MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 132
OCTOBER 1975, PAGES 1138–1143

Zeros of p-Adic L-Functions

By Samuel S. Wagstaff, Jr.

Abstract. The p-adic coefficients and zeros of certain formal power series defined by Iwasawa have been calculated modulo various powers of p. Using these results and Iwasawa's formula for the p-adic L-function $L_p(s; \chi)$ of Kubota and Leopoldt, several p-adic places of the zero of $L_p(s; \chi)$ were computed for the irregular primes $p \leqslant 157$.

1. Introduction. Let p be an odd prime and let i be an odd index $1 \leqslant i \leqslant p - 2$. Iwasawa [2] has defined various formal power series in T with p-adic integer coefficients,

$${}^ig(T) = {}^i\alpha + {}^i\beta T + {}^i\gamma T^2 + {}^i\delta T^3 + {}^i\epsilon T^4 + \dots,$$

which play an important role in the theory of class numbers of cyclotomic fields. These power series are of particular interest when p is an irregular prime and p divides the numerator of the Bernoulli number B_{i+1}, using the even index notation of [1]. As we shall see, this condition is equivalent to the condition ${}^i\alpha \equiv 0 \pmod p$. Iwasawa and Sims [4] verified that ${}^i\alpha \not\equiv 0 \pmod{p^2}$ and ${}^i\beta \not\equiv 0 \pmod p$ for the irregular prime pairs (p, i) with $p \leqslant 4001$, and W. Johnson [5] has extended their result to all irregular primes $p < 30000$. This implies that ${}^ig(T)$ has a unique zero ${}^i\omega$ in the ring $\mathbf{Z}_p$ of p-adic integers and that ${}^i\omega \equiv 0 \pmod p$.

In this paper we report on computations of some of the coefficients of ${}^ig(T)$ and of the zeros ${}^i\omega$ modulo higher powers of p. The zeros ${}^i\omega$ are related to zeros of certain p-adic L-functions which we also calculated. One important use of the latter numbers would be to test possible formulations of an analog of the Riemann Hypothesis for p-adic L-functions.

2. ${}^ig(T)$ and p-Adic L-Functions. We follow the notation of Iwasawa and Sims [4]. The rational numbers and the p-adic numbers are denoted by $\mathbf{Q}$ and $\mathbf{Q}_p$. Let F be the union of all the cyclotomic fields of p^nth roots of unity over $\mathbf{Q}$ for $n \geqslant 1$ and Γ denote the subgroup of the Galois group of F over $\mathbf{Q}$ corresponding to the group of 1-units in $\mathbf{Q}_p$. Let V be the group of all $(p-1)$st roots of unity in $\mathbf{Q}_p$.

For $a \in \mathbf{Q}_p$, let $\langle a \rangle$ denote the rational number b/p^m, where $p^m a \equiv b \pmod{p^m}$ and $0 \leqslant b < p^m$. Thus $\langle a \rangle$ is uniquely determined by a, although b and m are not. For odd indices $1 \leqslant i \leqslant p - 4$, we define ${}^ig(T)$ in the ring Λ of formal power series with coefficients in $\mathbf{Z}_p$. For such i and for $n \geqslant 0$, let

$${}^ig_n(T) = \sum_{m=0}^{p^n-1} \sum_{v \in V} \langle v(1+p)^m/p^{n+1} \rangle v^i (1+T)^m.$$

Received January 16, 1974; revised April 15, 1975.
AMS (MOS) subject classifications (1970). Primary 12B30, 12A35; Secondary 12–04.
Key words and phrases. p-adic L-functions, cyclotomic field, irregular primes.

Then ${}^ig_n(T)$ is a polynomial in T with coefficients in $\mathbf{Z}_p$ and degree less than p^n. As $n \longrightarrow \infty$, ${}^ig_n(T)$ converges on each coefficient of T^m to a power series ${}^ig(T)$ in Λ, and we have

$$(1) \qquad {}^ig(T) \equiv {}^ig_n(T) \mod (1 - (1 + T)^{p^n})\Lambda \qquad (n \geqslant 0).$$

Under the hypothesis that the first factor ${}^+h_0$ of the class number of the field of pth roots of unity over $\mathbf{Q}$ is prime to p, Iwasawa [3] has proved that for odd $i \neq 1$,

$${}^ig((1 + p)^{-s} - 1) = -L_p(s; \chi_i) \qquad (s \in \mathbf{Z}_p)$$

where χ_i is the character of integers modulo p, with values in $\mathbf{Q}_p$, such that $\chi_i(a) \equiv a^{p-i} \pmod p$ for all integers a, and $L_p(s; \chi_i)$ is the Kubota-Leopoldt [7] p-adic L-function. This hypothesis has been verified by the combined efforts of several authors [5], [6], [8] – [11] for all $p < 30000$. Iwasawa and Sims [4] and W. Johnson [5] have shown that for $p < 30000$, if p divides the numerator of B_{i+1}, then ${}^ig(T)$ has a unique zero ${}^i\omega$ and that ${}^i\omega \in p\mathbf{Z}_p$. It follows that, for such p and i, $L_p(s; \chi_i)$ has exactly one zero $s = {}^i\kappa \in \mathbf{Z}_p$ and that ${}^i\kappa$ is determined by

$$(2) \qquad (1 + p)^{-{}^i\kappa} = 1 + {}^i\omega.$$

3. Computation of ${}^i\alpha$. With $n = 0$ in (1), we have ${}^ig(T) \equiv {}^ig_0(T) \pmod{T\Lambda}$. Therefore ${}^i\alpha = {}^ig(0) = {}^ig_0(0) = \Sigma_{v \in V}\langle v/p\rangle v^i$. For $1 \leqslant a \leqslant p - 1$, let $v_a \in V$ be such that $v_a \equiv a \pmod p$. Thus we have

$$(3) \qquad {}^i\alpha = \sum_{a=1}^{p-1} \left\langle \frac{a}{p} \right\rangle v_a^i = \frac{1}{p} \sum_{a=1}^{p-1} a v_a^i.$$

For $1 \leqslant a \leqslant p - 1$, it is clear that

$$(i + 1)av_a^i \equiv iv_a^{i+1} + a^{i+1} \pmod{p^2}.$$

We sum over a. Since V is cyclic of order $p - 1$ and $p - 1 \nmid i + 1$, we have

$$\sum_{a=1}^{p-1} v_a^{i+1} = \sum_{v \in V} v^{i+1} = 0.$$

Hence

$$(i + 1) \sum_{a=1}^{p-1} av_a^i \equiv \sum_{a=1}^{p-1} a^{i+1} \equiv B_{i+1}p \pmod{p^2}.$$

Using (3), we find

$$(i + 1)\, {}^i\alpha p \equiv B_{i+1}p \pmod{p^2},$$

which shows that ${}^i\alpha \equiv 0 \pmod p$ if and only if p is an irregular prime and i is an odd index such that p divides B_{i+1}. Assuming that p does not divide ${}^+h_0$, it follows that $L_p(s; \chi_i)$ has no zero $s \in \mathbf{Z}_p$ unless (p, i) is such a pair.

Using Eq. (3), ${}^i\alpha$ was computed modulo p^7 for all irregular primes $p \leqslant 157$. Write ${}^i\alpha = \Sigma_{j=0}^{\infty} a_j p^j$. The values of $a_1, \ldots, a_6$ are given in Table I. (The a_2 of [4] is our a_1.) We have seen above that $a_0 = 0$ when p divides B_{i+1}.

After Table I was computed, we wondered whether perhaps $a_j = 1$ for sufficiently large j. But a calculation of ${}^{31}\alpha \pmod{37^{21}}$ showed that this fails. The first 21 p-adic places of ${}^{31}\alpha$ for $p = 37$ are:

0, 23, 3, 23, 24, 1, 1, 29, 27, 36, 0, 21, 23, 2, 8, 27, 1, 1, 5, 0, 18.

TABLE I

p	i	a_1	a_2	a_3	a_4	a_5	a_6
37	31	23	3	23	24	1	1
59	43	20	17	14	42	24	1
67	57	34	11	36	34	31	56
101	67	16	72	15	83	44	70
103	23	1	62	65	16	47	98
131	21	34	7	41	68	0	110
149	129	24	51	24	67	56	102
157	61	66	97	114	33	142	145
157	109	109	151	75	91	6	108

4. Computation of ${}^i\beta$, ${}^i\gamma$, etc. Let $1 \leqslant k < p$ and η_k be the coefficient of T^k in ${}^ig(T)$. Let $1 \leqslant n \leqslant p-1$. Then $(1-(1+T)^{p^n})\Lambda \subset (p^n, T^p)\Lambda$, so (1) implies

$$ {}^ig(T) \equiv {}^ig_n(T) \qquad (\mathrm{mod}(p^n, T^p)\Lambda). $$

Since $v_a \equiv a^{p^n} \pmod{p^{n+1}}$ for $n \geqslant 0$, we have the following congruences modulo p^n:

$$ \eta_k \equiv \sum_{m=0}^{p^n-1} \sum_{v\in V} \langle v(1+p)^m/p^{n+1}\rangle v^i \binom{m}{k} $$

$$ \equiv \sum_{a=1}^{p-1} v_a^i \sum_{m=0}^{p^n-1} \left\langle a^{p^n} \frac{(1+p)^m}{p^{n+1}} \right\rangle \binom{m}{k} \equiv \frac{1}{p} \sum_{a=1}^{p-1} a^{ip^n} \frac{1}{p^n} \sum_{m=0}^{p^n-1} B(a,m)\binom{m}{k}, $$

where

$$ B(a,m) \equiv a^{p^n}(1+p)^m \equiv a^{p^n}\left(1 + \binom{m}{1}p + \dots + \binom{m}{n}p^n\right) \qquad (\mathrm{mod}\ p^{n+1}) $$

and $0 \leqslant B(a,m) < p^{n+1}$. From the familiar identity $\binom{m}{k} = \sum_{r=0}^{k}\binom{m-j}{r}\binom{j}{k-r}$, we have

$$ \sum_{m=0}^{p^n-1}\binom{m}{j}\binom{m}{k} = \sum_{m=0}^{p^n-1}\sum_{r=0}^{k}\binom{m}{j+r}\binom{j+r}{r}\binom{j}{k-r} = \sum_{t=j}^{j+k}\binom{t}{j}\binom{j}{t-k}\sum_{m=0}^{p^n-1}\binom{m}{t}. $$

But

$$ \sum_{m=0}^{p^n-1}\binom{m}{t} = \binom{p^n}{t+1} \equiv 0 \qquad (\mathrm{mod}\ p^n) $$

for $t+1 < p$, and we have

$$\sum_{m=0}^{p^n-1} B(a, m)\binom{m}{k} \equiv a^{p^n} \sum_{j=0}^{n} p^j \sum_{m=0}^{p^n-1} \binom{m}{k}\binom{m}{j} \equiv 0 \pmod{p^n}$$

for $k + n + 1 < p$. Hence

$$^i\beta \equiv \frac{1}{p}\sum_{a=1}^{p-1} a^{ip^n} \frac{1}{p^n}\sum_{m=0}^{p^n-1} B(a, m)m \pmod{p^n},$$

$$^i\gamma \equiv \frac{1}{p}\sum_{a=1}^{p-1} a^{ip^n} \frac{1}{p^n}\sum_{m=0}^{p^n-1} B(a, m)\binom{m}{2} \pmod{p^n},$$

etc., and if the calculation is done in this order, only integers will be used. The inner sums must be computed modulo p^{2n+1}, and the outer sums modulo p^{n+1}. The calculation time is roughly proportional to p^{n+1}, the total number of terms.

Let $^i\beta = \Sigma_{j=0}^{\infty} b_j p^j$, $^i\gamma = \Sigma_{j=0}^{\infty} c_j p^j$, etc. The numbers b_j, c_j, d_j, and e_j which were calculated are shown in Table II.

TABLE II

p	i	b_0	b_1	b_2	b_3	c_0	c_1	c_2	d_0	d_1	e_0
37	31	16	6	32	32	29	20	28	2	13	22
59	43	33	45	6		46	2		45		
67	57	46	56	6		55	35		64		
101	67	59	19			95			92		
103	23	49	30			102			40		
131	21	106	13			122			59		
149	129	70	67			140			123		
157	61	109	82			92			129		
157	109	106	30			29			141		

5. Programming Details. All calculations were done using multiprecision integer routines on the IBM 360/75 at the University of Illinois. The program for b_3 for $p = 37$ took two and one half hours and was the longest running one. Most of the other numbers had been calculated earlier on the IBM 360/91 at Princeton University using floating point numbers in an unusual way. The largest single precision integer on the IBM 360 is $2^{31} - 1$, but integers as large as 2^{56} are exactly represented as double precision floating point numbers. Double precision floating point arithmetic is done automatically on the IBM 360, but double precision integer arithmetic is not, and the latter is much slower. Consider the inner sum $\Sigma_{m=0}^{p^3-1} B(a, m)m$ in the formula for $^i\beta \pmod{p^3}$. We have $B(a, m) < p^4$ and $m < p^3$. There are p^3 terms so the sum is less than p^{10}. For $p = 37$, a term in the sum might be too large to be represented as a single precision integer since $37^7 > 2^{31}$. However, $37^{10} < 2^{56}$ so the whole sum can be computed in ordinary double precision floating point numbers. For $p = 59$ and $p = 67$, we have $p^9 < 2^{56} < p^{10}$ so the partial sum had to be reduced modulo p^7 every so often to stay less than 2^{56}. Using this method, the entire computation of $^{31}\beta$ (modulo 37^3) required only 38 seconds.

6. Computation of $^i\omega$ and $^i\kappa$. The p-adic integer $^i\omega$ such that $^ig(^i\omega) = 0$ was computed modulo p^5 for $p = 37$, modulo p^4 for $p = 59$ and 67, and modulo p^3 for $p = 101$, 103, 131, 149, and 157. The number $^i\kappa$ satisfying (2) was computed modulo one lower power of p in each case. Let $^i\omega = \Sigma_{j=0}^{\infty} w_j p^j$ and $^i\kappa = \Sigma_{j=0}^{\infty} k_j p^j$. Then $w_0 = 0$ and $w_1 + k_0 \equiv 0 \pmod p$. Table III shows the values of w_j and k_j which were computed. The relations $w_1 \equiv -a_1/b_0 \pmod p$ and $0 \leqslant w_1 < p$ determine w_1. For $j = 2, 3, 4$, w_j was computed by trying the values $0, 1, \ldots, p-1$ successively and substituting into $^ig(w_1 p + \ldots + w_n p^j) \equiv 0 \pmod{p^{j+1}}$. Since $w_1 \neq 0$ in all the cases computed, it follows for these that $k_0 = p - w_1$ and $k_1 \equiv \binom{w_1}{2} - w_2 - 1 \pmod p$. Then for $j = 2, 3$, k_j is the number which satisfies $0 \leqslant k_j < p$ and $(1 + p)^{K(j)} \equiv 1 + {}^i\omega \pmod{p^{j+2}}$, where $K(j) = p^{j+1} - k_0 - k_1 p - \ldots - k_j p^j$.

TABLE III

p	i	w_1	w_2	w_3	w_4	k_0	k_1	k_2	k_3
37	31	24	33	8	35	13	20	30	8
59	43	28	14	42		31	9	15	
67	57	8	43	60		59	51	7	
101	67	10	45			91	100		
103	23	21	22			82	84		
131	21	59	74			72	64		
149	129	55	1			94	142		
157	61	21	105			136	104		
157	109	36	72			121	86		

We were unable to discern any pattern in the numbers $^i\omega$ and $^i\kappa$. It would be interesting, for example, if they were all rational numbers with small numerator and denominator. We searched for such a representation m/n with $|m|, |n| \leqslant p^2$ for $^i\omega/p$ and $^i\kappa$ and for $1 + {}^i\omega$, which has an important arithmetic meaning in the theory of cyclotomic fields (cf. [4, pp. 89–91]). For $p = 37$, $i = 31$ we found only

$$\frac{^i\omega}{p} \equiv \frac{-77}{652} = -\frac{(2p+3)}{18p-14} = -\frac{(2p+3)}{21i+1} \pmod{37^4}$$

and

$$^i\kappa \equiv \frac{-63}{109} = -\frac{p+26}{3p-2} = -\frac{2i+1}{3p-2} \pmod{37^4}.$$

No such representation for $1 + {}^i\omega$ was found. Dozens of congruences like the two above hold modulo 37^3 so there is no reason to believe that either of these congruences holds modulo 37^5.

Similar calculations were made for $p = 59$ and $p = 67$. But in these cases $^i\omega/p$ and $^i\kappa$ are known only modulo p^3 so we found dozens of congruences. In neither case was $^i\kappa \equiv -(2i + 1)/(3p - 2)$ one of them.

The author thanks Professor Iwasawa for suggesting that he make these calculations. He is grateful to the referee for suggesting numerous improvements in the original paper.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

1. Z. I. BOREVICH (BOREVIČ) & I. R. SHAFAREVICH (ŠAFAREVIČ), *Number Theory*, "Nauka", Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR 30 #1080; 33 #4001.

2. K. IWASAWA, "On some modules in the theory of cyclotomic fields," *J. Math. Soc. Japan*, v. 16, 1964, pp. 42–82. MR 35 #6646.

3. K. IWASAWA, "On p-adic L-functions," *Ann. of Math.* (2), v. 89, 1969, pp. 198–205. MR 42 #4522.

4. K. IWASAWA & C. C. SIMS, "Computation of invariants in the theory of cyclotomic fields," *J. Math. Soc. Japan*, v. 18, 1966, pp. 86–96. MR 34 #2560.

5. WELLS JOHNSON, "Irregular primes and cyclotomic invariants," *Math. Comp.*, v. 29, 1975, pp. 113–120.

6. V. V. KOBELEV, "Proof of Fermat's last theorem for all prime exponents less than 5500," *Dokl. Akad. Nauk SSSR*, v. 190, 1970, pp. 767–768 = *Soviet Math. Dokl.*, v. 11, 1970, pp. 188–190. MR 41 #3363.

7. T. KUBOTA & H. W. LEOPOLDT, "Eine p-adische Theorie der Zetawerte," *J. Reine Angew. Math.*, v. 214/215, 1964, pp. 328–339. MR 29 #1199.

8. D. H. LEHMER, E. LEHMER & H. S. VANDIVER, "An application of high-speed computing to Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 40, 1954, pp. 25–33. MR 15, 778.

9. J. L. SELFRIDGE, C. A. NICOL & H. S. VANDIVER, "Proof of Fermat's last theorem for all prime exponents less than 4002," *Proc. Nat. Acad. Sci. U.S.A.*, v. 41, 1955, pp. 970–973. MR 17, 348.

10. J. L. SELFRIDGE & B. W. POLLACK, "Fermat's last theorem is true for any exponent up to 25,000," *Notices Amer. Math. Soc.*, v. 11, 1964, p. 97. Abstract #608–138.

11. H. S. VANDIVER, "Examination of methods of attack on the second case of Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 40, 1954, pp. 732–735. MR 16, 13.