MATHEMATICS OF COMPUTATION
VOLUME 60, NUMBER 201
JANUARY 1993, PAGES 385–398

ON THE COEFFICIENTS OF THE MINIMAL POLYNOMIALS OF GAUSSIAN PERIODS

S. GUPTA AND D. ZAGIER

ABSTRACT. Let l be a prime number and m a divisor of $l-1$. Then the Gauss period $\omega = \zeta + \zeta^{\lambda} + \zeta^{\lambda^2} + \cdots + \zeta^{\lambda^{m-1}}$, where $\zeta = e^{2\pi i/l}$ and λ is a primitive mth root of unity modulo l, generates a subfield K of $\mathbb{Q}(\zeta)$ of degree $(l-1)/m$. In this paper we study the reciprocal minimal polynomial $F_{l,m}(X) = N_{K/\mathbb{Q}}(1-\omega X)$ of ω over $\mathbb{Q}$. It will be shown that for fixed m and every N we have $F_{l,m}(X) \equiv (B_m(X)^l/(1-mX))^{1/m} \pmod{X^N}$ for all but finitely many "exceptional primes" l (depending on m and N), where $B_m(X) \in \mathbb{Z}[[X]]$ is a power series depending only on m. A method of computation of this set of exceptional primes is presented. The generalization of the results to the case of composite l is also discussed.

1. STATEMENT OF RESULTS

Let l be an odd prime number[1] and $l-1 = m \cdot d$ a decomposition of $l-1$ into positive factors. Then there is a unique cyclic extension $K_d/\mathbb{Q}$ of degree d ramified only at l. It is contained in the cyclotomic field $\mathbb{Q}(\zeta)$ ($\zeta =$ primitive lth root of unity) and is generated over $\mathbb{Q}$ by the *Gaussian period*

$$\omega = \operatorname{Tr}_{\mathbb{Q}(\zeta)/K_d} = \zeta + \zeta^{\lambda} + \zeta^{\lambda^2} + \cdots + \zeta^{\lambda^{m-1}},$$

where $\lambda \in (\mathbb{Z}/l\mathbb{Z})^{\times}$ is a primitive mth root of unity modulo l. The minimal polynomial of ω,

$$f_{l,m}(X) = \prod_{r \in \mathscr{R}} (X - (\zeta^r + \zeta^{\lambda r} + \zeta^{\lambda^2 r} + \cdots + \zeta^{\lambda^{m-1} r})),$$

where $\mathscr{R}$ denotes a set of coset representatives for $(\mathbb{Z}/l\mathbb{Z})^{\times}$ modulo $\langle\lambda\rangle$, gives an explicit irreducible polynomial of degree d with cyclic Galois group and discriminant a power of l. We include l and m rather than l and d into the notation because we will be studying the coefficients of these polynomials for m fixed and l varying. Specifically, we will show that for m and n fixed the nth coefficient "from the end" of $f_{l,m}(X)$ is a polynomial in l for all but finitely many "exceptional" primes l, and we will describe the computation of this polynomial and of the set of exceptional primes. The statement about the nth coefficient being a polynomial in l for l large, and some of our other

Received by the editor August 19, 1991 and, in revised form, January 3, 1992.
1991 *Mathematics Subject Classification.* Primary 11L05, 11T22; Secondary 11Y40.

[1]The case of composite l will be considered briefly in §5.

0025-5718/93 $1.00 + $.25 per page

results, were first proved by Gurak [1, 2]; we will give a detailed comparison with Gurak's work at the end of §1.

To state the basic result conveniently, we turn $f_{l,m}(X)$ around, setting

$$F_{l,m}(X) = X^d f_{l,m}(X^{-1}) = \prod_{r \in \mathscr{R}} (1 - (\zeta^r + \zeta^{\lambda r} + \zeta^{\lambda^2 r} + \cdots + \zeta^{\lambda^{m-1} r}) X).$$

Clearly, this reciprocal polynomial also has cyclic Galois group and generates the field K_d.

Theorem 1. *For each integer $m \geq 1$ there exist power series $A_m(X)$, $B_m(X) \in \mathbb{Z}[[X]]$ related to one another by*

$$B_m(X) = (1 - mX) A_m(X)^m, \tag{1}$$

such that for each natural number N the congruence

$$F_{l,m}(X) \equiv A_m(X) B_m(X)^{(l-1)/m} \pmod{X^N} \tag{2}$$

holds for all but finitely many primes $l \equiv 1 \pmod{m}$.

Here, "all but finitely many" means all primes not belonging to a computable finite set depending only on m and N. The computation of A_m and B_m will be given in §2. The beginnings of these power series for $m \leq 10$ are given in Table 1. Theorem 1 implies that for fixed m and n the nth coefficient of $F_{l,m}(X)$ is a polynomial of degree $\leq n$ in l except for a finite number of exceptional primes l. If m is a power of a prime number p, then $B_m(X)$ is in fact a power series in X^p, as we can see in Table 1 and will prove in Theorem 2. In this case it follows that the power series in question has degree at most $[n/p]$ rather than n and in particular is actually a *constant* for $n < p$, is linear

TABLE 1. Coefficients of $A_m(X)$ and $B_m(X)$, $m \leq 10$

	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	X^{10}
$A_1(X)$	1	1	1	1	1	1	1	1	1	1	1
$B_1(X)$	1	0	0	0	0	0	0	0	0	0	0
$A_2(X)$	1	1	1	2	3	6	10	20	35	70	126
$B_2(X)$	1	0	−1	0	−1	0	−2	0	−5	0	−14
$A_3(X)$	1	1	2	4	11	29	73	207	574	1542	4435
$B_3(X)$	1	0	0	−2	0	0	−13	0	0	−158	0
$A_4(X)$	1	1	2	7	21	77	257	963	3377	12816	46240
$B_4(X)$	1	0	−2	0	−7	0	−50	0	−456	0	−4728
$A_5(X)$	1	1	3	11	44	180	796	3532	15906	72490	331282
$B_5(X)$	1	0	0	0	0	−24	0	0	0	0	−11052
$A_6(X)$	1	1	3	14	66	335	1736	9227	49744	271647	1497407
$B_6(X)$	1	0	−3	−4	−18	−60	−269	−1152	−5412	−25580	−125478
$A_7(X)$	1	1	4	20	110	638	3828	23412	146865	930385	5955040
$B_7(X)$	1	0	0	0	0	0	0	−720	0	0	0
$A_8(X)$	1	1	4	25	152	1034	6981	49554	350709	2553004	18557553
$B_8(X)$	1	0	−4	0	−34	0	−696	0	−19795	0	−672916
$A_9(X)$	1	1	5	31	221	1637	12510	98618	789167	6394033	52492327
$B_9(X)$	1	0	0	−6	0	0	−387	0	0	−68726	0
$A_{10}(X)$	1	1	5	38	289	2416	20428	179188	1587720	14328461	130327089
$B_{10}(X)$	1	0	−5	0	−55	−48	−1500	−3360	−58450	−214560	−2809859

TABLE 2. Coefficients of $A_5(X)B_5(X)^d$ and of $F_{l,5}(X)$

l:	11	31	41	61	71	101	131	151	181	191
d:	2	6	8	12	14	20	26	30	36	38
n: 0	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1
2	3	3	3	3	3	3	3	3	3	3
3	0	11	11	11	11	11	11	11	11	11
4	0	44	44	−17	44	44	44	44	44	44
5	0	36	−53	−169	−156	−300	−444	−540	−684	−732
6	0	32	153	325	−250	316	172	76	−973	−116
7	0	0	−160	167	749	1991	1660	−893	−870	−2069
8	0	0	59	−804	1560	−80	−4713	5721	2782	2818

in l for $p < n \leq 2p$, etc. For instance, if $m = 7$ we have

$$B_7(X) = 1 - 720X^7 - 48389400X^{14} - \cdots,$$

$$A_7(X) = 1 + X + 4X^2 + 20X^3 + 110X^4 + 638X^5 + 3828X^6 + 23412X^7 + \cdots,$$

so the coefficient of X^5 in $F_{l,m}(X)$ is 638 for all but finitely many primes $l \equiv 1 \pmod 7$ (in fact, as we shall see, for all such l except 29, 43, 71, 113, 197, 421, 463 and 547) and the coefficient of X^7 equals $(164604 - 720l)/7$ for all but finitely many l (namely, those mentioned and 211, 239, 281, 337, 379, 449, 757, 1583, 1597 and 2689). Table 2 illustrates Theorem 1 in the case $m = 5$ by giving the first coefficients of $F_{l,5}(X)$ for some small values of l and showing (broken line) how long each polynomial $F_{l,5}(X)$ agrees with the power series

$$\begin{aligned} A_5(X)B_5(X)^d = {} & 1 + X + 3X^2 + 11X^3 + 44X^4 + (180 - 24d)X^5 \\ & + (796 - 24d)X^6 + (3532 - 72d)X^7 + (15906 - 264d)X^8 \\ & + (72490 - 1056d)X^9 + (331282 - 15660d + 288d^2)X^{10} \\ & + (1544418 - 30444d + 288d^2)X^{11} \\ & + (7211960 - 118788d + 864d^2)X^{12} \\ & + (33850952 - 506484d + 3168d^2)X^{13} \\ & + (159612948 - 2238720d + 12672d^2)X^{14} + \cdots \\ & \qquad (l = 5d + 1). \end{aligned}$$

Clearly, the theorem is equivalent to saying that the nth coefficient of the *logarithm* of $F_{l,m}(X)$ is a linear function of l for all but finitely many l (for fixed m and n). More precisely, write

$$B_m(X) = \exp\left(-\sum_{n=1}^{\infty} \beta_m(n)\frac{X^n}{n}\right) \tag{3}$$

(it turns out that $\beta_m(n)$ is integral and nonnegative, which is the reason for including the minus sign and the factor $1/n$); then Theorem 1, except for the integrality statement, is equivalent to

Theorem 1′. *Fix integers* m, $n \in \mathbb{N}$. *Then the coefficient of* X^n *in* $\log F_{l,m}(X)$ *equals*

$$\frac{m^n - l\beta_m(n)}{mn}$$

for all $l \equiv 1 \pmod m$ *not belonging to an effectively determinable finite set* $\mathscr{E}_m(n)$.

In the notation of this theorem, the set of exceptional primes in Theorem 1 is simply $\bigcup_{n<N} \mathscr{E}_m(n)$, and the "new" exceptional primes for given n are the elements of the set $\mathscr{E}_m^0(n) = \mathscr{E}_m(n) \setminus \bigcup_{n'<n} \mathscr{E}_m(n')$. Examples of the sets $\mathscr{E}_m^0(n)$ for $m \le 12$ and some small values of n are given in Table 3 (when this set contains 25 or more primes, we have given only its first three and last three elements and its cardinality). The way to determine these sets will be explained in §3.

In general, the coefficients $\beta_m(n)$, and hence the power series $B_m(X)$ and $A_m(X)$ occurring in Theorem 1, are difficult to determine. A simple description of these coefficients in certain special cases is given by the following theorem:

Theorem 2. *The coefficients* $\beta_m(n)$ *for* $m = p^j$ (p *prime*, $j \ge 1$) *and* $m = 2p$ ($p > 2$ *prime*) *are given by the generating functions*

$$\sum_{n=0}^{\infty} \frac{\beta_{p^j}(n)}{n!} X^n = \left(\sum_{\nu=0}^{\infty} \frac{X^{p\nu}}{\nu!^p} \right)^{p^{j-1}}, \tag{4}$$

$$\sum_{n=0}^{\infty} \frac{\beta_{2p}(n)}{n!} X^n = \sum_{r=-\infty}^{\infty} \left(\sum_{\nu=0}^{\infty} \frac{X^{2\nu+|r|}}{\nu!(\nu+|r|)!} \right)^p. \tag{5}$$

TABLE 3. New exceptional primes for $m \le 6$

	$m=3$	$m=4$	$m=5$	$m=6$
$n=3$	—	5	11	7
4	7	—	61	13
5	13	13, 17	41	19
6	—	—	31,71,181,521	31
7	19, 31	29, 37	101, 151, 191, 461	37, 43
8	43	—	131, 241, 251, 401, 421, 991	—
9	—	41, 53	281, 331, 491, 641, 881, 941, 1871	61, 67, 73
10	37, 73	—	271, 311, 661, 1181	79
11	67	61, 73, 101	211, 431, 601, 631, 691, 751, 1051, 1481, 1531, 1621, 1741, 2531, 2801, 3001, 3011, 9091	97, 103
12	—	—	701, 761, 971, 1021, 1201, 1321, 1381, 1511, 1721, 1801, 2141, 2371, 2441, 2741, 5051, 13421	109
13	61, 79, 103	89, 97, 109	541, 571, 811, 821, 1031, 1171, 1291, 1301, 1471, 1861, 1901, 2381, 2551, 2671, 4421, 4561, 4621, 4831, 7741, 7841, 12391, 19141	127, 139, 157
14	97, 157	—	911, 961, 1061, 1151, 1451, 1571, 2081, 2251, 2351, 2411, 2791, 3121, 3301, 3371, 3511, 3931, 4001, 4201, 4231, 4441, 6121, 6521, 6971	151, 163
15	—	113, 137, 173, 197	1091, 2011, 2161, 2221, 3221, 3331, 4951	181, 199, 211

TABLE 3 (continued). New exceptional primes for $7 \leq m \leq 12$

m	n	exceptional primes
7	3	43
	4	29, 71, 547
	5	113, 197, 421, 463
	6	211, 379, 449, 757, 2689
	7	239, 281, 337, 1583, 1597
	8	127, 491, 673, 743, 827, 911, 953, 967, 1051, 1289, 1303, 1471, 2213, 2297, 2549, 2591, 3067, 4159, 4663, 5153, 7673, 10039, 10501, 11243
	9	617, 631, 659, ... , 33601, 35281, 91309 (35 primes)
	10	1429, 1723, 2087, ... , 89237, 209441, 212633 (52 primes)
8	3	17
	4	41
	5	73, 89, 97, 113, 257
	6	137, 313
	7	193, 233, 241, 281, 337, 353, 409, 433, 641, 1297
	8	401, 673, 1201
	9	449, 457, 521, 569, 577, 593, 601, 617, 761, 769, 809, 881, 929, 937, 953, 1033, 1097, 1217, 1289, 1481, 1553, 1609, 2417, 2473
	10	977, 1049, 1409, 1433, 2129
9	3	19
	4	37
	5	73, 109, 163, 199
	6	127, 181, 433, 487
	7	271, 307, 379, ... , 3511, 3547, 5779 (28 primes)
	8	811, 829, 883, ... , 18757, 19387, 19603 (38 primes)
	9	1567, 1999, 2053, ... , 9901, 14347, 18253 (27 primes)
	10	1369, 2467, 2683, ... , 120763, 131041, 132499 (115 primes)
10	3	11, 31
	4	41, 61
	5	71, 101, 131, 181, 211
	6	151, 191, 241, 271, 281, 461, 521
	7	251, 311, 331, 401, 421, 431, 541, 571, 631, 991, 1031
	8	491, 601, 641, 691, 701, 751, 761, 881, 911, 941, 971, 1321, 1481, 2801
	9	661, 811, 821, 1021, 1051, 1061, 1091, 1151, 1171, 1201, 1231, 1291, 1301, 1361, 1601, 1831, 1871, 1901, 2371, 2381, 2441
	10	1181, 1381, 1451, ... , 3931, 4001, 4421 (25 primes)
11	3	23, 683
	4	67, 89, 419, 661, 991
	5	331, 353, 397, 463, 617, 1409, 2113, 2311, 3191, 4621, 35839, 39139, 51679
	6	199, 727, 859, ... , 353827, 715397, 825353 (27 primes)
	7	1013, 1277, 1607, ... , 809447, 7605071, 51828151 (74 primes)
12	3	13
	4	37, 61, 73
	5	97, 109, 157, 193, 241
	6	181, 229, 277, 313, 373, 409, 601
	7	337, 349, 397, 421, 433, 457, 541, 613, 709, 733, 757, 829, 1021
	8	577, 661, 673, 769, 853, 1009, 1213, 1297, 1453, 1789, 1933
	9	877, 937, 997, ... , 2797, 3217, 3361 (27 primes)
	10	1249, 1381, 1429, 1657, 1669, 1693, 1753, 1861, 1873, 2113, 2137, 2161, 2293, 2341, 2437, 2677, 2953, 3709, 3769, 3853, 4297, 5233, 6481
	11	1993, 2017, 2029, ... , 8221, 8461, 9901 (42 primes)
	12	289, 2713, 2857, ... , 9241, 10453, 12541 (43 primes)

In particular, the coefficients $\beta_m(n)$ *for* $m = p$ (p *prime*) *and* $m = 4$ *are given by*

$$\beta_p(n) = \begin{cases} \dfrac{n!}{(n/p)!^p} & \text{if } n \equiv 0 \pmod{p}, \\ 0 & \text{otherwise,} \end{cases} \tag{6}$$

$$\beta_4(n) = \begin{cases} \dfrac{n!^2}{(n/2)!^4} & \text{if } n \equiv 0 \pmod 2, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

If $m = p^j$ (p prime, $j \geq 1$), then the coefficient $\beta_m(n)$ is nonzero only if p divides n.

The cases $m = 3$ and 4 of this theorem were proved by D. and E. Lehmer [3] and the case $m = p$ by S. Gurak [2] (Corollary 2, p. 322).

If $m = 2$, then we can sum the series $\sum \beta_2(n)X^n/n$ explicitly to give closed formulas for the power series $A_2(X)$ and $B_2(X)$. However, here one can give much more information than in Theorem 1, since $f_{l,2}$ can be calculated in closed form, essentially as a Chebyshev polynomial (Theorem 3). The result, which will be proven in §4, is the formula

$$f_{l,2}(X) = \sum_{n=0}^{d} (-1)^{[\frac{d-n}{2}]} \binom{[\frac{d+n}{2}]}{n} X^n \qquad \left(d = \frac{l-1}{2}\right).$$

It was essentially known to Gauss (Disquisitiones Arithmeticae, Article 337).

As mentioned in the beginning of the section, several of our results overlap with the results in the papers [1] and [2] by S. Gurak, whose existence we learned about after completing our work. Specifically, Gurak proves in [1] that the coefficient of X^n in $F_{l,m}(X)$ is $P_{m,n}(l)$ for primes $l > n^{\phi(m)}$ (ϕ = Euler totient function), where $P_{m,n}$ is a polynomial of degree $\leq n/p$ (p = smallest prime factor of m). Equation (10) of [1] (resp. equation (28) of [2]) is equivalent to our Theorem 1′ and thus to all parts of Theorem 1 except for the integrality of the power series A_m and B_m. The explicit description of these power series in the special cases $m = p$ and $m = 4$ were also given in [2], as mentioned after Theorem 2. The description of the algorithm for finding the exceptional sets $\mathscr{E}_m(n)$, and the numerical computations concerning them, are new.

2. Proof of Theorem 1

Using the Taylor series of $\log(1 - T)$ around $T = 0$, we find

$$\log F_{l,m}(X) = -\sum_{n=1}^{\infty} \left(\sum_{r \in \mathscr{R}} \left(\zeta^r + \zeta^{\lambda r} + \zeta^{\lambda^2 r} + \cdots + \zeta^{\lambda^{m-1} r}\right)^n \right) \frac{X^n}{n}.$$

Replacing the inner sum by one over all $r \in (\mathbb{Z}/l\mathbb{Z})^\times$ simply multiplies it by m, since the value of the summand is independent of the choice of coset representative r, and there are m cosets. Hence, the inner sum equals

$$\begin{aligned} \frac{1}{m} \sum_{r \not\equiv 0 \pmod l} \left(\sum_{i=0}^{m-1} \zeta^{\lambda^i r} \right)^n &= -m^{n-1} + \frac{1}{m} \sum_{r \pmod l} \sum_{i_1, \ldots, i_n = 0}^{m-1} \zeta^{(\lambda^{i_1} + \cdots \lambda^{i_n}) r} \\ &= -m^{n-1} + \frac{l}{m} \beta_{l,m}(n), \end{aligned}$$

where

$$\beta_{l,m}(n) = \#\{(i_1, \ldots, i_n) \in (\mathbb{Z}/m\mathbb{Z})^n \mid \lambda^{i_1} + \cdots + \lambda^{i_n} = 0 \text{ in } \mathbb{Z}/l\mathbb{Z}\}$$

(recall that λ here refers to a fixed primitive mth root of unity in $(\mathbb{Z}/l\mathbb{Z})^\times$);

to obtain this formula, we have added and subtracted a term corresponding to $r = 0$ and then used the fact that $\sum_{r \pmod l} \zeta^{kr}$ equals l if $k \equiv 0 \pmod l$ and vanishes otherwise.

We now define coefficients $\beta_m(n)$ ($n \geq 1$) by

$$\beta_m(n) = \#\{(i_1, \dots, i_n) \in (\mathbb{Z}/m\mathbb{Z})^n \mid \lambda_0^{i_1} + \cdots + \lambda_0^{i_n} = 0\},$$

where $\lambda_0 = e^{2\pi i/m}$ is a primitive root of unity in the complex number field rather than in the finite field $\mathbb{F}_l$. We will show that $\beta_{l,m}(n) = \beta_m(n)$ for all but finitely many primes $l \equiv 1 \pmod m$, for fixed m and n. This implies Theorem 1′ and hence, with $B_m(X)$ defined by equation (3), Theorem 1 (except for the asserted integrality of the power series A_m and B_m), because for $l = md + 1$ prime and sufficiently large (depending on N and m) we have

$$\begin{aligned}\log F_{l,m}(X) &\equiv \sum_{n=1}^{N-1} \left(\frac{m^n}{m} - \frac{md+1}{m}\beta_m(n)\right)\frac{X^n}{n} \\ &\equiv -\frac{1}{m}\log(1 - mX) + \left(d + \frac{1}{m}\right)\log B_m(X) \\ &\equiv \log A_m(X) + d \log B_m(X) \pmod{X^N}.\end{aligned}$$

Let $\Phi_m(x)$ be the mth cyclotomic polynomial, i.e., the irreducible monic polynomial (of degree $\varphi(m)$, the Euler totient function of m) of λ_0 over $\mathbb{Q}$. Then a polynomial $P(x)$ with rational coefficients vanishes at λ_0 if and only if it is divisible by $\Phi_m(x)$. Thus,

$$\beta_m(n) = \#\{\mathbf{i} = (i_1, \dots, i_n) \in (\mathbb{Z}/m\mathbb{Z})^n \mid \Phi_m(x) | P_{\mathbf{i}}(x)\},$$

where $P_{\mathbf{i}}(x)$ denotes the polynomial $x^{i_1} + \cdots x^{i_n}$. (Strictly speaking, this is not a polynomial unless we choose actual integer representatives of the classes $i_\nu \pmod m$, say $0 \leq i_\nu < m$, but obviously the condition that Φ_m divide $P_{\mathbf{i}}$ is independent of this choice, since $\Phi_m(x) | (x^m - 1)$.) Obviously, every n-tuple $\mathbf{i}$ contributing to $\beta_m(n)$ also contributes to $\beta_{l,m}(n)$, since $\lambda \in \mathbb{F}_l^\times$ is a root of the polynomial $\Phi_m(x)$ and hence of all of its multiples. Hence, $\beta_{l,m}(n)$ is at least as large as $\beta_m(n)$, but might be larger. However, the fact that $\Phi_m(x)$ is irreducible over $\mathbb{Q}$ means that the g.c.d. of $\Phi_m(x)$ with any polynomial $P(x)$ not divisible by it is 1. In particular, if $\mathbf{i}$ is an index in $(\mathbb{Z}/m\mathbb{Z})^n$ not counted in $\beta_m(n)$, i.e., one for which $P_{\mathbf{i}}$ is not divisible by Φ_m, then there are polynomials with rational coefficients $g(x)$ and $h(x)$ (depending on m and n) such that $g(x)\Phi_m(x) + h(x)P_{\mathbf{i}}(x) \equiv 1$. If the prime $l \equiv 1 \pmod m$ does not occur in the denominator of any coefficient of g or h, then we can reduce this equation $\pmod l$, and the fact that $\Phi_m(\lambda)$ vanishes then implies that $P_{\mathbf{i}}(\lambda)$ is also nonzero modulo l. The condition that l does not occur in the denominators of g or h is equivalent to the condition that l should not divide the *resultant* of Φ_m and $P_{\mathbf{i}}$ (essentially, the smallest positive integer R such that the equation $g(x)\Phi_m(x) + h(x)P_{\mathbf{i}}(x) \equiv R$ is solvable with polynomials $g, h \in \mathbb{Z}[x]$). Therefore, Theorem 1′ is true if we take for $\mathscr{E}_m(n)$ the union over all $\mathbf{i} \in (\mathbb{Z}/m\mathbb{Z})^n$ with $\Phi_m \nmid P_{\mathbf{i}}$ of the set of primes $l \equiv 1 \pmod m$ dividing the resultant of Φ_m and $P_{\mathbf{i}}$.

It remains to prove the integrality of the coefficients of the power series $A_m(X)$ and $B_m(X)$. Pick an integer $N > 0$. By Theorem 1, there is an integer d_0 (depending on m and N) such that the first N coefficients of $A_m B_m^d$ are equal to those of $F_{l,m}$, and hence integral, for all $d \geq d_0$ for which $l = md + 1$ is prime. If d_1 and d_2 are two such values of d, then it follows by division (since the power series A_m and B_m start with 1) that $B_m^{d_1 - d_2}$ also has integral coefficients up to degree N. But if B_m^a and B_m^b have integral coefficients, then so does $B_m^{(a,b)}$, where (a, b) denotes the g.c.d. of a and b, because this g.c.d. can be written as $ar + bs$ for some integers r and s. This proves that $B_m(X)^\mu$ has integral coefficients up to order N, where μ is the greatest common divisor of all of the differences $d_1 - d_2$ with $d_i \geq d_0$ and $md_i + 1$ prime. Dirichlet's theorem on primes in arithmetic progression implies that μ equals 1 if m is even and 2 if m is odd. (Indeed, it is obvious that this value of μ divides all d, and hence all differences of d, with the stated property. Conversely, the definition of μ says that all sufficiently large primes l which are congruent to 1 modulo m are in fact congruent to a fixed number l_1 modulo μm, and hence—by Dirichlet's theorem—that there is only one arithmetic progression $\{k\mu m + c\}_{k \geq 1}$ with $(c, \mu m) = 1$ and $c \equiv 1 \pmod{m}$. But this implies that $\varphi(\mu m) = \varphi(m)$ and hence that $\mu = 1$ if m is even, $\mu | 2$ if m is odd.) Therefore, B_m^d has integral coefficients up to degree N for large d with $md + 1$ prime, so the fact that $A_m B_m^d$ also has integral coefficients up to this degree implies that A_m does as well. Since N was arbitrary, it follows that $A_m(X)$ has integral coefficients, as claimed, and then $B_m(X)$ must, too, because of equation (1). (For m odd, the first part of our argument gave only the integrality of the coefficients of the square of B_m.) This completes the proof of Theorem 1.

Remark. For $m \geq 1$ define

$$C_m(X) = \exp\left(\sum_{n=1}^{\infty} \frac{(nm-1)!}{n!^m} X^n\right).$$

Then Theorem 2 implies that $C_m(X)$ has integral coefficients when m is prime (since then $C_m(X) = B_m(X^{1/m})^{-1}$). Numerical calculations for small m suggested that this remains true also for m composite. Maxim Kontsevich showed us how to prove the stronger assertion that $C_m(X)^{1/(m-1)!}$ has integral coefficients. This is best possible, since $C_m(X)$ begins with $1 + (m-1)!X + O(X^2)$.

3. Proof of Theorem 2 and determination of the exceptional set

In this section we discuss the computation of the coefficients $\beta_m(n)$ and $\beta_{l,m}(n)$ and the determination of the primes l for which they differ.

Obviously, the polynomial $P_{\mathbf{i}}(x)$ corresponding to $\mathbf{i} = (i_1, \ldots, i_n)$ depends only on the set $\mathbf{i}$ up to permutation and hence on the numbers $n_i = \#\{\nu \mid i_\nu = i\}$, $0 \leq i \leq m-1$. These numbers n_i satisfy $n_i \geq 0$ and $n_0 + \cdots + n_{m-1} = n$; conversely, for any such integers n_i there are $n!/(n_0! \cdots n_{m-1}!)$ corresponding n-tuples $\mathbf{i}$, for each of which $P_{\mathbf{i}}(x)$ is the polynomial $n_0 + n_1 x + \cdots + n_{m-1} x^{m-1}$. Hence,

$$\beta_m(n) = \sum_{\substack{n_0, n_1, \dots, n_{m-1} \geq 0 \\ n_0+n_1+\cdots+n_{m-1}=n \\ \Phi_m(x) \mid n_0+n_1x+\cdots+n_{m-1}x^{m-1}}} \frac{n!}{n_0! \cdots n_{m-1}!}. \tag{8}$$

The third condition in the summation can be replaced by $n_0 + n_1\lambda_0 + \cdots + n_{m-1}\lambda_0^{m-1} = 0$, and if λ_0 is replaced in this with the mth root of unity $\lambda \in \mathbb{Z}/l\mathbb{Z}$, then the same expression gives a formula for $\beta_{l,m}(n)$.

We now consider m of some special types. If $m = p$ is prime, then the cyclotomic polynomial Φ_m is the polynomial $1+x+\cdots+x^{p-1}$ of degree $m-1$, so the last condition under the summation sign in (8) can be satisfied only if $n_0 = n_1 = \cdots = n_{m-1}$, in which case the common value must be $n/m = n/p$. This proves (6) of Theorem 2. More generally, if $m = p^j$, then $\Phi_m(x) = (x^m - 1)/x^{m'-1} = 1 + x^{m'} + \cdots + x^{m'(p-1)}$, where $m' = m/p = p^{j-1}$. If this divides $n_0+n_1x+\cdots+n_{m-1}x^{m-1}$, then the quotient is $n_0+n_1x+\cdots+n_{m'-1}x^{m'-1}$ and the sequence $(n_0, n_1, \dots, n_{m-1})$ is just the sequence $(n_0, n_1, \dots, n_{m'-1})$ repeated p times. Hence,

$$\beta_m(n) = \sum_{\substack{n_0, n_1, \dots, n_{m'-1} \geq 0 \\ p(n_0+n_1+\cdots+n_{m'-1})=n}} \frac{n!}{(n_0! \cdots n_{m'-1}!)^p}.$$

Multiplying this by $X^n/n!$ and summing over n, we obtain the generating function given in (4). Obviously, (6) is a special case of (4), but we have preferred to give it separately since it is simpler and since here one can give a closed formula for each $\beta_m(n)$. This is also the case for $m = 4$, where equation (4) gives $\beta_4(n) = 0$ for n odd and

$$\beta_4(2n) = \sum_{n_0+n_1=n} \frac{(2n)!}{n_0!^2 n_1!^2} = \binom{2n}{n} \sum_{n_0=0}^{n} \binom{n}{n_0}^2 = \binom{2n}{n}^2,$$

proving equation (7). Finally, if $m = 2p$ with p an odd prime, then $\Phi_m(x) = (x^p + 1)/(x + 1) = 1 - x + x^2 - \cdots + x^{p-1}$, and it is easily checked that $n_0 + n_1x+\cdots+n_{2p-1}x^{2p-1}$ is divisible by this if and only if $(n_0, n_1, \dots, n_{2p-1})$ has the form $(n_0, n_1, \dots, n_{p-1}, n_0 + r, n_1 - r, \dots, n_{p-1} + r)$ for some integers $n_0, \dots, n_{p-1}$ and r satisfying $2(n_0 + \cdots + n_{p-1}) + r = n$; this easily leads to (5) by setting $A = n_0 + \cdots + n_{p-1}$ if $r \geq 0$, $A = n_0 + \cdots + n_{p-1} + r$ if $r < 0$. In general, the smaller the difference between $m - 1$ and $\varphi(m)$ the easier it is to analyze the divisibility condition in (8) and hence to give an explicit description of the coefficients $\beta_m(n)$.

Finally, we discuss the computation of the exceptional set $\mathscr{E}_m(n)$. For fixed values of m and n, we consider n-tuples $\mathbf{i} = (i_1, \dots, i_n) \in (\mathbb{Z}/m\mathbb{Z})^n$ and denote by $R_{\mathbf{i}}$ the resultant of the polynomials $P_{\mathbf{i}}$ and $\Phi_m(x)$. This resultant is easily computed as the norm of the algebraic number $P_{\mathbf{i}}(\lambda_0)$, i.e., as the product of the numbers $P_{\mathbf{i}}(\lambda)$ as λ ranges over the primitive mth roots of unity in $\mathbb{C}$. The number of n-tuples $\mathbf{i}$ with $R_{\mathbf{i}} = 0$ is $\beta_m(n)$, and the primes $l \equiv 0 \pmod{m}$ dividing any nonzero $R_{\mathbf{i}}$ are the members of the exceptional set $\mathscr{E}_m(n)$. Obviously two values of $\mathbf{i}$ which are equivalent under (i) permutation of the i_j's, (ii) translations $i_j \mapsto i_j + c \pmod{m}$ for any $c \in (\mathbb{Z}/m\mathbb{Z})$, or (iii) scalings $i_j \mapsto ki_j \pmod{m}$ for any $k \in (\mathbb{Z}/m\mathbb{Z})^\times$ give the same value of $R_{\mathbf{i}}$,

TABLE 4. Examples of resultant computations

$m = 7,\ n = 5$: i	$R_{\mathbf{i}}$	$m = 11,\ n = 4$: i	$R_{\mathbf{i}}$	$m = 12,\ n = 3$: i	$R_{\mathbf{i}}$
(0,0,0,0,1)	$29 \cdot 113$	(0,0,0,1)	$67 \cdot 661$	(0,0,1)	13
(0,0,0,1,1)	463	(0,0,1,1)	2^{10}	(0,0,2)	7^2
(0,0,0,1,2)	421	(0,0,1,2)	23^2	(0,0,3)	5^2
(0,0,0,1,3)	$2^3 \cdot 71$	(0,0,1,3)	991	(0,0,4)	3^2
(0,0,0,1,6)	13^2	(0,0,1,5)	$23 \cdot 67$	(0,0,6)	1
(0,0,1,1,2)	29	(0,0,1,7)	419	(0,1,2)	2^2
(0,0,1,1,3)	197	(0,0,1,10)	1	(0,1,3)	13
(0,0,1,1,4)	1	(0,1,2,3)	1	(0,1,4)	1
(0,0,1,2,3)	43	(0,1,2,4)	23	(0,1,5)	2^2
(0,0,1,2,4)	2^6	(0,1,2,5)	89	(0,1,6)	1
(0,0,1,2,5)	29	(0,1,3,4)	1	(0,2,4)	2^4
(0,0,1,2,6)	2^3			(0,2,6)	1
(0,1,2,3,4)	1			(0,3,6)	1

so we need only compute the resultants for inequivalent values of $\mathbf{i}$. Table 4 shows the results of this computation for all inequivalent n-tuples $\mathbf{i}$ in the cases $(m, n) = (7,5)$, $(11,4)$, and $(12,3)$, illustrating the way that the corresponding entries of Table 3 were computed. (Note that only the prime divisors of $R_{\mathbf{i}}$ congruent to 1 modulo m must be taken—this is automatic if the prime occurs to the first power—and also that the primes occurring for a given value of n may be new exceptional primes for any $n' \leq n$.) However, in these three examples there are only about a dozen inequivalent n-tuples $\mathbf{i}$, whereas, for example, computing the final entry in Table 3 required looking at over thirty thousand inequivalent orbits.

4. THE CASE $m = 2$

In this case we find from (3) and (6)

$$\frac{B_2'(X)}{B_2(X)} = -\sum_{n=1}^{\infty} \frac{(2n)!}{n!^2} X^{2n-1} = \frac{1}{X}\left(1 - \frac{1}{\sqrt{1-4X^2}}\right),$$

from which we obtain the closed formulas and power series expansions

$$B_2(X) = \frac{1}{2}\left(1 + \sqrt{1-4X^2}\right) = 1 - \sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{n+1} X^{2n+2},$$

$$A_2(X) = \frac{1}{2}\left(1 + \sqrt{\frac{1+2X}{1-2X}}\right) = \frac{1}{2} + \sum_{n=0}^{\infty} \binom{2n}{n}\left(\frac{1}{2}X^{2n} + X^{2n+1}\right).$$

However, here we can give complete formulas on the polynomials $F_{l,m}(X)$. First of all, the mth root of unity λ here is just $-1 \pmod{l}$, so we can extend the definition of $F_{l,m}(X)$ to all odd values of l by

$$F_{l,2}(X) = P_d(X) := \prod_{j=1}^{d} (1 - (\zeta_l^j + \zeta_l^{-j})\, X) \qquad (\zeta_l = e^{2\pi i/l},\ \ l = 2d+1).$$

TABLE 5. Coefficients of $A_2(X)\,B_2(X)^d$

	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	X^{10}	X^{11}	...
$d=1$	1	1	0	1	1	3	4	10	15	35	56	126	...
2	1	1	−1	0	0	1	1	4	5	15	21	56	...
3	1	1	−2	−1	0	0	0	1	1	5	6	21	...
4	1	1	−3	−2	1	0	0	0	0	1	1	6	...
5	1	1	−4	−3	3	1	0	0	0	0	0	1	...
6	1	1	−5	−4	6	3	−1	0	0	0	0	0	...
7	1	1	−6	−5	10	6	−4	−1	0	0	0	0	...

Theorem 3. *The polynomials* $P_d(X)$ *are given by the closed formula*

$$P_d(X) = \frac{1}{2}\left(1+\sqrt{\frac{1+2X}{1-2X}}\right)\left(\frac{1+\sqrt{1-4X^2}}{2}\right)^d + \frac{1}{2}\left(1-\sqrt{\frac{1+2X}{1-2X}}\right)\left(\frac{1-\sqrt{1-4X^2}}{2}\right)^d, \tag{9}$$

by the recursion

$$P_d(X) = P_{d-1}(X) - X^2 P_{d-2}(X) \qquad (d \geq 2) \tag{10}$$

(with the initial conditions $P_0(X) = 1$, $P_1(X) = 1 + X$*), by the generating function*

$$\sum_{d=0}^{\infty} P_d(X)\,T^d = \frac{1+XT}{1-T+X^2T^2}, \tag{11}$$

or by the expansion

$$P_d(X) = \sum_{n=0}^{d} (-1)^{[n/2]} \binom{[d-\frac{n}{2}]}{[\frac{n}{2}]} X^n. \tag{12}$$

Clearly, this sharpens Theorem 1: equation (9) implies that the congruence $F_{l,2} = A_2 B_2^d$ holds modulo X^{2d+1}, which determines $F_{l,2}$ completely since its degree equals d (cf. Table 5), while (12) gives all the coefficients of the polynomial $F_{l,2}(X)$ explicitly.

Proof. Define P_d by (9) (rather than as $F_{l,2}$). Then

$$\sum_{d=0}^{\infty} P_d(X)\,T^d = \frac{\frac{1}{2}\left(1+\sqrt{\frac{1+2X}{1-2X}}\right)}{1-\frac{1}{2}(1+\sqrt{1-4X^2})T} + \frac{\frac{1}{2}\left(1-\sqrt{\frac{1+2X}{1-2X}}\right)}{1-\frac{1}{2}(1-\sqrt{1-4X^2})T} = \frac{1+XT}{1-T+X^2T^2}.$$

This proves (11). The recursion (10) follows by multiplying both sides by $1 - T + X^2T^2$ and comparing coefficients of T^d, while (12) follows by expanding the right-hand side as a geometric series

$$\frac{1+TX}{1-T+T^2X^2} = (1+TX)\sum_{n=0}^{\infty}\frac{(-1)^n T^{2n} X^{2n}}{(1-T)^{2n+1}} = \sum_{n=0}^{\infty}\frac{(-1)^{[n/2]}T^n}{(1-T)^{2[n/2]+1}}X^n$$

and using the binomial theorem. This proves the equivalence of (9)–(12).

Now let $Q_d(X) = X^d P_d(X^{-1})$, the reciprocal polynomial of $P_d(X)$. Then the generating function of the $Q_d(X)$ is

$$\sum_{d=0}^{\infty} Q_d(X)\, T^d = \sum_{d=0}^{\infty} P_d(X^{-1})\,(XT)^d = \frac{1+T}{1-XT+T^2}.$$

Substituting $X = z + z^{-1}$ gives

$$\sum_{d=0}^{\infty} Q_d\big(z+z^{-1}\big)\, T^d = \frac{1+T}{1-(z+z^{-1})T+T^2} = \frac{1+T}{(1-zT)(1-z^{-1}T)}$$

$$= \frac{1}{1-z}\left(\frac{1}{1-z^{-1}T} - \frac{z}{1-zT}\right) = \sum_{d=0}^{\infty} \frac{z^{-d}-z^{d+1}}{1-z}\, T^d,$$

whence $Q_d\big(z+z^{-1}\big) = z^{-d}\big(1+z+z^2+\cdots+z^{2d}\big)$. Thus Q_d has the d roots $\zeta_l^j + \zeta_l^{-j}$ $(1 \le j \le d)$, where $l = 2d+1$. Since Q_d is monic (because $P_d(X)$ has constant term 1) and has degree d, this property uniquely characterizes $Q_d(X)$, so $Q_d(X) = \prod_j \big(X - \zeta_l^j - \zeta_l^{-j}\big)$, the reciprocal polynomial of $F_{l,2}$. This completes the proof of Theorem 3. We observe that the property of Q_d just used can be rewritten via the substitution $z = e^{i\theta}$ as

$$Q_d(2\cos\theta) = \frac{\sin(d+\frac{1}{2})\theta}{\sin\frac{1}{2}\theta} = \frac{\sin(d+1)\theta + \sin d\theta}{\sin\theta},$$

so that $Q_d(X)$ can be expressed in terms of the classical Chebyshev polynomials $S_n(X)$ by $Q_d(X) = S_{2d}(\sqrt{X}) = S_d(X) + S_{d-1}(X)$.

5. Composite l

In this section we give a partial generalization of our results to the case of composite l. Let $m_1, \ldots, m_s$ be fixed positive integers and consider integers of the form $l = l_1 \cdots l_s$, where the l_i are distinct primes of the form $l_i = m_i d_i + 1$, $d_i > 1$. Then the group $G = (\mathbb{Z}/l\mathbb{Z})^\times$ contains a subgroup H of order $m = m_1 \cdots m_s$ given by

$$H = \big\{x \pmod{l} \mid x^{m_i} \equiv 1 \text{ cf. } (\mathrm{mod} l_i \text{ for } i = 1, \ldots, s\big\}.$$

If we identify G with the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ (ζ a primitive lth root of unity), then H corresponds to a subfield K of $\mathbb{Q}(\zeta)$ of degree $d = d_1 \cdots d_s$. This field contains, and by the result in the Appendix of [2] is in fact generated by, the number

$$\omega = \mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta) = \sum_{x \in H} \zeta^x.$$

We denote the conjugates $\sum_{x \in H} \zeta^{jx}$ $(j \in G/H)$ of ω by $\omega^{(j)}$ and set

$$F(X) = F_{l_1,\ldots,l_s;m_1,\ldots,m_s}(X) = \prod_{j \in G/H} \big(1 - \omega^{(j)} X\big).$$

Then the same calculation as at the beginning of §2 gives

$$\log F(X) = -\sum_{n \ge 1} S_n X^n / n$$

with

$$S_n = \sum_{j\in G/H} (\omega^{(j)})^n = \frac{1}{|H|}\sum_{j\in G}\sum_{x_1,\dots,x_n\in H} \zeta^{j(x_1+\cdots+x_n)}$$
$$= \frac{1}{m}\sum_{k|l}\mu\left(\frac{l}{k}\right)\cdot k\cdot \#\{(x_1,\dots,x_n)\in H^n \mid x_1+\cdots+x_n\equiv 0 \pmod k\},$$

where the last equality follows from the standard evaluation of the Ramanujan sum $\sum_{j\in G}\zeta^{jx}$. We can write each divisor k of l as $\prod_{i\in I} l_i$ for some subset I of $J=\{1,\dots,s\}$. The expression $\#\{\cdots\}$ is multiplicative in the obvious sense, and we find

$$S_n = \frac{1}{m}\sum_{I\subset J}\prod_{i\notin I}(-m_i^n)\prod_{i\in I}(l_i\,\beta_{l_i,m_i}(n)).$$

Thus, if we define for any set $\mathscr{M}$ of (not necessarily distinct) positive integers a power series $B_{\mathscr{M}}(X)$ by

$$B_{\mathscr{M}}(X) = \exp\left(-\sum_{n=1}^{\infty}\beta_{\mathscr{M}}(n)\frac{X^n}{n}\right), \qquad \beta_{\mathscr{M}}(n) := \prod_{m\in\mathscr{M}}\beta_m(n)$$

(this is a priori in $\mathbb{Q}[[X]]$ but actually in $\mathbb{Z}[[X]]$, as we shall see below), then we find that

$$F(X) \equiv \prod_{I\subset J} B_{\mathscr{M}_I}(m_{I'}X)^{(-1)^{s-|I|}\prod_{i\in I} l_i/m} \pmod{X^N} \tag{13}$$

(with $\mathscr{M}_I=\{m_i,\ i\in I\}$, $m_{I'}=\prod_{i\notin I} m_i$) for any $N>0$, so long as no l_i is in the exceptional set $\mathscr{E}_{m_i}(n)$ for any $n<N$. For $s=1$ the power series on the right of (13) is $B_{\{m\}}(X)^{l/m}B_{\varnothing}(mX)^{-1/m}$, which agrees with Theorem 1 since $B_{\{m\}}(X)=B_m(X)$ and $B_{\varnothing}(X)=1-X$. For $s=2$ we obtain instead

$$\left(\frac{B_{\{m_1,m_2\}}(X)^{l_1l_2}(1-m_1m_2X)}{B_{m_1}(m_2X)^{l_1}B_{m_2}(m_1X)^{l_2}}\right)^{1/m}$$

or

$$\left[B_{\{m_1,m_2\}}(X)\right]^{d_1d_2}\left[\left(\frac{B_{\{m_1,m_2\}}(X)}{B_{m_1}(m_2X)}\right)^{1/m_2}\right]^{d_1}\left[\left(\frac{B_{\{m_1,m_2\}}(X)}{B_{m_2}(m_1X)}\right)^{1/m_1}\right]^{d_2}$$
$$\times\left[\left(\frac{B_{\{m_1,m_2\}}(X)(1-m_1m_2X)}{B_{m_1}(m_2X)B_{m_2}(m_1X)}\right)^{1/m_1m_2}\right].$$

Using the integrality of $B_{\mathscr{M}}(X)$ and the same argument as at the end of §2, we can show that each of the four expressions in square brackets is a power series with integral coefficients (and similarly for $s\geq 3$). This generalizes the integrality statement of Theorem 1.

It remains to prove the integrality of $B_{\mathscr{M}}(X)$ for any set $\mathscr{M}$. But this follows easily from the corresponding statement for $|\mathscr{M}|=1$. Indeed, a well-known and easily proved integrality criterion says that a power series of the form $\exp(\sum_{n=1}^{\infty}\beta(n)X^n/n)$ has integral coefficients if and only if the coefficients $\beta(n)$ are integers such that $\beta(n)\equiv\beta(n/p) \pmod{p^\nu}$ whenever $p^\nu|n$,

$\nu \geq 1$. The integrality of $B_m(X)$ implies that the numbers $\beta(n) = \beta_m(n)$ satisfy these congruences. It follows that the numbers $\beta(n) = \beta_{\mathcal{M}}(n)$ also do and hence that $B_{\mathcal{M}}(X) \in \mathbb{Z}[[X]]$.

All of the contents of this section except for the statements about integrality can be found essentially in [2] (Corollary 4, Prop. 3, and their proofs).

Acknowledgment

The first author would like to thank James L'Heureux of West Chester University, one of whose questions led him to work on this paper.

Bibliography

1. S. Gurak, *Minimal polynomials for Gauss circulants and cyclotomic units*, Pacific J. Math. **102** (1982), 347–353.
2. ———, *Minimal polynomials for circular numbers*, Pacific J. Math. **112** (1984), 313–331.
3. D.H. Lehmer and E. Lehmer, *Cyclotomy with short periods*, Math. Comp. **41** (1983), 743–758.

Department of Mathematics, West Chester University of Pennsylvania, West Chester, Pennsylvania 19383
E-mail address: sgupta@wcu.bitnet

Max-Planck-Institut für Mathematik, Gottfried-Claren-Strasse 26, D-5300 Bonn 3, Germany
E-mail address: zagier@mpim-bonn.mpg.de