x$$

reemplazamos $x := 2^{2k-1}$ y obtenemos la factorización

$$2^{4k-2}+1 = (2^{2k-1}+1)^2 - 22^{2k-1} = (2^{2k-1}+1)^2 - 2^{2k-2} = (2^{2k-1}+1)^2 - (2^{k-1})^2$$

De modo que

$$2^{4k-2}+1 = (2^{2k-1}+1-2^k)(2^{2k-1}+1+2^k) = (2^{2k-1}-2^k+1)(2^{2k-1}+2^k+1)$$

en la identidad

$$x^3 + 1 = (x + 1)\phi_3(-x) = (x * 1)[(x + 1)^2 - 3x]$$

Al reemplazar $x := 3^{2k-1}$ y operar como antes se obtiene

$$3^{6k-3} + 1 = (3^{2k-1} + 1)(3^{2k-1} - 3^k + 1)(3^{2k-1} + 3^k + 1)$$

Mientras que se reemplazamos $x := 12^{2k-1}$ se obtiene

$$12^{6k-3} + 1 = (12^{2k-1} + 1)(12^{2k-1} - 2^{2k-1}3^k + 1)(12^{2k-1} + 2^{2k-1}3^k + 1).$$

Otras identidades que generan mas igualdades son

Chichi copiar uno en ciruclo

Como ejercicio sugerimos reemplazar en la primera $x := 5^{2k-1}$; en la segunda $x := 6^{2k-1}$; y en la tercera $x := 7^{2k-1}$; al operar se obtienen otras identidades similares a las anteriores.

Bibliografía

Billhart, Lehmer, Selfridge, Tuckerman, Wagstaff, Factorization of $b^n \pm 1$, b=2,3,5,6,7,10,11,12 up to high powers, Contemporary Mathematics, Vol. 22, American Mathematical Society, www.ams.org, este libro esta disponible gratis en internet, sino lo consigue, solicitar archivo .pdf al director de la revista.