Cyclotomic Polynomials and Primitive Roots

1 Cyclotomic Polynomials

We recall that the Möebius function is defined by setting for any integer m

$$\mu(m) = \begin{cases} (-1)^k & \text{if } m \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases} \tag{1.1}$$

For instance the following table gives first ten values of μ

m	1	2	3	4	5	6	7	8	9	10
$\mu(m)$	1	-1	-1	0	-1	1	-1	0	0	1

It is customary to define a partial order on the natural numbers by setting $d \preceq n$ if and only if d divides n. Sometimes the symbol "|" is used instead of "$\preceq$". The importance of the Möebius function derives from the following basic result.

Theorem 1.1 *If $\{A_n\}_{n\geq 1}$ and $\{B_n\}_{n\geq 1}$ are two sequences of numbers related by the equations*

$$B_n = \sum_{d\preceq n} A_d \quad \forall n \geq 1, \tag{1.2}$$

then $\forall n \geq 1$,

$$A_n = \sum_{m\preceq n} B_m \mu(n/m) \tag{1.3}$$

and conversely if the relation 1.3 holds then 1.2 must hold as well.

Proof

Note that if we set $B_m = \sum_{d\preceq m} A_d$ in the right hand side of 1.3 it becomes

$$\sum_{m\preceq n} \left(\sum_{d\preceq m} A_d \right) \mu(n/m).$$

Changing order of summation this can be rewritten as

$$\sum_{d} A_d \left(\sum_{d\preceq m\preceq n} \mu(n/m) \right) \tag{1.4}$$

Now it develops that for any two integers $d \preceq n$ we have

$$\sum_{d\preceq m\preceq n} \mu(n/m) = \begin{cases} 1 & if \text{d=n} \\ 0 & otherwise \end{cases} \tag{1.5}$$

The reason for this is that if $d \preceq m \preceq n$ then we can write $m = dm'$ and $n = dn'$ which allows us to cancel the common factor d and rewrite this sum as

$$\sum_{m'\preceq n'} \mu(n'/m'). \tag{1.6}$$

Clearly, when $d = n$ then $n' = 1$ and this sum reduces to the single term $\mu(1) = 1$. This gives the first case of 1.5. On the other hand when d is strictly less than n, then in 1.6 the sum runs over all divisors of n' which only have distinct prime factors. Since those that have a even number of such factors contribute a 1 to the sum and those that have an odd number of such factors contribute a -1 and there is an equal number of each, their contributions do cancel out completely, yielding the second case of 1.5. We can now use 1.5 in 1.4 and see that the sum there reduces to the single term A_n, yielding the desired identity 1.3.

If an integer n has the factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, \ldots, p_k$ are distinct primes then it is customary to set

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \tag{1.7}$$

This formula defines the so called *Euler ϕ-function* and it gives the the number of integers m in the interval $[1, n]$ that have no factor in common with n. In symbols, we may express this fact by writing

$$\phi(n) = \#\{m \in [1, n] \mid (m, n) = 1\}$$

where as customary the symbol (m, n) denotes the greatest common divisor of m and n. It is not difficult to see that 1.7 may also be rewritten in the form

$$\phi(n) = \sum_{d \preceq n} \mu(d)\frac{n}{d}. \tag{1.8}$$

An example will suffice to convince the reader of the validity of this identity. Let $n = 2^3 3^2 5$. Note that the definition 1.1 gives that $\mu(d)$ vanishes for any d that is divisible by the square of a prime. Thus the only divisors of n that contribute to the sum in the right hand side of 1.8, when $n = 2^3 3^2 5$ are

$$1, 2, 3, 5, 2 \times 3, 2 \times 5, 3 \times 5, 2 \times 3 \times 5$$

Consequently, the right hand side of 1.8 in this case reduces to

$$n\left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2 \times 3} + \frac{1}{2 \times 5} + \frac{1}{3 \times 5} - \frac{1}{2 \times 3 \times 5}\right)$$

However, this may also be rewritten as

$$n\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

which shows that 1.7 and 1.8 are one and the same in this case. The general case can be verified in exactly the same manner.

We recall that a root of unity $\omega = e^{2\pi ir/n}$ is said to *belong to the exponent e* or that *e is the exponent of ω* and write $E(\omega) = e$ if and only if

$$\begin{cases} \omega^e = 1 & \text{and} \\ \omega^s \neq 1 & \text{for any } s < e. \end{cases}$$

We recall that the Cyclotomic polynomial $\Phi_m(x)$ may be defined by setting

$$\Phi_m(x) = \prod_{E(\omega)=m} = (1 - \frac{x}{\omega}). \tag{1.9}$$

The following identities are basic:

Theorem 1.2

$$1 - x^n = \prod_{d \preceq n} \Phi_d(x) \tag{1.10}$$

$$\Phi_n(x) = \prod_{m \preceq n} (1 - x^m)^{\mu(n/m)} \tag{1.11}$$

Proof

Note that if $\omega^n = 1$ then the exponent $E(\omega)$ must divide n, for if not the greatest common divisor $d = (E(\omega), n)$ would be strictly smaller than $E(\omega)$ and since we would also have $\omega^d = 1$ we would contradict the very definition of $E(\omega)$. This given, the first identity is immediate since the the roots of the polynomial $1 - x^n$ are the complex numbers

$$\omega = e^{2\pi i \frac{r}{n}}$$

for $r = 0, 1, \ldots, n-1$ and each must belong to an exponent d which, as we have seen, must necessarily divide n. This remark may be translated in the equalities

$$1 - x^n = \prod_{\omega^n=1} \left(1 - \frac{x}{\omega}\right) = \prod_{d \preceq n} \prod_{E(\omega)=d} \left(1 - \frac{x}{\omega}\right),$$

The last of which is 1.10. To prove 1.11 we equate the logarithms of both sides of 1.10 and get

$$\log(1 - x^n) = \sum_{d \preceq n} \log \Phi_d(x).$$

We can thus use Theorem 1.1 with $A_n = \log \Phi_n(x)$ and $B_n = \log(1 - x^n)$ and derive that

$$\log \Phi_n(x) = \sum_{m \preceq n} \left(\log(1 - x^m)\right) \mu(n/m)$$

and 1.11 follows by equating the exponentials of both sides.

Formula 1.11 gives a practical way to compute a given cyclotomic polynomial. For instance, when $n = 6$ from the above table we get

m	1	2	3	6
n/m	6	3	2	1
$\mu(n/m)$	1	-1	-1	1
$1 - x^m$	$1 - x$	$1 - x^2$	$1 - x^3$	$1 - x^6$

Thus

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

We give below a list of the polynomials $\Phi_{p-1}(x)$ as p runs over the first 14 primes.

$$\begin{aligned}
\Phi_1(x) &= -1 + x \\
\Phi_2(x) &= 1 + x \\
\Phi_4(x) &= 1 + x^2 \\
\Phi_6(x) &= 1 - x + x^2 \\
\Phi_{10}(x) &= 1 - x + x^2 - x^3 + x^4 \\
\Phi_{12}(x) &= 1 - x^2 + x^4 \\
\Phi_{16}(x) &= 1 + x^8 \\
\Phi_{18}(x) &= 1 - x^3 + x^6 \\
\Phi_{22}(x) &= 1 - x + x^2 - x^3 + x^4 - x^5 + x^6 - x^7 + x^8 - x^9 + x^{10} \\
\Phi_{28}(x) &= 1 - x^2 + x^4 - x^6 + x^8 - x^{10} + x^{12} \\
\Phi_{30}(x) &= 1 + x - x^3 - x^4 - x^5 + x^7 + x^8 \\
\Phi_{36}(x) &= 1 - x^6 + x^{12} \\
\Phi_{40}(x) &= 1 - x^4 + x^8 - x^{12} + x^{16} \\
\Phi_{42}(x) &= 1 + x - x^3 - x^4 + x^6 - x^8 - x^9 + x^{11} + x^{12}
\end{aligned}$$

We should point out the following important relation between the Euler ϕ-function and the cyclotomic polynomials.

Theorem 1.3

$$\deg \Phi_n(x) = \phi(n) \tag{1.12}$$

In particular

$$\sum_{d \preceq n} \phi(d) = n \tag{1.13}$$

Proof.

The degree of the polynomial $\Phi_n(x)$ may be computed by adding the degrees of the factors in the numerator of 1.11 and subtracting the degrees of the factors in the denominator. In other words we must have

$$\deg \Phi_n(x) = \sum_{m \preceq n} m\ \mu(n/m),$$

and 1.13 then follows from the identity in 1.8. We also see from formula 1.10 that n, which is the degree of $1 - x^n$ must also be equal to the sum of the degrees of the factors $\Phi_d(x)$ as d varies over the divisors of n. This establishes 1.14 and completes our proof.

2 Primitive Roots

We recall that if p is a prime then from Euler's theorem we get that

$$a^{p-1} \equiv 1(\text{mod}p) \quad (\text{for}a = 1, 2, \ldots, p-1) \tag{2.1}$$

This given, we say that a is a *primitive root* modulo p if and only if

$$a^i \not\equiv 1(\text{for all}i < p-1). \tag{2.2}$$

We have the following basic fact

Theorem 2.1 *If a is a primitive root modulo p then the successive powers*

$$a^1, a^2, \ldots, a^{p-1} \tag{2.3}$$

give, modulo p, a permutation of the integers

$$1, 2, \ldots, p-1 \tag{2.4}$$

Proof.

Since $a^{p-1} = 1$, none of the powers in 2.3 are congruent to 0 modulo p thus each evaluates (mod p) to one of the integers in 2.4. To show that the two sets of numbers in 2.3 and 2.4 are identical we need only check that the integers in 2.3 are all different. However, this must be so, for otherwise we would have two integers $1 \leq i < j \leq p-1$ such that

$$a^i \equiv a^j(\text{mod}p)$$

But then, multiplying by a^{p-1-i} both sides of this relation we would get that

$$a^{j-i} \equiv 1(\text{mod}p)$$

and since, $j - i < p - 1$ this would contradict the assumption that a is a primitive root modulo p. This completes our proof.

We shall make use of the following basic result from number theory, which is proved in exactly the same manner the analogous result is established in the complex number case.

Theorem 2.2 *When p is a prime, a polynomial equation of degree n and integer coefficients*

$$a_o + a_1 x + a_2 x^2 + \cdots + a_n x^n \equiv 0(\text{mod}p)$$

has at most n distinct solutions.

The following is a criterion that helps identify primitive roots at least in the case of sufficiently small primes.

Theorem 2.3 *Each prime p has exactly $\phi(p-1)$ primitive roots. In fact, a is a primitive root (mod p) if and only if*

$$\Phi_{p-1}(a) \equiv 0(\text{mod}p) \tag{2.5}$$

Proof.

If a is any of the integers in 2.4 by Euler's theorem we have

$$0 \equiv 1 - a^{p-1} \mod p$$

making use of formula 1.10, for $n = p-1$ and $x = a$, we can rewrite this in the form

$$0 \equiv \prod_{d \preceq p-1} \Phi_d(a) \mod p.$$

Since p is prime, this equation can hold true if and only if at least one of the factors $\Phi_d(a)$ vanishes mod p. To visually understand the manner in which this factors are vanishing, it is best to represent what happens by means of a table T whose rows are indexed by divisors of $p-1$ and whose columns are indexed by the numbers $1, 2, \ldots, p-1$. Let for a moment, $T_{d,a}$ denote the entry in this table that is at the intersection of the row indexed by the divisor d and the column indexed by a. This given, let us set

$$T_{d,a} = \begin{cases} 1 & if \Phi_d(a) \equiv 0 \mod p \\ 0 & if \Phi_d(a) \not\equiv 0 \mod p \end{cases}$$

Clearly, the number of ones in the row indexed by d, (by theorem 2.2), cannot exceed the degree of $\Phi_d(x)$. This gives (in view of 1.13)

$$\sum_{a \in [1,p-1]} T_{d,a} \leq \deg \Phi_d(x) = \phi(d).$$

Now, formula 1.14 with $n = p-1$ gives

$$\sum_{d \preceq p-1} \phi(d) = p - 1$$

Therefore we must conclude that

$$\sum_{d \preceq p-1} \sum_{a \in [1,p-1]} T_{d,a} \leq p - 1$$

In other words the total number of ones in the table is at most $p-1$. On the other hand, since as we have noted, each $a = 1, 2, \ldots, p-1$ must satisfy one of the equations $\Phi_d(x) \equiv 0$, there must be:

at least one entry equal to 1 **in each column!** $(*)$

This gives

$$\sum_{a \in [1,p-1]} \sum_{d \preceq p-1} T_{d,a} \geq p - 1$$

These two inequalities have the following two immediate consequences:

1. There is exactly one entry equal to 1 in each column,
2. The row indexed by d has exactly $\phi(d)$ entries equal to 1

Indeed, from (*), we deduce that the negation of (1) forces the number of 1's to be greater than $p-1$ while the negation of (2) forces the number of 1's to be less than $p-1$. In particular, from (2) (for $d = p-1$) we deduce that exactly $\phi(p-1)$ of the numbers $a = 1, 2, \ldots, p-1$ are solutions of

$$\Phi_{p-1}(x) \equiv 0 \mod p. \tag{2.6}$$

To complete the proof we need only show that the primitive roots coincide with the solutions of this equation. To this end note that if a is not a primitive root mod p then it must satisfy an equation $1 - a^r \equiv 0 \pmod{p}$ with some $r < p-1$. This given, from 1.10 with $n = r$ and $x = a$ we derive that $\Phi_d(a) \equiv 0$ for some divisor d of r. This forces $T_{d,a} = 1$. Since $d \leq r < p-1$, we deduce from (1) above, that there can be no 1 at the intersection of this column with the row indexed by $p-1$. In other words a cannot be a solution of 2.6. Conversely, if a is a primitive root mod p, then it cannot satisfy any of the equations $\Phi_d(x) \equiv 0 \pmod{p}$ for any $d < p-1$ for otherwise from 1.10 with $x = a$ and $n = d$ we would deduce that $1 - x^d \equiv 0 \pmod{p}$ contradicting the assumption that a is primitive. In summary, the primitive roots and only the primitive roots constitute the $\phi(p-1)$ solutions of 2.6. This completes our proof.

To see an example, let us seek for the primitive roots modulo 7. We may ask if 2 is primitive. The theorem requires that 2 be a solution of $\Phi_6(x) \equiv 0 \pmod 7$. However, we see that

$$\Phi_6(2) = 1 - 2 + 2^2 \equiv 3 \mod 7$$

So 2 is not primitive. Let us try 3. In this case we get

$$\Phi_6(3) = 1 - 3 + 3^2 = 7 \equiv 0 \mod 7$$

and we must conclude that 3 is primitive (mod 7). It develops that in the search for primitive roots we need only find one since all the others can be obtained as powers of it. In fact we have the following result:

Theorem 2.4 *If a is a primitive root* mod p *then the set of primitive roots* mod p *may be constructed as the set of powers*

$$\{a^r \mid (r, p-1) = 1\} \tag{2.7}$$

Proof.

We simply note that the numbers a^r with r relatively prime with $p-1$ must all be primitive. In fact, if the greatest common divisor of r and $p-1$ is 1 the we can find an integer s such that

$$rs \equiv 1 \mod p-1.$$

This gives that if $b = a^r$ then

$$b^s = a^{rs} \equiv a \mod p$$

and if b where not primitive then for some $i < p-1$ we would get

$$1 \equiv (b^i)^s \equiv (b^s)^i \equiv a^i \equiv 1 \mod p$$

which would contradict the primitivity of a. Since the cardinality of the set in 2.7 is given by $\phi(p-1)$ and the number of primitive roots is (by theorem 2.7) also given by $\phi(p-1)$. These two sets must coincide as asserted.

Exercises.

1. Find the cyclotomic polynomial $\Phi_{256}(x)$.
2. Find the smallest primitive root modulo 257
3. Find all primitive roots modulo 19.
4. Solve the equation
$$x^5 \equiv 2 \pmod{19}.$$
5. Solve the equation
$$14x^7 \equiv 11 \pmod{19}$$