Glasgow Math. J. **52** (2010) 391–400. © Glasgow Mathematical Journal Trust 2010.
doi:10.1017/S001708951000008X.

ON MOD p REPRESENTATIONS WHICH ARE DEFINED OVER $\mathbb{F}_p$: II

L. J. P. KILFORD
Department of Mathematics, University Walk, Bristol BS8 1TW, United Kingdom
E-mail: l.kilford@gmail.com
Web page: http://www.maths.bris.ac.uk/~maljpk/

and GABOR WIESE
Universität Duisburg-Essen, Institut für Experimentelle Mathematik,
Ellernstraße 29, 45326 Essen, Germany
E-mail: gabor.wiese@uni-due.de
Web page: http://maths.pratum.net/

(Received 29 May 2009; accepted 18 December 2009)

Abstract. The behaviour of Hecke polynomials modulo p has been the subject of some studies. In this paper we show that if p is a prime, the set of integers N such that the Hecke polynomials $T_{\ell,k}^{N,\chi}$ for all primes ℓ, all weights $k \geq 2$ and all characters χ taking values in $\{\pm 1\}$ splits completely modulo p has density 0, unconditionally for $p = 2$ and under the Cohen–Lenstra heuristics for $p \geq 3$. The method of proof is based on the construction of suitable dihedral modular forms.

2000 *Mathematics Subject Classification.* Primary 11F33; secondary 11F25, 11R29.

1. Introduction. Let N and k be positive integers and let ℓ and p be prime numbers. We will let $S_k(\Gamma_0(N), \chi)$ be the space of holomorphic cusp forms of integer weight k for the congruence subgroup $\Gamma_0(N)$ and the Dirichlet character χ of modulus N, and we will define $T_{\ell,k}^{N,\chi}$ to be the characteristic polynomial of the Hecke operator T_ℓ acting on $S_k(\Gamma_0(N), \chi)$. We will call this polynomial the *Hecke polynomial*.

We recall that for modular forms in characteristic 0, there is a well-known conjecture (Maeda's conjecture) which says that the characteristic polynomials of the Hecke operators acting on modular forms for the full modular group $\mathrm{SL}_2(\mathbb{Z})$ are irreducible.

CONJECTURE 1 (Maeda's Conjecture). Let k be a positive integer and let ℓ be a prime number. The Hecke polynomial $T_{\ell,k}^{1,1} \in \mathbb{Z}[X]$ is irreducible with Galois group S_n, where n is the dimension of $S_k(\mathrm{SL}_2(\mathbb{Z}))$ as a complex vector space.

This conjecture lends itself to numerical verification. Methods introduced in [**5**] prove that certain Hecke polynomials are irreducible and have full Galois group, and results such as those in [**1**, **2**, **7**] show that if a certain $T_{\ell,k}^{1,1}$ is irreducible, then other $T_{r,k}^{1,1}$ must be irreducible also.

In the characteristic p case, however, things are obviously different. The paper [**9**], using methods developed in [**7**], gives a list of spaces of modular forms for which one can prove that all of the Hecke polynomials $T_{\ell,k}^{N,1}$ split into linear factors modulo p.

It is then asked whether these are all such spaces. In this paper we will give at least a partial answer to this question, which depends for odd primes p on the Cohen–Lenstra heuristics on class groups of imaginary quadratic fields.

THEOREM 2. *Let p be a prime; if $p \geq 3$, then assume the Cohenheuristics. Then the set of integers N, such that the Hecke polynomials $T_{\ell,k}^{N,\chi}$ for all primes ℓ, all weights $k \geq 2$ and all characters $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\} \subseteq \mathbb{F}_p^\times$ split completely modulo p, has density 0.*

It should be pointed out that for given p and given level N, the weight of an eigenform over $\overline{\mathbb{F}}_p$ can always be adjusted to lie between 2 and $p^2 - 1$.

It should also be noted that a natural generalization of Maeda's conjecture in characteristic 0 to congruence subgroups cannot be true in general; in [**10**], a Hecke eigenform of weight 2 on $\Gamma_0(63)$ is exhibited such that for a set of primes ℓ of positive density, the characteristic polynomial of the Hecke operator T_ℓ acting on the span of all the Galois conjugates of the form is reducible. In other words, the ℓth coefficient does not generate the whole coefficient field for a set of primes ℓ of positive density. This phenomenon is due to the existence of a nontrivial inner twist. Even in the absence of nontrivial inner twists, numerical evidence suggests that there should exist examples where the set of such ℓ is still infinite, although of density 0.

Theorem 2 will be proved in Section 3 for $p = 2$ and in Section 4 for odd p. It will be derived from a statement on the class groups of imaginary quadratic fields that implies the existence of dihedral modular forms mod p whose coefficient fields are not the prime field $\mathbb{F}_p$ (see Section 2).

One can imagine other ways for constructing mod p eigenforms with q-expansions not in $\mathbb{F}_p$. For instance, one could use families of hyperelliptic curves of genus greater than 1 whose Jacobians are of GL_2-type in order to treat those primes p that have a nontrivial residue degree in the endomorphism algebra of the Jacobian tensored with $\mathbb{Q}$ (which is the coefficient field of the corresponding holomorphic eigenform). However, it does not seem obvious how to obtain the desired density 1 statement on the levels.

Moreover, techniques of level raising and the like, as they are for instance used in [**8**], also easily yield mod p Hecke eigenforms having a nontrivial coefficient field. However, the levels will always contain at least a square, excluding a density 1 statement.

2. Dihedral Galois representations and Hypothesis H_p.

DEFINITION 3. Let p be a prime number. An abelian group C is called *p-suitable* if G has a cyclic quotient of order h such that $p \nmid h$ and $h \nmid (p^2 - 1)$.

The condition of p-suitability is equivalent to the existence of a cyclic quotient H of G such that H is isomorphic to a subgroup of $\overline{\mathbb{F}}_p^\times$ but not to a subgroup of $\mathbb{F}_{p^2}^\times$.

We now prove the following results about p-suitable groups.

PROPOSITION 4. *Let G be a p-suitable abelian group and let H be a cyclic quotient of G of order h such that $H \subset \overline{\mathbb{F}}_p^\times$ without being isomorphic to a subgroup of $\mathbb{F}_{p^2}^\times$. Then the group*

$$D = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x \in H \right\rangle \subseteq \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

is isomorphic to the dihedral group D_h of order $2h$ and not all the traces of elements of D lie in $\mathbb{F}_p$.

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

Proof. Let $x \in H$. One just needs to observe that conjugation by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ maps $\left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} x^{-1} & 0 \\ 0 & x \end{smallmatrix}\right)$ in order to see that D is actually isomorphic to D_h. Suppose that $x + x^{-1} = a \in \mathbb{F}_p$. Then x is a root of the polynomial $X^2 - aX + 1 \in \mathbb{F}_p[X]$, and consequently, $x \in \mathbb{F}_{p^2}$. The assumption excludes that this happens for all $x \in H$. □

PROPOSITION 5. *Let $K/\mathbb{Q}$ be an imaginary quadratic field of discriminant d and let C be its class group. If C is p-suitable, then there exists an irreducible odd dihedral Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ of conductor $|d|$ such that not all its traces lie in $\mathbb{F}_p$.*

Proof. Let H and h be as in Proposition 4. Note that $\mathrm{Gal}(K/\mathbb{Q})$ acts on C and, hence, also on H by inversion. We now view H as an unramified character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \overline{\mathbb{F}}^{\times}$ of order h. We choose σ to be a lift to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Then we have that $\chi(\sigma\tau\sigma^{-1}) = \chi(\tau^{-1}) = \chi(\tau)^{-1}$ for any $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. This means that we can identify the group D from Proposition 4 in a natural way with the image of the irreducible Galois representation $\mathrm{Ind}_{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(\chi)$. This Galois representation is odd, since complex conjugation plays the role of σ and, consequently, has determinant -1. Moreover, a well-known formula gives the conductor. For more details, see [**16**]. □

If $M \subset N$ are two sets of natural numbers, then we say that M *has density* $\alpha = \Delta(M, N)$ *in* N if the limit for $x \to \infty$ of

$$\frac{\#\{m \in M \mid m \leq x\}}{\#\{m \in N \mid m \leq x\}}$$

exists, and is equal to α.

We will also introduce some notation for class groups. We denote by $\mathrm{CL}(\mathbb{Q}(\sqrt{-d}))$ the class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$.

Let p be a prime. We consider the following Hypothesis, which we denote by (H_p).

HYPOTHESIS (H_p). *The density of the set*

$$\{N \in \mathbb{N} \mid \exists\, d \in \mathbb{N} \text{ squarefree}, d \equiv 3 \mod 4, d \mid N, \mathrm{CL}(\mathbb{Q}(\sqrt{-d})) \text{ is } p\text{-suitable}\}$$

exists and is 1.

We will establish (H_2) by a result on the exponent of class groups. Unfortunately, we do not know of any way of proving (H_p) for odd p, but we shall show that (H_p) is a consequence of the Cohen–Lenstra heuristics.

PROPOSITION 6. *Assume Hypothesis (H_p). Then the conclusion of Theorem 2 is true.*

Proof. Let $N \in \mathbb{N}$ such that there is a squarefree $d \equiv 3 \mod 4$ with $d \mid N$ for which $\mathrm{CL}(\mathbb{Q}(\sqrt{-d}))$ is p-suitable. It suffices to show that there is a cuspidal Hecke eigenform f modulo p of level N, quadratic Dirichlet character and some weight such that it has some coefficient $a_n(f)$ in its q-expansion that does not lie in $\mathbb{F}_p$.

Let us take such an N and d. By means of Proposition 5, there is an odd dihedral Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ of conductor d such that not all its traces lie in $\mathbb{F}_p$. By work of Hecke, ρ is known to be modular of level d, weight 1 for the quadratic Dirichlet character belonging to $\mathbb{Q}(\sqrt{-d})$. This means that there is a holomorphic Hecke eigenform f in the specified level, weight and character whose

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

coefficients of the standard q-expansion $a_\ell(f)$ at primes ℓ reduce modulo a suitable prime lying above p to the trace of a Frobenius element at ℓ. In particular, there is a prime ℓ such that the Hecke polynomial at ℓ is not completely split modulo p. Noting that via the degeneracy maps, f gives rise to a form in level N settles the claim for odd p.

In order to treat the case $p = 2$, we use the well-known fact that there is a congruence modulo a prime above 2 of f and another modular form of the same level and the trivial Dirichlet character. □

3. Exponents of class groups and Proof of (H_2). In this section, we will show Hypothesis (H_2). Let us call a positive integer $d \equiv 3 \mod 4$ which is squarefree 2-*suitable* if $\mathrm{CL}(\mathbb{Q}(\sqrt{-d}))$ is 2-suitable. In order to show that the set of positive integers N having a 2-suitable squarefree positive divisor $d \equiv 3 \mod 4$ has density 1, we first need to rule out the possibility that the only cyclic quotients are of order $2^2 - 1 = 3$. To do this, we recall the following result on class groups with small exponent.

THEOREM 7 (Boyd–Kisilevksy [**4**], Weinberger [**15**]). *There are only finitely many negative fundamental discriminants d such that $\mathrm{CL}(\mathbb{Q}(\sqrt{d}))$ has exponent 3.*

We note that this result is ineffective because it relies on Siegel's ineffective lower bound for the size of the class group. A computation is reported in [**13**] which says that the largest fundamental discriminant with absolute value less than 10^6 such that the exponent is 3 is -4027; $\mathrm{CL}(\mathbb{Q}(\sqrt{-4027}))$ is isomorphic to $C_3 \times C_3$; it is possible that this is the largest such fundamental discriminant.

We now note by genus theory that if $d \equiv 3 \mod 4$ is a prime number, then the 2-part of the class group of $\mathbb{Q}(\sqrt{-d})$ is trivial, so this means that for all but finitely many of these d both of the conditions of 2-suitability are satisfied. We will now use a well-known theorem of Landau to show that the set of natural numbers N which are divisible by such a d has density 1.

THEOREM 8 (Landau [**11**], pp. 668–669). *Let $\{a_i\}$ be r distinct residue classes modulo an integer A and let $\mathcal{P}$ be the set of prime numbers which are congruent to one of the a_i modulo A. If we let $M(x)$ be the number of natural numbers less than x whose prime factors are all in $\mathcal{P}$, then*

$$M(x) \sim c \cdot \frac{x}{(\log x)^{1-\frac{r}{\phi(A)}}},$$

where c is a positive constant and ϕ is Euler's ϕ-function. Note that $\frac{r}{\phi(A)}$ is the Dirichlet density of the set $\mathcal{P}$.

In particular, this means that the set of natural numbers whose prime factors are all congruent to a restricted set of the possible residue classes for a prime number modulo A has natural density 0, so the set of natural numbers with a prime factor d which is 2-suitable has density 1, which is what we wanted to show. This means that we have proved the following proposition.

PROPOSITION 9. *The hypothesis (H_2) is true, and therefore the conclusion of Theorem 2 is true if $p = 2$.*

The technique used to prove this hypothesis is likely to only give a density 0 result; we will now give some numerical data which suggests this.

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

Using a computer algebra package such as MAGMA [**3**] one finds that there are many quadratic imaginary fields whose class groups have trivial odd part; for instance, if we consider quadratic imaginary fields with fundamental discriminant of absolute value less than 4,000,000, there are 3,722 fields with class group of order 128,8,361 fields with class group of order 256 and 18,046 fields with class group of order 512. This numerical evidence seems to suggest that there are an infinite number of imaginary quadratic fields with class number a power of 2, as one can find fields with class number a very high power of 2; for instance, it can be shown that $\mathbb{Q}(\sqrt{-5000948753})$ has class number 65,536. For more numerical results, see [**12**, Section 10] which gives tables of the number of quadratic imaginary fields with small odd part with fundamental discriminant between $-500{,}000$ and $-1{,}000{,}000$.

4. Cohen–Lenstra heuristics and Hypothesis (H_p). In this section we want to make use of the Cohen–Lenstra heuristics [**6**] for class groups of imaginary quadratic fields. We first recall their principal definitions and their fundamental heuristic assumption. We will, however, specialize them directly to imaginary quadratic fields. We abbreviate the words *fundamental discriminant* by *f.d.*

DEFINITION 10 (Cohen–Lenstra [**6**], Definition 5.1). *(a) Let G be an abelian group. Define*

$$w(G) = (\#\operatorname{Aut}(G))^{-1}.$$

This will play the role of a weighting factor in the heuristics.

(b) Let $\underline{A}$ be a set of isomorphism classes of abelian groups and let f be a complex-valued function on $\underline{A}$. The $(\infty, 0, \underline{A})$-average of f is defined as

$$M_{(\infty,0,\underline{A})}(f) := \lim_{x\to\infty} \frac{\sum_{1\le a\le x}\sum_{G\in\underline{A},\#G=a} f(G)w(G)}{\sum_{1\le a\le x}\sum_{G\in\underline{A},\#G=a} w(G)},$$

if this limit exists.

We introduce some notation. For sake of shortness, we write $\mathrm{CL}(-d)$ for $\mathrm{CL}(\mathbb{Q}(\sqrt{-d}))$. Let S be a set of primes. We denote the prime-to-S-part of an abelian group C by $\pi^{(S)}(C)$ and the S-part by $\pi_{(S)}(C)$. Moreover, if $S = \{p\}$, then we write $\pi^{(p)}(C)$ and $\pi_{(p)}(C)$, respectively. In fact, we consider $\pi^{(S)}$ and $\pi_{(S)}$ as functions on (isomorphism classes of) finite abelian groups. We write $\underline{\mathrm{Ab}}_{(S)}$ for the set of isomorphism classes of finite abelian groups of order divisible only by primes in S. Accordingly, we use the notation $\underline{\mathrm{Ab}}^{(S)}$ to stand for the set of isomorphism classes of finite abelian groups of order coprime with any prime in S.

FUNDAMENTAL HEURISTIC ASSUMPTION 11 (Cohen–Lenstra [**6**], Fundamental Assumptions 8.1). Let f be a function on $\underline{\mathrm{Ab}}^{(2)}$ taking values in $\{0, 1\}$. Let

$$\mathcal{F} := \{d \in \mathbb{N} \mid -d \text{ is f.d.}\}$$

and define

$$\mathcal{F}_f := \{d \in \mathcal{F} \mid f(\pi^{(2)}(\mathrm{CL}(-d))) = 1\}.$$

Then the natural density $\Delta(\mathcal{F}_f, \mathcal{F})$ of $\mathcal{F}_f$ in $\mathcal{F}$ exists and is equal to $M_{(\infty,0,\underline{\mathrm{Ab}}^{(2)})}(f)$.

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

PROPOSITION 12. *Let S be a set of primes containing the prime 2 which has a density strictly smaller than 1. Assume the Cohen–Lenstra heuristics, i.e. assume that Fundamental Heuristic Assumption 11 is satisfied. Then the set*

$$\mathcal{F}_S := \{d \in \mathcal{F} \mid \#\pi^{(S)}(\mathrm{CL}(-d)) = 1\}$$

has natural density 0 in the set $\mathcal{F}$.

Proof. Let f be the function which sends the trivial abelian group to 1 and the isomorphism class of any nontrivial abelian group to 0. The principal input for this proof is [**6**, Proposition 5.6], which implies that

$$M_{(\infty,0,\underline{\mathrm{Ab}}^{(2)})}(f \circ \pi^{(S)}) = M_{(\infty,0,\underline{\mathrm{Ab}}^{(S)})}(f).$$

It follows directly from Definition 10 that the right-hand side term is equal to

$$\lim_{x\to\infty} \left(\sum_{a=1}^{x} \sum_{\substack{G \in \underline{\mathrm{Ab}}^{(S)} \\ \#G = a}} w(G) \right)^{-1}.$$

This limit is 0 because the sum is larger than

$$\sum_{\substack{p \text{ prime} \\ p \notin S}} \frac{1}{p-1},$$

which is divergent. Under the Fundamental Heuristic Assumption 11, the meaning of

$$M_{(\infty,0,\underline{\mathrm{Ab}}^{(2)})}(f \circ \pi^{(S)})$$

is the natural density of $\mathcal{F}_S$ in $\mathcal{F}$. □

For a subset $A \subseteq \mathbb{N}$, we introduce the following shorthand notation:

$$A(x) := \#\{a \in A \mid a < x\}.$$

We first prove a simple lemma on the natural density $\Delta(A, B)$.

LEMMA 13. *(a) Let $A \subseteq B \subseteq C$ be subsets of $\mathbb{N}$ such that $\Delta(A, B) = \Delta(B, C) = 1$. Then $\Delta(A, C) = 1$.*

(b) Let $A \subseteq B \subseteq C$ be subsets of $\mathbb{N}$ such that $\Delta(A, C) > 0$. Then $\Delta(A, C) = \Delta(B, C) > 0$ if and only if $\Delta(A, B) = 1$.

(c) Let n be any positive integer and let $A \subseteq B$ be subsets of $\mathbb{N}$ such that $\Delta(A, B) = 1$. Denote by $nA = \{na \mid a \in A\}$ and similarly for nB. Then $\Delta(nA, nB) = 1$.

(d) Let $A \subseteq B$ and $C \subseteq B$ be subsets such that $\Delta(A, B) = 1$ and $\Delta(C, B) = \alpha > 0$. Then $\Delta(A \cap C, C) = 1$.

(e) Let $A_n \subseteq A_{n+1}$ for all $n \in \mathbb{N}$ be subsets of a set $B \subseteq \mathbb{N}$ all having a natural density $\Delta(A_n, B)$. Assume that $\lim_{n\to\infty} \Delta(A_n, B) = 1$. Let $A = \bigcup_{n\in\mathbb{N}} A_n$. Then $\Delta(A, B) = 1$.

(f) Let $A_1 \subseteq B_1$ and $A_2 \subseteq B_2$ be subsets of $\mathbb{N}$ such that $\Delta(A_i, B_i) = 1$ for $i = 1, 2$. Then $\Delta(A_1 \cup A_2, B_1 \cup B_2) = 1$.

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

Proof. (a), (b) and (c) are clear.

(d) Choose $0 < \delta < \alpha$. There is a bound D such that $|\frac{C(x)}{B(x)} - \alpha| \leq \delta$ for all $x \geq D$. This implies $(\alpha - \delta)B(x) \leq C(x)$ for all $x \geq D$. Note the trivial inequality $C(x) - (A \cap C)(x) \leq B(x) - A(x)$, which is valid for all $x \in \mathbb{N}$. Now, let $\epsilon > 0$ be given. By assumption, there is a bound E_ϵ such that for all $x \geq E_\epsilon$ we have

$$B(x) - A(x) \leq \epsilon(\alpha - \delta)B(x).$$

Putting the inequalities together we obtain

$$C(x) - (A \cap C)(x) \leq \epsilon C(x)$$

for all $x \geq \max(E_\epsilon, D)$, and thus, the claim.

(e) Put $a_{n,x} = \frac{A_n(x)}{B(x)}$. For all x and all n we have $a_{n+1,x} \geq a_{n,x}$. By assumption, for fixed n, the limit $\lim_{x\to\infty} a_{n,x} =: a_n$ exists, we have $a_{n+1} \geq a_n$ for all n and $\lim_{n\to\infty} a_n = 1$.

Let $\epsilon > 0$ be given. There exists a bound C such that for all $n \geq C$ we have $1 \geq a_n \geq 1 - \frac{1}{2}\epsilon$. Moreover, there also exists a bound D such that for all $x \geq D$ we have $|a_{C,x} - a_C| \leq \frac{1}{2}\epsilon$. Hence, for all $x \geq D$ and all $n \geq C$ we have

$$1 - \epsilon \leq a_C - \frac{1}{2}\epsilon \leq a_{C,x} \leq a_{n,x} \leq 1.$$

The claim follows.

(f) Let $A = A_1 \cup A_2$ and $B = B_1 \cup B_2$. Note the following inequality which is valid for all $x \in \mathbb{N}$:

$$B(x) - A(x) \leq B_1(x) - A_1(x) + B_2(x) - A_2(x).$$

Let $\epsilon > 0$ be given. By assumption there exists a bound C such that for all $x \geq C$ we have $B_i(x) - A_i(x) \leq \frac{1}{2}\epsilon B_i(x)$ for $i = 1, 2$. Moreover, for all $x \in \mathbb{N}$ we have the inequality

$$B(x) \geq \max(B_1(x), B_2(x)) \geq \frac{1}{2}(B_1(x) + B_2(x)).$$

Putting the inequalities together yields

$$B(x) - A(x) \leq \epsilon B(x)$$

for all $x \geq C$, and thus $\Delta(A, B) = 1$. □

The next lemma will be useful for deriving Hypothesis (H_p) from the Cohen–Lenstra heuristics.

LEMMA 14. *(a) Let B be the set of positive integers that are $\equiv 3 \mod 4$ and let A be the subset of those that are squarefree. Let $A_N := \bigcup_{n=1}^{N}(2n-1)^2 A$. Then $\lim_{N\to\infty} \Delta(A_N, B) = 1$.*

(b) Let A be the set of positive integers that are $\equiv 3 \mod 4$ and B the set of positive integers that are $\equiv 1 \mod 4$. Let $C_N = B \setminus \bigcup_{i=1}^{N} p_i A$, where $p_1, p_2, \ldots$ are the prime numbers that are $\equiv 3 \mod 4$. Then $\lim_{N\to\infty} \Delta(C_N, B) = 0$.

(c) Let A be the set of positive integers that are not divisible by 4. Let $C_N = \mathbb{N} \setminus \bigcup_{n=0}^{N} 4^n A$. Then $\lim_{N\to\infty} \Delta(C_N, \mathbb{N}) = 0$.

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

Proof. (a) The set A_N is the subset of B of those integers that are divisible by some odd square $(2n-1)^2$ for $n \le N$. It is well known that $\Delta(A, B) = \frac{8}{\pi^2}$. Hence,

$$\Delta(A_N, B) = \Delta(A, B) \sum_{n=1}^{N} \frac{1}{(2n-1)^2} \xrightarrow{N\to\infty} \frac{8}{\pi^2}\frac{\pi^2}{8} = 1,$$

since $n^2 A \cap m^2 A = \emptyset$ for $n \neq m$. From this, the claim follows.

(b) The set C_N is contained in the set of positive integers n that are $\equiv 1 \mod 4$ and are not divisible by any of $p_1, p_2, \ldots, p_N$. The latter condition can be reformulated to say that n is a unit in $\mathbb{Z}/(p_1, p_2, \ldots, p_N)\mathbb{Z}$. Thus, the density of C_N in B is

$$\prod_{i=1}^{N} \frac{p_i - 1}{p_i} = \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right) = \left(\prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right)^{-1}\right)^{-1} = \left(\sum_{\substack{n=1 \\ \mathrm{cond}_N}}^{\infty} \frac{1}{n}\right)^{-1}$$

with the condition cond_N that n is only divisible by the primes $p_1, p_2, \ldots, p_N$. It is well known that the sequence $a_N := \sum_{n=1,\, \mathrm{cond}_N}^{\infty} \frac{1}{n}$ diverges, whence the claim follows.

(c) The set C_N is the set of positive integers divisible by 4^{N+1}, which obviously has density $1/4^{N+1}$, whence the claim. □

PROPOSITION 15. *Let p be an odd prime. Assume the Cohen–Lenstra heuristics, i.e. Fundamental Heuristic Assumption 11. Then Hypothesis (H_p) is satisfied, and therefore the conclusion of Theorem 2 is true for odd primes.*

Proof. Let S be the set of primes dividing $p(p^2-1)$. Let $\mathcal{F}$ and $\mathcal{F}_S$ be the sets in Proposition 12. Let $A = \mathcal{F} \setminus \mathcal{F}_S$.

The strategy of the proof is to extend the fact that A has natural density 1 in $\mathcal{F}$ to all positive integers, by first extending it to the integers $\equiv 3 \mod 4$, then to those $\equiv 1 \mod 4$ and finally by multiplying by 2 and powers of 4 to all integers.

Define

$$B_1 := \{d \in \mathbb{N} \mid d \equiv 3 \mod 4, d \text{ squarefree}\} \subset \mathcal{F}$$

and $A_1 := B_1 \cap A$. By Lemma 13 (d), we have $\Delta(A_1, B_1) = 1$. Due to the statement on finite unions, Lemma 13 (f), we have

$$\Delta\left(\bigcup_{n=1}^{N} (2n-1)^2 A_1, \bigcup_{n=1}^{N} (2n-1)^2 B_1\right) = 1.$$

Furthermore,

$$B_2 := \{n \in \mathbb{N} \mid n \equiv 3 \mod 4\} = \bigcup_{n=1}^{\infty} (2n-1)^2 B_1$$

and by Lemma 14 (a) also

$$\lim_{N\to\infty} \Delta\left(\bigcup_{n=1}^{N} (2n-1)^2 B_1, B_2\right) = 1.$$

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

By Lemma 13 (b), this immediately implies

$$\lim_{N\to\infty} \Delta\left(\bigcup_{n=1}^{N}(2n-1)^2 A_1, B_2\right) = 1,$$

whence Lemma 13 (e) yields

$$\Delta(A_2, B_2) = 1 \text{ with } A_2 = \bigcup_{n=1}^{N}(2n-1)^2 A_1.$$

We have achieved the first goal, namely, to extend the density one statement to the integers that are $\equiv 3 \mod 4$.

Next, we multiply the sets A_2 and B_2 by all the primes $\equiv 3 \mod 4$ in order to pass to the integers that are $\equiv 1 \mod 4$. Let $B_3 := \{n \in \mathbb{N} \mid n \equiv 1 \mod 4\}$. From Lemma 14 (b), we obtain

$$\lim_{N\to\infty} \Delta\left(\bigcup_{i=1}^{N} p_i B_2, B_3\right) = 1,$$

whence we get (using Lemma 13 (b) and (f))

$$\lim_{N\to\infty} \Delta\left(\bigcup_{i=1}^{N} p_i A_2, B_3\right) = 1.$$

Setting $A_3 := \bigcup_{i=1}^{\infty} p_i A_2$, we obtain from Lemma 13 (e)

$$\Delta(A_3, B_3) = 1.$$

Now we have also achieved our goal for the integers that are $\equiv 1 \mod 4$. We get those $\equiv 2 \mod 4$ simply by multiplying those that we have treated so far by 2. Let

$$A_4 := A_2 \cup A_3 \text{ and } B_4 := B_2 \cup B_3.$$

By Lemma 13 (f), it follows that $\Delta(A_4, B_4) = 1$. Moreover, the density of $A_5 := 2A_4$ in $B_5 := 2B_4$ is 1 by Lemma 13 (a).

Finally, using the same procedure and Lemma 14 (c), we find

$$\Delta(A_6, \mathbb{N}) = 1 \text{ with } A_6 := \bigcup_{n=0}^{\infty} 4^n A_5.$$

Now we note that the set A_6 is precisely the set of $n \in \mathbb{N}$ such that there is a squarefree $d \in \mathbb{N}$ such that $d \mid n$ and $d \equiv 3 \mod 4$ with the property that $d \notin \mathcal{F}_S$. Directly from the definition of p-suitability, it follows that such a d is p-suitable. □

REMARK 16. We remark that a straightforward generalization of [**14**, Corollary 3] yields that for a given prime p, the set of $d \in \mathbb{N}$ such that $-d$ is a fundamental discriminant and the class group of $\mathbb{Q}(\sqrt{-d})$ is a p-group that has density zero in $\mathbb{N}$.

However, we were unable to extend this result to groups whose orders are only divisible by primes in some finite set S. This would have sufficed to prove Hypothesis (H_p) without assuming the Cohen–Lenstra heuristics.

https://doi.org/10.1017/S001708951000008X Published online by Cambridge University Press

ACKNOWLEDGEMENTS. This project was started while the second author was visiting the University of Bristol. He would like to thank the University and the Heilbronn Institute for their hospitality. The work was finished while the first author was visiting the Institut für Experimentelle Mathematik (IEM). He would like to thank the IEM and Universität Duisburg-Essen for their hospitality. G.W. was partially supported by the European Research Training Network *Galois Theory and Explicit Methods* MRTN-CT-2006-035495 and by the Sonderforschungsbereich Transregio 45 of the Deutsche Forschungsgemeinschaft.

REFERENCES

1. S. Ahlgren, On the irreducibility of Hecke polynomials, *Math. Comput.* **77**(263) (2008), 1725–1731.

2. S. Baba and M. R. Murty, Irreducibility of Hecke polynomials, *Math. Res. Lett.* **10**(5–6) (2003), 709–715.

3. W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.* **24**(3–4) (1997), 235–265. Available at http://magma.maths.usyd.edu.au.

4. D. W. Boyd and H. Kisilevsky, On the exponent of the ideal class groups of complex quadratic fields, *Proc. Amer. Math. Soc.* **31** (1972), 433–436.

5. K. Buzzard, On the eigenvalues of the Hecke operator T_2, *J. Number Theory* **57**(1) (1996), 130–132.

6. H. Cohen and H. W. Lenstra, Jr, Heuristics on class groups of number fields, in *Number theory, Noordwijkerhout 1983* (Jager H., Editor), Lecture Notes in Mathematics, vol. 1068 (Springer, Berlin, 1984), 33–62.

7. J. B. Conrey, D. W. Farmer and P. J. Wallace, Factoring Hecke polynomials modulo a prime, *Pacific J. Math.* **196**(1) (2000), 123–130.

8. L. Dieulefait and G. Wiese, On modular forms and the inverse Galois problem, arXiv:0905.1288v1 [math.NT]

9. L. J. P. Kilford, On mod p modular representations which are defined over $\mathbb{F}_p$, *Glas. Mat. Ser. III* **43**(63, Pt. 1) (2008), 1–6.

10. K. T-L. Koo, W. Stein and G. Wiese, On the generation of the coefficient field of a newform by a single Hecke eigenvalue, *J. Théor. Nombres Bordeaux*. **20**(2) (2008), 373–384.

11. E. Landau, in *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*. 2d ed. With an appendix by (Bateman P. T. Editor). (Chelsea Publishing Co., New York, 1953).

12. M. Rosen and J. H. Silverman, On the independence of Heegner points associated to distinct quadratic imaginary fields, *J. Number Theory* **127**(1) (2007), 10–36.

13. M. Schütt, CM newforms with rational coefficients. *Ramanujan J.* **19**(2) (2009), 187–205.

14. K. Soundararajan, The number of imaginary quadratic fields with a given class number, *Hardy-Ramanujan J.* **30** (2007), 13–18.

15. P. J. Weinberger, Exponents of the class groups of complex quadratic fields, *Acta Arith.* **22** (1973), 117–124.

16. G. Wiese, Dihedral Galois representations and Katz modular forms. *Doc. Math.* **9** (2004), 123–133.