ACTA ARITHMETICA
165.3 (2014)

On the class numbers of real cyclotomic fields of conductor pq

by

Eleni Agathocleous (Nicosia)

1. Introduction. Let $\mathbb{Q}(\zeta_m)$ be the cyclotomic field of conductor m and denote by C its ideal class group and by $h = |C|$ its class number. In the same way let C^+ and h^+ denote the ideal class group and class number of the maximal real subfield $\mathbb{Q}(\zeta_m)^+$. The natural map $C^+ \to C$ is an injection [12, Theorem 4.14] and we have the well known result $h = h^+h^-$. The relative class number h^- is easy to compute as there is an explicit and easily computable formula for its order [12, Theorem 4.17]. The number h^+, however, is extremely hard to compute. The class number formula is not so useful as it requires the units of $\mathbb{Q}(\zeta_m)^+$ to be known. Methods that use the classical Minkowski bound become useless as m grows, and other methods based on Odlyzko's discriminant bounds (see [9] and [10]) are only applicable to fields with small conductor. Masley [8] computed the class numbers for real abelian fields of conductor ≤ 100, and van der Linden [7] was able to calculate the class numbers of a large collection of real abelian fields of conductor ≤ 200. For fields of larger conductor, however, the above methods cannot be effective.

Many of the other methods that were developed employ the well known Leopoldt decomposition of the class number h^+ of a real abelian field K (see [6]), which derives from Leopoldt's decomposition of the cyclotomic units into the product of the cyclotomic units of all cyclic subfields K_χ of K. More specifically, we have $h^+ = Q\prod_\chi h_\chi$, where the product runs over all non-trivial characters χ irreducible over the rationals, each 'class number' h_χ is the index of the cyclotomic units of K_χ in its full group of units E_χ, and Q is some value which equals 1 in the case where the extension $K/\mathbb{Q}$ is cyclic of prime order, but which is very hard to compute in the general case.

2010 *Mathematics Subject Classification*: Primary 11Y40.
Key words and phrases: computation of class numbers, real cyclotomic fields, non-prime conductor.

DOI: 10.4064/aa165-3-5 © Instytut Matematyczny PAN, 2014

A different method is introduced by Schoof [11] and is designed for real cyclotomic fields of prime conductor. Schoof developed an algorithm that computes the order of the module $B = \text{Units}/(\text{Cyclotomic Units})$, which is precisely equal to h^+ in the case he considers, where the conductor of the field is a prime number. One of the great advantages of his method is that it does not exclude the primes dividing the order of the extension, as opposed to other methods.

In this paper we extend Schoof's method to real cyclotomic fields of conductor equal to the product of two distinct odd primes. We apply our algorithm to real cyclotomic fields of conductor < 2000 and we calculate the l-part of h^+ for all odd primes $l < 10000$.

2. Our cyclotomic unit η. In our case, where the conductor of the field is not a prime number, the group of cyclotomic units has a complicated structure. We therefore work with a cyclic subgroup, yet of finite index in the group of units, which we present below.

Let p and q be distinct odd primes. From now on, G will denote the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{pq})^+/\mathbb{Q})$, E will denote the group of units of the real cyclotomic field $\mathbb{Q}(\zeta_{pq})^+$, and O its ring of integers. Without loss of generality we will always assume that $p < q$. Choose and fix g and h, primitive roots modulo p and q, respectively. Denote by $\eta_{(g,h)}$ the following real unit of $\mathbb{Q}(\zeta_{pq})^+$:

$$\eta_{(g,h)} = \zeta_{pq}^{-(p+q)}(1-\zeta_{pq}{}^{p+q})^2 \frac{\zeta_p^{-g/2}}{\zeta_p^{-1/2}} \frac{1-\zeta_p^g}{1-\zeta_p} \frac{\zeta_q^{-h/2}}{\zeta_q^{-1/2}} \frac{1-\zeta_q^h}{1-\zeta_q},$$

and by $H_{(g,h)}$ the group $\pm\eta_{(g,h)}^{\mathbb{Z}[G]}$. We will omit the subscripts and just write H and η, since we will let η_α denote the result of the action of the element $\alpha \in G$ on η. With this notation in mind, we are ready to prove a statement about the regulator of the units $\{\eta_\alpha\}_{\alpha\in G}$.

PROPOSITION 2.1. *Let E be the group of units of $\mathbb{Q}(\zeta_{pq})^+$ and $H = \pm\eta^{\mathbb{Z}[G]} = \pm\eta_{(g,h)}^{\mathbb{Z}[G]}$ as above, where g and h are any two fixed primitive roots modulo p and q, respectively. The index $[E : H]$ is always finite and equals*

$$[E:H] = \frac{2^{|G|-1}h^+}{|G|} \cdot \prod_{\chi=\chi_p\neq 1} \frac{1}{2}[2(\chi(q)^{-1}-1) + (\chi(g^{-1})-1)(q-1)]$$
$$\cdot \prod_{\chi=\chi_q\neq 1} \frac{1}{2}[2(\chi(p)^{-1}-1) + (\chi(h^{-1})-1)(p-1)],$$

where the characters χ in the first product are the even characters χ_p of conductor p, and those in the second product are the even characters χ_q of conductor q.

Proof. Define f by $f(\alpha) = \log|\eta_\alpha|$. We see that $\sum_\alpha f(\alpha) = \log|\prod_\alpha \eta_\alpha| = 0$. Denote by χ an even Dirichlet character and note that for any root of unity ζ we have $\log|\zeta^i(1-\zeta^j)| = \log|1-\zeta^j|$, where i and j are arbitrary. The regulator R of the units η_α is:

$$\begin{aligned}
R = R(\{\eta_\alpha\}) &= \pm\det\left(\log|\eta_{\alpha\beta}|\right)_{\alpha,\beta\neq 1} = \pm\det\left(f(\alpha\beta)\right)_{\alpha,\beta\neq 1}\\
&= \pm\det\left(f(\beta\alpha^{-1})\right)_{\alpha,\beta\neq 1} \quad \text{(by rearranging the rows)}\\
&= \pm\frac{1}{|G|}\prod_{\chi\neq 1}\sum_{\beta\in G}\chi(\beta)f(\beta) \quad \text{(by [12, Lemma 5.26(c)])}\\
&= \pm\frac{1}{|G|}\prod_{\chi\neq 1}\frac{1}{2}\sum_{\substack{1\le\beta\le pq\\(\beta,pq)=1}}\chi(\beta)\left[\log|1-\zeta_{pq}^{\beta(p+q)}|^2+\log\left|\frac{1-\zeta_p^{g\beta}}{1-\zeta_p^{\beta}}\right|+\log\left|\frac{1-\zeta_q^{h\beta}}{1-\zeta_q^{\beta}}\right|\right].
\end{aligned}$$

For a character χ and the second summand we have

$$\sum_{\substack{1\le\beta\le pq\\(\beta,pq)=1}}\chi(\beta)\left[\log|1-\zeta_p^{g\beta}|-\log|1-\zeta_p^{\beta}|\right]=0$$

for $f_\chi = pq$ by [12, Lemma 8.4] and for $f_\chi = q$ by [12, Lemmas 8.4, 8.5].

For $f_\chi = p$ and by applying [12, Lemmas 8.4 and 8.5], the above sum equals

$$\begin{aligned}
\chi(g)^{-1}\sum_{\substack{g\beta\,(\mathrm{mod}\,pq)\\(\beta,pq)=1}}\chi(g\beta)\log|1-\zeta_p^{g\beta}| - \sum_{\substack{1\le\beta\le pq\\(\beta,pq)=1}}\chi(\beta)\log|1-\zeta_p^{\beta}|&\\
= (\chi(g^{-1})-1)\sum_{\substack{1\le\alpha\le pq\\(\alpha,pq)=1}}\chi(\alpha)\log|1-\zeta_p^{\alpha}|.&
\end{aligned}$$

To sum up, the second summand gives:

$$\begin{cases}
0 & \text{if } f_\chi = pq,\\
(\chi(g^{-1})-1)(q-1)\sum_{1\le\alpha\le p}\chi(\alpha)\log|1-\zeta_p^{\alpha}| & \text{if } f_\chi = p,\\
0 & \text{if } f_\chi = q.
\end{cases}$$

Similarly, the third summand equals:

$$\begin{cases}
0 & \text{if } f_\chi = pq,\\
0 & \text{if } f_\chi = p,\\
(\chi(h^{-1})-1)(p-1)\sum_{1\le\alpha\le q}\chi(\alpha)\log|1-\zeta_q^{\alpha}| & \text{if } f_\chi = q.
\end{cases}$$

Summands of the form $0\cdot\log 0$ are treated as 0 in formulae as above.

Putting all three summands together and denoting by χ_{pq}, χ_p and χ_q the characters of conductor pq, p and q, respectively, we have

$$R = \pm\frac{1}{|G|}\prod_{\chi=\chi_{pq}\neq 1}\frac{1}{2}\cdot 2\chi(p+q)^{-1}\sum_{1\leq\beta\leq pq}\chi(\beta)\log|1-\zeta_{pq}^{\beta}|$$
$$\cdot\prod_{\chi=\chi_{p}\neq 1}\frac{1}{2}\big[2\chi(q)^{-1}(1-\chi(q))+(\chi(g^{-1})-1)(q-1)\big]\sum_{1\leq\alpha\leq p}\chi(\alpha)\log|1-\zeta_{p}^{\alpha}|$$
$$\cdot\prod_{\chi=\chi_{q}\neq 1}\frac{1}{2}\big[2\chi(p)^{-1}(1-\chi(p))+(\chi(h^{-1})-1)(p-1)\big]\sum_{1\leq\alpha\leq q}\chi(\alpha)\log|1-\zeta_{q}^{\alpha}|.$$

To show that $[E:H]$ is always finite it suffices to show that the regulator is never zero. Assume it is zero. Then for some character of conductor p the sum

$$2(\chi(q)^{-1}-1)+(\chi(g^{-1})-1)(q-1)$$

is zero, or for some character of conductor q the sum

$$2(\chi(p)^{-1}-1)+(\chi(h^{-1})-1)(p-1)$$

is zero. But

$$2(\chi(q)^{-1}-1)+(\chi(g^{-1})-1)(q-1)=0$$
$$\Leftrightarrow\ 2\chi(q)^{-1}+(q-1)\chi(g)^{-1}=2+(q-1),$$

which never happens as $\chi(g)^{-1}$ can never equal 1, since g is a primitive root. Similarly for a character of conductor q. Therefore, the regulator is never zero and this completes the proof of Proposition 2.1. ∎

Denote by P the factor

$$\frac{2^{|G|-1}}{|G|}\cdot\prod_{\chi=\chi_{p}\neq 1}\big[2(\chi(q)^{-1}-1)+(\chi(g^{-1})-1)(q-1)\big]$$
$$\cdot\prod_{\chi=\chi_{q}\neq 1}\big[2(\chi(p)^{-1}-1)+(\chi(h^{-1})-1)(p-1)\big],$$

which appears in the index $[E:H]$ in Proposition 2.1 above. We now have

$$[E:H]=P\cdot h^{+}.$$

One can take advantage of the fact that any choice of primitive roots g and h gives a finite index, and for each field $\mathbb{Q}(\zeta_{pq})^{+}$ one can choose the pair (g,h) with the property that $P_{(g,h)}$ is divisible by the smallest number of distinct primes. Furthermore, for the primes that appear in this $P_{(g,h)}$ one can check whether those primes divide the greatest common divisor of all the $P_{(g,h)}$ for every pair of primitive roots (g,h). In the case that a prime l does not divide the greatest common divisor, there is some pair (g_0,h_0) for which l does not divide $P_{(g_0,h_0)}$. We can therefore repeat the first part of our algorithm that we present in Section 5, for this pair (g_0,h_0) and for this prime l. We continue with the next step of the algorithm for this prime l only if it gives

a non-trivial factor. These facts are very useful in the computations, since they narrow down the number of primes that one needs to check to see if they divide h^+.

3. The module $B = E/H = E/\pm\eta^{\mathbb{Z}[G]}$. We denote by B the $\mathbb{Z}[G]$-module E/H, where $H = \pm\eta^{\mathbb{Z}[G]}$ as above. From Proposition 2.1 we know that the order of B is finite and equals the index $[E : H]$. Therefore, by generalizing Schoof's method, we can calculate the order of B and then multiply by $1/P$ to get h^+, as desired.

Since H is of finite index in E, the map

$$\Phi : \mathbb{Z}[G] \to E, \quad \alpha \mapsto \eta^a,$$

is a homomorphism whose image H is of finite index and therefore $\mathbb{Z}$-isomorphic to $\mathbb{Z}^{|G|-1}$. We have $H/\{\pm 1\} \cong \mathbb{Z}[G]/N_G$ as $\mathbb{Z}[G]$-modules, where N_G is the norm of G. Let $M > 1$ denote a power of a prime l. We let $F = \mathbb{Q}(\zeta_{pq})^+(\zeta_{2M})$ and $\Delta = \mathrm{Gal}(F/\mathbb{Q}(\zeta_{pq})^+)$.

The following lemma appears in [11]. We prove it again here as we found a few omissions in the original proof.

LEMMA 3.1. *The kernel of the natural map*

$$j : E/E^M \to F^*/F^{*M}$$

is trivial if l is odd, and it has order two and is generated by -1 if $l = 2$.

Proof. Fix an embedding $F \subset C$. Then $\mathbb{Q}(\zeta_{pq})^+$ identifies with a subfield of R. Suppose $0 < x \in E \subset R$ is in $\operatorname{Ker} j$. Then $x = y^M$ for some $y \in F^*$. Since $\mu_M \subset F$, we may assume that $y \in R$ and therefore $\mathrm{conj}(y) = y$, where conj is complex conjugation in Δ. Since Δ is commutative, $s(y) = s(\mathrm{conj}(y)) = \mathrm{conj}(s(y))$ for all $s \in \Delta$, therefore $s(y) = \pm y$ for all $s \in \Delta$, as y and all its conjugates are real Mth roots of x. If $l \neq 2$ then M is odd. Assume there exists $s \in \Delta$ with $s(y) = -y$. Then $x = s(x) = s(y^M) = (s(y))^M = (-y)^M = -x$, a contradiction. Therefore Δ fixes y and hence $y \in (\mathbb{Q}(\zeta_{pq})^+)^*$ and $x \in E^M$. Since we took $x > 0$, we need to check for -1 as well. Since M is odd, $(-1)^M = -1$, therefore $-1 \in E^M$ as well, and in this case j is an injection. If $l = 2$, we see that $s(y^2) = s(y)^2 = y^2$, therefore $y^2 \in \mathbb{Q}(\zeta_{pq})^{+*}$. The quadratic subextensions of $F/\mathbb{Q}(\zeta_{pq})^+$ are $\mathbb{Q}(\zeta_{pq})(i)$ and $\mathbb{Q}(\zeta_{pq})^+(\sqrt{\pm 2})$, and hence $y^2 = 2u^2$ or $= \pm u^2$ for some $u \in E$. If $y^2 = 2u^2$ then $2 = y^2v^2$ with v such that $vu = 1$, which cannot happen since then $(2) = (v)^2$ as ideals but 2 does not ramify in $\mathbb{Q}(\zeta_{pq})^+$. So we can only have the second case where $x = y^M = (y^2)^{2^{(k-1)}}$. For $k \geq 2$ we have $x = u^2$, and therefore $x \in E^M$. When $k = 1$ we have $x = y^2 = \pm u^2$, but since $x > 0$ we still get $x = u^2$, which implies that $x \in E^M$. For -1, observe that $-1 = \zeta_{2M}^M$, but -1 is not even a square in $\mathbb{Q}(\zeta_{pq})^+$, which means that $\operatorname{Ker} j = \langle -1 \rangle$ is of order two in this case. ∎

Let $\Omega = \mathrm{Gal}(F/\mathbb{Q})$. We have the following exact sequence of Galois groups:

$$0 \to \Delta \to \Omega \to G \to 0.$$

Let $\Re$ be any prime ideal of F of degree 1, ρ a prime ideal of $\mathbb{Q}(\zeta_{pq})^+$ and r a prime number such that $\Re \,|\, \rho \,|\, r$. We have $r \equiv \pm 1 \pmod{pq}$ and $r \equiv 1 \pmod{2M}$. Moreover, $|G| = (p-1)(q-1)/2$ and we consider the diagram

$$\begin{array}{ccccccccc}
\varepsilon \in E & \xrightarrow{f_1} & \vec{\varepsilon} \in (O/rO)^* & \xrightarrow{f_2} & (O_F/rO_F)^{*\Delta} & & & & \\
 & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_3'} & & & & \\
 & & \mu_M(O/rO) & \xleftarrow{f_2'} & \mu_M(O_F/rO_F)^{\Delta} & \xleftarrow{f_4} & (\mathbb{Z}/M\mathbb{Z})[\Omega]^{\Delta} & \xleftarrow{f_5} & (\mathbb{Z}/M\mathbb{Z})[G]
\end{array}$$

The maps $f_1, f_2, f_2', f_3, f_3', f_4, f_5$ are defined as in [11]. Let $f_{\Re} = f_5^{-1} f_4^{-1} f_3' f_2 f_1$. In a similar manner to the proof of Theorem 2.2 in [11], it can be shown that the maps $f_{\Re}$ correspond to the Frobenius elements of the primes over $\Re$ in $\mathrm{Gal}(F(\sqrt[M]{E})/F)$. Furthermore, every map in $\mathrm{Hom}_R(E/\pm E^M, R)$ is of the form $f_{\Re}$ for some $\Re \in S$, where S denotes the set of unramified prime ideals $\Re$ of $\mathbb{Q}(\zeta_{pq})^+(\zeta_{2M})$ of degree 1 and $R = (\mathbb{Z}/M\mathbb{Z})[G]$. We can therefore state the following theorem, whose proof we omit as it is very similar to that of Theorem 2.2 in [11].

THEOREM 3.2. *Let l and M be as above, and let I denote the augmentation ideal of $R = (\mathbb{Z}/M\mathbb{Z})[G]$. Then $B[M]^{\perp} \cong I/\{f_{\Re}(\eta) : \Re \in S\}$.*

4. The computations

4.1. Reformulating Theorem 3.2 in terms of polynomials. Let l be a fixed odd prime, $M > 1$ some fixed power of l, and G the Galois group of $\mathbb{Q}(\zeta_{pq})^+$. Then G is of order $(p-1)(q-1)/2$ and we have the isomorphisms

$$\begin{aligned} G &\cong \big((\mathbb{Z}/p\mathbb{Z})^\star \times (\mathbb{Z}/q\mathbb{Z})^\star\big)/\{\pm \mathbf{1}\} \\ &\cong \langle \sigma, \tau : \sigma^{(p-1)} = 1,\ \tau^{(q-1)} = 1,\ \sigma^{(p-1)/2}\tau^{(q-1)/2} = 1,\ \sigma\tau = \tau\sigma \rangle \end{aligned}$$

where $\sigma : \zeta_p \mapsto \zeta_p^{\gamma}$ and $\tau : \zeta_q \mapsto \zeta_q^{\delta}$ with γ and δ being fixed primitive roots modulo p and q, respectively. The third relation is that of complex conjugation. The primitive roots γ and δ will be fixed throughout and will always represent the generators of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $(\mathbb{Z}/q\mathbb{Z})^\times$, respectively. We see that

$$\mathbb{Z}[G] \cong \mathbb{Z}[x,y]/(x^{p-1} - 1, y^{q-1} - 1, x^{(p-1)/2} y^{(q-1)/2} - 1)$$

via the map that sends σ to x and τ to y. Similarly,

$$(\mathbb{Z}/M\mathbb{Z})[G] \cong (\mathbb{Z}/M\mathbb{Z})[x,y]/(x^{p-1} - 1, y^{q-1} - 1, x^{(p-1)/2} y^{(q-1)/2} - 1).$$

Using this notation, the maps $f_{\Re}$ that were introduced in the previous section can now be expressed as polynomials in the variables x and y as follows:

$$f_{\Re}(x,y) = \sum_{1\le i\le p-1} \sum_{1\le j\le (q-1)/2} \log_r(\eta_{(i,j)}) \cdot x^i \cdot y^j$$

where

$$\eta_{(i,j)} = \zeta_p^{-\gamma^i}\zeta_q^{-\delta^j}(1-\zeta_p^{\gamma^i}\zeta_q^{\delta^j})^2 \frac{\zeta_p^{-g\gamma^i/2}}{\zeta_p^{-\gamma^i/2}} \frac{1-\zeta_p^{g\gamma^i}}{1-\zeta_p^{\gamma^i}} \frac{\zeta_q^{-h\delta^j/2}}{\zeta_q^{-\delta^j/2}} \frac{1-\zeta_q^{h\delta^j}}{1-\zeta_q^{\delta^j}}.$$

Here, $\log_r$ denotes the discrete log which gives $\log_r \eta = s$ where $s \in \mathbb{Z}/M\mathbb{Z}$ is such that $\eta^{(r-1)/M} \equiv \zeta_M^s \pmod{\Re}$.

We note here that the second sum in the definition of $f_{\Re}(x,y)$ goes from 1 up to $(q-1)/2$ since we are in the real subfield of $\mathbb{Q}(\zeta_{pq})$.

Given the above, we can now reformulate Theorem 3.2 as follows:

THEOREM 4.1. *Let l be a fixed prime, and let $M > 1$ be some fixed power of l. Denote by R the ring*

$$(\mathbb{Z}/M\mathbb{Z})[x,y]/(x^{p-1}-1, y^{q-1}-1, x^{(p-1)/2}y^{(q-1)/2}-1),$$

and let $B[M]^{\perp}$ be as in Theorem 3.2. *Then*

$$B[M]^{\perp} \cong (x-1,y-1)/\{f_{\Re}(x,y) : \Re \in S\}$$

where $S = \{$the degree 1 prime ideals of $\mathbb{Q}(\zeta_{pq})^+(\zeta_{2M})\}$.

Proof. From our polynomial description of $\mathbb{Z}[G]$ above, it follows that the augmentation ideal of $(\mathbb{Z}/M\mathbb{Z})[G]$ is $(x-1,y-1)$. The result is now immediate from Theorem 3.2. ∎

4.2. The decomposition of the modules $B[M]^{\perp}$. Let $\tilde{G}$ denote the Galois group of the extension $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}$. We can write $\mathbb{Z}_l[\tilde{G}]$ as follows: For the same fixed prime l as above, write $p-1 = m_1 l^{a_1}$ and $q-1 = m_2 l^{a_2}$ where $l^{a_1} \parallel p-1$ and $l^{a_2} \parallel q-1$. Since now l does not divide m_1 and m_2,

$$\begin{aligned}
\mathbb{Z}_l[\tilde{G}] &\cong \mathbb{Z}_l[x,y]/(x^{p-1}-1, y^{q-1}-1) \\
&\cong \mathbb{Z}_l[x,y]/((x^{l^{a_1}})^{m_1}-1, (y^{l^{a_2}})^{m_2}-1) \\
&\cong \prod_{\phi_x,\phi_y} \mathbb{Z}_l[x,y]/(\phi_x(x^{l^{a_1}}), \phi_y(y^{l^{a_2}})) \\
&\cong \prod_{\phi_x} \mathbb{Z}_l[x]/(\phi_x(x^{l^{a_1}})) \otimes \prod_{\phi_y} \mathbb{Z}_l[y]/(\phi_y(y^{l^{a_2}}))
\end{aligned}$$

where the products run over all irreducible divisors ϕ_x of $x^{m_1}-1$ and ϕ_y of $y^{m_2}-1$. We see that $\mathbb{Z}_l[x]/(\phi_x(x^{l^{a_1}}))$ and $\mathbb{Z}_l[y]/(\phi_y(y^{l^{a_2}}))$ are complete local $\mathbb{Z}_l[\tilde{G}]$-algebras with maximal ideals $(l, \phi_x(x))$ and $(l, \phi_y(y))$, respectively, and the orders of their residue fields are l^{f_1} and l^{f_2}, where $f_1 = \deg(\phi_x(x))$ and $f_2 = \deg(\phi_y(y))$. Let Δ denote the subgroup of $\tilde{G}$ of order prime to l. From

the decomposition of $\mathbb{Z}_l[\tilde{G}]$ above, we can write any finite $\mathbb{Z}_l[\tilde{G}]$-module A as a product of its ϕ-parts:

$$A_{\phi_x,\phi_y} = A \otimes_{\mathbb{Z}_l[\tilde{G}]} \big(\mathbb{Z}_l[x]/(\phi_x(x^{l^{a_1}})) \otimes \mathbb{Z}_l[y]/(\phi_y(y^{l^{a_2}}))\big).$$

The simple Jordan–Hölder factors of each A_{ϕ_x,ϕ_y} over $\mathbb{Z}_l[\Delta]$ are the same as those over $\mathbb{Z}_l[\tilde{G}]$ since we 'removed' the powers of x and y dividing the order of $\tilde{G}$.

All of the above about the module A also holds in particular for B, the various $B[M]^{\perp}$ and their ϕ-parts $B[M]^{\perp}_{\phi_x,\phi_y}$. Therefore, when we want to find the Jordan–Hölder factors of B we can start by taking all combinations of the degrees f_1 and f_2. Since x and y are non-zero elements in the corresponding residue fields $[\mathbb{Z}_l[x]/(\phi_x(x^{l^{a_1}}))]/(l,\phi_x(x))$ and $[\mathbb{Z}_l[y]/(\phi_y(y^{l^{a_2}})]/(l,\phi_y(y))$, the orders of x and y in the ring attached to ϕ_x and ϕ_y must divide $l^{f_1}-1$ and $l^{f_2}-1$, respectively. Let $d_1 = \gcd(p-1, l^{f_1}-1)$ and $d_2 = \gcd(q-1, l^{f_2}-1)$, and let

$$R_{d_1,d_2} = (\mathbb{Z}/M\mathbb{Z})[x,y]/((x^{l^{a_1}})^{d_1}-1, (y^{l^{a_2}})^{d_2}-1).$$

Since the rings R_{d_1,d_2} and R_{ϕ_x,ϕ_y} are direct summands of R, any map from their modules $B[M]_{d_1,d_2}$ and $B[M]_{\phi_x,\phi_y}$, respectively, to R will end up in these smaller rings. Therefore we can refer to $B[M]^{\perp}_{d_1,d_2}$ and $B[M]^{\perp}_{\phi_x,\phi_y}$ as R_{d_1,d_2}- and R_{ϕ_x,ϕ_y}-modules, respectively, where

$$\text{(i)} \qquad B[M]^{\perp}_{d_1,d_2} \cong I_d/\langle (x^{l^{a_1}})^{d_1}-1, (y^{l^{a_2}})^{d_2}-1, \mathrm{cnj}, f_{\Re}(x,y) : \Re \in S\rangle$$

and similarly for $B[M]^{\perp}_{\phi_x,\phi_y}$. Here cnj denotes the conjugation relation already defined in Section 4.1. Basically $B[M]^{\perp}_{d_1,d_2}$ is the direct sum of the $B[M]^{\perp}_{\phi_x,\phi_y}$'s and we therefore have $|B[M]^{\perp}_{d_1,d_2}| = \prod_{\phi_x,\phi_y} |B[M]^{\perp}_{\phi_x,\phi_y}|$.

Since $(1 \pm \mathrm{cnj})/2$ are idempotents in $(\mathbb{Z}/M\mathbb{Z})[\tilde{G}]$ for M odd, the conjugation relation in the ideal

$$\text{(ii)} \qquad J = \langle (x^{l^{a_1}})^{d_1}-1, (y^{l^{a_2}})^{d_2}-1, \mathrm{cnj}, f_{\Re}(x,y) : \Re \in S\rangle$$

from (i) above makes $B[M]^{\perp}_{d_1,d_2}$ a $(\mathbb{Z}/M\mathbb{Z})[G]$-module as well.

Note that here the polynomials $f_{\Re}$ are restrictions of the Frobenius elements of Theorem 4.1 to this smaller extension determined by the set of polynomials $(x^{l^{a_1}})^{d_1}-1$ and $(y^{l^{a_2}})^{d_2}-1$. They are therefore of the form

$$\text{(iii)} \qquad f_{\Re}(x,y) = \sum_{1\le i\le d_1 l^{a_1}} \sum_{1\le j\le d_2 l^{a_2}} \log_r\Big(\prod_{\substack{m\equiv i \,(\mathrm{mod}\, d_1 l^{a_1}) \\ n\equiv j \,(\mathrm{mod}\, d_2 l^{a_2})}} \eta_{(m,n)} \Big) \cdot x^i \cdot y^j.$$

4.3. Gröbner bases. We make use of Gröbner bases, which we present here following [1], in order to handle the appearance of two variables in our calculations of the ideals J defined in the previous section, and enable calculating the order of the various $B[M]^{\perp}_{d_1,d_2}$.

As before, $d_1 = \gcd(p-1, l^{f_1}-1)$ and $d_2 = \gcd(q-1, l^{f_2}-1)$, where f_1 and f_2 are the degrees of some irreducible polynomials ϕ_x and ϕ_y, respectively. Again, let $B[M]^{\perp}_{d_1,d_2}$ be the corresponding R_{d_1,d_2}-module, and J the ideal as in (ii) above. All the computations for the calculation of the Frobenius polynomials were performed in PARI [2] and the computations for a basis for J in Mathematica [13], which allows the computations of bases for ideals whose elements are polynomials in more than one variable and their coefficients are in any ring $\mathbb{Z}/M\mathbb{Z}$, not necessarily a field.

In this section, $R = (\mathbb{Z}/M\mathbb{Z})[x, y]$ will be our polynomial ring in two variables x and y with coefficients in the Noetherian ring $\mathbb{Z}/M\mathbb{Z}$, which makes R Noetherian as well. Because of the appearance of more than one variable in our polynomials, we need to agree on the order of the variables and also find a way to compare elements. We call an element of the form $x^a y^b$ with a, b non-negative integers a *power product*, and we denote by T^2 the set of all power products in our polynomial ring R. Following [1], we define:

DEFINITION 4.2. By a *term order* on T^2 we mean a total order $<$ on T^2 which satisfies the following conditions:

(i) $1 < x^a y^b$ for all $1 \neq x^a y^b \in T^2$.
(ii) If $x^{a_1} y^{b_1} < x^{a_2} y^{b_2}$ then $x^{a_1} y^{b_1} x^c y^d < x^{a_2} y^{b_2} x^c y^d$ for all $x^c y^d \in T^2$.

The type of term order that we use here is the lexicographical order which we define below:

DEFINITION 4.3. The *lexicographical order* on T^2 with $x > y$ is defined as follows: For $(a_1, b_1), (a_2, b_2)$ with a_i, b_i positive integers, $x^{a_1} y^{b_1} < x^{a_2} y^{b_2}$ if and only if ($a_1 < a_2$ or ($a_1 = a_2$ and $b_1 < b_2$)). We therefore have

$$1 < y < y^2 < y^3 < \cdots < x < xy < xy^2 < \cdots < x^2 < \cdots .$$

Now that we have chosen a term order on our polynomial ring, for each polynomial

$$f = c_1 x^{a_1} y^{b_1} + \cdots + c_n x^{a_n} y^{b_n}$$

with $c_i \neq 0$ in $\mathbb{Z}/M\mathbb{Z}$ and $x^{a_1} y^{b_1} > \cdots > x^{a_n} y^{b_n}$, we can define:

- $\mathrm{lp}(f) = x^{a_1} y^{b_1}$, the *leading power product* of f,
- $\mathrm{lc}(f) = c_1$, the *leading coefficient* of f,
- $\mathrm{lt}(f) = c_1 x^{a_1} y^{b_1}$, the *leading term* of f.

Since the coefficients are not necessarily in a field, we need to redefine division.

DEFINITION 4.4. Let f and h be polynomials in R, and G a set of polynomials in R, $G = \{g_1, \ldots, g_n\}$. We say that f *reduces to* h *modulo* G *in one*

step, denoted

$$f \xrightarrow{G}_1 h,$$

if

$$h = f - (c_1 x^{a_1} y^{b_1} g_1 + \cdots + c_s x^{a_s} y^{b_s} g_s)$$

for $c_1, \ldots, c_s \in \mathbb{Z}/M\mathbb{Z}$ and with $\operatorname{lp}(f) = x^{a_i} y^{b_i} \operatorname{lp}(g_i)$ for all i such that $c_i \neq 0$ and $\operatorname{lt}(f) = c_1 x^{a_1} y^{b_1} \operatorname{lt}(g_1) + \cdots + c_s x^{a_s} y^{b_s} \operatorname{lt}(g_s)$.

Definition 4.5. Let f, h and $f_1, \ldots, f_s$ be polynomials in R, with $f_i \neq 0$ for all $1 \leq i \leq s$, and let $F = \{f_1, \ldots, f_s\}$. We say that f *reduces to* h *modulo* F, denoted

$$f \xrightarrow{F} h,$$

if there exist polynomials $h_1, \ldots, h_{t-1} \in R$ such that

$$f \xrightarrow{F}_1 h_1 \xrightarrow{F}_1 h_2 \xrightarrow{F}_1 \cdots \xrightarrow{F}_1 h_{t-1} \xrightarrow{F}_1 h.$$

Note that if

$$f \xrightarrow{F} h$$

then $f - h \in \langle f_1, \ldots, f_s \rangle$.

We will now recall [1, Theorem 4.1.12] which basically serves as the definition for a Gröbner basis. Here, the *leading term ideal* of an ideal V of our ring R, denoted by $\operatorname{LT}(V)$, is defined by

$$\operatorname{LT}(V) = \langle \{\operatorname{lt}(v) : v \in V\} \rangle.$$

Theorem 4.6. *Let V be an ideal of R, and let $G = \{g_1, \ldots, g_n\}$ be a set of non-zero polynomials in V. The following are equivalent:*

(i) $\operatorname{LT}(G) = \operatorname{LT}(V)$.

(ii) *For any polynomial $f \in R$ we have*

$$f \in V \quad \text{if and only if} \quad f \xrightarrow{G} 0.$$

(iii) *For all $f \in V$ we have $f = h_1 g_1 + \cdots + h_n g_n$ for some polynomials $h_1, \ldots, h_n \in R$ such that $\operatorname{lp}(f) = \max_{1 \leq i \leq n}(\operatorname{lp}(h_i) \operatorname{lp}(g_i))$.* ∎

Definition 4.7. A set G of non-zero polynomials contained in an ideal V of our ring R is called a *Gröbner basis* for V if G satisfies any one of the three equivalent conditions of Theorem 4.6 above. Obviously, G is a Gröbner basis for $\langle G \rangle$.

The Noetherian property of the ring R together with Theorem 4.6 yields the following result [1, Corollary 4.1.17]:

Theorem 4.8. *Let $V \subseteq R$ be a non-zero ideal. Then V has a finite Gröbner basis.* ∎

We compute in Mathematica a Gröbner basis for our ideal J of the ring R, which we denote by G_J. We see that the order of $B[M]^{\perp}_{d_1,d_2}$ is the order of the quotient $I_d/\langle G_J\rangle$.

In the last step of the algorithm we will also need to compute the annihilator of some ideal $\langle G_J\rangle$ over the finite ring R_{d_1,d_2}. For this we follow the method outlined in [1, Proposition 4.3.11] and we calculate the ideal quotient

$$(T : \langle G_J\rangle) = \{f \in R : f\langle G_J\rangle \subseteq T\}$$

where $T = \langle (x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1\rangle$ is the zero ideal of R_{d_1,d_2}. We see that

$$\mathrm{Ann}_{R_{d_1,d_2}}(\langle G_J\rangle) = (T : \langle G_J\rangle).$$

5. The algorithm

5.1. Step 1. Fix distinct odd primes p and q and an odd prime l. The product pq is the conductor of the field $\mathbb{Q}(\zeta_{pq})^+$ whose class number h^+ we want to calculate, and $M = l$ is the prime that we check to see if it divides h^+. Factor $x^{m_1} - 1$ and $y^{m_2} - 1$ into irreducibles in $\mathbb{Z}/l\mathbb{Z}$ where, as above, $\gcd(m_i, l) = 1$ for $i = 1, 2$ and $m_1 l^{a_1} = p - 1$ and $m_2 l^{a_2} = q - 1$. As before, let (f_1, f_2) be a pair of degrees of irreducible polynomials ϕ_x, ϕ_y, respectively, which appear in the factorization of $\mathbb{Z}[\tilde{G}]$. Let $d_1 = \gcd(p - 1, l^{f1} - 1)$ and $d_2 = \gcd(q - 1, l^{f_2} - 1)$. For various primes r with $r \equiv \pm 1 \pmod{pq}$ and $r \equiv 1 \pmod{2l}$ we calculate the Frobenius elements $f_{\mathfrak{R}}$ as in (iii) of Section 4.2. Let J_0 denote the zero ideal of R_{d_1,d_2} together with the conjugation relation cnj. We pick several Frobenius polynomials $f_{\mathfrak{R}_i}$ that we calculated above and we let $J_i = J_{i-1} + (f_{\mathfrak{R}_i})$. This ascending chain of ideals will computationally stabilize at some ideal $J^l \subseteq I_d$. If J^l happens to equal the whole ideal I_d then the module $B[l]_{d_1,d_2}$ is trivial. If, however, for some pair of degrees (f_1, f_2) we have a strict inclusion $J^l \subset I_d$ then the corresponding $B[l]^{\perp}_{d_1,d_2}$ is not trivial, if J^l has indeed stabilized at the correct ideal J. Hence we believe that l divides the index $[E : H]$.

As expected, in most cases the ideal J^l is the whole ideal I_d and so we do not continue to Steps 2 and 3 for this prime l. When we do get a non-trivial quotient I_d/J^l for some l, we do not proceed to the next step right away but we follow first the procedure outlined right after the proof of Proposition 2.1.

5.2. Step 2. In this step we repeat the procedure of Step 1 but with higher powers of l, i.e. for $M = l^2$, l^3, etc., and only for those primes which 'passed' Step 1. The coefficients of the Frobenius polynomials $f_{\mathfrak{R}}$ now lie in $\mathbb{Z}/M\mathbb{Z}$ and we have to make sure that the primes r satisfy $r \equiv 1 \pmod{2M}$ for the specific power M of l. As before, $R_{d_1,d_2} = (\mathbb{Z}/M\mathbb{Z})[x, y]/((x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1)$, and I_d is the ideal $(x - 1, y - 1)$ in R_{d_1,d_2}. As in Step 1, for

each M the sequence of ideals

$$J_0 \subset J_1 \subset \cdots \subset J_i \subset \cdots$$

will stabilize at some ideal J^M and the order of the quotients

$$\ldots, I_d/J^M, I_d/J^{lM}, \ldots$$

is non-decreasing. Since $B[M]^{\perp}_{d_1,d_2}$ is finite and its order is bounded above by $|B_{d_1,d_2}|$, which is finite and independent of M, the orders of the quotients I_d/J^M will have to stabilize. For some power M of l we will get $|I_d/J^{lM}| = |I_d/J^M|$, hence $I_d/J^{lM} \cong I_d/J^M$. Therefore M annihilates I_d/J^{lM} as well as its quotient $(I_d/J^{lM})/\langle f_{\Re}(x,y) : \Re \in S\rangle \cong B[lM]^{\perp}_{d_1,d_2}$. This implies that $M(B[lM]^{\text{dual}}_{d_1,d_2}) = 0$, which gives $M(B[lM]_{d_1,d_2}) = 0$ since $B[lM]^{\text{dual}}_{d_1,d_2}$ and $B[lM]_{d_1,d_2}$ are isomorphic as finite abelian groups. Therefore $B[lM]_{d_1,d_2} = B[M]_{d_1,d_2}$ and

$$|MB_{d_1,d_2}| = |B_{d_1,d_2}/B[M]_{d_1,d_2}| = |B_{d_1,d_2}|/|B[Ml]_{d_1,d_2}| = |lMB_{d_1,d_2}|.$$

Thus $(MB_{d_1,d_2})/l(MB_{d_1,d_2}) = 0$, and by Nakayama's lemma, $MB_{d_1,d_2} = 0$. Again, since B_{d_1,d_2} and $B^{\text{dual}}_{d_1,d_2}$ are isomorphic as finite abelian groups, we obtain $MB^{\perp}_{d_1,d_2} = 0$. Hence the map $g : I_d/J^M \to B^{\perp}_{d_1,d_2}$ is surjective.

Let $\text{GCD}(P_{(g,h)})$ denote the greatest common divisor of all the $P_{(g,h)}$ that were defined in the last paragraph of Section 2. We need to mention here that if $|I_d/J^M| = |\text{GCD}(P_{(g,h)})|_l$ then we do not have to proceed to Step 3 for this prime since $|I_d/J^M| \geq |B_{d_1,d_2}|_l \geq |\text{GCD}(P_{(g,h)})|_l$ and no power of l divides h^+.

5.3. Step 3. In this last step we determine the structure and hence the order of the module $B^{\perp}_{d_1,d_2}$, by showing that the surjective map $g : I_d/J^M \to B^{\perp}_{d_1,d_2}$ is actually an isomorphism.

Let M be as in Step 2, i.e. the power of l which annihilates $B^{\perp}_{d_1,d_2}$. Consider the following exact sequence, where ψ' raises an element to its Mth power:

$$0 \to B[M] \xrightarrow{\psi'} H/\pm H^M \to H/\pm E^M \to 0.$$

Since M annihilates $B^{\perp}_{d_1,d_2} \cong \text{Hom}_{R_{d_1,d_2}}(B_{d_1,d_2}, R_{d_1,d_2})$, this implies that M also annihilates B_{d_1,d_2}. Therefore, we obtain the following exact sequence of R_{d_1,d_2}-modules:

$$0 \to B_{d_1,d_2} \xrightarrow{\psi} (H/\pm H^M)_{d_1,d_2} \to (H/\pm E^M)_{d_1,d_2} \to 0$$

where the generator η_{d_1,d_2} of the unit groups is the unit η with the norm map

$$N_d = \frac{(x^{p-1}-1)(y^{q-1}-1)}{(x^{l^{a_1}d_1}-1)(y^{l^{a_2}d_2}-1)}$$

applied to it.

From the surjection $g : I_d/J^M \to B_{d_1,d_2}^{\perp}$ established in Step 2 we obtain the injection

$$\Psi : B_{d_1,d_2} \hookrightarrow (I_d/J^M)^{\perp}.$$

We have $(I_d/J^M)^{\perp} = \mathrm{Hom}_{R_{d_1,d_2}}(I_d/J^M, R_{d_1,d_2}) \cong R_{d_1,d_2}/\mathrm{Ann}_{R_{d_1,d_2}}(I_d/J^M)$, where $\mathrm{Ann}_{R_{d_1,d_2}}(I_d/J^M) = \mathrm{Ann}_{R_{d_1,d_2}}(I_d + J^M/J^M) = (J^M : I_d)$, which is the ideal quotient already discussed in Section 4.3. Therefore, $(I_d/J^M) \cong \mathrm{Ann}_{R_{d_1,d_2}}((J^M : I_d))$. One can think of $(J^M : I_d)$, which we denote by $\overline{J^M}$, as the ideal J^M modulo its I_d-part. Assume now that $\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M})$ annihilates $(H/\pm H^M)_{d_1,d_2}/\psi(B_{d_1,d_2})$. Then $\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M}) \subseteq \psi(B_{d_1,d_2})$. But now we have

$$|\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M})| \le |\psi(B_{d_1,d_2})| = |B_{d_1,d_2}| = |\Psi(B_{d_1,d_2})| \le |\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M})|.$$

Therefore the orders of I_d/J^M and $B_{d_1,d_2}^{\perp}$ are equal and so g is an isomorphism. Hence, if we show that $\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M})$ annihilates $(H/\pm E^M)_{d_1,d_2}$, from the second exact sequence above we will have proved that g is an isomorphism.

To find the annihilator $\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M})$ we first compute $\overline{J^M} = (J^M : I_d)$ and then the ideal quotient $(T : \overline{J^M})$ of Section 4.3. For each generator of $\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M})$, we need to apply a lift $h(x,y) \in \mathbb{Z}[x,y]$ of this generator to the unit $\eta_{d_1,d_2} \in (H/\pm E^M)_{d_1,d_2}$. If $\eta_{d_1,d_2}^{h(x,y)}$ is an Mth power of a unit in E then we are done. To see whether it is an Mth power we follow a method similar to the one in Gras and Gras [3] that we also mentioned in the Introduction. We reformulate here the main proposition from [3] in order to make it applicable to our case, and we prove it again, for l odd only, since we only calculate the odd l-parts of h^+.

We denote by η_d^h the unit $\eta_{d_1,d_2}^{h(x,y)}$ that we already described above, and by G_d the quotient of G containing the coset representatives of the embeddings in G, which map ζ_p to $\zeta_p^{g^i}$ and ζ_q to $\zeta_q^{h^j}$ for $1 \le i \le l^{a_1}d_1$ and $1 \le j \le l^{a_2}d_2$.

Proposition 5.1. *Let M be a fixed power of an odd prime l as above and consider the polynomial*

$$P(X) = \prod_{a \in G_d} \left(X - (a(\eta_d^h))^{1/M}\right)$$

where $(a(\eta_d^h))^{1/M}$ denotes the real Mth root of $a(\eta_d^h)$. If P has coefficients in $\mathbb{Z}$ then η_d^h is an Mth power in $\mathbb{Q}(\zeta_{pq})^+$.

Proof. Let N be the largest power of l for which the unit $(\eta_d^h)^{1/N}$ lies in $\mathbb{Q}(\zeta_{pq})^+$. If $M = N$ then we are done, so we assume $N < M$. Then $(\eta_d^h)^{1/N}$ is not an element of $(\mathbb{Q}(\zeta_{pq})^+)^l$ and therefore by [5, Chapter VIII, Theorem 16]

the polynomial

$$T(X) = X^{M/N} - (\eta_d^h)^{1/N}$$

is irreducible in $\mathbb{Q}(\zeta_{pq})^+$. Since $M/N \geq 3$, $T(X)$ has at least one complex root. Therefore $(\eta_d^h)^{1/M}$ has at least one Galois conjugate that is not real. But $P(X) \in \mathbb{Z}[X]$ implies that the Galois conjugates are roots of $P(X)$ which are real. Therefore we have a contradiction. ∎

Most of the times the $P(X)$'s are very large polynomials with huge coefficients. We can prove that the coefficients are integers by applying a method outlined in Schoof [11], which requires that we round off the coefficients of $P(X)$ and then show that this new polynomial divides $P(X^M)$.

6. Examples

6.1. The field of conductor $469 = 7 \cdot 67$. We confirm Hakkarainen's result [4] that 3 is the only odd prime < 10000 which divides h^+. However, he only obtained a 3^1 dividing h_ξ, whereas our results show that the 3-part of h^+ has order 3^2.

Let $r = 3$, $p = 7$, $q = 67$, and $\mathbb{Q}(\zeta_{pq})^+$ be the real cyclotomic field of conductor $pq = 469$. We first compute the factor $P_{(g,h)}$ for all pairs of primitive roots (g, h) and then their greatest common divisor $\mathrm{GCD}(P_{(g,h)})$. From the calculations we have $\mathrm{GCD}(P_{(g,h)}) = 2^{32}$, and so we see that it is best to run the test with the pair $(g', h') = (3 \pmod 7, 7 \pmod{67})$, for which $P_{(g',h')}$ has the smallest number of factors. In particular, $P_{(g',h')} = 2^{98} \cdot 17^2$. Next, we decompose the group ring $\mathbb{Z}[G]$ as shown in Section 4.2. We have $x^{p-1} - 1 = (x^3)^2 - 1$ and $y^{q-1} - 1 = (y^3)^{22} - 1$, and factoring into irreducibles in $\mathbb{Z}/3\mathbb{Z}$ gives

$$x^2 - 1 = (x + 1)(x + 2)$$

and

$$y^{22} - 1 = (y + 1)(y + 2)(y^5 + 2y^3 + y^2 + 2y + 2)(y^5 + 2y^3 + 2y^2 + 2y + 1)$$
$$\times (y^5 + 2y^4 + 2y^3 + 2y^2 + 1)(y^5 + y^4 + 2y^3 + y^2 + 2);$$

so we run Step 1 for all possible degrees d_1 and d_2, which in this case are $d_1 = 2$ and $d_2 = 2$ and 22. Step 1 showed 2, 3 and 17 to be the only primes < 10000 that are possible divisors of the index. Since we chose not to calculate the 2-part of h^+, the only primes we have to consider are 3 and 17. Before proceeding to Step 2, however, we run Step 1 again for the prime 17 because it did appear as a factor of $P_{(g',h')}$ but not of $\mathrm{GCD}(P_{(g,h)})$ and therefore it is possible that it might only divide $P_{(g',h')}$ and not h^+. The pair $(g_0, h_0) = (5 \pmod 7, 7 \pmod{67})$ does not have 17 as a factor of $P_{(g_0,h_0)}$, and Step 1 for 17 with this pair of primitive roots only gives trivial Jordan–Hölder factors. Therefore we proceed to the next steps only for the

prime 3. In Step 2 we repeat the same procedure as in Step 1 but with higher powers of 3. Below we show the Frobenius polynomials obtained for $M = 3$, 3^2 and 3^3 for the pair of degrees $(d_1, d_2) = (2, 2)$, the ideals J^M at which the ideals J_i stabilize and the orders of the quotients $|I_d/J^M|$.

For $M = 3$, $J^M = (y^2-1, y-x) \equiv ((y+1)(y-1), (y-1)-(x-1))$ with coefficients in $\mathbb{Z}/3\mathbb{Z}$. From the second polynomial in J^M we see that the two generators of the augmentation ideal I_d become equivalent in I_d/J^M. From the first one we have $y(y-1) \equiv -(y-1)$ in J^M, therefore we can only have constants in front of the only generator of I_d/J^M. Since we are in $\mathbb{Z}/3\mathbb{Z}$, we see that $|I_d/J^M| = 3$.

For $M = 9$, $J^M = (y^2-3y+2, 3-x-2y) = ((y-1)(y-2), -2(y-1)-(x-1))$ with coefficients in $\mathbb{Z}/9\mathbb{Z}$. The same reasoning as above for the ideal J^3 applies here as well and we have $|I_d/J^M| = 3^2$. Since $|I_d/J^3|$ is strictly smaller than $|I_d/J^{3^2}|$, we need to continue as above with $M = 3^3$.

For $M = 27$, $J^M = (9(y-1), 2-3y+y^2, 3-x-2y)$ with coefficients in $\mathbb{Z}/27\mathbb{Z}$. We see here that J^{3^3} is generated by the same polynomials as J^{3^2} but it has the extra polynomial $9(y-1)$, which reduces the number of constants to 9 instead of 27. Therefore $|I_d/J^{3^2}| = |I_d/J^{3^3}| = 9$ and so, as expected, the orders of these quotients stabilize with $M = 3^2$. The factors ϕ_x, ϕ_y contained in the ideals J above are $\phi_x(x) = x+1$ and $\phi_y(y) = y-2$. These are the only two factors that gave a non-trivial quotient I_d/J^M.

For the pair of degrees $(d_1, d_2) = (2, 22)$, the Frobenius polynomials give exactly the same ideals J^M as above and therefore we have the same two factors ϕ_x and ϕ_y. Hence, we only need to consider the case of $(d_1, d_2) = (2, 2)$.

l	The Frobenius maps for $M = 3$
$l_1 = 7521823$	$f_{\Re_1} = (y^5+y^4+2y^3+2y^2+2y+2)x^5 + (2y^5+2y^4+2y^3+2y^2+y+2)x^4 + (2y^5+y^4+y^2+1)x^3 + (2y^5+2y^4+2y^3+2y^2+y+2)x^2 + (y^5+y^4+y^3+2y+1)x + (y^5+y^4+y^3+2y)$
$l_2 = 8889427$	$f_{\Re_2} = (2y^5+2y^4+y^3+2y^2+y+2)x^5 + (2y^5+2y^3+2y^2+2y)x^4 + (2y^5+2y^4+y^3+2y+2)x^3 + (y^5+2y^3+2y^2+2y)x^2 + (2y^4+y)x + (y^5+2y^4+2y^3+2y^2+y)$
$l_3 = 9573229$	$f_{\Re_3} = (y^4+2y^3+2y+1)x^5 + (y^4+y^3+y^2)x^4 + (y^5+2y^2+y+2)x^3 + (2y^4+2y^3)x^2 + (2y^5+2y^4+y^3+y+2)x + (y^5+y^3+1)$
$l_4 = 10257031$	$f_{\Re_4} = (y^5+y+2)x^5 + (2y^5+2y^4+2y^3+2y^2)x^4 + (2y^4+2y^3+y^2+2y)x^3 + (y^5+y^2+y+1)x^2 + (2y^5+2y^4+y^2+2y+2)x + (2y^5+y^4+2y^3+y^2+y)$
$l_5 = 20514061$	$f_{\Re_5} = (2y^5+y^3+y^2+2y+1)x^5 + (2y^4+y^3+y^2+2y+2)x^4 + (2y^5+y^4+2y^3+y+2)x^3 + (y^2+y)x^2 + (2y^5+y^2+2y+1)x + (y^5+2y^3+y^2+y)$
$l_6 = 22565467$	$f_{\Re_6} = (2y^4+y^3+y^2+2)x^5 + (2y^5+2y^3+y+1)x^4 + (y^5+y^4+y^3+y^2+2y+1)x^3 + (2y^4+2y^3+y^2+y+2)x^2 + (y^5+2y^4+2y^3+y^2+2)x + (2y^5+2y^4+y^3+y^2+1)$

l	The Frobenius maps for $M = 3^2$
$l_1 = 7521823$	$f_{\Re_1} = (4y^5 + 7y^4 + 5y^3 + 8y^2 + 5y + 2)x^5 + (5y^5 + 8y^4 + 5y^3 + 2y^2 + 4y + 8)x^4 + (8y^5 + 4y^4 + 6y^3 + 7y^2 + 6y + 4)x^3 + (2y^5 + 8y^4 + 2y^3 + 2y^2 + y + 8)x^2 + (y^5 + 7y^4 + y^3 + 3y^2 + 8y + 7)x + (y^5 + 4y^4 + 7y^3 + 3y^2 + 2y + 6)$
$l_2 = 8889427$	$f_{\Re_2} = (2y^5 + 2y^4 + y^3 + 2y^2 + 4y + 5)x^5 + (2y^5 + 3y^4 + 8y^3 + 2y^2 + 5y + 3)x^4 + (2y^5 + 8y^4 + y^3 + 5y + 5)x^3 + (7y^5 + 6y^4 + 5y^3 + 2y^2 + 2y + 6)x^2 + (6y^5 + 2y^4 + 3y^2 + y)x + (y^5 + 2y^4 + 5y^3 + 2y^2 + y + 6)$
$l_3 = 9573229$	$f_{\Re_3} = (4y^4 + 8y^3 + 5y + 1)x^5 + (3y^5 + 7y^4 + 7y^3 + 7y^2 + 6y)x^4 + (y^5 + 6y^3 + 5y^2 + y + 2)x^3 + (6y^5 + 5y^4 + 5y^3 + 3y^2 + 3y + 3)x^2 + (5y^5 + 5y^4 + y^3 + 7y + 8)x + (4y^5 + 3y^4 + 7y^3 + 3y^2 + 6y + 7)$
$l_4 = 10257031$	$f_{\Re_4} = (y^5 + 3y^4 + y + 2)x^5 + (2y^5 + 5y^4 + 2y^3 + 8y^2)x^4 + (6y^5 + 2y^4 + 5y^3 + y^2 + 5y)x^3 + (4y^5 + 7y^2 + y + 4)x^2 + (8y^5 + 5y^4 + 6y^3 + y^2 + 2y + 8)x + (8y^5 + 7y^4 + 8y^3 + 4y^2 + 4y + 6)$
$l_5 = 20514061$	$f_{\Re_5} = (5y^5 + 3y^4 + 7y^3 + 7y^2 + 2y + 4)x^5 + (5y^4 + 7y^3 + 4y^2 + 2y + 2)x^4 + (5y^5 + 4y^4 + 8y^3 + 3y^2 + y + 2)x^3 + (3y^5 + 6y^4 + 3y^3 + y^2 + y + 3)x^2 + (8y^5 + 6y^4 + 3y^3 + 7y^2 + 8y + 7)x + (4y^5 + 3y^4 + 8y^3 + 7y^2 + 7y + 6)$
$l_6 = 22565467$	$f_{\Re_6} = (3y^5 + 5y^4 + y^3 + y^2 + 3y + 2)x^5 + (5y^5 + 6y^4 + 8y^3 + 7y + 7)x^4 + (y^5 + 7y^4 + 7y^3 + 4y^2 + 8y + 1)x^3 + (3y^5 + 5y^4 + 2y^3 + 7y^2 + 7y + 8)x^2 + (7y^5 + 2y^4 + 8y^3 + 7y^2 + 5)x + (2y^5 + 5y^4 + y^3 + y^2 + 7)$

l	The Frobenius maps for $M = 3^3$
$l_1 = 7521823$	$f_{\Re_1} = (13y^5 + 7y^4 + 14y^3 + 26y^2 + 14y + 20)x^5 + (5y^5 + 17y^4 + 5y^3 + 11y^2 + 13y + 26)x^4 + (17y^5 + 4y^4 + 24y^3 + 16y^2 + 6y + 4)x^3 + (20y^5 + 8y^4 + 11y^3 + 11y^2 + y + 26)x^2 + (y^5 + 25y^4 + 19y^3 + 21y^2 + 26y + 7)x + (10y^5 + 22y^4 + 25y^3 + 3y^2 + 2y + 6)$
$l_2 = 8889427$	$f_{\Re_2} = (20y^5 + 2y^4 + y^3 + 11y^2 + 22y + 23)x^5 + (2y^5 + 12y^4 + 26y^3 + 11y^2 + 14y + 21)x^4 + (2y^5 + 26y^4 + y^3 + 18y^2 + 14y + 23)x^3 + (16y^5 + 15y^4 + 14y^3 + 20y^2 + 11y + 15)x^2 + (6y^5 + 11y^4 + 21y^2 + 19y)x + (10y^5 + 11y^4 + 23y^3 + 11y^2 + 10y + 24)$
$l_3 = 9573229$	$f_{\Re_3} = (9y^5 + 4y^4 + 17y^3 + 18y^2 + 5y + 19)x^5 + (12y^5 + 16y^4 + 7y^3 + 7y^2 + 15y)x^4 + (10y^5 + 24y^3 + 14y^2 + 10y + 20)x^3 + (24y^5 + 5y^4 + 5y^3 + 3y^2 + 12y + 12)x^2 + (5y^5 + 5y^4 + 19y^3 + 9y^2 + 7y + 26)x + (13y^5 + 21y^4 + 25y^3 + 12y^2 + 6y + 16)$
$l_4 = 10257031$	$f_{\Re_4} = (10y^5 + 3y^4 + 18y^3 + 19y + 2)x^5 + (20y^5 + 14y^4 + 2y^3 + 17y^2 + 9y + 9)x^4 + (24y^5 + 2y^4 + 23y^3 + 10y^2 + 14y + 9)x^3 + (22y^5 + 9y^4 + 9y^3 + 7y^2 + 10y + 22)x^2 + (26y^5 + 5y^4 + 15y^3 + y^2 + 2y + 26)x + (17y^5 + 16y^4 + 26y^3 + 4y^2 + 22y + 15)$
$l_5 = 20514061$	$f_{\Re_5} = (14y^5 + 3y^4 + 25y^3 + 16y^2 + 11y + 22)x^5 + (18y^5 + 23y^4 + 16y^3 + 22y^2 + 2y + 20)x^4 + (23y^5 + 22y^4 + 17y^3 + 21y^2 + 10y + 20)x^3 + (21y^5 + 6y^4 + 12y^3 + 19y^2 + y + 3)x^2 + (17y^5 + 15y^4 + 21y^3 + 7y^2 + 26y + 16)x + (13y^5 + 3y^4 + 26y^3 + 25y^2 + 7y + 24)$
$l_6 = 22565467$	$f_{\Re_6} = (12y^5 + 23y^4 + 19y^3 + 10y^2 + 12y + 11)x^5 + (14y^5 + 24y^4 + 8y^3 + 25y + 7)x^4 + (10y^5 + 16y^4 + 7y^3 + 4y^2 + 8y + 1)x^3 + (21y^5 + 5y^4 + 20y^3 + 16y^2 + 16y + 8)x^2 + (25y^5 + 2y^4 + 8y^3 + 16y^2 + 5)x + (20y^5 + 14y^4 + y^3 + y^2 + 16)$

We now proceed to Step 3 of the algorithm where we prove that I_d/J^M is isomorphic to $B^{\perp}_{d_1,d_2}$. The computations for the ideal $\overline{J^M}$ gave us the basis $(-2+y, 1+x)$ in $\mathbb{Z}/9\mathbb{Z}$. Since the degree of both x and y in R_{d_1,d_2} is $3\cdot 2 = 6$, we compute the annihilator of $(-2+y^3, 1+x^3)$ in $(\mathbb{Z}/9\mathbb{Z})[x,y]/(x^6-1, y^6-1)$. We found the following polynomial to be the generator of $\mathrm{Ann}_{R_{d_1,d_2}}(\overline{J^M})$:

$$h(x,y) = 3 - 3x^3 - 3y^3 + 3x^3y^3.$$

Factoring $h(x,y)$ in $\mathbb{Z}[x,y]$ we get

$$\begin{aligned} h(x,y) &= 3(-1+x)(1+x+x^2)(-1+y)(1+y+y^2) \\ &= 3(x-1)(y-1)\Phi_3(x)\Phi_3(y) \end{aligned}$$

where Φ_k is the kth cyclotomic polynomial. Therefore, we apply to η the norm map $\frac{(x^6-1)(y^{66}-1)}{(x^{6/3}-1)(y^{6/3}-1)}$ instead of $\frac{(x^6-1)(y^{66}-1)}{(x^6-1)(y^6-1)}$, and then the annihilator $h'(x,y) = 3(-1+x)(-1+y)$. The polynomials $P(x)$ and $P(x^M)$ of Proposition 5.1 were calculated with a precision of 500 and are shown in the table below. Finally, we showed that $P(x)$ divides $P(x^M)$, hence proving rigorously that $3^2 \parallel h^+$.

$P(x)$	$x^4 - 35667454\cdot x^3 + 318041818710531\cdot x^2 - 35667454\cdot x + 1$
$P(x^M)$	$x^{36} - 364929542762806942594907901654249278525439344697663012299174707204\cdot$ $x^{27} + 33293392795267835243258623959180895487795677296162956508170492359406$ $4021927751129126080773734937639859205167814567455816497823744 06\cdot x^{18} -$ $364929542762806942594907901654249278525439344697663012299174707204\cdot x^9 + 1$

6.2. Step 3 for the field of conductor 1477 = 7 · 211. We found that the only primes $l < 10000$ dividing h^+ are 7 and 11. In this example we will show our work for $l = 7$ where there are more than one pair of (ϕ_x, ϕ_y) contained in J^M.

Step 2 of our algorithm showed that the orders of the quotients I_d/J^M stabilize at $M = 7$ with $J^M = (3+3y+y^2, 3+6x+4y+xy, 5+x^3+y)$ in $\mathbb{Z}/7\mathbb{Z}$ for both possible combinations of (d_1, d_2), and we therefore choose the smaller pair $(6,6)$. The pairs of (ϕ_x, ϕ_y) contained in J^M are $(x+3, y-1)$, $(x+4, y+4)$, $(x+5, y-1)$. As expected, $|B[M]^{\perp}_{d_1,d_2}| = \prod_{\phi_x,\phi_y} |B[M]^{\perp}_{\phi_x,\phi_y}| = 7^3$ (we found $|B[M]^{\perp}_{\phi_x,\phi_y}| = 7$ for each pair (ϕ_x, ϕ_y)). We have $|\mathrm{GCD}(P_{(g,h)})|_7 = 7^2$, hence, after Step 3, we will have proved that $7 \parallel h^+$.

The computations for the annihilator gave us only one generator:

$$\begin{aligned} h(x,y) &= \Phi_3(x)\Phi_3(y)\Phi_{21}(y)\big(4 + 2x - 4x^2 + 5x^3 + 2y^7 - 6xy^7 + 5x^2y^7 - x^3y^7 \\ &\quad - 4y^{14} + 5xy^{14} - 3x^2y^{14} + 2x^3y^{14} + 5y^{21} - xy^{21} + 2x^2y^{21} + x^3y^{21}\big) \\ &= \Phi_3(x)\Phi_3(y)\Phi_{21}(y)h'(x,y). \end{aligned}$$

From basic properties of cyclotomic polynomials, we can establish the relation

$$(*) \qquad \Gamma'_\delta = \prod_{k \in D(|\Gamma|) \setminus D(\delta)} \Phi_k(\sigma)$$

where Γ is any finite cyclic group of order $|\Gamma|$, $D(|\Gamma|) = \{k \in N : k \,|\, |\Gamma|\}$ and Γ'_δ is the sum of all the elements of the subgroup $\Gamma_\delta = \langle \sigma^\delta \rangle$ of index δ in Γ.

Let us recall that our Galois group $\tilde{G}$ of the extension $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}$ is such that $\tilde{G} \cong \tilde{G}_1 \times \tilde{G}_2$ where $\tilde{G}_i$ is finite cyclic of order $p-1 = 6$ and $q-1 = 270$ in this example, for $i = 1$ and 2 respectively. As $(d_1, d_2) = (6, 6)$ and $l^{a_2} = 7$ we have the subgroup $\tilde{G}_1 \times \tilde{G}_2$ of $\tilde{G}$ of order $6 \cdot 42$. As we work in the real subfield $\mathbb{Q}(\zeta_{pq})^+$, we can assume that the subgroup $G_1 \times G_2$ of $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{pq})^+/\mathbb{Q})$ is of order $6 \cdot 21$. We then see that $\Phi_3(y) \cdot \Phi_{21}(y) = (G_2)'_7$, which, according to the formula $(*)$ above, is the sum of the elements of the group $(G_2)_7$ of index 7 in G_2. The norm map that we therefore need to apply to η is $\frac{(x^6-1)(y^{210}-1)}{(x^{6/3}-1)(y^{42/7}-1)}$, and then the annihilator $h'(x, y)$. The polynomials $P(x)$ and $P(x^M)$ of Proposition 5.1 were calculated with a precision of 1000 and we showed that $P(x)$ divides $P(x^M)$, hence proving rigorously that $7 \,\|\, h^+$. The polynomial $P(x)$ is presented below, whereas $P(x^M)$ is omitted as it is too long.

$P(x)$ $x^{12} - 25328567281808559792011754083332056676 4 \cdot x^{11} + 160384080137275763786753982056153848499322525476713900459594970568564239997 46 \cdot x^{10} - 744769611043367581754856181864922703880369945908566382010839778928526681384354044370 0 \cdot x^9 + 869117683565729211234991593257060756356797825718765783832627442647577671131436873144346703615 \cdot x^8 - 1045502371457459906661385781160012228359906832607656705019244404117434162718039857442427623338144074 \cdot x^7 + 3160639438009043605335829264657720206479102762418767642516600675728776830819615633429388073183683860322 96 \cdot x^6 - 332994422221005688150106678790168231474573847302521901074582820819381171053952530361771079019937283128757 4 \cdot x^5 + 8770948069995020839912713521744301221518786226568051634630457643479432149168032626544704205804528987979615 \cdot x^4 - 1944459765899336452214557670670811109932072061509042393676059914702050701273432145 0 \cdot x^3 + 1077702622713709586698103579794845313506944729939069654287 1 \cdot x^2 - 2076231097007974511677023650 14 \cdot x + 1$

6.3. Step 3 for the field of conductor $1355 = 5 \cdot 271$. We found that the only prime $l < 10000$ dividing h^+ is 37. Step 2 of our algorithm showed that the orders of the quotients I_d/J^M stabilize at $M = 37$ with $J^M = (9 + 27y + y^2, 8 + x + 28y)$ in $\mathbb{Z}/37\mathbb{Z}$ and with $(d_1, d_2) = (4, 18)$. The only two factors that gave a non-trivial quotient I_d/J^M were $\phi_x(x) = x + 1$ and $\phi_y(y) = y + 28$. The computations for the annihilator gave us only one

generator:

$$h(x,y) = \Phi_4(x)\Phi_2(y)\Phi_6(y)\Phi_{18}(y)\big(4+33x+21y+16xy+27y^2+10xy^2+3y^3 +34xy^3+25y^4+12xy^4+11y^5+26xy^5+30y^6+7xy^6+28y^7+9xy^7+36y^8+xy^8\big) = \Phi_4(x)\Phi_2(y)\Phi_6(y)\Phi_{18}(y)h'(x,y)$$

According to the formula $(*)$ above, $\Phi_4(x) = (G_1)'_2$ and $\Phi_2(y)\Phi_6(y)\Phi_{18}(y) = (G_2)'_9$, hence the norm map that we need to apply to η is $\frac{(x^4-1)(y^{270}-1)}{(x^{4/2}-1)(y^{18/9}-1)}$, and then the annihilator $h'(x,y)$. The polynomials $P(x)$ and $P(x^M)$ of Proposition 5.1 were calculated with a precision of 7000 and we showed that $P(x)$ divides $P(x^M)$, hence proving rigorously that $37 \parallel h^+$. The polynomial $P(x)$ is given below, whereas $P(x^M)$ is omitted as it is too long.

$P(x)$	$x^4 - 534186444472275956720533076216968091508192072459731400996 \cdot x^3 +$ 713387893644829910093808777084352864619005729280623587687584533335920045607442656991580319886482921214362374480 06 $\cdot x^2 - 53418644447227595672053307621$ 6968091508192072459731400996 $\cdot x + 1$

7. Table and discussion of the results. We applied Steps 1 and 2 of the algorithm to real cyclotomic fields of conductor $pq < 2000$. We tested the divisibility of $|B| = [E : H] = P \cdot h^+$ by all primes $l < 10000$. All the primes appearing in the greatest common divisor of the $P_{(g,h)}$ for all pairs of primitive roots (g,h) came up as possible divisors, as expected. These primes are listed in the 'GCD' column of Table 1 below. Since we do not calculate the 2-part of h^+ or the l-part for $l > 10000$, we leave out the powers of 2 as well as the primes > 10000 from the 'GCD'. Therefore, if a '1' appears in the 'GCD' column for some field, this means that no odd primes < 10000 divide the greatest common divisor of the various $P_{(g,h)}$. However, there are always powers of 2 in the 'GCD', as we see from our calculations of the index $[E : H]$ in Section 2. In the 'l' column we present all other primes that Step 1 gave to be possible divisors of h^+, besides the ones that already appear in the 'GCD' column. Step 2 verified for all fields that indeed, for some M, we have $|B[M]_{d_1,d_2}| = |B[lM]_{d_1,d_2}|$. As mentioned right before Section 5.3 above, we proceed to Step 3 only for those primes l with $|I_d/J^M| > |\mathrm{GCD}(P_{g,h})|_l$. Finally, in the 'Degree' column we list the smallest degrees $(d_1 l^{a_1}, d_2 l^{a_2})$ for which the module $B^+_{d_1,d_2}$ turned out to be non-trivial, and the '$\tilde{h}^+$' column shows the l-part of h^+ for all odd primes $l < 10000$. The order of appearance of the degrees in the 'Degree' column corresponds to the order of appearance of the primes in the '$\tilde{h}^+$'. column. For example, for the field of conductor $13 \cdot 97$, $\tilde{h}^+ = 5 \cdot 7^2 \cdot 97$ with corresponding degrees $(4,4)$ for the prime 5, $(6,6)$ for the prime 7 and $(12,96)$ for the prime 97.

For the primes l not dividing the degree of the extension, our results agree with Hakkarainen [4]. For those primes l that divide the degree of the extension, our results complete his results in the sense that we verified that either no higher powers of l divide h^+, or there are indeed such higher powers of l. We found five such fields where higher powers of l divide h^+, and we mark them with an asterisk in the column '$\tilde{h}^+$' of Table 1.

Table 1

f	GCD	l	Degree	$\tilde{h}^+$	f	GCD	l	Degree	$\tilde{h}^+$
3·107	1	3	(2,2)	3	7·61	1	5	(2,20)	5
7·67	1	3	(6,6)	3^2 (∗)	11·43	$3^4{\cdot}5^2{\cdot}7^4$	-	(10,6)	3
13·37	7·19	-	(6,18)	19	19·29	5	-	(2,4)	5
17·37	$3^4{\cdot}19$	5	(4,4), (2,18)	5·19	17·41	$3^3{\cdot}7$	-	(2,2)	3
19·37	$3^{16}{\cdot}5$	13, 37	(6,12), (18,36)	13·37	3·251	1	11	(2,10)	11
7·109	3^4	13	(6,12)	13	19·41	5^2	41	(2,40)	41
5·157	$3^2{\cdot}79$	-	(2,6)	3	13·61	$3^{20}{\cdot}5{\cdot}7$	37	(6,60), (12,12)	3·37 (∗)
19·43	1	5	(2,2)	5	11·79	1	79	(2,78)	79
7·127	$3^4{\cdot}7^2$	-	(6,42)	7	13·71	3^3	61	(12,10)	61
5·197	$3^3{\cdot}11$	-	(2,2)	3	3·331	1	3	(2,6)	3^2 (∗)
3·367	1	3	(2,6)	3	17·67	$3^7{\cdot}11^7$	89	(8,22), (8,22)	11·89 (∗)
7·163	1	19	(6,18)	19	17·71	3^2	17,	(16,2),	17
19·61	$3^3{\cdot}7$	73	(18,12)	73	17·73	$3^4{\cdot}7{\cdot}37{\cdot}109$	5	(4,4)	5
7·173	1	7	(6,2)	7	3·419	1	3	(2,2)	3
11·113	5·37	41	(10,8)	41	31·41	$3^3{\cdot}5^6$	7	(6,2)	7·
13·97	7^3	5, 97	(4,4), (6,6), (12,96)	$5{\cdot}7^2{\cdot}97$			11, 31,	(10,10), (30,10),	11· 31
13·101	$3{\cdot}5^2$	31	(6,10)	31	17·79	5	17	(16,2)	17
5·271	$3^3{\cdot}5$	37	(4,18)	37	5·277	$3^2{\cdot}139$	5, 7	(4,4), (2,6)	5·7
19·73	$3^4{\cdot}7{\cdot}101$	17, 19, 37	(18,8), (18,18), (18,36)	$17^2{\cdot}19{\cdot}37$	7·199	1	5	(2,2)	5
5·293	$3^2{\cdot}7^2$	-	(4,4)	3^2	7·211	$3^2{\cdot}5^2{\cdot}7^2$	11	(6,42), (2,10)	7·11
3·503	1	3	(2,2)	3	17·89	$11^3{\cdot}17{\cdot}41$	13	(4,4) (16,8)	13·17
37·43	$3^{26}{\cdot}7^8{\cdot}11{\cdot}19{\cdot}487$	43	(6,42)	43	3·541	1	13	(2,12)	13
3·547	1	5	(2,2)	5	13·127	$3^3{\cdot}7$	5	(12,2)	5^2
7·241	1	13	(6,12)	13	5·347	3·29	5	(4,2)	5
37·47	23^5	5	(4,2)	5	17·103	$3^7{\cdot}17^7$	-	(8,6), (16,34)	$3^2{\cdot}17$ (∗)
3·587	1	7	(2,2)	7	5·353	$3^2{\cdot}59$	-	(2,2)	3
5·373	$3^2{\cdot}11{\cdot}17$	5	(4,4)	5	11·173	3	173	(2,172)	173
17·113	$3^3{\cdot}19$	17, 29	(16,16), (4,28)	$17^3{\cdot}29$	13·149	$3^2{\cdot}5^2{\cdot}7$	109	(6,2), (12,4)	3·109

Acknowledgements. The author wishes to thank Professor Lawrence Washington for his advice and guidance during the writing of the thesis that

this paper is based on, as well as the Cy-Tera of the Cyprus Institute and the Mathematics Department of the University of Maryland College Park for their permission to run parts of this project on their machines.

References

[1] W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Amer. Math. Soc., Providence, RI, 1994.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's guide to PARI-GP (version 2.3.0)*, Université Bordeaux I, Bordeaux, 2000.

[3] G. Gras et M.-N. Gras, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de* $\mathbf{Q}$, Bull. Sci. Math. 101 (1977), 97–129.

[4] T. Hakkarainen, *On the computation of the class numbers of real abelian fields*, Dissertation, Univ. of Turku, 2007.

[5] S. Lang, *Algebra*, Addison-Wesley, Reading, MA, 1965.

[6] H. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat. 1953, no. 2, 48 pp.

[7] F. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. 39 (1982), 693–707.

[8] J. Masley, *Class numbers of real cyclic number fields with small conductor*, Compos. Math. 37 (1978), 297–319.

[9] A. Odlyzko, *Lower bounds for discriminants of number fields*, Acta Arith. 29 (1976), 275–297.

[10] A. Odlyzko, *Lower bounds for discriminants of number fields II*, Tôhoku Math. J. 29 (1977), 209–216.

[11] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. 72 (2003), 913–937.

[12] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, Berlin, 1997.

[13] Wolfram Research, Mathematica 6.0 for Linux x86, Champaign, IL, 1988.

Eleni Agathocleous
Ministry of Education
Nicosia, Cyprus
E-mail: elena.agathocleous@gmail.com

Permanent postal address:
20 Zaloggou St., Apt. 401
3022, Limassol, Cyprus

Received on 16.1.2014
and in revised form on 30.7.2014 (7704)