

## THE GLOBAL ROOT NUMBER FOR $J_0(p)$

E. KOWALSKI

Let  $p$  be a prime, and consider  $A = J_0(p)$ , the Jacobian of  $X_0(p)$ . Its  $L$ -function is given by

$$L(A, s) = \prod_{f \in S_2^*(p)} L(f, s)$$

where  $S_2^*(p)$  is the set of newforms of level  $p$ . Each  $L(f, s)$  satisfies a functional equation

$$\Lambda(f, s) = \varepsilon(f)p^{1/2-s}\Lambda(f, 1-s)$$

where  $\Lambda(f, s) = (2\pi)^{-s}\Gamma(s+1/2)L(f, s)$  and the sign for  $f$  is

$$\varepsilon(f) = -w_p(f), \text{ where } f | w_p = w_p(f)f,$$

$w_p$  being the Atkin-Lehner involution. We wish to compute the *global* sign of the functional equation for  $L(A, s)$ :

$$\Lambda(A, s) = \varepsilon(A)p^{g(p)(1/2-s)}\Lambda(A, 1-s)$$

where  $g(p) = |S_2^*(p)| = \dim A(p)$  and

$$\Lambda(A, s) = \prod_f \Lambda(f, s).$$

**Lemma 1.** *We have for  $p$  prime*

$$\varepsilon(A) = (-1)^{\frac{1}{2}\text{Tr}(1+w_p)},$$

where the trace is acting on  $S_2(p)$ .

*Proof.* Because  $w_p$  is an involution, its eigenvalues are  $\pm 1$ , and in particular one has

$$w_p(f) = (-1)^{\frac{1}{2}(w_p(f)-1)}.$$

Then taking the product over  $f$  we have

$$\varepsilon(A) = \prod_f \varepsilon(f) = (-1)^{g(p) + \frac{1}{2}(\text{Tr}(w_p) - g(p))} = (-1)^{\frac{1}{2}\text{Tr}(1+w_p)}.$$

□

*Remark 2.* In particular, notice that  $\text{Tr}(1+w_p) \equiv 0 \pmod{2}$ , i.e.

$$\text{Tr}(w_p) \equiv g(p) \pmod{2}.$$

This is not obvious from the computation of  $\text{Tr}(w_p)$  (see below) and thus “reproves” part of genus theory for imaginary quadratic fields...

The genus  $g(p)$  of  $X_0(p)$  and the trace of  $w_p$  are computed classically, respectively, using the Riemann-Hurwitz formula and the Selberg trace formula.

**Lemma 3.** *We have*

$$g(p) = \frac{p+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{p}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{p}\right)\right)$$

and for  $p > 3$

$$\text{Tr}(w_p) = 1 - \frac{1}{2} \sum_{\substack{-4p=df^2 \\ d \text{ disc}}} h(d),$$

where the condition on  $d$  is that  $d < 0$  be a discriminant of an order in an imaginary quadratic field, and  $h(d)$  is the class-number of the order of discriminant  $d$ .

The restriction  $p > 3$  is of course no problem since  $g(3) = 0$ .

*Proof.* For the first formula, see e.g. Shimura's book, and for the second, see e.g. Brumer's Astérisque 228 article. (The sum there has  $H_1(s^2 - 4p)$  and extends to  $s^2 \leq 4p$  such that  $p \mid s$ , which means  $s = 0$ , etc).  $\square$

We can express  $\text{Tr}(w_p)$  more concretely by getting into congruence classes modulo 4 and 8. Namely, if  $p \equiv 3 \pmod{4}$ , then  $-p$  is the discriminant of  $\mathbf{Q}(\sqrt{-p})$  and the equation  $-4p = df^2$  above has two solutions,  $(d, f) = (-p, 2)$  and  $(d, f) = (-4p, 1)$ , hence we obtain

$$\text{Tr}(w_p) = 1 - \frac{1}{2}(h(-4p) + h(-p)), \text{ for } p \equiv 3 \pmod{4}.$$

By a well-known formula (see e.g. Cox), we have

$$h(-4p) = 2h(-p) \left(1 - \frac{1}{2} \left(\frac{-p}{2}\right)\right) = h(-p) \left(2 - \left(\frac{-p}{2}\right)\right),$$

so using the value of the Kronecker symbol we have

$$\text{Tr}(w_p) = \begin{cases} 1 - h(-p) & \text{if } p \equiv 7 \pmod{8} \\ 1 - 2h(-p) & \text{if } p \equiv 3 \pmod{8}. \end{cases}$$

Only in the second case is  $\text{Tr}(w_p) \pmod{4}$  easy to know: by genus theory, one has  $h(-p) \equiv 1 \pmod{2}$  hence  $1 - 2h(-p) \equiv 3 \pmod{4}$  if  $p \equiv 3 \pmod{8}$ .

In the case  $p \equiv 1 \pmod{4}$ , then  $-4p$  is the discriminant of  $\mathbf{Q}(\sqrt{-p})$  and the only solution is  $(d, f) = (-4p, 1)$ , hence

$$\text{Tr}(w_p) = 1 - \frac{1}{2}h(-4p) \text{ if } p \equiv 1 \pmod{4}.$$

The value of  $g(p)$  modulo 4, on the other hand, depends on the class of  $p$  modulo 48.

**Lemma 4.** *The following table gives  $g(p) \pmod{4}$ :*

$p \pmod{48}$	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
$g(p) \pmod{4}$	3	0	0	1	0	1	1	2	1	2	2	3	2	3	3	0

Putting together the two results, we obtain “one-fourth” of the values of  $\varepsilon(A)$ :

**Proposition 5.** *If  $p \equiv 3 \pmod{8}$ , then*

$$\varepsilon(A) = \begin{cases} 1 & \text{if } p \equiv 11 \text{ or } 19 \pmod{48} \\ -1 & \text{if } p \equiv 35 \text{ or } 43 \pmod{48}. \end{cases}$$

In the other cases of  $p \pmod{48}$ , there does not seem to be such a simple “congruence” formula. However one can make numerical experiments and they suggest the reasonable result that the signs  $\pm 1$  should be equiprobable for  $\varepsilon(J_0(p))$  as  $p \rightarrow +\infty$ . A proof, from the result above, is tantamount to proving two equidistribution results for  $h(-p) \pmod{4}$ ,  $p \equiv 7 \pmod{8}$  and  $h(-4p) \pmod{8}$ ,  $p \equiv 1 \pmod{4}$ .

Here are some numerical data: let

$$N(x) = \sum_{p \leq x} \varepsilon(J_0(p)),$$

then for  $X = 10^6$ , one finds

$$\sup_{p \leq X} N(x) = 166 \text{ and } \inf_{p \leq X} N(x) = -195.$$

*Remark 6.* Henri Cohen remarked – as a result of the striking coincidence that he was computing the left-hand side just as I was coming to ask about the right-hand side... – that

$$\Gamma_p\left(\frac{1}{2}\right) \equiv h(-p) \pmod{4} \text{ for } p \equiv 3 \pmod{4},$$

where  $\Gamma_p$  is the  $p$ -adic Gamma function defined on  $\mathbf{Z}_p$ ; the formula makes sense because  $\Gamma_p(1/2)^2 = 1 \in \mathbf{Z}$ , hence the value of  $\Gamma_p(1/2)$  is  $\pm 1$  (see e.g. Lang, “Cyclotomic fields”, vol. 2). One may wonder if more general statements of this kind exist?