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 $p \leq 157$.

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

$$i g(T) = i\alpha + i\beta T + i\gamma T^2 + i\delta T^3 + i\varepsilon T^4 + \ldots,$$

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 $i\beta \not\equiv 0 \pmod{p^2}$ and $i\delta \not\equiv 0 \pmod{p}$ for the irregular prime pairs $(p, i)$ with $p \leq 4001$, and W. Johnson [5] has extended their result to all irregular primes $p \leq 30000$. This implies that $i g(T)$ has a unique zero $i\omega$ in the ring $\mathbb{Z}_p$ 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 $i g(T)$ 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. $i g(T)$ 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 $\mathbb{Q}$ and $\mathbb{Q}_p$. Let $F$ be the union of all the cyclotomic fields of $p^n$th roots of unity over $\mathbb{Q}$ for $n \geq 1$ and $\Gamma$ denote the subgroup of the Galois group of $F$ over $\mathbb{Q}$ corresponding to the group of $1$-units in $\mathbb{Q}_p$. Let $V$ be the group of all $(p - 1)$st roots of unity in $\mathbb{Q}_p$.

For $a \in \mathbb{Q}_p$, let $(a)$ denote the rational number $b/p^m$, where $p^m a \equiv b \pmod{p^m}$ and $0 \leq b < p^m$. Thus $(a)$ is uniquely determined by $a$, although $b$ and $m$ are not.

For odd indices $1 \leq i \leq p - 4$, we define $i g(T)$ in the ring $\Lambda$ of formal power series with coefficients in $\mathbb{Z}_p$. For such $i$ and for $n \geq 0$, let

$$i g_n(T) = \sum_{m=0}^{p^n-1} \sum_{v \in V} \omega(1 + p)^m/p^{n+1} \cdot v(1 + T)^m.$$
Then \( i g_n (T) \) is a polynomial in \( T \) with coefficients in \( \mathbb{Z}_p \) and degree less than \( p^n \). As \( n \to \infty \), \( i g_n (T) \) converges on each coefficient of \( T^m \) to a power series \( i g(T) \) in \( \Lambda \), and we have

\[
(1) \quad i g(T) \equiv i g_n (T) \mod (1 - (1 + T) p^n ) \Lambda \quad (n \geq 0).
\]

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

\[
i g((1 + p)^{-s} - 1) = -L_p (s; \chi_i) \quad (s \in \mathbb{Z}_p)
\]

where \( \chi_i \) is the character of integers modulo \( p \), with values in \( \mathbb{Q}_p \), such that \( \chi_i (a) \equiv a^{p^{i-1}} \mod p \) 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 \( i g(T) \) has a unique zero \( i \omega \) and that \( i \omega \in p \mathbb{Z}_p \). It follows that, for such \( p \) and \( i \), \( L_p (s; \chi_i) \) has exactly one zero \( s = i \kappa \in \mathbb{Z}_p \) and that \( i \kappa \) is determined by

\[
(2) \quad (1 + p)^{-i \kappa} = 1 + i \omega.
\]

3. Computation of \( i \alpha \). With \( n = 0 \) in (1), we have \( i g(T) \equiv i g_0 (T) \mod T \Lambda \). Therefore \( i \alpha = i g(0) = i g_0 (0) = \sum_{v \in V} (v/p) v^j \). For \( 1 \leq a \leq p - 1 \), let \( v_a \in V \) be such that \( v_a = a \mod p \). Thus we have

\[
(3) \quad i \alpha = \sum_{a=1}^{p-1} \frac{p-1}{p} v_a^j = \frac{1}{p} \sum_{a=1}^{p-1} a v_a^i.
\]

For \( 1 \leq a \leq p - 1 \), it is clear that

\[
(i + 1) a v_a^j \equiv i v_a^{i+1} + a^{i+1} \mod p^2.
\]

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

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

Hence

\[
(i + 1) \sum_{a=1}^{p-1} a v_a^i \equiv \sum_{a=1}^{p-1} a^{i+1} = B_{i+1} p \mod p^2.
\]

Using (3), we find

\[
(i + 1) \alpha p \equiv B_{i+1} p \mod p^2,
\]

which shows that \( i \alpha \equiv 0 \mod p \) 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 \( s \in \mathbb{Z}_p \) unless \( (p, i) \) is such a pair.

Using Eq. (3), \( i \alpha \) was computed modulo \( p^7 \) for all irregular primes \( p \leq 157 \).

Write \( i \alpha = \sum_{j=0}^{p-1} a_j p^j \). 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 \( 31^\alpha \pmod{37^2} \) 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**

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

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

\[
i\sigma(T) \equiv i\sigma_n(T) \pmod{(p^n, T^p)^{\Lambda}}.
\]

Since \( v_a = a_{p^n} \pmod{p^{n+1}} \) for \( n \geq 0 \), we have the following congruences modulo \( p^n \):

\[
\eta_k \equiv \sum_{m=0}^{p^n-1} \sum_{u \in U} (u(1 + p)^m/p^{n+1}) a_i(m/k)
\]

\[
\equiv \sum_{a=1}^{p-1} a^i \sum_{m=0}^{p^n-1} \left( a^{p_n} \frac{(1 + p)^m}{p^{n+1}} \right)^{m/k} \equiv \frac{1}{p} \sum_{a=1}^{p-1} a^{p_n} \frac{p^{n-1}}{m=0} B(a, m)^{(m/k)},
\]

where

\[
B(a, m) = a^{p_n} (1 + p)^m \equiv a^{p_n} \left( 1 + \binom{m}{1} p + \ldots + \binom{m}{n} p^n \right) \pmod{p^{n+1}}
\]

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

\[
\sum_{m=0}^{p^n-1} \binom{m}{k} = \sum_{m=0}^{p^n-1} \sum_{r=0}^{k} \binom{m}{j+r} \binom{j+r}{j} \left( \sum_{r=0}^{j+k} \binom{j}{t} \binom{j+k}{t-k} \right)^{m/k} \sum_{m=0}^{p^n-1} \left( \binom{m}{t} \right).
\]

But

\[
\sum_{m=0}^{p^n-1} \binom{m}{t} = \binom{p^n}{t+1} \equiv 0 \pmod{p^n}
\]

for \( t + 1 < p \), and we have
\[ \sum_{m=0}^{n-1} B(a, m) \binom{m}{k} \equiv a^n \sum_{j=0}^{n} p^j \sum_{m=0}^{n-1} \binom{m}{j} \binom{m}{k} \equiv 0 \pmod{p^n} \]

for \( k + n + 1 < p \). Hence

\[ i_\beta \equiv \frac{1}{p} \sum_{a=1}^{p-1} a^p \sum_{m=0}^{n-1} B(a, m) m \pmod{p^n}, \]

\[ i_\gamma \equiv \frac{1}{p} \sum_{a=1}^{p-1} a^p \sum_{m=0}^{n-1} B(a, m) \binom{m}{2} \pmod{p^n}, \]

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 \( i_\beta = \sum_{j=0}^{\infty} b_j p^j \), \( i_\gamma = \sum_{j=0}^{\infty} c_j p^j \), etc. The numbers \( b_j, c_j, d_j, \) and \( e_j \) which were calculated are shown in Table II.

**Table II**

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

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 \( \sum_{m=0}^{n-1} B(a, m) m \) 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 \( 31_\beta \pmod{37^3} \) required only 38 seconds.
6. Computation of \( ^i\omega \) and \( ^i\kappa \). The \( p \)-adic integer \( ^i\omega \) such that \( ^i\omega = 0 \) 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 \( w_1 \equiv -a/b \pmod{p} \) and \( 0 \leq w_1 < p \) 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 \( ^i\omega (w_1 p + \ldots + w_np^n) \equiv 0 \pmod{p^{j+1}} \). Since \( w_1 \neq 0 \) in all the cases computed, it follows for these that \( k_0 \equiv p - w_1 \) and \( k_j \equiv (w_1^j - w_2 - \ldots - w_j) \pmod{p} \). Then for \( j = 2, 3, k_j \) is the number which satisfies \( 0 \leq k_j < p \) and \( (1 + p)^K(j) \equiv 1 + \omega \pmod{p^{j+2}} \), where \( K(j) = p^{j+1} - k_0 - k_1 p - \ldots - k_j p^j \).

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

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 \( |m|, |n| < p^2 \) 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

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

No such representation for \( 1 + \omega \) was found. Dozens of congruences like the two above hold modulo 37, so there is no reason to believe that either of these congruences holds modulo 37.

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.