

an  $x$  such that  $a^{2m}x = a^m$ . Let  $q$  denote an arbitrary primary divisor of  $(a^{2m})$  of index  $m$ . Then also  $a^m \equiv 0 \pmod{q}$  as follows at once from the assumption that  $q$  is of index  $m$ . Hence  $(a^m)$  and  $(a^{2m})$  have precisely the same primary ideal divisors of index  $m$ ; thus, by hypothesis, it follows that  $(a^m) = (a^{2m})$ . That is, there exists an  $x$  such that  $a^{2m}x = a^m$ , and  $a^m$  is regular. Thus  $\mathfrak{R}$  is  $m$ -regular.

We conclude with the following theorem:

**THEOREM 7.** *A necessary and sufficient condition that a commutative ring  $\mathfrak{R}$ , with unit element, be  $m$ -regular is that all direct indecomposable ideals be primary of index  $m$ .\**

It is known<sup>†</sup> that in an arbitrary ring with unit element every ideal is the intersection of its direct indecomposable ideal divisors. If these are all primary of index  $m$ , the preceding theorem shows that  $\mathfrak{R}$  is  $m$ -regular.

Suppose  $\mathfrak{R}$  is  $m$ -regular, and let  $\mathfrak{f}$  be a direct indecomposable ideal in  $\mathfrak{R}$ . Then  $\mathfrak{R}/\mathfrak{f}$  is irreducible and is also  $m$ -regular. Thus, by Theorem 2,  $\mathfrak{R}/\mathfrak{f}$  is a special primary ring and  $\mathfrak{f}$  is therefore a primary ideal in  $\mathfrak{R}$ . Theorem 6 then states that  $\mathfrak{f}$  is of index  $m$ , and the proof is completed.

SMITH COLLEGE

---

## A FORMULA FOR THE COEFFICIENTS OF THE CYCLOTOMIC POLYNOMIAL<sup>‡</sup>

J. E. EATON

Despite the widespread use of the roots of unity in the solution of many mathematical questions, the problem of characterizing the irreducible equation

$$F_n(x) = x^r + a_1x^{r-1} + \dots + a_r = 0$$

whose roots are the primitive  $n$ th roots of unity has received little attention. It is well known that  $r = \phi(n)$ , that  $F_n(1) = p$  for  $n = p^\alpha$  (where  $p$  is a prime) and  $F_n(1) = 1$  otherwise. For  $n$  a power of a prime  $a_i$  is 1 or 0. In 1883 Migotti<sup>§</sup> proved that for  $n$  a product of two primes  $a_i$  is  $\pm 1$  or 0. In 1895 Bang<sup>||</sup> showed that for  $n$  a product of

\* Cf. S, Theorem 10.

† See S, §4.

‡ Presented to the Society, February 26, 1938.

§ Sitzungsberichte der Akademie der Wissenschaften, Vienna, (2), vol. 87 (1883), pp. 7-14.

|| Nyt Tidsskrift for Mathematik, (B), vol. 6 (1895), pp. 6-12.

three primes the absolute value of any coefficient is less than the smallest of the primes.

I. Schur\* in 1931 proved that there exist cyclotomic polynomials with coefficients arbitrarily large in absolute value. Bungers† in 1934 proved the same theorem, under the assumption that there exist infinitely many prime pairs, for  $n$  a product of three primes. In 1936 E. Lehmer‡ modified Bungers' proof so as to eliminate his unproved assumption of the existence of infinitely many prime pairs.

Although these results are extremely interesting, the only information they yield of the nature of the coefficients for an arbitrary  $n$  is that there is no bound on them independent of  $n$ . The purpose of this note is to derive a formula for the coefficients of any cyclotomic polynomial. The formula thus obtained may be of some use in numerical work. Its value in problems of a theoretical nature appears to be more limited.

Before we proceed to the actual derivation of the formula, let us first establish four lemmas.

LEMMA 1. Consider a fixed number, say  $m$ , of indeterminates  $x_i$ . Let  $\sum$  mean the usual  $\sum$ -function and  $\sum'$  the sum as if the exponents were distinct. If

$$a_1 = a_2 = \dots = a_u, \quad a_{u+1} = a_{u+2} = \dots = a_{u+v}, \quad \dots, \\ a_{k-w+1} = a_{k-w+2} = \dots = a_k,$$

then

$$\sum x_1^{a_1} x_2^{a_2} \dots x_k^{a_k} = \frac{1}{u!} \frac{1}{v!} \dots \frac{1}{w!} (-1)^k \sum_{i=1}^{k!} g_i : S$$

where  $g_i$  is an element of the symmetric group on  $k$  letters, written in cyclic form (not omitting cycles containing but one letter), and where

$$(a_1^{(1)}, a_2^{(1)}, \dots, a_r^{(1)}) (a_1^{(2)}, a_2^{(2)}, \dots, a_s^{(2)}) \dots (a_1^{(j)}, a_2^{(j)}, \dots, a_i^{(j)}) : S \\ = (-1)^j S_{a_1^{(1)}+a_2^{(1)}+\dots+a_r^{(1)}} S_{a_1^{(2)}+a_2^{(2)}+\dots+a_s^{(2)}} \dots S_{a_1^{(j)}+a_2^{(j)}+\dots+a_i^{(j)}},$$

wherein  $S_i = \sum x^i$  and  $a_j^{(i)}$  is some  $a_k$ .

PROOF. We first note that  $u!v! \dots w! \sum x_1^{a_1} x_2^{a_2} \dots x_r^{a_r} = \sum' x_1^{a_1} x_2^{a_2} \dots x_r^{a_r}$ . The proof is by induction on  $k$ .  $\sum' x_1^{a_1} = (-1) [(a_1) : S]$

\* His proof is given in a paper by E. Lehmer, this Bulletin, vol. 42 (1936), p. 389. I have drawn upon this paper for all the references contained in the present article.

† Göttingen Dissertation, 1934.

‡ E. Lehmer, op. cit., pp. 389-392.

$= (-1)[-S_{a_1}] = S_{a_1}$ . Hence the theorem is true for  $k = 1$ . We assume it true for  $k \leq n$ . We have

$$\begin{aligned} \sum' x_{n+1}^{a_{n+1}} \sum' x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} &= \sum' x_1^{a_1+a_{n+1}} x_2^{a_2} \cdots x_n^{a_n} \\ &+ \sum' x_1^{a_1} x_2^{a_2+a_{n+1}} \cdots x_n^{a_n} + \cdots \\ &+ \sum' x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n+a_{n+1}} \\ &+ \sum' x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} x_{n+1}^{a_{n+1}}, \\ \sum' x_1^{a_1} x_2^{a_2} \cdots x_{n+1}^{a_{n+1}} &= \sum' x_{n+1}^{a_{n+1}} \sum' x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \\ &- \sum' x_1^{a_1+a_{n+1}} x_2^{a_2} \cdots x_n^{a_n} - \cdots \\ &- \sum' x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n+a_{n+1}} \\ &= - \left\{ (-1)^n \sum_{i=1}^{n!} [(a_{n+1})g_i] : S + (-1)^n \sum_{i=1}^n h_i^{(1)} : S \right. \\ &\quad \left. + \cdots + (-1)^n \sum_{i=1}^{n!} h_i^{(n)} : S \right\}, \end{aligned}$$

where  $h_i^{(j)}$  is obtained from the element  $g_i$  by replacing  $a_j$  by  $a_j, a_{n+1}$ . Hence

$$\sum' x_1^{a_1} x_2^{a_2} \cdots x_{n+1}^{a_{n+1}} = (-1)^{n+1} \sum_{i=1}^{(n+1)!} g_i : S.$$

LEMMA 2. *In the symmetric group on  $n$  letters,  $n > 1$ , the number of elements with an even number of cycles equals the number of elements with an odd number of cycles (provided cycles with but one letter are not omitted).*

PROOF. In Lemma 1, let  $x_1 = 1$  and  $x_j = 0, (j = 2, 3, \dots, n)$ . Then  $S_i = 1$  for all  $i$ , and

$$x_1 x_2 \cdots x_n = \frac{1}{n!} (-1)^n \sum_{i=1}^{n!} g_i : S = \frac{1}{n!} (-1)^n (J - K)$$

where  $J$  is the number of elements in the symmetric group on  $n$  letters with an even number of cycles,  $K$  the number with an odd number of cycles. Since  $x_1 x_2 \cdots x_n = 0, J = K$ .

LEMMA 3. *If  $n$  is square free and the product of  $k$  primes, then the coefficient  $a_1$  in  $F_n(x)$  is  $(-1)^{k+1}$ .*

PROOF. The proof is by induction on  $k$ . The theorem is obviously

true for  $k=1$ . We assume it to be true for  $k=t$ . Let  $m$  be the product of  $t$  different primes. Then  $F_m(x) = x^r + (-1)^{t+1}x^{r-1} + \dots + 1$ . Let  $p$  be a prime not dividing  $m$  and  $\epsilon, \epsilon^2, \dots, \epsilon^{p-1}$  the primitive  $p$ th roots of unity. Then

$$F_{mp}(x) = [x^r + (-1)^{t+1}\epsilon x^{r-1} + \dots + \epsilon^r][x^r + (-1)^{t+1}\epsilon^2 x^{r-1} + \dots + \epsilon^{2r}] \dots [x^r + (-1)^{t+1}\epsilon^{p-1}x^{r-1} + \dots + \epsilon^{(p-1)r}].$$

Expanding, we have

$$F_{mp}(x) = x^{r(p-1)} + (-1)^{t+1}(\epsilon + \epsilon^2 + \dots + \epsilon^{p-1})x^{r(p-1)-1} + \dots + 1.$$

Since  $\epsilon + \epsilon^2 + \dots + \epsilon^{p-1} = -1$ , the induction is established.

LEMMA 4. Let  $x_1, x_2, \dots, x_r$  be the primitive  $n$ th roots of unity, where  $n$  is square free. Let  $(i, n) = p_1 p_2 \dots p_t = s$ . Then  $S_i = S_1$  if  $s=1$  and  $(-1)^t \phi(s) S_1$  otherwise.

PROOF. Let  $i = qs$  where  $(q, n) = 1$ . Then

$$x_1^i + x_2^i + \dots + x_r^i = x_1^{qs} + x_2^{qs} + \dots + x_r^{qs} = x_{j_1}^s + x_{j_2}^s + \dots + x_{j_r}^s.$$

But  $x_j^s$  is a primitive  $(n/s)$ th root of unity. Moreover, every  $(n/s)$ th root of unity appears in the above expression the same number of times, namely

$$\frac{\phi(n)}{\phi(n/s)} = \phi(s).$$

Hence, by Lemma 3, if  $k$  is the number of primes contained in  $n$ ,

$$S_i = (-1)^{k-t+1} \phi(s) = (-1)^t \phi(s) S_1.$$

We are now in a position to investigate the main problem. We need only consider  $n$  which are square free; for let  $m$  be the largest square free number dividing  $n$ . Then  $F_n(x) = F_m(x^{n/m})$ .

In considering square free  $n$ , we restrict ourselves first to the case where  $n$  is the product of an odd number of primes. Then, by Lemma 3,  $S_1 = -1$ . From Lemma 1,

$$(1) \quad (-1)^i a_i = \sum x_1 x_2 \dots x_i = \frac{1}{i!} (-1)^i \sum_{k=1}^i g_k : S.$$

Suppose  $g_k = c_1^{(r_1)} \dots c_\nu^{(r_\nu)}$ , where  $c_\mu^{(r_\mu)}$ ,  $(\mu = 1, \dots, \nu)$ , is a cycle on  $r_\mu$  letters,  $r_1 + r_2 + \dots + r_\nu = i$ . Then  $g_k : S = \prod_\mu (c_\mu^{(r_\mu)} : S) = \prod_\mu (-S_{r_\mu})$  since all exponents in (1) are 1. If  $r_\mu$  is prime to  $n$ ,  $-S_{r_\mu} = -S_1 = 1$ ;

and if for all  $g_k$ , all  $r_\mu$  were prime to  $n$ , we would have the relation

$$(2) \quad \sum_{k=1}^{i!} g_k : S = i! = G_i.$$

To obtain the actual value of  $\sum g_k : S$ , we take  $G_i$  as an "approximation" and determine corrections to be added due to certain  $r_\mu$  not prime to  $n$ . A correction is first determined for cycles "associated with the length  $p$ ,  $p|n$ ." A cycle  $c^{(r)}$  is associated with the length  $p$  if  $p|r$ , and the correction is obtained by using the "better" value  $c^{(r)} : S = -(p-1)$  instead of 1, while cycles not associated with the length  $p$  are left as 1. This is done for all  $p|n$  and  $p \leq i$ . (The better value is the correct value only if  $(r, n) = p$ .) Then a correction is determined for cycles associated with the length  $pq$ ,  $pq|n$ ,  $pq \leq i$ , and so on.

The first approximation (2) yields  $a_i = [G_i]/i!$ . In correcting for cycles associated with the length  $p$ ,  $p|n$ , consider first those substitutions having a cycle of length  $p$ . They are of the form  $c^{(p)}g$ , where  $g$  is an element of the symmetric group on  $(i-p)$  letters. Since, by Lemma 4,  $S_p = (p-1)$ , we have  $c^{(p)}g : S = -(p-1)(g : S)$  (with the minus sign taken because of the reduction in the number of cycles operating on  $S$ ). A cycle of length  $p$  may be chosen in  $i!/[p(i-p)!]$  ways. If we assume that the cycles of  $g$  operating on  $S$  are evaluated for  $S_j = S_1$ , and if we note that we have previously evaluated, in (2), this expression as  $-(-1)(g : S)$ , the value of  $a_i$  becomes

$$(3) \quad a_i = \frac{1}{i!} \left[ G_i - p \frac{i!}{p(i-p)!} G_{i-p} \right].$$

However, if a substitution has  $r$  cycles of length  $p$ , we have counted it  $C_{r,1} = r$  times.

Consider now those substitutions having a cycle of length  $2p$ . They are  $i!/[2p(i-2p)!]$  in number and have been previously evaluated, in (2), as  $-(-1)(g : S)$  instead of the better value  $-(p-1)(g : S)$  ( $g$  now is an element of the symmetric group on  $(i-2p)$  letters). Those substitutions having 2 cycles of length  $p$  are

$$\frac{1}{2} \frac{i!}{p(i-p)!} \frac{(i-p)!}{p(i-2p)!} = \frac{i!}{2p^2(i-2p)!}$$

in number. They have been previously evaluated, in (3), as

$$(-1)(-1)(g : S) + (2p)(-1)(g : S) = (1-2p)(g : S)$$

instead of  $(p^2-2p+1)(g : S)$ . If we again assume that the cycles of  $g$

operating on  $S$  are evaluated for  $S_j = S_1$ , the value of  $a_i$  becomes

$$a_i = \frac{1}{i!} \left[ G_i - p \frac{i!}{p(i-p)!} G_{i-p} - p \frac{i!}{2p(i-2p)!} G_{i-2p} + p^2 \frac{i!}{2p^2(i-2p)!} G_{i-2p} \right].$$

However, if a substitution has  $r$  cycles of length  $2p$ , we have counted it  $C_{r,1}$  times; and if a substitution has  $r$  cycles of length  $p$ , we have counted it  $C_{r,2}$  times.

We proceed now to the general case, namely that of substitutions having  $k_1$  cycles of length  $p$ ,  $k_2$  cycles of length  $2p$ ,  $\dots$ ,  $k_s$  cycles of length  $sp$ . Let  $\sum jk_j = k$  and  $\sum k_j = t$ . (We assume that we have already considered all substitutions with  $(k-1)p$  or less letters involved in cycles associated with the length  $p$ .) Each combination of  $(t-j)$ , ( $j \geq 1$ ), of the cycles of such a substitution has already introduced the correction  $(-1)^{t-j} p^{t-j}$ . Hence this substitution has been previously evaluated as

$$\left[ (-1)^t \sum_j (-1)^j C_{t,t-j} p^{t-j} \right] (g:S).$$

There are  $(h/k!)i!/[p^t(i-kp)!]$  such substitutions, where  $h$  is the number of elements in the symmetric group on  $k$  letters having  $k_1$  cycles of length 1,  $k_2$  cycles of length 2,  $\dots$ ,  $k_s$  cycles of length  $s$ . If we let  $k_1, k_2, \dots, k_s$  assume all values compatible with  $\sum jk_j = k$ , we have

$$a_i = \frac{1}{i!} \left[ G_i - \frac{i!}{(i-p)!} G_{i-p} + \left( \frac{1}{2} - \frac{1}{2} \right) \frac{i!}{(i-2p)!} G_{i-2p} + \dots + \left( \frac{h' - h''}{k!} \right) \frac{i!}{(i-kp)!} G_{i-kp} \right],$$

where  $h'$  is the number of elements in the symmetric group on  $k$  letters having an even number of cycles and  $h''$  the number having an odd number of cycles. However, by Lemma 2,  $h' = h''$ ; moreover, from its definition,  $G_u = u!$ . Hence the correction, due to cycles associated with the length  $p$ , which must be added to the first approximation of  $a_i$  is  $-1$ . If we apply this process to cycles associated with each of the  $t$  primes less than  $i$  dividing  $n$ , the value of  $a_i$  becomes  $a_i = 1 - t$ .

The situation for cycles of length  $pq$ ,  $pq | n$ ,  $pq \leq i$ , is slightly different. We have previously evaluated them as  $(-p-q+1)(g:S)$ . Since

their correct value by Lemma 4 is  $[-(p-1)(q-1)(-1)](g:S)$ , the adjustment must be made as  $pq(g:S)$ . An analysis similar to the case for a single prime shows that to the value of  $a_i$  previously computed must be added the following correction for cycles associated with the length  $pq$ :

$$\frac{1}{i!} \left[ \frac{i!}{(i-pq)!} G_{i-pq} + \left( \frac{1}{2} + \frac{1}{2} \right) \frac{i!}{(i-2pq)!} G_{i-2pq} + \dots + \left( \frac{h' + h''}{k!} \right) \frac{i!}{(i-kpq)!} G_{i-kpq} + \dots \right].$$

As before,  $h'$  is the number of elements in the symmetric group on  $k$  letters having an even number of cycles, and  $h''$  the number having an odd number of cycles. Hence  $h' + h'' = k!$ . Thus each multiple of  $pq \leq i$  adds 1 to  $a_i$ .

The proper adjustment for a cycle of length  $p_1 p_2 \dots p_t$ , such that  $p_1 p_2 \dots p_t | n$ ,  $p_1 p_2 \dots p_t \leq i$ , is  $(-1)^t p_1 p_2 \dots p_t (g:S)$ . This may be established quite easily by induction on  $t$ . The theorem was seen to be true for  $t=1$ . We assume it to be true for  $t \leq k$ . Then a cycle of length  $p_1 p_2 \dots p_{k+1}$ ,  $p_1 p_2 \dots p_{k+1} | n$ ,  $p_1 p_2 \dots p_{k+1} \leq i$ , at that stage in the process when all cycles associated with a length which is a product of less than  $k+1$  primes dividing  $n$  have been evaluated, has introduced the following number into  $a_i$ :

$$(4) \quad (-1)^k \left[ \sum^{k+1} p_1 p_2 \dots p_k - \sum^{k+1} p_1 p_2 \dots p_{k-1} + \dots + (-1)^k \right] (g:S).$$

However, by Lemma 4, the correct evaluation is

$$(5) \quad (-1)^{k+1} \phi(p_1 p_2 \dots p_{k+1})(g:S).$$

But the difference between (5) and (4) is

$$(-1)^{k+1} p_1 p_2 \dots p_{k+1}(g:S),$$

which then is the correction that must be made.

If  $t$  is odd, the analysis of the case for a single prime shows that each divisor  $p_1 p_2 \dots p_t$  of  $n$  less than or equal to  $i$  subtracts 1 from  $a_i$ . If  $t$  is even, the argument for two primes shows that each multiple of each such factor less than or equal to  $i$  adds 1 to  $a_i$ .

There remains to consider only the adjustments necessary for the simultaneous occurrence of cycles of length  $r_1, r_2, \dots, r_s$ , respectively, where  $r_i | n$ . The formula for the correction, which we shall establish by induction, is  $(-1)^t r_1 r_2 \dots r_s (g:S)$ , where  $t$  is the number

of primes (not necessarily distinct) appearing in the product  $r_1 r_2 \cdots r_s$ . We have previously shown the formula to be true for  $t=1$ . We assume it to be true for  $t \leq k$ . Then the  $s$  cycles of length  $r_1, r_2, \dots, r_s$ , respectively, at that point when cycles associated with lengths whose product contains less than  $(k+1)$  primes have all been evaluated, have introduced the following number into  $a_i$ :

$$(6) \quad (-1)^k \left[ \sum^{k+1} p_1 p_2 \cdots p_k - \sum^{k+1} p_1 p_2 \cdots p_{k-1} + \cdots + (-1)^k \right] (g:S)$$

where the summations are taken as if  $p_1, p_2, \dots, p_{k+1}$  were distinct. However, by Lemma 4, the correct evaluation is

$$(7) \quad (-1)^{k+1} \phi(r_1) \phi(r_2) \cdots \phi(r_s) (g:S).$$

The difference between (7) and (6) is

$$(-1)^{k+1} r_1 r_2 \cdots r_s (g:S),$$

and the induction is complete.

In applying the adjustment to all possible combinations of sets of cycles, where each set is associated with some  $r_i$ , we should note that the method of grouping the cycles used in analyzing the case for a single prime may still be used within each set. Hence the sum of any number, say  $t$ , of different divisors of  $n$  containing an odd number of primes plus the sum of any number of multiples of different divisors of  $n$  containing an even number of primes adds or subtracts 1 to  $a_i$  as  $t$  is even or odd. Note that  $(-1)^t$  is the same whether  $t$  is defined as above or as in the previous paragraph. Also note that we must specify "different divisors," for if some  $r_i = r_j$ , our method of grouping would have accounted for the cycles at an earlier stage in the process.

If  $n$  is square free and the product of an even number of primes, the same general methods apply. However, certain differences arise due to the fact that  $S_1=1$  instead of  $-1$  as previously. A cycle of length  $p$  must be evaluated as  $(p-1)(g:S)$ . After correcting for all cycles associated with the length  $p, p|n$ , we have

$$a_i = \frac{1}{i!} \left[ G_i + \frac{i!}{(i-p)!} G_{i-p} + \left( \frac{1}{2} + \frac{1}{2} \right) \frac{i!}{(i-2p)!} G_{i-2p} + \cdots + \left( \frac{h' + h''}{k!} \right) \frac{i!}{(i-kp)!} G_{i-kp} + \cdots \right].$$

Since  $S_1=1$ , we have  $G_0=1, G_1=-1$ , and  $G_j=0$  for  $j>1$ . ( $G_u$ , we recall, is  $\sum^{u!} g_k : S$  evaluated for  $S_j=S_1$ .) Hence any multiple of  $p$  equal

to  $i$  adds 1 to  $a_i$ , and any multiple of  $p$  equal to  $i-1$  subtracts 1 from  $a_i$ . This is true of any product of an odd number of primes dividing  $n$ . A product of an even number of primes subtracts or adds 1 to  $a_i$  if it equals  $i$  or  $i-1$ , respectively. However multiples of such expressions have no effect. The extension to sums of divisors is immediate.

We have thus established the following theorem:

**THEOREM.** *Let  $F_n(x) = x^n + a_1x^{n-1} + \dots + a_r = 0$  be the irreducible equation of the primitive  $n$ th roots of unity.*

**A.** *Let  $m$  be the largest square free number dividing  $n$  and  $a'_i$  a coefficient of  $F_m$ . Then if  $i = kn/m$ ,  $a_i = a'_k$ ; if  $n/m$  does not divide  $i$ ,  $a_i = 0$ .*

**B.** *Let  $n$  be square free and the product of an odd number of primes. Then*

$$a_i = 1 + \sum \epsilon_d$$

where the following conditions hold:

(a) *The summation is extended over all  $d \leq i$ .*

(b) *The number  $d$  is the sum of any number, say  $t$ , of different divisors of  $n$  containing an odd number of primes plus the sum of any number of multiples of different divisors of  $n$  containing an even number of primes.*

(c)  $\epsilon_d = (-1)^t$ .

**C.** *Let  $n$  be square free and the product of an even number of primes. Then*

$$a_1 = -1; \quad a_i = \sum \epsilon_d - \sum \epsilon_{d'}, \quad i > 1,$$

where the following conditions hold:

(a) *The summations are extended over all  $d = i$  and all  $d' = i-1$ , respectively.*

(b) *Both  $d$  and  $d'$  are the sum of any number of multiples of different divisors of  $n$  containing an odd number of primes plus the sum of any number, say  $t$ , of different divisors of  $n$  containing an even number of primes.*

(c)  $\epsilon_d = (-1)^t$ .

YALE UNIVERSITY