CYCLOTOMIC POLYNOMIALS AND PRIME NUMBERS

YVES GALLOT

ABSTRACT. The sequence of numbers generated by the cyclotomic polynomials $\Phi_n(2)$ contains the Mersenne numbers $2^p - 1$ and the Fermat numbers $2^{2^m} + 1$. Does an algorithm involving $O(n)$ modular operations exist to test the primality of $\Phi_n(b)$?

1. Cyclotomic polynomials

Let n be a positive integer and let ζ_n be the complex number $e^{2\pi i/n}$. The n^{th} cyclotomic polynomial is, by definition

$$\Phi_n(x) = \prod_{\substack{1 \le k < n \\ \gcd(k,n)=1}} (x - \zeta_n^k) \tag{1.1}$$

Clearly the degree of $\Phi_n(x)$ is $\varphi(n)$, where φ is the Euler function. We have

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{1.2}$$

and conversely, by using the Möbius function, we can write

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}. \tag{1.3}$$

Date: November 12, 2000; revised January 5, 2001.

2000 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A41.

Key words and phrases. prime numbers, cyclotomic polynomials.

$\Phi_n(x)$ is a monic polynomial with integer coefficients. It can be shown that $\Phi_n(x)$ is irreductible over $\mathbb{Q}$. The first sixteen of them are given below:

$\Phi_1(x) = x - 1$ $\qquad$ $\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$ $\qquad$ $\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ $\qquad$ $\Phi_6(x) = x^2 - x + 1$

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ $\qquad$ $\Phi_8(x) = x^4 + 1$

$\Phi_9(x) = x^6 + x^3 + 1$ $\qquad$ $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$

$\Phi_{11}(x) = x^{10} + x^9 + x^8 + \cdots + x + 1$ $\qquad$ $\Phi_{12}(x) = x^4 - x^2 + 1$

$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + \cdots + x + 1$ $\qquad$ $\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$

$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ $\qquad$ $\Phi_{16}(x) = x^8 + 1$

Theorem 1.1. *If p is a prime then*

$$\Phi_{pm}(x) = \Phi_m(x^p) \text{ when } p \text{ divides } m,$$
$$\Phi_{pm}(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} \text{ when } p \text{ does not divide } m.$$

Proof.

$$\begin{aligned}\Phi_{pm}(x) &= \prod_{\substack{d \mid pm \\ p \mid d}} (x^d - 1)^{\mu(\frac{pm}{d})} \prod_{\substack{d \mid pm \\ p \nmid d}} (x^d - 1)^{\mu(\frac{pm}{d})} \\ &= \Phi_m(x^p) \prod_{\substack{d \mid pm \\ p \nmid d}} (x^d - 1)^{\mu(\frac{pm}{d})}\end{aligned}$$

If $p \mid m$ then $\frac{pm}{d} = ap^2$ and $\mu(\frac{pm}{d}) = 0$.
If $p \nmid m$ then $\mu(\frac{pm}{d}) = \mu(p)\mu(\frac{m}{d}) = -\mu(\frac{m}{d})$. □

It follows that if $n_1, n_2, \ldots, n_k$ are positive integers then

$$\Phi_{n_1^{\alpha_1} n_2^{\alpha_2} \ldots n_k^{\alpha_k}}(x) = \Phi_{n_1 \cdot n_2 \ldots n_k}(x^{n_1^{\alpha_1 - 1} n_2^{\alpha_2 - 1} \ldots n_k^{\alpha_k - 1}})$$

and if p is prime and $r \geq 1$, then

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}.$$

Theorem 1.2. *If $q > 1$ is an odd integer then*

$$\Phi_{2q}(x) = \Phi_q(-x).$$

Proof.

$$\begin{aligned}\Phi_{2q}(x) &= \prod_{d \mid 2q} (x^d - 1)^{\mu(\frac{2q}{d})} = \prod_{d \mid q} (x^d - 1)^{\mu(\frac{2q}{d})} (x^{2d} - 1)^{\mu(\frac{2q}{2d})} \\ &= \prod_{d \mid q} (x^d + 1)^{\mu(\frac{q}{d})} = \prod_{d \mid q} -((-x)^d - 1)^{\mu(\frac{q}{d})}.\end{aligned}$$

If $q \neq 1$ is odd then $\varphi(q)$ is even. □

Theorem 1.3. *If $n > 1$ then $\Phi_n(0) = 1$.*

Proof. By induction with $x^n - 1 = \Phi_n(x)(x-1)\prod_{\substack{d|n \\ d\neq 1,n}} \Phi_d(x)$ and $x = 0$. □

Theorem 1.4. *If $n > 1$ then*

$$\Phi_n(1) = p \text{ when } n \text{ is a power of a prime } p,$$
$$\Phi_n(1) = 1 \text{ otherwise.}$$

Proof. If n is not a prime power, let $n = p^r m$ where p is prime and such that $(p, m) = 1$. $\Phi_{p^r m}(1) = \Phi_{pm}(1^{r-1}) = \frac{\Phi_m(1^p)}{\Phi_m(1)}$ and the result follows by induction because $\Phi_m(1) \neq 0$. □

2. Factors of $\Phi_n(b)$

Theorem 2.1. *Let $n = p^m$ with p prime. If $p \mid (b-1)$ then $p \mid \Phi_n(b)$. All other prime factors of $\Phi_n(b)$ are of the form $kn+1$.*

Proof. See [8, Theorem 48]. □

The other forms can have some small factors:
$\Phi_{18}(2) = 2^6 - 2^3 + 1 = 57 = 3 \times 19$
$\Phi_{20}(2) = 2^8 - 2^6 + 2^4 - 2^2 + 1 = 205 = 5 \times 41$
$\Phi_{21}(2) = 2^{12} - 2^{11} + 2^9 - 2^8 + 2^6 - 2^4 + 2^3 - 2 + 1 = 2359 = 7 \times 337$
then Theorem 2.1 cannot be extended to any n.

Theorem 2.2. *Every prime factor of $b^n - 1$ must either be of the form $kn+1$ or be a divisor of $b^d - 1$, where $d < n$ and $d \mid n$.*

Proof. See [9, Theorem 2.4.3]. □

Since $\Phi_n(b) \mid (b^n - 1)$, conditions of Theorem 2.2 are true for any factor of a cyclotomic polynomial, but we have a better result:

Theorem 2.3. *If p is a prime factor of $\Phi_n(b)$ and is a divisor of $b^d - 1$, where $d < n$, then $p^2 \mid (b^n - 1)$ and $p \mid n$.*

Proof. [6] Let $r > 0$ such that $p^r \mid (b^n - 1)$ but $p^{r+1} \nmid (b^n - 1)$. If $p^r \mid (b^d - 1)$ then $p \nmid \frac{b^n-1}{b^d-1}$. But by Eq.1.2, $p \mid \Phi_n(b) \mid \frac{b^n-1}{b^d-1}$, a contradiction.

Let e_r the order of b modulo p^r. If $p^r \mid (b^m - 1)$ then $e_r \mid m$. Since $p^r \mid (b^{e_{r+1}} - 1)$, we have $e_{r+1} = ke_r$. Let $b^{e_r} = 1 + \alpha p^r$, then by the binomial theorem $b^{ke_r} \equiv 1 + \alpha k p^r \pmod{p^{r+1}}$. If $p \mid \alpha$, $e_{r+1} = e_r$, else $p \mid k$. Therefore either $e_r = e_1 = n$ (in which case $n \mid (p-1)$) or $p \mid n$. □

Thus we have:

Theorem 2.4. *Every prime factor of $\Phi_n(b)$ must either be of the form $kn+1$ or be a divisor of n and of $b^d - 1$, where $d \mid n$.*

According to [7, Page 268], this result was proved by Legendre in 1830.

3. Primality test of $\Phi_n(b)$ by factoring $\Phi_n(b) - 1$

From Theorem 1.3 we have $\Phi_n(x) - 1 = x^r P(x)$ where $r \geq 1$. If $r > \deg(P)/2$ and if the complete factorization of b is known then the primality of $\Phi_n(b)$ can be proved with theorems of [2].

Theorem 3.1. [3] *If $n = 2^\alpha 3^\beta$ then a theorem of Pocklington* [2, Th 4][7, p. 52] *is sufficient to test the primality of $\Phi_n(b)$ when b is factorized.*

Proof. If $\beta = 0$ then $\Phi_n(b) - 1 = b^{2^\alpha}$. If $\alpha = 0$ then $\Phi_n(b) - 1 = b^{3^{\beta-1}}(b^{3^{\beta-1}} + 1)$. Else $\Phi_n(b) = \Phi_6(b^{2^{\alpha-1}+3^{\beta-1}})$ and $\Phi_n(b) - 1 = b^{2^{\alpha-1}+3^{\beta-1}}(b^{2^{\alpha-1}+3^{\beta-1}} - 1)$. $\square$

No other case of polynomial factorization by x^r large enough is known:

Conjecture 3.2. [3] *If $\Phi_n(x) - 1 = x^r P(x)$ and $n \neq 2^\alpha 3^\beta$ then $r < \deg(P)/2$.*

Note that if n has many divisors, $\Phi_n(b) - 1$ has often enough polynomial factors to complete the primality proof for some small b. See [4] for criteria of divisibility of $\Phi_n(x) - 1$ by $\Phi_k(x)$.

Note also the generalization of the well-known results about Fermat and Mersenne numbers $2^{F_m - 1} \equiv 1 \pmod{F_m}$ and $2^{M_p - 1} \equiv 1 \pmod{M_p}$:

Theorem 3.3. *If $\Phi_n(b)$ has no prime factor $p \leq n$ then $b^{\Phi_n(b)-1} \equiv 1 \pmod{\Phi_n(b)}$.*

Proof. By Eq.1.2, $b^{\Phi_n(b)-1} - 1 = \prod_{d|(\Phi_n(b)-1)} \Phi_d(b)$. By Theorem 2.4, if $\Phi_n(b)$ has no prime factor $p \leq n$ then $\Phi_n(b) = kn+1$. Therefore $\Phi_n(b)$ divides $b^{\Phi_n(b)-1} - 1$. $\square$

4. Primes of the form $\Phi_n(2)$

If $n = 2^m$ then $\Phi_{2^m}(2) = 2^{2^{m-1}} + 1 = F_{m-1}$ (Fermat number). If p is prime then $\Phi_p(2) = 2^p - 1 = M_p$ (Mersenne number). If $p \neq 2$ then $\Phi_{2p}(2) = \Phi_p(-2) = (2^p + 1)/3$.

The first probable primes of the form $\Phi_n(2)$ were computed by the author. The primality of these numbers was proved for $n \leq 3000$ by the author with the implementation of Adleman-Pomerance-Rumely-Cohen-Lenstra's test of the UBASIC package [5] and for $3000 < n \leq 6500$ by Phil Carmody with Titanix [1] (see Table 1 and Table 2).

Fermat and Mersenne primes are two sparse subclasses of the dense class of the primes of the form $\Phi_n(2)$. But how to prove the primality of $\Phi_n(2)$ with only $O(n)$ operations modulo $\Phi_n(2)$ when n is not a prime or a power of 2?

Table 1. Values of n for which $\Phi_n(2)$ is prime, for $1 \leq n \leq 6500$

2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 22, 24, 26, 27, 30, 31, 32, 33, 34, 38, 40, 42, 46, 49, 56, 61, 62, 65, 69, 77, 78, 80, 85, 86, 89, 90, 93, 98, 107, 120, 122, 126, 127, 129, 133, 145, 150, 158, 165, 170, 174, 184, 192, 195, 202, 208, 234, 254, 261, 280, 296, 312, 322, 334, 345, 366, 374, 382, 398, 410, 414, 425, 447, 471, 507, 521, 550, 567, 579, 590, 600, 607, 626, 690, 694, 712, 745, 795, 816, 897, 909, 954, 990, 1106, 1192, 1224, 1230, 1279, 1384, 1386, 1402, 1464, 1512, 1554, 1562, 1600, 1670, 1683, 1727, 1781, 1834, 1904, 1990, 1992, 2008, 2037, 2203, 2281, 2298, 2353, 2406, 2456, 2499, 2536, 2838, 3006, 3074, 3217, 3415, 3418, 3481, 3766, 3817, 3927, 4167, 4253, 4423, 4480, 5053, 5064, 5217, 5234, 5238, 5250, 5325, 5382, 5403, 5421, 6120.

References

1. Marcel Martin, *Titanix: a primality prover using the Goldwasser, Kilian and Atkin algorithm*, 2000, http://www.znz.freesurf.fr/
2. J. Brillhart, D. H. Lehmer, and J. L. Selfridge, *New Primality Criteria and Factorizations of $2^m \pm 1$*, Math. Comp. **29** (1975), 620–647.
3. D. Broadhurst, *communication to PrimeForm egroup*, 2000.

TABLE 2. Values of n for which $\Phi_n(2)$ is a probable prime, for $6500 \leq n \leq 44497$

6925, 7078, 7254, 7503, 7539, 7592, 7617, 7648, 7802, 7888, 7918, 8033, 8370, 9583, 9689, 9822, 9941, 10192, 10967, 11080, 11213, 11226, 11581, 11614, 11682, 11742, 11766, 12231, 12365, 12450, 12561, 13045, 13489, 14166, 14263, 14952, 14971, 15400, 15782, 15998, 16941, 17088, 17917, 18046, 19600, 19937, 20214, 20678, 21002, 21382, 21701, 22245, 22327, 22558, 23209, 23318, 23605, 23770, 24222, 24782, 27797, 28958, 28973, 29256, 31656, 31923, 33816, 34585, 35565, 35737, 36960, 39710, 40411, 40520, 42679, 42991, 43830, 43848, 44497.

4. C. K. Caldwell, *Unique (period) primes and the factorization of cyclotomic polynomials minus one*, Mathematica Japonica **26:1** (1997), 189–195.
5. Yuji Kida, *UBASIC: a BASIC with ultra-fast multi-precision arithmetic*, 1989, http://archives.math.utk.edu/software/msdos/number.theory/ubasic/
6. C. Nash, *private communication*, 1999.
7. P. Ribenboim, *The New Book of Prime Number Records*, 3rd ed., Springer-Verlag, New York, 1995.
8. D. Shanks, *Solved and Unsolved Problems in Number Theory*, 4th ed., Chelsea, New York, 1993.
9. H.C. Williams, *Edouard Lucas and Primality Testing*, A Wiley-Interscience publication, Canadian Mathematical Society series of monographs, 1998.