Factorización de enteros del tipo $b^n \pm 1$

Jorge A. Vargas

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 enseñan computación consideren su utilidad

1 Introducción

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.

las referencias contenidas en su bibliografía son también de interés.

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

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

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

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, esto es, con $d := d + 1$.

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 con un procesador ATTDSP32C realiza $25.000.000 = 25.10^6$ operaciones por segundo, por consiguiente, si el número N tiene 500 cifras el tiempo de cómputo para saber si N es primo es aproximadamente $50 * 10^{506}$

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

$$2 * 10^{500}/25.10^6 = 2/25 * 10^{494}$$

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

$$2 * 10^{250}/25 * 10^6 = 2/25 * 10^{244}$$

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 artículos 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);

Si sólo se desea saber si N es primo, se usa el comando

isprime(N);

La pregunta que uno se hace, es ¿cómo estan hechos esos programas?, si usted abre la ayuda o un manual de dicho programa encontrará indicaciones al respecto.

A continuación presentamos un método para encontrar la 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,

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

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

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,

$$\phi_p(x) = x^{p-1} + \cdots + x + 1.$$

(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

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

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 define los subsiguientes dá como resultado 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 natural, se 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 $b^n - 1$.

¡Notar que por este método no hace falta calcular $b^n - 1$!

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 para transformar a casos conocidos, como

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

se tiene

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

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

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

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

Factorización de $2^n - 1, n \leq 45$

Factores primos

n

2 3
3 7
4 3.5
5 3^1

6 3.3.7
7 127
8 3.5.17
9 7.73
10 3.11.31

11 23.89
12 3.3.5.7.13
13 8191
14 3.43.127
15 7.31.151

16 3.5.17.257
17 131071
18 3.3.3.7.19.73
19 524287
20 3.5.5.11.31.41

21 7.7.127.337
22 3.23.89.683
23 47.178481
24 3.3.5.7.13.17.241
25 31.601.1801

26 3.2731.8191
27 7.73.262657
28 3.5.29.43.113.127
29 233.1103.2089
30 3.3.7.11.31.151.331

31 2147483647
32 3.5.17.257.65537
33 7.23.89.599479
34 3.43691.131071
35 31.71.127.122921

36 3.3.3.5.7.13.19.37.73.109
37 223.616318177
38 3.174763.524287
39 7.79.8191.121369
40 3.5.5.11.17.31.41.61681

41 13367.164511353
42 3.3.7.7.43.127.337.5419
43 431.9719.2099863
44 3.5.23.89.397.683.2113
45 7.31.73.151.631.23311

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

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

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

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

Si mientras que 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

$x^5 - 1 = (x-1)\Phi_5(x) = (x-1)[(x^2 + 3x + 1)^2 - 5x(x+1)^2]$
$x^6 + 1 = (x^2+1)\Phi_6(x^2) = (x^2+1)[(x^2 + 3x + 1)^2 - 6x(x+1)^2]$
$x^7 + 1 = (x+1)\Phi_7(-x) = (x+1)[(x+1)^6 - 7x(x^2 + x + 1)^2]$

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 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.

Facultad de Matemática, Astronomía y Física (FaMAF).
Universidad Nacional de Córdoba.