ERRATA:  

SHIMURA CURVES OF GENUS AT MOST TWO

JOHN VOIGHT

This note gives errata for the article Shimura curves of genus at most two [3]. These mistakes do not affect the main result; the list of curves is still complete and all curves have the correct signature (these signatures were independently verified, as in §5). The author would like to thank James Rickards.

ERRATA

(1) In the script to count, a human error caused the classical modular curve $X_0(11)$ to be counted as genus 0. The corrected counts are 257, 335, 266 of genus 0, 1, 2 up to equivalence, and 334, 589, 438 of genus 0, 1, 2 fixing a unique field in each isomorphism class.

(2) Section 2, second paragraph: this is not a bijection, but a two-to-one map—an embedding and its conjugate give the same embedded finite subgroup.

(3) Lemma 2.1: The factor 2 from the previous mistake cancels the 2 in the denominator, so the corrected formula is:

$$e_q = \frac{1}{h(F)} \sum_{R \in \mathcal{K}_q} \frac{h(R)}{Q(R)} \prod_p m(R_p, \mathcal{O}_p).$$

(The formula that was implemented included both of these mistakes, the effect of which cancelled out.)

(4) Lemma 2.1: should be $Q(R) = [N_{K_q/F}(R^*) : \mathbb{Z}_p^+]$.

(5) Corollary 2.4: Same as the previous error: we have instead

$$e_q = \frac{1}{h(F)} \prod_{p \in \mathfrak{D}} \left(1 - \left(\frac{K_q}{p}\right) \right) \sum_{R \in \mathcal{K}_q} \frac{h(R)}{Q(R)}.$$

(6) Lemma 2.5 is incorrect as stated. The detailed correction is given in the next section.

Embedding numbers

Lemma 2.5 is incorrect as stated. 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 $R_p = \mathbb{Z}_{F,p}[\gamma_p]$ and let $\pi$ be a uniformizer at $p$, and let $f_p(x) = x^2 - t_p x + n_p$ denote the minimal polynomial of $\gamma_p$. Let $d_p = t_p^2 - 4n_p$ and let $k(p)$ denote the residue class field of $p$. 

Date: July 29, 2023.
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 $p | \mathfrak{N}$. Let $e = \text{ord}_p(\mathfrak{N})$ and for $s \geq e$ let
\[ E(s) = \{ x \in \mathbb{Z}_F/p^s : f_p(x) \equiv 0 \pmod{p^s} \}. \]
If $\text{ord}_p(d_p) = 0$ then
\[ m(R_p, \mathcal{O}_p) = \#E(e). \]
Otherwise,
\[ m(R_p, \mathcal{O}_p) = \#E(e) + \#\text{img} (E(e + 1) \to \mathbb{Z}_F/p^e). \]

The corrected lemma is then as follows.

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

- If $r = 0$, then
  \[ m(R_p, \mathcal{O}_p) = 1 + \left( \frac{K_q}{p} \right). \]
- If $e < r$, then
  \[ m(R_p, \mathcal{O}_p) = \begin{cases} 2\kappa(e-1)/2, & \text{if } e \text{ is odd;} \\ \kappa(e/2-1)(\kappa+1), & \text{if } e \text{ is even}. \end{cases} \]
- If $e = r$, then
  \[ m(R_p, \mathcal{O}_p) = \begin{cases} \kappa(r-1)/2, & \text{if } r \text{ is odd;} \\ \kappa r/2 + \kappa r/2 - 1 \left( 1 + \left( \frac{K_q}{p} \right) \right), & \text{if } r \text{ is even}. \end{cases} \]
- If $e > r > 0$, then
  \[ m(R_p, \mathcal{O}_p) = \begin{cases} 0, & \text{if } r \text{ is odd;} \\ \kappa r/2 - 1(\kappa+1) \left( 1 + \left( \frac{K_q}{p} \right) \right), & \text{if } r \text{ is even}. \end{cases} \]

**Proof.** Since $p$ is odd, without loss of generality we may assume that $\text{trd}(\gamma_p) = 0$, and hence $E(s)$ is in bijection with
\[ E(s) = \{ x \in \mathbb{Z}_F/p^s : x^2 \equiv d_p \pmod{p^s} \}. \]
First suppose $r = 0$. By Proposition 2.3(c), we have $m = m(R_p, \mathcal{O}_p) = \#E(e)$, and by Hensel’s lemma we see that $\#E(e) = 0$ or 2 according as $d_p$ is a square or not in $\mathbb{Z}_F$. In all other cases, we have the second case of Proposition 2.3(c).

Now suppose that $e < r$. The solutions to the equation $x^2 \equiv 0 \pmod{p^s}$ are those with $x \equiv 0 \pmod{p^{s/2}}$. Thus $\#E(e) = \kappa^{e-[e/2]} = \kappa^{e/2}$ and we see that $\#\text{img} (E(e+1) \to R/p^e) = \kappa^{-(e+1)/2}$, 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 $\#E(e) = \kappa^{e/2}$. Now to count the second contributing set, we must solve $x^2 \equiv d_p \pmod{p^{e+1}}$. If $e = r$ is odd then this congruence has no solution. If instead $e$ is even then we must solve $y^2 = (x/p^r)^2 \equiv d_p/p^r \pmod{p}$ where $\pi$ is a uniformizer at $p$. This latter congruence has zero or two solutions according as $d_p$ 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 $x^2 \equiv d_p \pmod{p^e}$. If $r$ is even, there are no solutions if $d_p$ is not a square and otherwise the solutions are $x \equiv y \pmod{p^{e-r/2}}$ 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 Virgile Ducet and to Steve Donnelly for bringing this error to his attention.

References

