(*March 16, 2004*)

Factoring $x^n - 1$: cyclotomic and Aurifeuillian polynomials

Paul Garrett <garrett@math.umn.edu>

Polynomials of the form $x^2 - 1$, $x^3 - 1$, $x^4 - 1$ have at least one systematic factorization

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1)$$

Equivalently, polynomials like $x^2 - y^2$, $x^3 - y^3$, and $x^4 - y^4$ have factorizations

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$$

For odd n, replacing y by $-y$ gives a variant

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1})$$

For composite exponent n one obtains several different factorizations

$$x^{30} - 1 = (x^{15})^2 - 1 = (x^{15} - 1)(x^{15} + 1)$$

$$x^{30} - 1 = (x^{10})^3 - 1 = (x^{10} - 1)(x^{20} + x^{10} + 1)$$

$$x^{30} - 1 = (x^6)^5 - 1 = (x^6 - 1)((x^6)^4 + \ldots + 1)$$

Such *algebraic* factorizations yield *numerical* partial factorizations of some special large numbers, such as

$$2^{33} - 1 = (2^{11})^3 - 1 = (2^{11} - 1)(2^{22} + 2^{11} + 1)$$

$$2^{33} - 1 = (2^3)^{11} - 1 = (2^3 - 1)(2^{30} + \ldots + 1)$$

Thus, $2^{33} - 1$ has factors $2^3 - 1 = 7$ and $2^{11} - 1 = 23 \cdot 89$. It is then easier to complete the *prime* factorization

$$2^{33} - 1 = 7 \cdot 23 \cdot 89 \cdot 599479$$

But that largish number 599479 might be awkward to understand.

How do we verify that a number such as $N = 599479$ is **prime**? That is, how do we show that N is not evenly divisible by any integer D in the range $1 < D < N$?

One *could* divide N by all integers D between 1 and N, but this is needlessly slow, since if D evenly divides N and $D > \sqrt{N}$ then N/D is an integer and $N/D < \sqrt{N}$.

That is, we need only do trial divisions by D for $D \le \sqrt{N}$.

And, after dividing by 2, we need only divide by *odd* numbers D thereafter.

Also, we need only divide by primes, if convenient.

For example, since $N = 101$ is not divisible by the primes $D = 2, 3, 5, 7$ no larger than $\sqrt{101} \sim 10$, we see that 101 is prime.

Congruences: Recall that

$$a = b \bmod m$$

means that m divides $a - b$ evenly. Thus, for example,

$$6 = 1 \bmod 5$$

$$10 = -1 \bmod 11$$

$$35 = 1012 \bmod 977$$

One might worry that in the prime factorization

$$2^{33} - 1 = 7 \cdot 23 \cdot 89 \cdot 599479$$

the large number 599479 is left over after algebraic factoring. But Fermat and Euler proved that *a prime factor p of $b^n - 1$ either divides $b^d - 1$ for a divisor $d < n$ of the exponent n, or else $p = 1 \bmod n$.*

Since here the exponent 33 is odd, and since primes bigger than 2 are odd, in fact we can say that if a prime p divides $2^{33} - 1$ and is not $7, 23, 89$, then $p = 1 \bmod 66$.

Thus, in testing 599479 for divisibility by $D \le \sqrt{599479} \sim 774$ we do not need to test all odd numbers, but only $67, 133, 199, \ldots$ and only need to do

$$599479/66 \sim 11$$

trial divisions to see that 599479 is prime.

So $2^n - 1$ is not prime unless the exponent n is prime. For p prime, if $2^p - 1$ is prime, it is a **Mersenne prime**.

Not every number of the form $2^p - 1$ is prime, even with p prime. For example,

$$2^{11} - 1 = 23 \cdot 89$$

$$2^{23} - 1 = 47 \cdot 178481$$

$$2^{29} - 1 = 233 \cdot 1103 \cdot 2089$$

$$2^{37} - 1 = 223 \cdot 616318177$$

$$2^{41} - 1 = 13367 \cdot 164511353$$

Nevertheless, usually the largest known prime at any moment is a Mersenne prime, such as

$$2^{6972593} - 1$$

Theorem *(Lucas-Lehmer)* Let $L_o = 4$, $L_n = L_{n-1}^2 - 2$. For p an odd prime, $2^p - 1$ is **prime** if and only if

$$L_{p-2} = 0 \bmod 2^p - 1$$

We want the *complete* factorization of $x^n - 1$ into *irreducible* polynomials with rational coefficients (which cannot be factored further without going outside the rational numbers). The irreducible factors are **cyclotomic polynomials**. For example,

$$x^{18} - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^6+x^3+1)(x^6-x^3+1)$$

has familiar-looking factors, but

$$x^{15} - 1 = (x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1)$$

has an unfamiliar factor. How do we get all these?

For *complex* α the polynomial $x - \alpha$ is a factor of $x^n - 1$ if and only if $\alpha^n = 1$. This happens if and only if

$$\alpha = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = e^{2\pi i k/n}$$

for some $k = 0, 1, 2, \ldots, n-1$. These are n^{th} *roots of unity*, and they account for the n complex roots of $x^n - 1 = 0$.

Among the n^{th} roots of unity are d^{th} roots of unity for divisors d of n. For example, among the 6^{th} roots of unity are square roots and cube roots of 1 also, not to mention 1 itself. An n^{th} root of unity is *primitive* if it is *not* a d^{th} root of unity for any $d < n$ dividing n.

The primitive complex n^{th} roots of unity are

$$\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = e^{2\pi i k/n}$$

with $0 < k < n$ and $\gcd(k, n) = 1$. Indeed, if $\gcd(k, n) = d > 1$, then

$$(e^{2\pi i k/n})^{(n/d)} = e^{2\pi i k/d} = 1$$

since d divides k evenly.

For example, the primitive complex 6^{th} roots of 1 are

$$e^{2\pi i \cdot 1/6} \quad e^{2\pi i \cdot 5/6}$$

The primitive complex 10^{th} roots of 1 are

$$e^{2\pi i \cdot 1/10} \quad e^{2\pi i \cdot 3/10} \quad e^{2\pi i \cdot 7/10} \quad e^{2\pi i \cdot 9/10}$$

One definition of the n^{th} **cyclotomic polynomial** $\Phi_n(x)$ is

$$\Phi_n(x) = \prod_{\alpha \text{ primitive } n^{\text{th}} \text{ root of } 1} (x - \alpha)$$

This does *not* make immediately clear that the coefficients are *rational*, which they *are*. It is also not immediately clear how to compute the cyclotomic polynomials from this.

But this definition *does* give the important property

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

where $d|n$ means that d divides n evenly.

A naive computational approach comes from the idea that roots α of $\Phi_n(x) = 0$ should satisfy $\alpha^n - 1 = 0$ but not $\alpha^d - 1 = 0$ for smaller d. Thus, for *prime* p indeed

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

We might *try*

$$\Phi_n(x) = \frac{x^n - 1}{x^d - 1 \text{ for } d < n \text{ dividing } n} (?)$$

But this is not quite right. For example,

$$\Phi_6(x) \neq \frac{x^6 - 1}{(x-1)(x^2-1)(x^3-1)}$$

shows that this attempted definition tries to remove more factors of $x - 1$ that there are in $x^6 - 1$.

Correcting this,

$$\Phi_6(x) = (x^6 - 1) \cdot \frac{1}{(x^{6/2} - 1)(x^{6/3} - 1)} \cdot (x^{6/6} - 1) = \frac{(x^6 - 1)(x - 1)}{(x^3 - 1)(x^2 - 1)} = x^2 - x + 1$$

That is, we include *all* 6^{th} roots of unity, take away those which are cube roots or square roots, and put back those we have counted twice, namely 1. Similarly,

$$\Phi_{30}(x) =$$

$$(x^{30} - 1) \cdot \frac{1}{(x^{15} - 1)(x^{10} - 1)(x^6 - 1)} \cdot (x^5 - 1)(x^3 - 1)(x^2 - 1) \cdot \frac{1}{(x - 1)}$$
$$= \frac{(x^{30} - 1)(x^5 - 1)(x^3 - 1)(x^2 - 1)}{(x^{15} - 1)(x^{10} - 1)(x^6 - 1)(x - 1)} = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$$

That is, we *include* all 30^{th} roots of unity, *take away* 15^{th}, 10^{th}, and 6^{th} roots, *put back* those we have counted twice, namely 5^{th}, cube, and square roots, and then *take away* again those we've counted 3 times, namely 1.

Systematically incorporating the idea of compensating for over-counting we have the *correct* expression

$$\Phi_n(x) = (x^n - 1) \times \frac{1}{\prod_{\text{prime } p|n} (x^{n/p} - 1)} \times \prod_{\text{distinct primes } p,q|n} (x^{n/pq} - 1) \times \frac{1}{\prod_{\text{distinct primes } p,q,r|n} (x^{n/pqr} - 1)} \times \ldots$$

Using the property

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

gives a more elegant approach, by rearranging:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} \Phi_d(x)}$$

By induction, if $\Phi_d(x)$ has rational coefficients for $d < n$, then so does $\Phi_n(x)$. Also, inductively, if we know $\Phi_d(x)$ for $d < n$ then we can compute $\Phi_n(x)$. Grouping helps. For example,

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = \frac{x^{15} - 1}{\Phi_3(x)(x^5 - 1)} = \frac{x^{10} + x^5 + 1}{\Phi_3(x)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

by direct division at the last step. We can be a little clever. For example,

$$\Phi_{30}(x) = \frac{x^{30} - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_5(x)\Phi_6(x)\Phi_{10}(x)\Phi_{15}(x)}$$

Use

$$x^{15} - 1 = \Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)$$

to simplify to

$$\Phi_{30}(x) = \frac{x^{30}-1}{\Phi_2(x)\Phi_6(x)\Phi_{10}(x)(x^{15}-1)} = \frac{x^{15}+1}{\Phi_2(x)\Phi_6(x)\Phi_{10}(x)}$$

Use

$$x^{10} - 1 = \Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)$$

to get

$$\Phi_{30}(x) = \frac{x^{15}+1}{\Phi_2(x)\Phi_6(x)\Phi_{10}(x)} = \frac{(x^{15}+1)\Phi_1(x)\Phi_5(x)}{\Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)\cdot\Phi_6(x)} = \frac{(x^{15}+1)(x^5-1)}{\Phi_6(x)(x^{10}-1)}$$

$$= \frac{(x^{15}+1)}{\Phi_6(x)(x^5+1)} = \frac{(x^{10}+x^5+1)}{x^2-x+1} = \frac{(x^{10}-x^5+1)}{x^2-x+1} = x^8+x^7-x^5-x^4-x^3+x+1$$

by direct division at the last step.

Based on fairly extensive hand calculations, one might suspect that all coefficients of all cyclotomic polynomials are either $+1$, -1, or 0, but this is not true. It *is* true for n prime, and for n having at most 2 distinct prime factors, but not generally. The smallest n where $\Phi_n(x)$ has an exotic coefficient is $n = 105$. It is no coincidence that $105 = 3\cdot 5\cdot 7$ is the product of the first 3 primes above 2.

$$\Phi_{105}(x) = \frac{x^{105}-1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_7(x)\Phi_{15}(x)\Phi_{21}(x)\Phi_{35}(x)} = \frac{x^{105}-1}{\Phi_3(x)\Phi_{15}(x)\Phi_{21}(x)(x^{35}-1)}$$

$$= \frac{x^{70}+x^{35}+1}{\Phi_3(x)\Phi_{15}(x)\Phi_{21}(x)} = \frac{(x^{70}+x^{35}+1)(x^7-1)}{\Phi_{15}(x)(x^{21}-1)} = \frac{(x^{70}+x^{35}+1)(x^7-1)\Phi_1(x)\Phi_3(x)\Phi_5(x)}{(x^{15}-1)(x^{21}-1)}$$

$$= \frac{(x^{70}+x^{35}+1)(x^7-1)(x^5-1)\Phi_3(x)}{(x^{15}-1)(x^{21}-1)}$$

Instead of direct polynomial computations, we do *power series* computations, imagining that $|x| < 1$, for example. Thus,

$$\frac{-1}{x^{21}-1} = \frac{1}{1-x^{21}} = 1 + x^{21} + x^{42} + x^{63} + \ldots$$

We anticipate that the degree of $\Phi_{105}(x)$ is $(3-1)(5-1)(7-1) = 48$ (why?). We also observe that the coefficients of all cyclotomic polynomials are the same back-to-front as front-to-back (why?). Thus, we'll use power series in x and ignore terms of degree above 24.

Thus

$$\Phi_{105}(x) = \frac{(x^{70}+x^{35}+1)(x^7-1)(x^5-1)(x^2+x+1)}{(x^{15}-1)(x^{21}-1)} = (1+x+x^2)(1-x^7)(1-x^5)(1+x^{15})(1+x^{21})$$

$$= (1+x+x^2)\times(1-x^5-x^7+x^{12}+x^{15}-x^{20}+x^{21}-x^{22}) =$$

$$1+x+x^2-x^5-x^6-x^7-x^7-x^8-x^9+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}-x^{20}-x^{21}-x^{22}+x^{21}+x^{22}+x^{23}-x^{22}-x^{23}-x^{24}$$

$$= 1+x+x^2-x^5-x^6-2x^7-x^8-x^9+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}-x^{20}-x^{22}-x^{24}$$

Looking closely, we have a $-2x^7$.

In fact, $\Phi_n(x)$ cannot be factored further using only rational coefficients.

For prime p, this follows from **Eisenstein's criterion**: for $f(x)$ with integer coefficients, highest-degree coefficient 1, all lower-degree coefficients divisible by p, and constant term *not* divisible by p, $f(x)$ cannot be factored (with rational coefficients).

For example, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ itself does not have the right kind of coefficients, but a variation does:

$$\Phi_5(x+1) = \frac{(x+1)^5 - 1}{(x+1) - 1} = x^4 + 5x^3 + 10x^2 + 10x + 5$$

And

$$\Phi_7(x+1) = \frac{(x+1)^7 - 1}{(x+1) - 1} = x^6 + 7x^5 + 21x^4 + 35x^3 + 35x^2 + 21x + 7$$

Less well known are *Lucas-Aurifeullian-LeLasseur* factorizations such as

$$x^4 + 4 = (x^4 + 4x^2 + 4) - (2x)^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

More exotic are

$$\frac{x^6 + 27}{x^2 + 3} = (x^2 + 3x + 3)(x^2 - 3x + 3)$$

$$\frac{x^{10} - 5^5}{x^2 - 5} = (x^4 + 5x^3 + 15x^2 + 25x + 25) \times (x^4 - 5x^3 + 15x^2 - 25x + 25)$$

and

$$\frac{x^{12} + 6^6}{x^4 + 36} = (x^4 + 6x^3 + 18x + 36x + 36) \times (x^4 - 6x^3 + 18x - 36x + 36)$$

and further

$$\frac{x^{14} + 7^7}{x^2 + 7} = (x^6 + 7x^5 + 21x^4 + 49x^3 + 147x^2 + 343x + 343) \times (x^6 - 7x^5 + 21x^4 - 49x^3 + 147x^2 - 343x + 343)$$

These Aurifeuillian factorizations yield further factorizations of special large numbers, such as

$$2^{22} + 1 = 4 \cdot (2^5)^4 + 1 = (2(2^5)^2 + 2(2^5) + 1)(2(2^5)^2 - 2(2^5) + 1) = 2113 \cdot 1985 = 2113 \cdot 5 \cdot 397$$

and similarly

$$\frac{3^{33} + 1}{3^{11} + 1} = \frac{27 \cdot (3^5)^6 + 1}{3 \cdot (3^5)^2 + 1} = (3(3^5)^2 + 3(3^5) + 1)(3(3^5)^2 + 3(3^5) + 1) = 7 \cdot 25411 \cdot 176419$$

Where do these come from? For an odd prime p

$$\Phi_p(x^2) = \frac{(x^2)^p - 1}{\Phi_1(x^2)} = \frac{(x^{2p} - 1)\Phi_p(x)}{\Phi_1(x)\Phi_2(x)\Phi_p(x)} = \Phi_{2p}(x)\Phi_p(x)$$

Replacing x by $\sqrt{p} \cdot x$ in this equality gives

$$\Phi_p(px^2) = \Phi_{2p}(\sqrt{p}\,x)\Phi_p(\sqrt{p}\,x)$$

The factors on the right-hand side no longer have rational coefficients. But their linear factors can be *regrouped* into two batches of $p-1$ which *do* have rational coefficients, and these are the Aurifeuillian factors of $\Phi_{2p}(px^2)$.

From Galois theory, using $p = 1 \bmod 4$, for $\zeta = e^{2\pi i/2p}$, $\sqrt{p}$ is a Gauss sum

$$\sqrt{p} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)_2 \zeta^{2k} \in \mathbf{Q}(\zeta)$$

with quadratic symbol $\left(\frac{k}{p}\right)_2 = \pm 1$ depending whether k is a square mod p or not. The automorphisms of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ are

$$\sigma_a : \zeta \to \zeta^a$$

for $a \in \mathbf{Z}/p^\times$, and

$$\sigma_a(\sqrt{p}) = \sqrt{p} \cdot \left(\frac{a}{p}\right)_2$$

Then

$$\Phi_p(px^2) = \prod_{\left(\frac{k}{p}\right)_2 = 1} (\sqrt{p}\, x - \zeta^k) \times \prod_{\left(\frac{k}{p}\right)_2 = -1} (\sqrt{p}\, x - \zeta^k)$$

is the Aurifeuillian factorization into two factors with rational coefficients.

To *compute* the Aurifeuillian factors? From the Galois theory view, it turns out that there are polynomials $f(x)$ and $g(x)$ with *rational* coefficients such that

$$\Phi_p(x) = f(x)^2 \pm pxg(x)^2$$

with $+1$ for $p = 1$ mod 4, -1 for $p = 3$ mod 4. Then replacing x by $\mp px^2$ gives a difference of squares, which factors

$$\Phi_p(-px^2) = f(-px^2)^2 - p^2x^2g(-px^2)^2 = \big(f(-px^2) - pxg(-px^2)\big) \times \big(f(-px^2) + pxg(-px^2)\big)$$

For example,

$$\Phi_3(x) = x^2 + x + 1 = (x+1)^2 - 3x$$

Then

$$\Phi_3(3x^2) = (3x^2+1)^2 - 9x^2 = (3x^2 + 3x + 1)\,(3x^2 - 3x + 1)$$

And

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = (x^2 + 3x + 1)^2 + 5x(x+1)^2$$

The latter ingredients are not so hard to determine. If we know

$$x^4 + x^3 + x^2 + x + 1 = f(x)^2 + 5xg(x)^2$$

it is reasonable to take $f(x) = x^2 + ax \pm 1$ and try to find parameter a so that $f(x)^2$ differs from $\Phi_5(x)$ by some $5xg(x)^2$.

$$\frac{(x^2 + ax + 1)^2 - \Phi_5(x)}{x} = (2a-1)x^2 + (1 + a^2)x + (2a - 1)$$

Trying $a = 0, 1, 2, \ldots$ yields a good result for $a = 3$:

$$5x^2 + 10x + 5 = 5(x+1)^2$$

References:

Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, page 309 ff.

Brillhart, Lehmer, Selfridge, Tuckerman, Wagstaff *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers.*

R.P. Brent *On computing factors of cyclotomic polynomials*, Math. of Comp. **61**, 1993.

http://www.math.umn.edu /˜garrett/m/number_theory/aurifeuillian.pdf