CAUCHY'S CYCLOTOMIC FUNCTION AND FUNCTIONAL POWERS*

BY E. T. BELL

1. *Introduction.* Let $\phi(n)$ as usual denote the totient of n. Cauchy's function is the polynomial $F_n(x)$ of degree $\phi(n)$, whose zeros are the primitive nth roots of unity. If $a, b, c, e, \cdots$ are the distinct prime divisors (>1) of n,

$$F_n(x) = N_n(x)/D_n(x), \tag{1}$$

where

$$N_n(x) \equiv (x^n - 1)\prod(x^{n/ab} - 1)\prod(x^{n/abce} - 1) \cdots,$$
$$D_n(x) \equiv \prod(x^{n/a} - 1)\prod(x^{n/abc} - 1) \cdots.$$

An anonymous writer† in L'Intermédiaire des Mathématiciens (vol. 24 (1917), pp. 5–6), stated that $\prod F_d(1) = n$, where d ranges over all divisors of n, also that the value of $F_n(-1)$ is 2 if n is a power of 2, $F_p(1)$ if n is double an odd prime p, but is 1 in all remaining cases. The second part seems to be incorrect. For example, $F_2(x) = x+1$, $F_{18}(x) = x^6 - x^3 + 1$, $F_{50}(x) = x^{20} - x^{15} + x^{10} - x^5 + 1$, and hence for $n = 2, 18, 50$ the respective values of $F_n(-1)$ are 0, 3, 5, not 2, 1, 1 as demanded by the assertion. To obtain in §3 the correct values of $F_n(-1)$ it is convenient to prove in §2 the first result stated, which in turn depends upon a theorem of Trudi, which we shall also prove in §2 as several details of the proof are useful. Finally, in §§4, 5 we connect $F_n(x)$ in a new way with other numerical functions, to illustrate what are here called *functional powers*.

We shall need $G_n(x)$ defined by

$$G_n(x) = M_n(x)/R_n(x), \tag{2}$$

* Presented to the Society, San Francisco Section, June 18, 1927.

† Quoted from the *Report on Algebraic Numbers*, Bulletin of the National Research Council, vol. 5, Part 3, No. 28 (1923), p. 32, where it is also stated that no reply is given in L'Intermédiaire for 1917–19. References to other writers cited here will be found on pp. 31, 32 of the *Report*.

where

$$M_n(x) \equiv (x^n + 1)\prod(x^{n/ab} + 1) \cdots,$$
$$R_n(x) \equiv \prod(x^{n/a} + 1)\prod(x^{n/abc} + 1) \cdots.$$

Hence if $n=2^\alpha m$, m odd, $\alpha>0$, we have

$$(3)\qquad F_m(x^{2^\alpha}) = G_m(x^{2^{\alpha-1}})G_m(x^{2^{\alpha-2}}) \cdots G_m(x)F_m(x).$$

For the same n, α, m, it follows from (1) on resolving each difference of 2 squares into a product of a sum and difference, and comparing with (1), that

$$(4)\qquad F_n(x) = F_m(x^{2^\alpha})/F_m(x^{2^{\alpha-1}}),$$

which is the special case of Dickson's recursion formula (his prime p here $=2$, *Report*, p. 32) which will be required presently.

2. *Proof that* $\prod F_d(n)=1$. Let $\mu(n)$ be Möbius' function; $\mu(1)=1$, $\mu(n)=0$ if n is divisible by a square >1, and in the contrary case $\mu(n)=1$ or -1 according as the number of prime divisors of n is even or odd. Then we may write from (1),

$$(5)\qquad F_n(x) = \prod(x^d - 1)^{\mu(\delta)},$$

where $\prod$ extends to all pairs (d, δ) of conjugate divisors >0 of n, so that $d\delta=n$. If n is divisible by precisely t distinct primes, $\mu(\delta)$ takes the value 1 for exactly

$$\binom{t}{0}+\binom{t}{2}+\binom{t}{4}+\binom{t}{6}+\cdots = 2^{t-1}$$

values of δ, and it takes the value -1 for precisely

$$\binom{t}{1}+\binom{t}{3}+\binom{t}{5}+\cdots = 2^{t-1}$$

values of δ. Hence 2^{t-1} factors $x-1$ may be cancelled in $F_n(x)$ as written in (1) or (5), after which no factor in the numerator or denominator vanishes when $x=1$. Since

$$(x^k - 1)/(x - 1) = x^{k-1} + x^{k-2} + \cdots +x+ 1$$

has the value k when $x=1$, we find, after cancellation as indicated,

$$F_n(1) = \frac{n\prod(n/ab)\cdots}{\prod(n/a)\prod(n/abc)\cdots},$$

and hence, by the same argument as before, we may cancel all n's and get

$$F_n(1) = \frac{\prod(a)\prod(abc)\cdots}{\prod(ab)\prod(abce)\cdots}.$$

Consider all the products j at a time of the t distinct primes $a, b, c, e, \cdots$ and let their product be P. Among these products there are precisely $\binom{t-1}{j-1}$ that contain a given prime, say a; for with a may be taken all products $j-1$ at a time of the remaining $t-1$ primes. By convention $\binom{s}{0}=1$, $s\geqq 0$. Thus each prime factor in all the $\binom{t}{j}$ products occurs precisely $\binom{t-1}{j-1}$ times, and therefore the product of all the $\binom{t}{j}$ products is P^k, $k\equiv\binom{t-1}{j-1}$. In the numerator of $F_n(1)$ the possible values of j are 1, 3, 5, $\cdots$; in the denominator, provided $t>1$, they are 2, 4, 6, $\cdots$. Hence, if $t>1$, $F_n(1)=P^u/P^v$, where $u=v=2^{t-2}$. If $t=1$, we have $n=p^\alpha$, p prime, and from (1),

$$F_n(x) = (x^{p^\alpha}-1)/(x^{p^{\alpha-1}}-1),$$

which after cancellation of $x-1$ as before, gives $F_n(1)$ $=p^\alpha/p^{\alpha-1}=p$. Finally then we have Trudi's result that

$$F_n(1) = 1, \quad \text{or} \quad p, \tag{6}$$

according as n is not or is a power p^α of a prime p.

Let $n=a^\alpha b^\beta \cdots c^\gamma$ be the resolution of n into its prime factors. By (6), among all the divisors d of n only

$$a^A, b^B, \cdots, c^C \quad (0 < A \leqq \alpha, 0 < B \leqq \beta, \cdots, 0 < C \leqq \gamma) \tag{7}$$

give values of d for which $F_d(1)=1$, while for the typical case $d=a^A$, $F_d(1)=a$. Hence from (6), (7),

$$\prod F_\alpha(1) = a^\alpha b^\beta \cdots c^\gamma = n,$$

where $\prod$ refers to all divisors d of n.

3. *Value of* $F_n(-1)$. Referring to (1), and noting that there are the same number of binomial factors in $N_n(x)$, $D_n(x)$, also that $x^m-1=-2$ when m is odd and $x=-1$, we see that

$$(8) \qquad F_m(-1) = 1, \qquad (m \text{ odd}).$$

Henceforth, let $n=2^\alpha m$, m odd, >1. If in (2) we cancel all factors $x+1$ and set $x=-1$ in the result, we get (by §2),

$$(9) \qquad G_m(-1) = F_m(1).$$

Again, if $\alpha=1$, it follows from (4), (3) that

$$(10) \qquad F_{2m}(x) = G_m(x),$$

and hence by (9)

$$(11) \qquad F_{2m}(-1) = F_m(1),$$

the value of which is known from (6). If $\alpha>1$, we see from (4), (3) that

$$(12) \qquad F_n(x) = G_m(x^{2^{\alpha-1}}),$$

which by (10) holds also when $\alpha=1$. Now if $\beta>0$, the value of each binomial factor in $G_n(x^2)^\beta$ for $x=-1$ is 2, and since (see(2)) $M_n(x)$ and $R_n(x)$, by §2, have equal numbers of such factors, it follows from (12) that $F_n(-1)=1$ when $\alpha>1$. There remains only the case $F_s(-1)$, $s=2^\alpha$, $\alpha>0$. We have $F_2(x)=x+1$, $F_2(-1)=0$; while if $\alpha>1$,

$$F_s(x) = (x^{2^\alpha}-1)/(x^{2^{\alpha-1}}-1) = x^{2^{\alpha-1}}+1,$$

and hence $F_s(-1)=2$ for this s.

Hence if $n=2^\alpha\mu$, where $\mu\geqq 1$ is odd, the value of $F_n(-1)$ is 0 if $\alpha=\mu=1$; it is 2 if $\alpha>1$, $\mu=1$; it is p if $\alpha=1$ and $\mu=p^\beta$, $\beta>0$, $p>1$ prime (odd or even); $F_1(-1)=-2$; in all other cases $F_n(-1)=1$.

4. *Functional Powers.* It will be necessary to recall a few definitions and theorems from previous papers. A second theorem of Trudi's ((14) below) is a simple example of

what may be called the extraction of functional roots, for reasons which we now explain.

We call $f(x)$ a *numerical function* of x if $f(1)\neq 0$ and if $f(x)$, for each integral value >0 of x, takes a single finite value. Let $f_j(x)$ $(j=1,\cdots,k)$ be numerical functions, and let $\sum$ refer to all sets $(d_1, d_2, \cdots, d_k)$ of positive integral solutions of $d_1, d_2, \cdots, d_k=n$ for n fixed. Then, as explained in a previous note,* $\sum f_1(d_1)f_2(d_2)\cdots f_k(d_k)$ is written as a *symbolic product* $f_1 f_2\cdots f_k$, called simply the *product* of the numerical functions $f_1, f_2, \cdots, f_k$ with the *parameter* n. Two such products are *equal*, $f=g$, only when the sums which they represent are equal for all values of the parameter, which may therefore be suppressed in the notation. The multiplication thus defined is abstractly identical with that in common algebra, being associative, commutative, and distributive, and having the unique unity ϵ, where $\epsilon(1)=1$, $\epsilon(n)=0$, $n>0$. If f is any given numerical function, there exists a unique numerical function f', called the *reciprocal* of f, such that $ff'=\epsilon$, and we may write $f'\equiv\epsilon/f$. The set of all numerical functions is an abelian group under multiplication as just defined. If only functions having the same parameter are added the set is a field, but the consequences of addition are uninteresting.

In a former paper,† we assigned to f^g, where f, g are numerical functions, the meaning

$$f^g \equiv \prod [f(d)]^{g(\delta)},$$

where the product extends to all pairs (d, δ) of conjugate divisors of the arbitrary constant integer $n>0$. Equality of such functional powers, $f^g=h^k$, where f, g, h, k are numerical functions, is defined as equality for all integers $n>0$ of the corresponding products, and as before we may

---

* This Bulletin, vol. 27 (1921), pp. 273–275. This method was first developed in University of Washington Publications in Science, No. 1, 1915.

† L'Enseignement Mathématique, 1923, pp. 305–308.

omit reference to the parameter n. It was shown that each of the following equalities implies the other,

$$f^g = h^k, \quad f^{gl} = h^{kl},$$

all the letters denoting numerical functions, and gl, kl being products as defined above. Hence the algebra of functional powers is abstractly identical with that of powers in common algebra. In particular then the following are equivalent relations,

$$f^g = h^k, \quad f^{\epsilon/k} = h^{\epsilon/g},$$

and the second is said to be derived from the first by *extracting the* gkth (functional) *root of both members* (or by raising both members to the $\epsilon/(gk)$th power).

In the last paper cited, and from a more comprehensive point of view in another,* I established a triple isomorphism between the several algebraic varieties (fields, rings, rays, etc.) usually considered in arithmetic and the above products $fg \cdots$ and powers f^g on the one hand, and, on the other, with the algebra of polynomials in two indeterminates in an arbitrary field. This isomorphism refers the derivation of relations between given numerical functions $f, g, h, k, \cdots$, such as $fg=hk$, $f^g=h^k$, etc., to identities between the polynomials described. It is mentioned here because the few relations required presently for purposes of illustration were obtained, without computations, by its means; we may assume them known.

5. *Cauchy's Function as a Functional Power.* Understanding the variable x in (1) we consider $F_n(x)$ as a numerical function of n and write $F_n(x) \equiv F_n \equiv F(n)$, and similarly for $X_n(x) \equiv x^n - 1 \equiv X(n)$. Then (5) is equivalent to

$$F = X^{\mu}. \tag{13}$$

* Transactions of this Society, vol. 25 (1923), pp. 135–154.

Let $u(n)=1$ for all integers $n>0$. Then, ϵ being the unit defined in §4, $\mu u=\epsilon$. Hence (13) implies

$$F^u = X^\epsilon \equiv X. \tag{14}$$

In full (14) is $\prod F_d(x)=x^n-1$, where $\prod$ refers to all divisors d of n, a theorem due to Trudi.

It will be of interest to write down a few further consequences of raising (13) to functional powers (including the extraction of roots). Let $w(n)=n$ for all integers $n>0$. Then $\phi=\mu w$ (ϕ as in §1), and hence

$$F^w = X^\phi, \tag{15}$$

or in full,

$$\prod [F(d)]^\delta = \prod [X(d)]^{\phi(\delta)},$$

the products extending to all pairs (d, δ) of conjugate divisors of n. Again, if $k(n)=1$ or 0 according as n is or is not the square of an integer >0, and $\lambda(n)=1$ or -1 according as the total (not the number of distinct) prime divisors of n is even or odd, $\mu k=\lambda$. Hence, raising both members of (13) to the kth power we have

$$F^k = X^\lambda. \tag{16}$$

As a last example (the number may be multiplied indefinitely by the methods indicated), let $\nu(n)=$ the number of divisors of n. Then $\mu\nu=u$, and

$$F^\nu = X^u, \tag{17}$$

which in full is

$$\prod [F(d)]^{\nu(\delta)} = \prod (x^d - 1).$$

Similarly, if we write $G_n(x)\equiv G_n\equiv G(n)$, $Y_n(x)\equiv x^n+1 \equiv Y(n)$, it follows from (2) that (F, X) may be replaced by (G, Y) in (13)–(17) and in any relation of a similar kind.

CALIFORNIA INSTITUTE OF TECHNOLOGY