

ERRATUM: SHIMURA CURVES OF GENUS AT MOST TWO

JOHN VOIGHT

Lemma 2.5 is incorrect as stated [3]. This mistake does not affect any other result in the paper; the list of curves is still complete and all curves have the correct signature (these signatures were independently verified, as in §5).

We give a complete and corrected statement and proof below. We retain the notation from §2. In particular, let $R_{\mathfrak{p}} = \mathbb{Z}_{F,\mathfrak{p}}[\gamma_{\mathfrak{p}}]$ and let π be a uniformizer at \mathfrak{p} , and let $f_{\mathfrak{p}}(x) = x^2 - t_{\mathfrak{p}}x + n_{\mathfrak{p}}$ denote the minimal polynomial of $\gamma_{\mathfrak{p}}$. Let $d_{\mathfrak{p}} = t_{\mathfrak{p}}^2 - 4n_{\mathfrak{p}}$ and let $k(\mathfrak{p})$ denote the residue class field of \mathfrak{p} .

We will use the following proposition in the proof; see Hijikata [1, §2] and Vignéras [2, §III.3].

Proposition 2.3 (Hijikata [1, Theorem 2.3]).

(c) Suppose $\mathfrak{p} \mid \mathfrak{N}$. Let $e = \text{ord}_{\mathfrak{p}}(\mathfrak{N})$ and $r = \text{ord}_{\mathfrak{p}}(\mathfrak{f})$, and for $s \geq e$ let

$$E(s) = \{x \in \mathbb{Z}_F/\mathfrak{p}^s : f_{\mathfrak{p}}(x) \equiv 0 \pmod{\mathfrak{p}^s}\}.$$

If $\text{ord}_{\mathfrak{p}}(d_{\mathfrak{p}}) = 0$ then

$$m(R_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) = \#E(e).$$

Otherwise,

$$m(R_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) = \#E(e) + \#\text{img}(E(e+1) \rightarrow R/\mathfrak{p}^e).$$

The corrected lemma is then as follows.

Lemma 2.5. Let \mathfrak{p} be an odd prime. Suppose $e = \text{ord}_{\mathfrak{p}}(\mathfrak{N}) \geq 1$, let $r = \text{ord}_{\mathfrak{p}}(d_{\mathfrak{p}})$, and let $\kappa = \#k(\mathfrak{p})$.

• If $r = 0$, then

$$m(R_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) = 1 + \left(\frac{K_q}{\mathfrak{p}}\right).$$

• If $e < r$, then

$$m(R_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) = \begin{cases} 2\kappa^{(e-1)/2}, & \text{if } e \text{ is odd;} \\ \kappa^{e/2-1}(\kappa+1), & \text{if } e \text{ is even.} \end{cases}$$

• If $e = r$, then

$$m(R_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) = \begin{cases} \kappa^{(r-1)/2}, & \text{if } r \text{ is odd;} \\ \kappa^{r/2} + \kappa^{r/2-1} \left(1 + \left(\frac{K_q}{\mathfrak{p}}\right)\right), & \text{if } r \text{ is even.} \end{cases}$$

• If $e > r > 0$, then

$$m(R_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) = \begin{cases} 0, & \text{if } r \text{ is odd;} \\ \kappa^{r/2-1}(\kappa+1) \left(1 + \left(\frac{K_q}{\mathfrak{p}}\right)\right), & \text{if } r \text{ is even.} \end{cases}$$

Date: November 4, 2009.

Proof. Since \mathfrak{p} is odd, without loss of generality we may assume that $\text{trd}(\gamma_{\mathfrak{p}}) = 0$, and hence $E(s)$ is in bijection with

$$E(s) = \{x \in \mathbb{Z}_F/\mathfrak{p}^s : x^2 \equiv d_{\mathfrak{p}} \pmod{\mathfrak{p}^s}\}.$$

First suppose $r = 0$. Then in particular $r = 0$. By Proposition 2.3(c), we have $m = m(R_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) = \#E(e)$, and by Hensel's lemma we see that $\#E(e) = 0$ or 2 according as $d_{\mathfrak{p}}$ is a square or not in $\mathbb{Z}_{F,\mathfrak{p}}$. In all other cases, we have the second case of Proposition 2.3(c).

Now suppose that $e < r$. The solutions to the equation $x^2 \equiv 0 \pmod{\mathfrak{p}^s}$ are those with $x \equiv 0 \pmod{\mathfrak{p}^{\lceil s/2 \rceil}}$. Thus $\#E(e) = \kappa^{e - \lceil e/2 \rceil} = \kappa^{\lfloor e/2 \rfloor}$ and we see that $\#\text{img}(E(e+1) \rightarrow R/\mathfrak{p}^e) = \kappa^{e - \lceil (e+1)/2 \rceil}$, so $m = 2\kappa^{(e-1)/2}$ if e is odd and $m = \kappa^{e/2} + \kappa^{e/2-1} = \kappa^{e/2-1}(\kappa + 1)$ if e is even.

If $e = r$, then again $\#E(e) = \kappa^{\lfloor e/2 \rfloor}$. Now to count the second contributing set, we must solve $x^2 \equiv d_{\mathfrak{p}} \pmod{\mathfrak{p}^{e+1}}$. If $e = r$ is odd then this congruence has no solution. If instead e is even then we must solve $y^2 = (x/\pi^{r/2})^2 \equiv d_{\mathfrak{p}}/\pi^r \pmod{\mathfrak{p}}$ where π is a uniformizer at \mathfrak{p} . This latter congruence has zero or two solutions according as $d_{\mathfrak{p}}$ is a square, and given such a solution y we have the solutions $x \equiv y \pmod{\pi^{r/2+1}}$ to the original congruence, and hence there are 0 or $2\kappa^{r-(r/2+1)} = 2\kappa^{r/2-1}$ solutions, as claimed.

Finally, suppose $e > r > 0$. If r is odd, there are no solutions to $x^2 \equiv d_{\mathfrak{p}} \pmod{\mathfrak{p}^e}$. If r is even, there are no solutions if $d_{\mathfrak{p}}$ is not a square and otherwise the solutions are $x \equiv y \pmod{\mathfrak{p}^{e-r/2}}$ as above so they total $2\kappa^{r/2} + 2\kappa^{r/2-1} = 2\kappa^{r/2-1}(\kappa + 1)$. \square

The author would like to thank Steve Donnelly for bringing this error to his attention.

REFERENCES

- [1] Hijikata, Explicit Formula of the Traces of Hecke Operators for $\Gamma_0(N)$.
- [2] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., vol. 800, Springer, Berlin, 1980.
- [3] John Voight, Shimura curves of genus at most two, *Math. Comp.* **78** (2009), 1155–1172.