The cyclotomic polynomials

Notes by G.J.O. Jameson

1. The definition and general results

We use the notation $e(t) = e^{2\pi it}$. Note that $e(n) = 1$ for integers n, $e(\frac{1}{2}) = -1$ and $e(s+t) = e(s)e(t)$ for all s, t.

Consider the polynomial $x^n - 1$. The *complex* factorisation is obvious: the zeros of the polynomial are $e(k/n)$ for $1 \leq k \leq n$, so

$$x^n - 1 = \prod_{k=1}^{n} \left[x - e\left(\frac{k}{n}\right) \right]. \tag{1}$$

One of these factors is $x - 1$, and when n is even, another is $x + 1$. The remaining factors can be combined in pairs of the form

$$[x - e(k/n)][x - e(-k/n)] = x^2 - 2x \cos \frac{2\pi k}{n} + 1$$

to give the factorisation into linear and quadratic *real* factors.

We will describe a constructive factorisation into polynomials with *integer* coefficients, and then present some applications to number theory. We write (a, b) for the gcd of a and b, and

$$E_n = \{k : 1 \leq k \leq n,\ (k, n) = 1\}.$$

By definition, the number of members of E_n is Euler's $\phi(n)$. The *cyclotomic polynomials* Φ_n are defined for all $n \geq 1$ by

$$\Phi_n(x) = \prod_{k \in E_n} \left[x - e\left(\frac{k}{n}\right) \right]. \tag{2}$$

(This is the usual notation; be careful to distinguish Φ_n and $\phi(n)$!)

It is clear that Φ_n is a monic polynomial (with, apparently, complex coefficients) of degree $\phi(n)$. We note some elementary cases:

$n = 1$: $E_1 = \{1\}$, hence $\Phi_1(x) = x - 1$.

$n = 2$: $E_2 = \{1\}$ and $e(\frac{1}{2}) = -1$, hence $\Phi_2(x) = x + 1$.

$n = 4$: $E_4 = \{1, 3\}$ and $e(\frac{1}{4}) = i$, hence $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$.

1.1. *For prime p,*

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

Proof. Consider the factorisation of $x^p - 1$ given by (1) (with $n = p$). To obtain $\Phi_p(x)$, remove the factor $x - 1$ corresponding to $k = p$. □

Let $n \geq 3$. Denote by E_n^* the members k of E_n with $k < \frac{n}{2}$. Then E_n consists of the pairs $(k, n-k)$ with $k \in E_n^*$ (note that $\frac{1}{2}n \notin E_n$). Hence $\phi(n)$ is even and E_n^* has $\frac{1}{2}\phi(n)$ members. Since $e[(n-k)/n] = e(-k/n)$, we have the following factorisation of $\Phi_n(x)$ into quadratic real factors:

$$\Phi_n(x) = \prod_{k \in E_n^*} [x - e(k/n)][x - e(-k/n)] = \prod_{k \in E_n^*} (x^2 - 2x \cos \frac{2\pi k}{n} + 1). \tag{3}$$

We deduce some properties of $\Phi_n(x)$ as a function of a real variable.

1.2. *For all $n \geq 3$,*

(i) $\Phi_n(x)$ *has real coefficients;*

(ii) $\Phi_n(0) = 1$*;*

(iii) $\Phi_n(x) > 0$ *for all real x;*

(iv) $\Phi_n(x)$ *is strictly increasing for $x > 1$;*

(v) for all $x > 0$, $(x-1)^{\phi(n)} < \Phi_n(x) < (x+1)^{\phi(n)}$.

Proof. (i) and (ii) are obvious. For $-1 < a < 1$, write $f_a(x) = x^2 - 2ax + 1$. Then $f_a(x) = (x-a)^2 + (1-a^2) > 0$ for all x, and is strictly increasing for $x \geq 1$: hence (iii) and (iv). Also, $(x-1)^2 < f_a(x) < (x+1)^2$ for all $x > 0$: hence (v). □

1.3 PROPOSITION. *Let $n \geq 2$. Let $\phi(n) = m$ and $\Phi_n(x) = \sum_{r=0}^m c_r x^r$. Then:*

(i) $\Phi_n(x) = x^m \Phi_n(1/x)$ *for $x \neq 0$,*

(ii) $c_{m-r} = c_r$ *for $0 \leq r \leq m$.*

Proof. This is trivial for $n = 2$, so assume $n > 2$. Write $\cos(2\pi k/n) = a_k$. By (3),

$$x^m \Phi_n\left(\frac{1}{x}\right) = \prod_{k \in E_n^*} x^2 \left(1 - \frac{2a_k}{x} + \frac{1}{x^2}\right) = \prod_{k \in E_n^*} (x^2 - 2a_k x + 1) = \Phi_n(x).$$

Hence $\sum_{r=0}^m c_r x^r = \sum_{r=0}^m c_r x^{m-r} = \sum_{r=0}^m c_{m-r} x^r$ for all $x \neq 0$, so $c_{m-r} = c_r$ for each r. □

We now explain how the cyclotomic polynomials provide a factorisation of $x^n - 1$.

1.4 LEMMA. *Let $n = n_1 d$. Then*

$$\Phi_d(x) = \prod \{[x - e(k/n)] : 1 \leq k \leq n,\ (k, n) = n_1\}.$$

Proof. By definition, $\Phi_d(x) = \prod_{r \in E_d} [x - e(r/d)]$. Now $r/d = (n_1 r)/n$ and $(r, d) = 1$ iff $(n_1 r, n) = n_1$; also, $r \leq d$ iff $n_1 r \leq n$. Writing $k = n_1 r$, we see that $\Phi_d(x)$ equates to the stated product. □

1.5 THEOREM. *For all $n \geq 1$,*

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{4}$$

Proof. Every k such that $1 \leq k \leq n$ has $(k, n) = n_1$ for some divisor n_1 of n. When d runs through the divisors of n, so does $n_1 = n/d$. Hence

$$\prod_{d|n} \Phi_d(x) = \prod_{k=1}^{n} [x - e(k/n)] = x^n - 1. \qquad \square$$

1.6 COROLLARY. *For $n \geq 2$,*

$$\prod \{\Phi_d(x) : d|n, d > 1\} = 1 + x + \cdots + x^{n-1}.$$

Proof. In (4), divide both sides by $\Phi_1(x) = x - 1$. The statement follows by continuity at $x = 1$. $\square$

It follows at once from (4) that if m divides n, then

$$\prod \{\Phi_d(x) : d|n,\ d \not| m\} = \frac{x^n - 1}{x^m - 1}. \tag{5}$$

A typical deduction (which will be generalised by later results) is:

1.7. *For prime p,*

$$\Phi_{p^k}(x) = \frac{y^p - 1}{y - 1} = 1 + y + \cdots + y^{p-1},$$

where $y = x^{p^{k-1}}$. In particular, $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$.

Proof. In (5), take $m = p^{k-1}$ and $n = p^k$. The only divisor of n that is not a divisor of m is p^k. The statement follows. $\square$

Example. Let p, q be distinct primes. By 1.5, $x^{pq} - 1 = \Phi_1(x)\Phi_p(x)\Phi_q(x)\Phi_{pq}(x)$. With 1.1, this gives

$$\Phi_{pq}(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}. \tag{6}$$

In particular,

$$\Phi_{2p}(x) = \frac{x^p + 1}{x + 1} = 1 - x + x^2 - \cdots + x^{p-1}.$$

1.8 THEOREM. *For all n, $\Phi_n(x)$ has integer coefficients.*

Proof. Assume that $\Phi_r(x)$ has integer coefficients for all $r < n$. By (4), $x^n - 1 = \Phi_n(x)g_n(x)$, where

$$g_n(x) = \prod_{d|n,\, d<n} \Phi_d(x).$$

Write $\Phi_n(x) = \sum_{r=0}^{m} c_r x^r$ (where $m = \phi(n)$) and $g_n(x) = \sum_{s=0}^{n-m} a_s x^s$. By the induction hypothesis, each a_s is an integer. Also, $a_0 = g_n(0) = -1$. If any of the coefficients c_r are not integers, let c_k be the first one that is not. Then the coefficient of x^k in the product $\Phi_n(x)g_n(x)$ is $c_0a_k + c_1a_{k-1} + \cdots + c_{k-1}a_1 - c_k$, which is not an integer. But this product is $x^n - 1$, so this is a contradiction. □

Alternative proof. By the division algorithm in $\mathbb{Z}[x]$, since $g_n(x)$ is monic, there are polynomials $q(x)$, $r(x)$, with integer coefficients, such that $x^n - 1 = q(x)g_n(x) + r(x)$ and either $r = 0$ or $\deg r < \deg g_n$. So $g_n(x)[\Phi_n(x) - q(x)] = r(x)$, hence $\Phi_n(x) = q(x)$. □

Hence $\Phi_n(a)$ is an integer when a is an integer. Also, for positive integers a and $n \geq 2$,

$$\Phi_n(a) \equiv \Phi_n(0) \equiv 1 \bmod a.$$

Note. It can be shown that $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$, so that (4) is the complete factorisation of $x^n - 1$ in this ring (e.g. [vdW, p. 160–161]). This is important in Galois theory, but not for the topics considered here.

1.9 LEMMA. *If n is odd, then the elements $\{n + 2r : r \in E_n\}$ (considered mod $2n$) comprise E_{2n}.*

Proof. Suppose that $(r, n) = 1$ and that d divides $n + 2r$ and $2n$. Then d is odd, since $n + 2r$ is odd, so d divides n. Hence $d|2r$, so $d|r$. So $d = 1$. Hence $(n + 2r, 2n) = 1$. If $n + 2r \equiv n + 2s \bmod 2n$, then $r \equiv s \bmod n$, so the elements $n + 2r$ ($r \in E_n$) are distinct mod $2n$. Since $\phi(2n) = \phi(n)$, the statement follows. □

1.10. *If $n \geq 3$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$.*

Proof. Recall that $e(\frac{1}{2} + t) = -e(t)$. By the Lemma,

$$\Phi_{2n}(x) = \prod_{r \in E_n} \left[x - e\left(\frac{n + 2r}{2n}\right)\right] = \prod_{r \in E_n} \left[x + e\left(\frac{r}{n}\right)\right].$$

Since $\phi(n)$ is even, this equals $\prod_{r \in E_n}[-x - e(r/n)] = \Phi_n(-x)$. □

Alternatively, one can give an induction proof of 1.10, using 1.5.

Möbius inversion of (4). The expression in (6) can be extended to general n. Recall that the Möbius function μ is defined by $\mu(1) = 1$, $\mu(n) = (-1)^k$ if n is square-free with k prime factors and $\mu(n) = 0$ for other n. The Möbius inversion theorem states: *if $\beta_n = \sum_{d|n} \alpha_d$ for all $n \geq 1$, then $\alpha_n = \sum_{d|n} \beta_d \mu(n/d)$ for $n \geq 1$.* By applying this to $\log a_n$ and $\log b_n$, we deduce: if $a_n > 0$ and $b_n = \prod_{d|n} a_d$ for all n, then $a_n = \prod_{d|n} b_d^{\mu(n/d)}$ for all n. So (4) can be inverted as follows:

1.11 THEOREM. *For all $n \geq 1$ and $x \neq \pm 1$,*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{7}$$

Proof. This follows in the way just stated for $x > 1$, since then $x^d - 1 > 0$ for each d. The statement can be rewritten in the form $\Phi_n(x)Q(x) = P(x)$, where $P(x)$ and $Q(x)$ are polynomials. Since it holds for $x > 1$, it holds for all real x. □

A variant, valid also when $x = 1$, is as follows: let $f_n(x) = 1 + x + \cdots + x^{n-1}$ $(n \geq 2)$ and $f_1(x) = 1$. By Möbius inversion of 1.6, with $\Phi_1(x)$ replaced by 1, we have for $n \geq 2$:

$$\Phi_n(x) = \prod_{d|n} f_d(x)^{\mu(n/d)}.$$

We can now show that once Φ_n is known for square-free values of n, it can be derived for other n by a simple substitution.

1.12 THEOREM. *Let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$. Write $p_1 p_2 \dots p_r = n_0$ and $n_1 = n/n_0$. Then $\Phi_n(x) = \Phi_{n_0}(x^{n_1})$.*

Proof. The divisors of n_0 are the numbers $d = \prod_{j=1}^r p_j^{\varepsilon_j}$, with each ε_j in $\{0, 1\}$. Denote this set of divisors by d. Then

$$\Phi_{n_0}(x) = \prod_{d \in D} (x^d - 1)^{\mu(n_0/d)}.$$

The divisors e of n that have $\mu(n/e) \neq 0$ are the numbers $\prod_{j=1}^r p_j^{a_j}$ with $a_j \geq k_j - 1$ for each j. These are exactly the numbers $n_1 d$ $(d \in D)$, and $n/n_1 d = n_0/d$. Hence

$$\Phi_n(x) = \prod_{d \in D} (x^{n_1 d} - 1)^{\mu(n_0/d)} = \Phi_{n_0}(x^{n_1}). \qquad \square$$

1.13 COROLLARY. *If p is prime and does not divide m, then*

$$\Phi_{mp^k}(x) = \Phi_{mp^{k-1}}(x^p) = \Phi_{mp}(x^{p^{k-1}}).$$

Proof. Let $mp^{k-1} = n$, $mp^k = n'$ and write $n = n_0 n_1$ and $n' = n_0' n_1'$ as in 1.12. Then $n_0' = n_0$ and $n_1' = p n_1$. By 1.12, $\Phi_{n'}(x) = \Phi_n(x^p)$. The second equality follows by iteration, or similarly. □

In particular, $\Phi_{4m}(x) = \Phi_{2m}(x^2)$ (and so is an even function) for any m.

Example. Let p, q be distinct primes. Then $\Phi_{p^k q}(x) = \Phi_{pq}(y)$, where $y = x^{p^{k-1}}$. In particular, $\Phi_{2p^k}(x) = (y^p + 1)/(y + 1)$. Also, $\Phi_{2^k q}(x) = (y^q + 1)/(y + 1)$, where $y = x^{2^{k-1}}$.

With the results now at our disposal, we can write down $\Phi_n(x)$ for a selection of values of n:

n	$\Phi_n(x)$	n	$\Phi_n(x)$
1	$x-1$	9	x^6+x^3+1
2	$x+1$	10	$x^4-x^3+x^2-x+1$
3	x^2+x+1	12	x^4-x^2+1
4	x^2+1	16	x^8+1
5	$x^4+x^3+x^2+x+1$	18	x^6-x^3+1
6	x^2-x+1	20	$x^8-x^6+x^4-x^2+1$
8	x^4+1	72	$x^{24}-x^{12}+1$

Example. The factorisation of x^6-1 given by (4) is

$$(x-1)(x+1)(x^2+x+1)(x^2-x+1).$$

To determine $\Phi_n(x)$ when n has two or more odd prime factors, one has to calculate coefficients, as in the following example.

Example. Determine $\Phi_{15}(x)$. Denote it by $\sum_{r=0}^{8} c_r x^r$. By (6),

$$(c_8x^8+c_7x^7+\cdots+c_1x+c_0)(x^3-1)(x^5-1)=(x^{15}-1)(x-1).$$

Equating coefficients, we find $c_0=1,\ c_1=-1,\ c_2=0,\ c_3=c_0=1,\ c_4=c_1=-1$. By 1.3, $c_{8-r}=c_r$. Hence

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

Another deduction from 1.11 is the following identity, which turns out to be very useful:

1.14 PROPOSITION. *If p is prime, p does not divide m and $k\geq 1$, then for all x,*

$$\Phi_{mp^k}(x)=\frac{\Phi_m(x^{p^k})}{\Phi_m(x^{p^{k-1}})}.$$

Proof. Write $mp^k=n$. The divisors j of n with $\mu(n/j)\neq 0$ are the numbers dp^k and dp^{k-1} for divisors d of m. So $\Phi_n(x)=P_1(x)P_2(x)$, where

$$P_1(x)=\prod_{d|m}(x^{dp^k}-1)^{\mu(m/d)}=\Phi_m(x^{p^k}),$$

$$P_2(x)=\prod_{d|m}(x^{dp^{k-1}}-1)^{\mu(pm/d)}=\frac{1}{\Phi_m(x^{p^{k-1}})},$$

since $\mu(pm/d)=-\mu(m/d)$. The statement is a polynomial identity, valid for all real x. □

1.15. *For $n \geq 2$,*

$$\Phi_n(1) = \begin{cases} p & \text{if } n = p^k \text{ } (p \text{ prime}, k \geq 1), \\ 1 & \text{otherwise.} \end{cases}$$

Proof. The statement for $n = p^k$ is clear from 1.7. Otherwise, n can be expressed as mp^k with $p \nmid m$ and $m > 1$, $k \geq 1$. By 1.14,

$$\Phi_n(1) = \frac{\Phi_m(1)}{\Phi_m(1)} = 1. \qquad \square$$

We sketch two alternative proofs, both illuminating.

Proof 2. By 1.12, it is enough to show that $\Phi_n(1) = 1$ for n of the form $p_1 p_2 \dots p_k$, where $k \geq 2$. Assume this for lower values of k. By 1.6, $\prod_{d|n, d>1} \Phi_d(1) = n$. Now $\Phi_{p_j}(1) = p_j$, and by hypothesis, these are the only proper divisors d of n with $\Phi_d(1) \neq 1$. So the stated product is $p_1 p_2 \dots p_k \Phi_n(1) = n\Phi_n(1)$, hence $\Phi_n(1) = 1$. $\square$

Proof 3. By the variant of 1.11, $\Phi_n(1) = \prod_{d|n} d^{\mu(n/d)}$, so $\log \Phi_n(1) = \sum_{d|n} \mu(n/d) \log d$. A well-known convolution identity equates this to the von Mangoldt function $\Lambda(n)$, defined by: $\Lambda(p^k) = \log p$ for prime p and $\Lambda(n) = 0$ for other n. $\square$

Since $\Phi_n(x)$ is strictly increasing for $x \geq 1$, it follows that $\Phi_n(x) > 1$ for all $x > 1$.

Recall that $\Phi_n(x) = x^m \Phi_n(1/x)$. By differentiation, one finds that $\Phi_n'(1) = \frac{1}{2} m \Phi_n(1)$.

1.16. *For integers $a \geq 1$ and $n \geq 2$, $\Phi_n(a)$ is odd unless $n = 2^k$ and a is odd.*

Proof. If a is even, then $\Phi_n(a)$ is odd, since it is congruent to 1 mod a. If a is odd, then $\Phi_n(a) \equiv \Phi_n(1) \bmod 2$. By 1.15, $\Phi_n(1)$ is odd except when $n = 2^k$. $\square$

We now restate identity (7) in a more specific form, concentrating on square-free n: let $n = p_1 p_2 \dots p_k$, where $p_1 < p_2 < \dots < p_k$, with $k \geq 2$ and $p_1 \geq 3$ (for $p_1 = 2$, then apply 1.10). Let D, E respectively be the set of products of even and of odd numbers of the p_j. Then D and E each have 2^{k-1} members, because $\sum_{r=0}^{k} (-1)^r \binom{k}{r} = (1-1)^k = 0$. Let

$$P(x) = \prod_{d \in D} (x^d - 1), \qquad Q(x) = \prod_{e \in E} (x^e - 1).$$

Then $\Phi_n(x)$ equals $P(x)/Q(x)$ if k is even and $Q(x)/P(x)$ if k is odd.

We can deduce some information about the first (and last) few coefficients:

1.17. *Let $n = p_1 p_2 \dots p_k$ as above, and let $\Phi_n(x) = \sum_{r=0}^{m} c_r x^r$. Then $c_0 = 1$ and:*

(i) *if k is even, then $c_1 = -1$, $c_r = 0$ for $2 \le r < p_1$, $c_{p_1} = 1$, $c_{p_1+1} = -1$;*

(ii) *if k is odd, then $c_r = 1$ for $1 \le r < p_1$ and $c_{p_1} = c_{p_1+1} = 0$.*

Proof. Let $D' = D \setminus \{1\}$. The smallest element of D' is p_1p_2, so

$$P(x) = (x-1)\prod_{d\in D'}(x^d - 1) = 1 - x - x^{p_1p_2} + p(x),$$

where $p(x)$ is composed of higher powers of x. The two smallest elements of E are p_1 and p_2, so $Q(x) = 1 - x^{p_1} - x^{p_2} + q(x)$, where $q(x)$ is composed of higher powers.

If k is even, then $\Phi_n(x)Q(x) = P(x)$. By equating coefficients, we obtain the values stated for $r < p_1$, also $c_{p_1} = c_0 = 1$ and $c_{p_1+1} = c_1 = -1$.

If k is odd, then $\Phi_n(x)P(x) = Q(x)$. For $1 \le r < p_1$, we see that $c_r - c_{r-1} = 0$, so $c_r = c_0 = 1$. Also, $c_{p_1} - c_{p_1-1} = -1$, so $c_{p_1} = 0$, and $c_{p_1+1} - c_{p_1} = 0$. □

Recall from 1.3 that $c_{m-r} = c_r$. So, for example, for even k, $\Phi_n(x)$ is of the form

$$x^m - x^{m-1} + x^{m-p_1} - x^{m-p_1-1} + \cdots - x^{p_1+1} + x^{p_1} - x + 1.$$

The results on c_1 can be summarised in the form $c_1 = -\mu(n)$, since 1.12 shows that $c_1 = 0$ when n is not square-free. Also, it follows from the original definition that $c_{m-1} = -\sum_{k\in E_n} e(k/n)$, so our statement is equivalent to $\sum_{k\in E_n} e(k/n) = \mu(n)$, a special case of the "Ramanujan sum".

Note. From the examples seen so far, one might be led to suppose that the coefficients in $\Phi_n(x)$ are always 1, 0 or -1. However, none of these examples have more than two distinct prime factors. For $n = 3 \times 5 \times 7 = 105$, by solving for coefficients as above, one finds that $c_7 = -2$.

Inequalities for $\Phi_n(x)$.

Recall from 1.2 that for $n \ge 3$, $\Phi_n(x)$ lies between $(x-1)^{\phi(n)}$ and $(x+1)^{\phi(n)}$. With 1.14, this gives the following inequality, which looks rather special, but is just what is needed for the proof of Zsigmondy's theorem in Section 2.

1.18. *Let $n = mp^k$, where p is prime, $k \ge 1$ and p does not divide m. Let $x \ge 2$ and $y = x^{p^{k-1}}$. Then*

$$\left(\frac{y^p - 1}{y+1}\right)^{\phi(m)} < \Phi_n(x) < \left(\frac{y^p+1}{y-1}\right)^{\phi(m)}.$$

Further, $\Phi_n(x) > [y^{p-2}(y-1)]^{\phi(m)}$.

Proof. By 1.14,

$$\Phi_n(x) = \frac{\Phi_m(y^p)}{\Phi_m(y)}.$$

Now $(y-1)^{\phi(m)} < \Phi_m(y) < (y+1)^{\phi(m)}$, and similarly for y^p. The first statement follows. The second statement is derived by noting that $y^p - 1 \geq y^{p-2}(y^2-1)$. □

We now investigate the comparison between $\Phi_n(x)$ and x^m, where $m = \phi(n)$. (Any readers who are more interested in the number-theoretic applications can omit this and move on to section 2.) By 1.2, $\Phi_n(x) \leq (x+1)^m$. We will show that (for $x \geq 2$) this bound can be improved to x^m or $[x/(x-1)]x^m$, depending on whether the number of prime factors of n is even or odd. Since $\Phi_n(x)/x^m = \Phi_n(1/x)$, the statement $\Phi_n(x) < x^m$ for $x \geq 2$ is equivalent to $\Phi_n(x) < 1$ for $0 < x \leq \frac{1}{2}$, and it is rather neater to prove the statement in this second form. We will apply the following simple Lemma to the $P(x)$ and $Q(x)$ introduced above.

1.19 LEMMA. *If $1 \leq n_1 < n_2 < \ldots < n_k$, where $k \geq 2$, then for $0 < x < 1$,*

$$(1-x^{n_1})(1-x^{n_2})\ldots(1-x^{n_k}) > 1 - \frac{x^{n_1}}{1-x}.$$

Proof. It is elementary that if $0 \leq a_j < 1$ for each j, then $(1-a_1)(1-a_2)\ldots(1-a_k) > 1-(a_1+a_2+\cdots+a_k)$. Hence the stated product is greater than

$$1 - x^{n_1} - x^{n_2} - \cdots - x^{n_k} > 1 - x^{n_1}(1+x+x^2+\cdots) = 1 - \frac{x^{n_1}}{1-x}. \quad \square$$

1.20 PROPOSITION. *Suppose that n has k distinct prime factors. Write $\phi(n) = m$. If k is even, then $1 - x < \Phi_n(x) < 1$ for $0 < x \leq \frac{1}{2}$ and*

$$(x-1)x^{m-1} < \Phi_n(x) < x^m \qquad \text{for } x \geq 2.$$

If k is odd, then $1 < \Phi_n(x) < 1/(1-x)$ for $0 < x \leq \frac{1}{2}$ and

$$x^m < \Phi_n(x) < \frac{x^{m+1}}{x-1} \qquad \text{for } x \geq 2.$$

Proof. We prove the statements for $0 < x \leq \frac{1}{2}$: the statements for $x \geq 2$ then follow, by the identity $\Phi_n(x) = x^m\Phi_n(1/x)$. Also, if we can prove the statements for square-free n, the statements for other n then follow, by 1.12 (in fact, $1-x$ can be replaced by $1-x^{n_1}$, in the notation of 1.12). So let $n = p_1p_2\ldots p_k$, where $p_1 < p_2 < \ldots < p_k$. If $k = 1$, so $n = p$ (say), then $\Phi_p(x) = (1-x^p)/(1-x)$, and it is clear that the stated inequalities hold (and that the upper inequality is asymptoticaly optimal). So we assume that $k \geq 2$.

Let D, E, $P(x)$, $Q(x)$ be as in 1.17, but we now write $P(x)$ in the form $\prod_{d\in D}(1-x^d)$. Recall that $\Phi_n(x)$ is $P(x)/Q(x)$ if k is even and $Q(x)/P(x)$ if k is odd. The stated inequalities follow if we can show that $1 - x < P(x)/Q(x) < 1$ for $0 < x \leq \frac{1}{2}$.

Since $1 \in D$, we have $P(x) < 1 - x$. Meanwhile, the smallest member of E is $p_1 \geq 2$, so, by the Lemma,

$$Q(x) > 1 - \frac{x^2}{1-x}.$$

Hence for $0 < x \leq \frac{1}{2}$,

$$Q(x) - P(x) > x - \frac{x^2}{1-x} = \frac{x - 2x^2}{1-x} \geq 0,$$

so $P(x) < Q(x)$.

Also, $Q(x) < 1 - x^{p_1}$. Apart from 1, the smallest member of D is $p_1 p_2$, so, by the Lemma,

$$P(x) > (1-x)\left(1 - \frac{x^{p_1 p_2}}{1-x}\right) = 1 - x - x^{p_1 p_2}.$$

So we will have $P(x) > (1-x)Q(x)$ if $x^{p_1 p_2} < x^{p_1}(1-x)$, or $x^{p_1(p_2-1)} < 1 - x$. Now $p_1(p_2 - 1) \geq 4$, so it is sufficient if $x^4 < 1 - x$, which is satisfied when $0 < x \leq \frac{1}{2}$ (and in fact when $x \leq 0.724$). □

Note. For $k = 2$, it is easily seen from (6) that $1 - x < \Phi_n(x) < 1$ for all x in $(0, 1)$. However, in general the inequalities comparing $\Phi_n(x)$ with 1 do not extend to $(0, 1)$. Indeed, for any $k \geq 2$ (even or odd), we have $\Phi_n(1) = 1$ and $\Phi_n'(1) > 0$, so that $\Phi_n(x) < 1$ on some interval $(1 - \delta, 1)$. Meanwhile, for $n = 210 = 2 \times 3 \times 5 \times 7$, calculation (from (7), assisted by 1.10) shows that $\Phi_n(0.9) > 1$.

In particular, $2^{m-1} < \Phi_n(2) < 2^m$ if k is even and $2^m < \Phi_n(2) < 2^{m+1}$ if k is odd. One can deduce a fact that is quoted sometimes: $\Phi_n(2) > n$ for all n except 1 and 6. This is not really a natural comparison, and we will leave it aside. However, we include the following weaker statement, which can serve as an alternative to 1.18 for the purpose of Zsigmondy's theorem:

1.21. *Let $n \geq 2$ and let p be the largest prime factor of n. Then $\Phi_n(2) \geq p$, with strict inequality except when $n = 6$.*

Proof. It is enough to prove the statement for square-free n. For then if $n = n_0 n_1$ as in 1.12 (with $n_1 > 1$), it follows that $\Phi_n(2) = \Phi_{n_0}(2^{n_1}) > \Phi_{n_0}(2) \geq p$, since $\Phi_{n_0}(x)$ is strictly increasing. If $n = p$ (prime), then $\Phi_p(2) = 2^p - 1 > p$. So assume that $n = p_1 p_2 \ldots p_k$, with $k \geq 2$ and p the largest p_j. Then $\phi(n) \geq p - 1$, so $\Phi_n(2) > 2^{p-2}$, which is greater than p if $p \geq 5$. This leaves only the case $n = 2 \times 3 = 6$, and we note that $\Phi_6(2) = 3$. □

2. Prime factorisation of $\Phi_n(a)$ and number-theoretic applications

We now consider the prime factorisaton of $\Phi_n(a)$. We show that it is closely connected to the order of a modulo these primes. If $(a,p) = 1$, the *order* of a mod p, denoted by $\mathrm{ord}_p(a)$, is the smallest $n \geq 1$ such that $a^n \equiv 1 \bmod p$. Recall: *if* $\mathrm{ord}_p(a) = n$ *and* r *is any positive integer such that* $a^r \equiv 1$ *mod* p*, then* r *is a multiple of* n. By Fermat's little theorem, if p is prime and $\mathrm{ord}_p(a) = n$, then n divides $p-1$, so $p \equiv 1 \bmod n$. .

It is not hard to determine orders using modular arithmetic. As a background to the following results, we record the values of $\mathrm{ord}_p(2)$ and $\mathrm{ord}_p(3)$ for primes $p \leq 41$:

p	3	5	7	11	13	17	19	23	29	31	37	41
$\mathrm{ord}_p(2)$	2	4	3	10	12	8	18	11	28	5	36	20
$\mathrm{ord}_p(3)$	–	4	6	5	3	16	18	11	28	30	18	8

Example. There is no prime p such that $\mathrm{ord}_p(2) = 6$. For then p would have to divide $2^6 - 1 = 63 = 3^2 \times 7$. However, $\mathrm{ord}_3(2) = 2$ and $\mathrm{ord}_7(2) = 3$.

We shall see, as an application of cyclotomic polynomials, that this example is quite exceptional (Zsigmondy's theorem, below). We now start describing the connection. Note first that prime factors of $\Phi_n(a)$ do not divide a, since $\Phi_n(a) \equiv 1 \bmod a$.

2.1. *If* p *is prime and* $\mathrm{ord}_p(a) = n$*, then* p *divides* $\Phi_n(a)$.

Proof. Then p divides $a^n - 1$ and does not divide $a^d - 1$ (so does not divide $\Phi_d(a)$) for any $d < n$. Since $a^n - 1 = \prod_{d|n} \Phi_d(a)$, it follows that p divides $\Phi_n(a)$. □

As a first application, we have the following estimate:

2.2. *Let* $a \geq 2$ *and let* $N(n,a)$ *be the number of primes* p *such that* $\mathrm{ord}_p(a) = n$*. Then*

$$N(n,a) \leq \frac{\phi(n)\log a + 1}{\log(n+1)}.$$

Proof. Let these primes be $p_1, p_2, \ldots, p_k$. Then $p_j \geq n+1$ for each j, and $p_1 p_2 \ldots p_k \leq \Phi_n(a)$. By 1.20, $\Phi_n(a) \leq 2a^{\phi(n)}$. So $(n+1)^k \leq 2a^{\phi(n)}$, hence $k\log(n+1) \leq \phi(n)\log a + 1$. □

Without cyclotomic polynomials, one would obtain a similar estimate with n replacing $\phi(n)$, since clearly $p_1 p_2 \ldots p_k \leq a^n - 1$.

Primes p with $\mathrm{ord}_p(a) = n$ are called *Zsigmondy factors* of $\Phi_n(a)$ (they are also called *primitive* prime factors of $a^n - 1$). Note that they satisfy $p \equiv 1 \bmod n$. We now show that non-Zsigmondy prime factors of $\Phi_n(a)$ can occur. We will make repeated use of the following elementary lemma on congruences;

2.3 LEMMA. *Suppose that p is prime and $a \equiv 1 \bmod p$. Then:*

(i) $(a^p - 1)/(a-1) = 1 + a + \cdots + a^{p-1}$ *is a multiple of p;*

(ii) $a^p \equiv 1 \mod p^2$*;*

(iii) If $p \geq 3$, then $1 + a + \cdots + a^{p-1} \equiv p \mod p^2$ (so is not a multiple of p^2).

Proof. (i), (ii). $1 + a + \cdots + a^{p-1} \equiv p \bmod p$, so is a multiple of p. Also, $a^p - 1 = (a-1)(1 + a + \cdots + a^{p-1})$, in which both factors are multiples of p.

(iii) Let $a = kp+1$. By the binomial theorem, $a^r \equiv 1 + rkp \bmod p^2$. Hence (since $p-1$ is even),

$$\sum_{r=0}^{p-1} a^r \equiv p + kp \sum_{r=0}^{p-1} r = p + \tfrac{1}{2}k(p-1)p^2 \equiv p \mod p^2. \qquad \square$$

Recall that $\Phi_p(a) = 1 + a + \cdots + a^{p-1}$ for prime p. So if $a \equiv 1 \bmod p$ (so that $\mathrm{ord}_p(a) = 1$), then p itself is a factor (but not a Zsigmondy factor) of $\Phi_p(a)$. This remark can be generalised, as follows:

2.4 PROPOSITION. *Suppose that p is prime and $\mathrm{ord}_p(a) = m$. Let $n = mp^k$, where $k \geq 1$. Then p divides $\Phi_n(a)$. However, if $n \geq 3$, then p^2 does not divide $\Phi_n(a)$.*

Proof. We use (7). Let D be the set of divisors d of m with $\mu(m/d) \neq 0$. The divisors j of n with $\mu(n/j) \neq 0$ are dp^k and dp^{k-1} for $d \in D$. Now $(m, p^t) = 1$, so m divides dp^t only when $d = m$. Hence when $d < m$, p does not divide $a^{dp^t} - 1$. By (7), $\Phi_n(a)$ is of the form

$$\frac{b^p - 1}{b - 1} \prod_{d \in D,\, d<m} \frac{f_d(a)}{g_d(a)},$$

where $b = a^{mp^{k-1}}$ and the terms $f_d(a)$, $g_d(a)$ are not multiples of p. Now $b \equiv 1 \bmod p$, so by 2.3(i), $(b^p - 1)/(b-1)$ is a multiple of p. So p divides $\Phi_n(a)$.

By 2.3(iii), if $p \geq 3$, then p^2 does not divide $(b^p - 1)/(b-1)$, so p^2 does not divide $\Phi_n(a)$. This statement also holds when $p = 2$ and $n > 2$: then $m = 1$, so $n = 2^k$ for some $k \geq 2$, and $\Phi_n(a) = a^{2^{k-1}} + 1$. Now $r^2 \equiv 1 \bmod 4$ for odd r, so $\Phi_n(a) \equiv 2 \bmod 4$. $\square$

Note 1. For p, m, n as in 2.4, m divides $p-1$, so p is the largest prime factor of n.

Note 2. The second statement in 2.4 fails for $n = 2$ (so $p = 2$, $m = 1$): $\Phi_2(7) = 8 = 2^3$.

Note 3. Under the hypotheses of 2.4, p divides $\Phi_{mp^r}(a)$ for $0 \leq r \leq k$, so p^{k+1} divides $a^n - 1$ (however, this can be proved quite easily without cyclotomic polynomials).

Note 4. By a well-known result in number theory, if m divides $p-1$, then the condition

$\mathrm{ord}_p(a) = m$ is satisfied by exactly $\phi(m)$ values of a mod p. For example, $\mathrm{ord}_5(a) = 4$ if a is congruent to 2 or 3 mod 5.

We now establish a very striking fact: non-Zsigmondy prime factors of $\Phi_n(a)$ only occur in the way described in 2.4, so that for a given n, there is at most one such factor, the largest prime factor of n. Consider first the special case $n = p$. Let q be a non-Zsigmondy prime factor of $\Phi_p(a)$. Then $a^p \equiv 1 \bmod q$, so $\mathrm{ord}_q(a)$ divides p. By assumption, it is not p, so it is 1, hence $a \equiv 1 \bmod q$. Hence

$$\Phi_p(a) = 1 + a + \cdots + a^{p-1} \equiv p \mod q.$$

Since $\Phi_p(a)$ is a multiple of q, it follows that $q = p$: the only possible non-Zsigmondy factor of $\Phi_p(a)$ is p itself, and it is a factor exactly when $a \equiv 1 \bmod p$.

This reasoning can be adapted without too much trouble to the general case. The neat version given here is due to Roitman [Roi].

2.5 THEOREM. *Let $n \geq 2$, $a \geq 2$. Let p be the largest prime factor of n, and let $n = mp^k$. Then:*

(i) p is a prime factor of $\Phi_n(a)$ iff $\mathrm{ord}_p(a) = m$ (in which case m divides $p - 1$);

(ii) all other prime factors q of $\Phi_n(a)$ have $\mathrm{ord}_q(a) = n$ (hence $q \equiv 1 \bmod n$).

Proof. We prove the statements together. Let q be a prime factor of $\Phi_n(a)$ with $\mathrm{ord}_q(a) = s < n$. Then $a^n \equiv 1 \bmod q$, so s divides n. Also, s divides $q - 1$. Let r be a prime factor of n/s, and write $n/r = h$. Then s divides h, so $a^h \equiv 1 \bmod q$. Write $a^h = c$. By (5), $\Phi_n(a)$ divides

$$\frac{a^n - 1}{a^h - 1} = \frac{c^r - 1}{c - 1} = 1 + c + \cdots + c^{r-1},$$

which is congruent to r mod q, since $c \equiv 1 \bmod q$. But it is a multiple of q, so $r = q$. So q is the *only* prime factor of n/s, hence $n = sq^k$ for some $k \geq 1$. Since s divides $q - 1$, this shows that q is the largest prime factor of n, so $q = p$ and $s = m$. So p is the only possible non-Zsigmondy factor of $\Phi_n(a)$, and if it is one, then $\mathrm{ord}_p(a) = m$. The converse was shown in 2.4. □

Example. Since $\Phi_4(a) = a^2 + 1$, the case $n = 4$ in 2.5 reproduces the well-known fact that any odd prime factor of $a^2 + 1$ is congruent to 1 mod 4.

2.6 COROLLARY. *If q is a prime factor of $\Phi_n(a)$, then the following statements are equivalent: (i) $\mathrm{ord}_q(a) = n$, (ii) q does not divide n, (iii) $q \equiv 1$ mod n.* □

2.7 COROLLARY. *For $k \geq 1$, every prime factor q of $\Phi_n(kn)$ is congruent to* 1 mod n.

Proof. Since $\Phi_n(kn) \equiv 1 \bmod kn$, q does not divide n. By 2.6, $q \equiv 1 \bmod n$. □

This corollary has a pleasant application to prime numbers:

2.8. *For every $n \geq 2$, there are infinitely many primes congruent to* 1 mod n.

Proof. First, let p_1 be a prime factor of $\Phi_n(n)$. Then $p_1 \equiv 1 \bmod n$. Having found primes $p_1, p_2, \ldots, p_r$ congruent to 1 mod n, let $N = np_1p_2 \ldots p_r$, and choose a prime factor q of $\Phi_n(N)$. Then $q \equiv 1 \bmod n$, and $q \not| N$, so $q \neq p_j$ for each j. □

Probably the most important application of cyclotomic polynomials is the next result, usually known as Zsigmondy's theorem, though in fact it was first proved by Bang in 1886.

2.9 THEOREM. *For every $a \geq 2$ and $n \geq 3$ except the case $a = 2$, $n = 6$, there exists at least one prime q such that* $\mathrm{ord}_q(a) = n$. *Equivalently, there is a Zsigmondy factor of* $\Phi_n(a)$.

Proof 1, using 1.21. Assume, for a particular a and n, that there is no such q. Let p be the largest prime factor of n. By 2.5 and 2.4, p is the only prime factor of $\Phi_n(a)$ and p^2 does not divide $\Phi_n(a)$, so in fact $\Phi_n(a) = p$. In 1.21, we saw that if $a = 2$, this only occurs when $n = 6$. Since Φ_n is strictly increasing, it never occurs with $a \geq 3$. □

Proof 2, using 1.18. Assume there is no such q. Again, it follows that $\Phi_n(a) = p$; further, $n = p^k m$, where m divides $p - 1$.

If $p = 2$, then $n = 2^k$, where $k \geq 2$, so $\Phi_n(a) = a^{2^{k-1}} + 1 > 2$, a contradiction.

Now suppose that $p \geq 3$. By 1.18, $\Phi_n(a) > b^{p-2}$, where $b = a^{p^{k-1}}$. So we require $b^{p-2} < p$. For $p \geq 5$, this does not occur for any $b \geq 2$. For $p = 3$, it occurs only for $b = 2$, which implies that $a = 2$ and $k = 1$. Also m is 1 or 2, so n is 3 or 6. However, $\Phi_3(2) = 7$, which is not a factor of 3 (or we can just note that $\mathrm{ord}_7(2) = 3$). So $a = 2$, $n = 6$ is the only case in which there is no Zsigmondy factor. □

Note on the case $n = 2$: This case is easily handled. To have $\mathrm{ord}_q(a) = 2$ for some prime $q > 2$, we require q to divide $a^2 - 1 = (a+1)(a-1)$ but not $a-1$, hence q must divide $a + 1$. Clearly, such a q exists provided that a is not of the form $2^k - 1$.

Zsigmondy (in 1892) established a more general version of the theorem in which $a^n - 1$ is replaced by $a^n - b^n$.

Let us call a number *pure* (not a standard term) if it is of the form mp^k, where p is prime and m divides $p - 1$, and *impure* otherwise. Clearly, if n is impure, then for all a,

every prime factor of $\Phi_n(a)$ is a Zsigmondy factor. Many numbers are impure, for example any of the form $p^j q^k$, where $p < q$ and p^j does not divide $q-1$ (e.g. 12, 15, 28, 36).

Some examples of pure numbers are those of the form p^k, $2p^k$, 4.5^k. For $n = p^k$, the condition $\mathrm{ord}_p(a) = m$ equates to $a \equiv 1 \bmod p$, and for $n = 2p^k$, it equates to $a \equiv -1 \bmod p$. Rather simpler proofs of 2.4 and 2.5 can be given for these two cases.

We illustrate these facts by the first few values of $\Phi_6(a) = a^2 - a + 1$. In accordance with the remarks above, 3 is a prime factor exactly when $a \equiv 2 \bmod 3$, and all other prime factors are congruent to 1 mod 6.

a	$\Phi_6(a)$	a	$\Phi_6(a)$	a	$\Phi_6(a)$
1	1	5	$21 = 3 \times 7$	9	73
2	3	6	31	10	$91 = 7 \times 13$
3	7	7	43	11	$111 = 3 \times 37$
4	13	8	$57 = 3 \times 19$	12	$133 = 7 \times 19$

For further illustration, we list the values of $\Phi_n(2)$ and $\phi_n(3)$ (in factorised form) for selected small values of n. We record the largest prime factor of n, denoted as before by p.

n	p	$\Phi_n(2)$	$\Phi_n(3)$	n	p	$\Phi_n(2)$	$\Phi_n(3)$
2	2	3	2^2	10	5	11	61
3	3	7	13	11	11	23×89	23×3851
4	2	5	2×5	12	3	13	73
5	5	31	11^2	14	7	43	547
6	3	3	7	15	5	151	4561
7	7	127	1093	16	2	257	$2 \times 17 \times 193$
8	2	17	2×41	18	3	3×19	19×37
9	3	73	757	20	5	5×41	5×1181

Note from the example $\Phi_5(3) = 11^2$ that Zsigmondy factors, unlike non-Zsigmondy factors, can appear squared.

Example. To find $\Phi_{48}(2)$ and factorise it: By 1.12, $\Phi_{48}(x) = \Phi_6(x^8) = x^{16} - x^8 + 1$, hence $\Phi_{48}(2) = 65281$. Any prime factors must be congruent to 1 mod 48. The first candidate is 97, and we find that $65281 = 97 \times 673$.

Write $\Phi_n^*(a)$ for $\Phi_n(a)$ with any non-Zsigmondy factors removed. In other words, if $n = mp^k \geq 3$ and p divides $\Phi_n(a)$, then $\Phi_n^*(a) = \Phi_n(a)/p$, otherwise $\Phi_n^*(a) = \Phi_n(a)$. This is not a new polynomial, since (for a given n), the division by p occurs only for certain values of a. All prime factors q of $\Phi_n^*(a)$ have $\mathrm{ord}_q(a) = n$, so that $q \equiv 1 \bmod n$. Hence $\Phi_n^*(a) \equiv 1 \bmod n$, and if $m \neq n$, $\Phi_m^*(a)$ and $\Phi_n^*(a)$ have no prime factors in common, so are coprime.

Application to pseudoprimes

Fix $a > 1$. We write $F(a)$ for the set of positive integers m such that $a^{m-1} \equiv 1 \bmod m$. By Fermat's theorem, $F(a)$ includes all primes that are not divisors of a. Note that if $m \in F(a)$, then $(a, m) = 1$. A *composite* member of $F(a)$ is called an *a-pseudoprime*. We denote the set of such numbers by $PS(a)$.

If, for some n, we know that m divides $a^n - 1$ and $m \equiv 1 \bmod n$, then $m \in F(a)$, since $a^n \equiv 1 \bmod m$ and $m - 1$ is a multiple of n. These conditions are satisfied by $m = \Phi_n^*(a)$ (and its divisors), so we have:

2.10. *For all $a \geq 2$ and $n \geq 2$, we have $\Phi_n^*(a) \in F(a)$, so is in $PS(a)$ if it is composite. The same applies to any composite divisor of $\Phi_n^*(a)$.* □

In particular, if p is prime and does not divide $a - 1$, then by 2.5, $\Phi_p^*(a) = \Phi_p(a) = (a^p - 1)/(a - 1)$, and this number belongs to $F(a)$. Similarly for $\Phi_{2p}(a) = (a^p + 1)/(a + 1)$ if p does not divide $a + 1$. These facts were observed by Cipolla in 1904.

For readers familiar with the notion, we mention that $\Phi_n^*(a)$ is actually a *strong a*-pseudoprime if composite, since a has the same order n modulo each of its prime factors.

The following further result was also noted by Cipolla in the case $n = p$.

2.11. *If $n \geq 3$ is odd, then $\Phi_n^*(a)\Phi_{2n}^*(a) \in PS(a)$ except in the case $a = 2$, $n = 3$.*

Proof. By (4), the stated product divides $a^{2n} - 1$. Now $\Phi_n^*(a) \equiv 1 \bmod n$ and is odd (by 1.16), so $\Phi_n^*(a) \equiv 1 \bmod 2n$. By 2.9, both factors are greater than 1. □

Example. The cases $n = 5$, 7, 9 give the 2-pseudoprimes 11×31, 43×127, 19×73.

Of course, it follows that there are infinitely many a-pseudoprimes for each $a \geq 2$. We now describe a refinement in which the number of prime factors is specified. It was first proved for the case $a = 2$ by Erdös in 1949.

With a fixed, write $m(p) = \mathrm{ord}_p(a)$. Consider a square-free number $n = p_1 p_2 \ldots p_k$. Write $n/p_j = r_j$. Clearly, $n \in PS(a)$ if and only if $a^{n-1} \equiv 1 \bmod p_j$, equivalently, $m(p_j)$ divides $n - 1$, for each j. Further, this condition is equivalent to $m(p_j)$ dividing $r_j - 1$ for each j, since $m(p_j)$ divides $p_j - 1$ and $n - 1 = p_j r_j - 1 = (p_j - 1)r_j + (r_j - 1)$.

2.12 PROPOSITION. *For every $a \geq 2$ and $k \geq 2$, there are infinitely many square-free a-pseudoprimes with k prime factors.*

Proof. First we prove the case $k = 2$. Let p (≥ 3) be a prime not dividing $a - 1$ or $a + 1$. Choose prime factors q_1 of $\Phi_p(a)$ and q_2 of $\Phi_{2p}(a)$. By 2.5, $q_1 \equiv 1 \bmod p$, hence also mod $2p$, and $q_2 \equiv 1 \bmod 2p$. Further, $q_1 q_2$ divides $a^{2p} - 1$, so $q_1 q_2 \in PS(a)$. Since $m(q_1) = p$, a different such pseudoprime is obtained for each p.

Now assume the statement for a particular k. Take $n = q_1 q_2 \dots q_k \in PS(a)$. Then $m(q_j)$ divides $n - 1$ for each j. By Zsigmondy's theorem, there is a prime q with $m(q) = n - 1$. Then $n - 1$ divides $q - 1$, so $m(q_j)$ divides $qn - 1 = q(n - 1) + (q - 1)$. So by the criterion stated above, $qn \in PS(a)$. Also, $q > n$, from which it is easily seen that a different choice of n will generate a different qn. This proves the statement for $k + 1$. □

Application to Wieferich primes

Fix $a \geq 2$. If p is prime and not a divisor of a, then by Fermat's little theorem, $a^{p-1} \equiv 1 \bmod p$. How many primes satisfy the stronger condition that $a^{p-1} \equiv 1 \bmod p^2$? This is equivalent to p^2 being a-pseudoprime. For $a = 2$, such primes are known as *Wieferich primes*, and they do not occur frequently: computation has shown that there are only two less than 10^9, namely 1093 and 3511. For $a = 3$, it is easily seen that the condition is satisfied by $p = 11$, but the second example is 1,006,003 [Rib, p. 347]. It has not been proved that there are infinitely many Wieferich primes, or even (despite their apparent preponderance) that there are infinitely many non-Wieferich primes.

Without offering any progress on these questions, we show how they can be rephrased in terms of cyclotomic polynomials. We need the following lemma, which is well-known in the context of pseudoprimes:

2.13 LEMMA. *If p is prime, $a^{p-1} \equiv 1 \bmod p^2$ and $\operatorname{ord}_p(a) = n$, then $a^n \equiv 1 \bmod p^2$.*

Proof. Then $a \equiv a^p \bmod p^2$, so $a^n \equiv a^{pn} \bmod p^2$. But $a^n \equiv 1 \bmod p$, so by Lemma 2.3, $a^{pn} \equiv 1 \bmod p^2$. □

2.14. *Suppose that p is prime and not a divisor of a. Let $\operatorname{ord}_p(a) = n$. Then the following statements are equivalent:*

(i) $a^{p-1} \equiv 1 \bmod p^2$,

(ii) p^2 *divides* $\Phi_n(a)$.

Proof. If (ii) holds, then $a^n \equiv 1 \bmod p^2$. But n divides $p - 1$, so (i) holds.

Conversely, assume (i). Then, by the Lemma, p^2 divides $a^n - 1$. Since $\operatorname{ord}_p(a) = n$, p does not divide $\Phi_d(a)$ for any $d < n$. Since $a^n - 1 = \prod_{d|n} \Phi_d(a)$, it follows that p^2 divides $\Phi_n(a)$. □

Hence all the Zsigmondy factors of $\Phi_n(2)$ (for any n) that do not appear squared are non-Wieferich primes. From our table of values, we see that these include, for example,

$$11,\ 13,\ 17,\ 19,\ 23,\ 31,\ 41,\ 43,\ 73,\ 89,\ 127,\ 151,\ 257.$$

To show that there are infinitely many non-Wieferich primes, it would be sufficient to show that there are infinitely many values of n for which such factors occur.

References

[Rib] P. Ribenboim, *The New Book of Prime Number Records*, Springer (1995).

[Roi] Moishe Roitman, On Zsigmondy primes, *Proc. Amer. Math. Soc.* **125** (1997) 1913–1919.

[vdW] B.L. van der Waerden, *Modern Algebra, vol. 1*, Frederick Ungar (1949).