
A COMPUTATIONAL STUDY OF THE ASYMPTOTIC BEHAVIOUR OF COEFFICIENT FIELDS OF MODULAR FORMS

by

Marcel Mohyla & Gabor Wiese

Abstract. — The article motivates, presents and describes large computer calculations concerning the asymptotic behaviour of arithmetic properties of coefficient fields of modular forms. The observations suggest certain patterns, which deserve further study.

Résumé. — Le but de cet article est de motiver, présenter et décrire de nombreux calculs menés sur ordinateur concernant le comportement asymptotique de propriétés arithmétiques des corps des coefficients de formes modulaires. Les observations suggèrent plusieurs questions qui méritent d'être étudiées ultérieurement.

1. Introduction

A recent breakthrough in Arithmetic Geometry is the proof of the Sato-Tate conjecture by Barnet-Lamb, Clozel, Geraghty, Harris, Shepherd-Barron and Taylor ([BLGHT], [CHT], [HSHT], [T]). It states that the normalised Hecke eigenvalues $\frac{a_p(f)}{2p^{(k-1)/2}}$ on a holomorphic newform f of weight $k \geq 2$ (and trivial Dirichlet character⁽¹⁾) are equidistributed with respect to a certain measure (the so-called Sato-Tate measure), when p runs through the set of prime numbers. The name *horizontal* Sato-Tate is sometimes used for this situation.

The reversed situation, to be referred to as *vertical* horizontal Sato-Tate, was successfully treated by Serre in [S]. He fixes a prime p and allows any sequence of positive integers (N_n, k_n) with even k_n and $p \nmid N_n$ such that $N_n + k_n$ tends to infinity and proves that $\frac{a_p(f)}{2p^{(k-1)/2}}$

2000 Mathematics Subject Classification. — 11F33 (primary); 11F11, 11Y40.

Key words and phrases. — Modular forms, coefficient fields, asymptotic behaviour, congruences, Hecke algebras.

G. W. would like to thank Gabriel Chênevert for inspiring discussions of variants of Sato-Tate. More thanks are due to Pierre Parent, Christophe Ritzenthaler, René Schoof and Mark Watkins for interesting discussions and suggestions. G. W. acknowledges partial support by the European Research Training Network *Galois Theory and Explicit Methods* MRTN-CT-2006-035495 and by the Sonderforschungsbereich Transregio 45 *Periods, moduli spaces and arithmetic of algebraic varieties* of the Deutsche Forschungsgemeinschaft.

⁽¹⁾We only make this assumption for the sake of simplicity of the exposition.

is equidistributed with respect to a certain measure depending on p (which is related to the Sato-Tate measure), when f runs through all the newforms in any of the spaces of cusp forms of level $\Gamma_0(N_n)$ and weight k_n . A corollary is that for fixed positive even weight k , the set

$$(1.1) \quad \{[\mathbb{Q}_f : \mathbb{Q}] \mid f \text{ newform of level } \Gamma_0(N_n) \text{ and weight } k\}$$

is unbounded for any sequence N_n tending to infinity. Here, \mathbb{Q}_f denotes the number field obtained from \mathbb{Q} by adjoining all Hecke eigenvalues on f .

In this article we perform a first computational study towards a (weak) arithmetic analogue of vertical Sato-Tate, where the name *arithmetic* refers to taking a finite place of \mathbb{Q} , as opposed to the infinite place used in usual Sato-Tate (the assertion of usual Sato-Tate concerns the Hecke eigenvalues as real numbers). An arithmetic analog of horizontal Sato-Tate is Chebotarev's density theorem. Consider, for example, a normalised cuspidal Hecke eigenform f with attached Galois representation $\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_\ell)$.⁽²⁾ Fix some $x \in \mathbb{Z}_\ell$ and let $n \in \mathbb{N}$. Let G be the image of the composite representation $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_f} \text{GL}_2(\mathbb{Z}_\ell) \twoheadrightarrow \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ and let $d(x)$ be the number of elements in G with trace equal to x modulo ℓ^n . Then the density of the set $\{p \mid |a_p - x|_\ell \leq \ell^{-n}\}$ is equal to $\frac{d(x)}{|G|}$ by Chebotarev's density theorem; hence, the situation is completely clear. Whereas at the infinite place horizontal Sato-Tate seems to be more difficult than vertical Sato-Tate, the situation appears to be reversed for arithmetic analogs. We are not going to propose such an analogue. But, we are going to study related questions by means of computer calculations. For instance, as a motivation let us consider the set

$$(1.2) \quad \{[\mathbb{F}_{\ell,f} : \mathbb{F}_\ell] \mid f \in S_k(N_n; \overline{\mathbb{F}}_\ell) \text{ normalised Hecke eigenform}\}$$

in analogy to Equation 1.1. Here, $S_k(N_n; \overline{\mathbb{F}}_\ell)$ denotes the $\overline{\mathbb{F}}_\ell$ -vector space of cuspidal modular forms over $\overline{\mathbb{F}}_\ell$ (see Section 2 for definitions) and $\mathbb{F}_{\ell,f}$ is defined by adjoining to \mathbb{F}_ℓ all Hecke eigenvalues on f . It is easy to construct sequences (N_n, k_n) for which the set in question is infinite (see e.g. [DiWi] and [W]), but it does not seem simple to obtain all natural numbers as degrees. Most importantly, it seems to be unknown whether this set is infinite when (N_n) is the sequence of prime numbers, $k = 2$ and $\ell > 2$.

Concerning properties of modular forms in positive characteristic, there is other, much more subtle information than just the degrees of $\mathbb{F}_{\ell,f}$ to be studied, e.g. congruences between modular forms. In order to take the full information into account, in this article we examine the properties of the \mathbb{F}_ℓ -Hecke algebras $\overline{\mathbb{T}}_k(N_n)$ on $S_k(N_n; \overline{\mathbb{F}}_\ell)$ asymptotically for fixed weight k (mostly 2) and running level N_n (mostly the set of prime numbers) by means of experimentation. More precisely, we investigate three quantities:

- (a) The deviation of $\overline{\mathbb{T}}_k(N_n)$ from being semisimple. In Section 3, we include a proposition relating nonsemisimplicity to congruences, ramification and certain indices. Our experiments suggest that for odd primes ℓ , the Hecke algebra $\overline{\mathbb{T}}_k(N_n)$ tends to be close to

⁽²⁾Again, it is only for simplicity of the exposition that we are taking \mathbb{Z}_ℓ instead of $\overline{\mathbb{Q}}_\ell$.

semisimple, whereas the situation seems to be completely different for $p = 2$ (see Section 4.1).

- (b) The average residue degree of $\overline{\mathbb{T}}_k(N_n)$. That is the arithmetic mean of the degrees of $\mathbb{F}_{\ell, f}$ for all f in $S_k(N_n; \overline{\mathbb{F}}_\ell)$. Our computations (see Section 4.2) strongly suggest that this quantity is unbounded. More precisely, we seem to observe a certain asymptotic behaviour, which we formulate as a question.
- (c) The maximum residue degree of $\overline{\mathbb{T}}_k(N_n)$. That is the maximum of the degrees of $\mathbb{F}_{\ell, f}$ for all f in $S_k(N_n; \overline{\mathbb{F}}_\ell)$. Our experiments suggest that this quantity is 'asymptotically' proportional to the dimension of $S_k(N_n; \overline{\mathbb{F}}_\ell)$.

In Section 4 we describe our computations and derive certain questions from our observations. However, we do not attempt to propose any heuristic explanations in this article. This will have to be the subject of subsequent studies, building on refined and extended computations. We see (b) and (c) as strong evidence for the infinity of the set in Equation 1.2, when N_n runs through the primes. Generally speaking, there appears to be some regularity in the otherwise quite erratic behaviour of the examined quantities, lending some support to the hope of finding a formulation of an arithmetic analogue of vertical Sato-Tate.

2. Background and notation

We start by introducing the necessary notation and explaining the background. For facts on modular forms, we refer to [DI]. Let us fix an integer k and a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$. Denote by $S_k(\Gamma)$ the complex vector space of holomorphic cusp forms of weight k for Γ . Define $\mathbb{T} := \mathbb{T}_k(\Gamma)$ to be the \mathbb{Z} -Hecke algebra of weight k for Γ , i.e. the subring of $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma))$ spanned by all Hecke operators T_n for $n \in \mathbb{N}$. If $\Gamma = \Gamma_0(N)$ we simply write $\mathbb{T}_k(N)$. We use similar notation in other contexts, too. It is an important theorem that \mathbb{T} is free of finite rank as a \mathbb{Z} -module, hence has Krull dimension one as a ring, and that the map

$$(2.3) \quad \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{C}) \rightarrow S_k(\Gamma), \quad \phi \mapsto \sum_{n=1}^{\infty} \phi(T_n)q^n$$

with $q = q(z) = e^{2\pi iz}$ defines an isomorphism of \mathbb{C} -vector spaces, which is compatible with the natural Hecke action. For any ring A , define $S_k(\Gamma; A) := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, A)$ equipped with the natural Hecke action (i.e. \mathbb{T} -action), so that we have $S_k(\Gamma) \cong S_k(\Gamma; \mathbb{C})$. We think of elements in $S_k(\Gamma; A)$ in terms of formal q -expansions, i.e. as formal power series in $A[[q]]$, by an analog of Eq. 2.3. Note that normalised Hecke eigenforms, i.e. those $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma; A)$ that satisfy $a_1 = 1$ and $T_n f = a_n f$, precisely correspond to ring homomorphisms $\phi : \mathbb{T} \rightarrow A$ with $\phi(T_n) = a_n$. When A is an integral domain, a normalised eigenfunction gives rise to a prime ideal \mathfrak{p} of \mathbb{T} , namely the kernel of ϕ . We may think of \mathbb{T}/\mathfrak{p} as the smallest subring of A generated by the a_n for $n \in \mathbb{N}$: the *coefficient ring of f in A* . Note that $\mathrm{Aut}(A)$ acts on $S_k(\Gamma; A)$ by composing $\phi : \mathbb{T} \rightarrow A$ with $\sigma \in \mathrm{Aut}(A)$. Obviously, this action does not change the ideal \mathfrak{p} corresponding to an eigenform.

We fix a prime number p . We put $\widehat{\mathbb{T}} := \widehat{\mathbb{T}}_k(\Gamma) := \mathbb{T}_k(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $\widehat{\mathbb{T}}_\eta := \mathbb{T}_k(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Q}_p = \widehat{\mathbb{T}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $\overline{\mathbb{T}} := \overline{\mathbb{T}}_k(\Gamma) := \mathbb{T}_k(\Gamma) \otimes_{\mathbb{Z}} \mathbb{F}_p = \widehat{\mathbb{T}} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$. Note the isomorphisms $S_k(\Gamma; \overline{\mathbb{Z}}_p) \cong \text{Hom}_{\mathbb{Z}_p}(\widehat{\mathbb{T}}, \overline{\mathbb{Z}}_p)$, $S_k(\Gamma; \overline{\mathbb{Q}}_p) \cong \text{Hom}_{\mathbb{Z}_p}(\widehat{\mathbb{T}}, \overline{\mathbb{Q}}_p)$ and $S_k(\Gamma; \overline{\mathbb{F}}_p) \cong \text{Hom}_{\mathbb{Z}_p}(\widehat{\mathbb{T}}, \overline{\mathbb{F}}_p) \cong \text{Hom}_{\mathbb{F}_p}(\overline{\mathbb{T}}, \overline{\mathbb{F}}_p)$.

The $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ -conjugacy classes of normalised eigenforms in $S_k(\Gamma; \overline{\mathbb{Q}}_p)$ (by which we mean the classes for the $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ -action described above) are in bijection with the prime (and automatically maximal) ideals of $\widehat{\mathbb{T}}_\eta$ and also in bijection with the minimal prime ideals of $\widehat{\mathbb{T}}$, whose set is denoted by $\text{MinSpec}(\widehat{\mathbb{T}})$. The second bijection is explicitly given by taking preimages for the injection $\widehat{\mathbb{T}} \hookrightarrow \widehat{\mathbb{T}}_\eta$. Note that $\widehat{\mathbb{T}}$ has Krull dimension one, meaning that any prime ideal is either minimal (i.e. not containing any smaller prime ideal) or maximal. Moreover, the $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ -conjugacy classes of normalised eigenforms in $S_k(\Gamma; \overline{\mathbb{F}}_p)$ are in bijection with $\text{Spec}(\overline{\mathbb{T}}) = \text{MaxSpec}(\overline{\mathbb{T}})$. Furthermore, $\text{Spec}(\overline{\mathbb{T}})$ is in natural bijection with $\text{MaxSpec}(\widehat{\mathbb{T}})$ under taking preimages for the natural projection $\widehat{\mathbb{T}} \rightarrow \overline{\mathbb{T}}$. By a result in commutative algebra, we have direct product decompositions

$$\widehat{\mathbb{T}} = \prod_{\mathfrak{m} \in \text{MaxSpec}(\widehat{\mathbb{T}})} \widehat{\mathbb{T}}_{\mathfrak{m}}, \quad \overline{\mathbb{T}} = \prod_{\mathfrak{m} \in \text{MaxSpec}(\widehat{\mathbb{T}})} \overline{\mathbb{T}}_{\mathfrak{m}} \quad \text{and} \quad \widehat{\mathbb{T}}_\eta = \prod_{\mathfrak{p} \in \text{Spec}(\widehat{\mathbb{T}}_\eta)} \widehat{\mathbb{T}}_{\eta, \mathfrak{p}},$$

where the factors are the localisations at the prime ideals indicated by the subscripts.

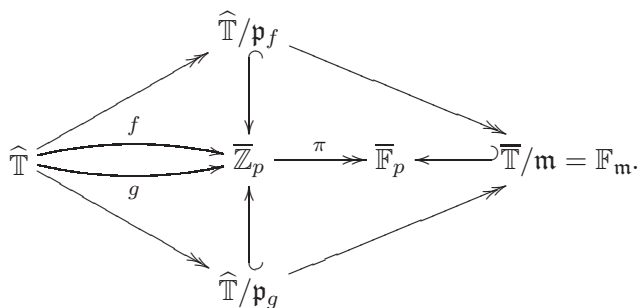
Definition 2.1. — We say that two $\mathfrak{p}_1, \mathfrak{p}_2 \in \text{MinSpec}(\widehat{\mathbb{T}})$ are *congruent* if they lie in the same maximal ideal $\mathfrak{m} \in \text{MaxSpec}(\widehat{\mathbb{T}})$. For $\mathfrak{p} \in \text{MinSpec}(\widehat{\mathbb{T}})$, we call $\widehat{\mathbb{T}}/\mathfrak{p}$ the *local coefficient ring* and $L_{\mathfrak{p}} := \text{Frac}(\widehat{\mathbb{T}}/\mathfrak{p})$ the *local coefficient field*. We say that $\mathfrak{p} \in \text{MinSpec}(\widehat{\mathbb{T}})$ is *ramified* if $L_{\mathfrak{p}}$ is a ramified extension of \mathbb{Q}_p . We denote by $i_{\mathfrak{p}}$ the index of $\widehat{\mathbb{T}}/\mathfrak{p}$ in the ring of integers of $L_{\mathfrak{p}}$. The residue field $\widehat{\mathbb{T}}/\mathfrak{m} \cong \overline{\mathbb{T}}/\mathfrak{m}$ will be denoted by $\mathbb{F}_{\mathfrak{m}}$ and will be called the *residual coefficient field*.

We now establish the connection with the usual understanding of the terms in the definition. Let $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ be the algebraic integers and the algebraic numbers, respectively. As \mathbb{T} is of finite \mathbb{Z} -rank, the set of normalised eigenforms in $S_k(\Gamma)$ is the same as the set of normalised eigenforms in $S_k(\Gamma; \overline{\mathbb{Z}})$. Fix homomorphisms

$$\begin{array}{ccc} \overline{\mathbb{Z}} \xrightarrow{\iota} \overline{\mathbb{Z}}_p & \text{giving rise to} & S_k(\Gamma; \overline{\mathbb{Z}}) \xrightarrow{\iota} S_k(\Gamma; \overline{\mathbb{Z}}_p) \\ \searrow \pi & & \searrow \pi \\ & & \mathbb{F}_p \qquad \qquad \qquad S_k(\Gamma; \overline{\mathbb{F}}_p) \end{array}$$

From this perspective, a holomorphic normalised Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma)$ gives rise to an eigenform in $S_k(\Gamma; \overline{\mathbb{F}}_p)$, called the *reduction of f modulo p* , whose formal q -expansion is $\pi(f) := \sum_{n=1}^{\infty} \pi(a_n) q^n \in \overline{\mathbb{F}}_p[[q]]$. The reduction corresponds to $\mathfrak{m} \in \text{MaxSpec}(\widehat{\mathbb{T}})$ and to $\mathfrak{m} \in \text{Spec}(\overline{\mathbb{T}})$ (we use the same symbol due to the natural bijection between the two sets). The form f also gives rise to an eigenform in $S_k(\Gamma; \overline{\mathbb{Q}}_p)$, which corresponds to $\mathfrak{p}_f \in \text{MinSpec}(\widehat{\mathbb{T}})$ and to $\mathfrak{p}_f \in \text{Spec}(\widehat{\mathbb{T}}_\eta)$ (the same symbol is used again due to the natural bijection explained above).

Let $g = \sum_{n=1}^{\infty} b_n q^n$ be another holomorphic normalised Hecke eigenform. If $\pi(f) = \pi(g)$, then clearly $\mathfrak{p}_f \subset \mathfrak{m}$ and $\mathfrak{p}_g \subset \mathfrak{m}$, i.e. \mathfrak{p}_f and \mathfrak{p}_g are congruent. Conversely, let $\mathfrak{p}_f, \mathfrak{p}_g \in \text{MinSpec}(\widehat{\mathbb{T}})$ such that $\mathfrak{p}_f \subset \mathfrak{m}$ and $\mathfrak{p}_g \subset \mathfrak{m}$ for some $\mathfrak{m} \in \text{MaxSpec}(\widehat{\mathbb{T}})$, so that \mathfrak{p}_f and \mathfrak{p}_g are congruent. The ideals \mathfrak{p}_f and \mathfrak{p}_g correspond to $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ -conjugacy classes in $S_k(\Gamma; \overline{\mathbb{Q}_p})$ and we can choose $f, g \in S_k(\Gamma; \overline{\mathbb{Z}_p})$ corresponding to \mathfrak{p}_f and \mathfrak{p}_g with $\pi(f) = \pi(g)$. We illustrate the situation by the diagram



Note that f, g can already be found in $S_k(\Gamma; \overline{\mathbb{Z}}) \subset S_k(\Gamma)$. This justifies our usage of the term *congruence*.

Moreover, the local coefficient ring $\widehat{\mathbb{T}}/\mathfrak{p}$ can be identified with $\mathbb{Z}_{p,f} := \mathbb{Z}_p[\iota(a_n) | n \in \mathbb{N}]$ and its fraction field $L_{\mathfrak{p}}$ with $\mathbb{Q}_{p,f} := \mathbb{Q}_p(\iota(a_n) | n \in \mathbb{N})$, whence $i_{\mathfrak{p}}$ is the index of $\mathbb{Z}_{p,f}$ in its normalisation. Furthermore, the residual coefficient field, i.e. $\mathbb{F}_{\mathfrak{m}} = \overline{\mathbb{T}}/\mathfrak{m}$, can be interpreted as $\mathbb{F}_p[\pi(a_n) | n \in \mathbb{N}]$. The relation to the arithmetic of the coefficient field $\mathbb{Q}_f := \mathbb{Q}(a_n | n \in \mathbb{N})$ and the coefficient ring $\mathbb{Z}_f := \mathbb{Z}[a_n | n \in \mathbb{N}]$ is apparent.

In order to conclude this background section, we point out that in the case $k = 2$, the coefficient ring \mathbb{Z}_f is the endomorphism ring of the abelian variety A_f attached to f . From that point of view, the following analysis can also be interpreted as a study of the arithmetic of the endomorphism algebras of GL_2 -abelian varieties.

3. Semisimplicity of Hecke algebras

We recall that a finite dimensional commutative K -algebra, where K is a field, is *semisimple* if and only if it is isomorphic to a direct product of fields (which are necessarily finite field extensions of K).

In this section we first study the semisimplicity of the Hecke algebra $\widehat{\mathbb{T}}_{\eta}$. In the case when it is semisimple, we relate the non-semisimplicity of the mod p Hecke algebra $\overline{\mathbb{T}}$ to three phenomena: congruences between $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ -conjugacy classes of newforms, ramification at p of the coefficient fields of newforms and the p -index of the local coefficient ring in the ring of integers of the local coefficient field.

Let $f = \sum_{n=1}^{\infty} a_n(f)q^n \in S_k(\Gamma_1(M))^{\text{new}}$ be a normalised Hecke eigenform and let m be any positive integer. We define the \mathbb{C} -vector space $V_f(m)$ to be the span of $\{f(q^d) \mid d \mid m\}$, where

d runs through all positive divisors of m (including 1 and m). Newform theory states that

$$S_k(\Gamma_1(N)) \cong \bigoplus_{m|N} \bigoplus_{f \in S_k(\Gamma_1(N/m))^{\text{new}}} V_f(m).$$

This is an isomorphism of Hecke modules. The Hecke operators T_n for $(n, m) = 1$ restricted to $V_f(m)$ are scalar matrices with $a_n(f)$ as diagonal entries. We now describe the Hecke operator T_ℓ on $V_f(m)$ for a prime ℓ . Suppose that $\ell^r \parallel m$. Let ϵ be the Dirichlet character of f . Consider the $(r+1) \times (r+1)$ -matrix

$$A := A_f(m, \ell) := \begin{pmatrix} a_\ell(f) & 1 & 0 & 0 & \dots & 0 \\ -\delta\epsilon(\ell)\ell^{k-1} & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 1 \\ 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix},$$

where $\delta = 0$ if $\ell \mid (N/m)$ and $\delta = 1$ otherwise. The Hecke operator T_ℓ is then given on $V_f(m)$ (for a certain natural basis) by a diagonal block matrix having only blocks equal to A on the diagonal, where each block on the diagonal corresponds to a divisor of m/ℓ^r . Let \mathbb{T} be the Hecke algebra of $S_k(\Gamma_1(N))$ (as in Section 2). The algebra $\mathbb{T}_\mathbb{Q} := \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ is semisimple if and only if $\mathbb{T}_\mathbb{C} := \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C}$ is semisimple (if and only if $\widehat{\mathbb{T}}_\eta$ is semisimple). By the above discussion, $\mathbb{T}_\mathbb{C}$ is semisimple if and only if all the matrices $A_f(m, \ell)$ that appear are diagonalisable.

Proposition 3.1. — *Assume the notation above, $M = N/m$ and $k \geq 2$. Moreover, if $k \geq 3$ assume Tate's conjecture (see [CE], Section 1).*

- (a) *Assume $\ell \nmid M$. Then $A_f(m, \ell)$ is diagonalisable if and only if $r \leq 2$.*
- (b) *Assume that $\ell \mid M$ and that either $\ell \parallel M$ or that ϵ cannot be defined mod M/ℓ . Then $A_f(m, \ell)$ is diagonalisable if and only if $r \leq 1$.*
- (c) *Assume that $\ell^2 \mid M$ and that ϵ can be defined modulo M/ℓ . Then $A_f(m, \ell)$ is diagonalisable if and only if $r = 0$.*

Proof. — (a) Assume $r \geq 1$ (otherwise the result is trivial) and call B the top left 2×2 -block of $A = A_f(m, \ell)$. The characteristic polynomial of B is $g(X) = X^2 - a_\ell(f)X + \epsilon(\ell)\ell^{k-1}$. We have $g(0) \neq 0$ and $g(X)$ has discriminant $a_\ell(f)^2 - 4\epsilon(\ell)\ell^{k-1}$, which is non-zero, since $|a_\ell(f)| = 2|\ell|^{(k-1)/2}$ would contradict [CE], Theorem 4.1. Consequently, A is diagonalisable if and only if apart from B there is at most one more row and column.

In cases (b) and (c), note that A is in Jordan form. The result is now immediate, since $a_\ell(f)$ is non-zero for (b) and zero for (c) (see [DS], 1.8). \square

We have the immediate corollary (which is Theorem 4.2 in [CE]).

Corollary 3.2. — *Let N be cubefree and $k \geq 2$. If $k \geq 3$ assume Tate's conjecture (see [CE], Section 1). Then the Hecke algebras $\mathbb{T}_k(\Gamma_1(N)) \otimes \mathbb{Q}$ and $\widehat{\mathbb{T}}_k(\Gamma_1(N))_\eta$ as well as $\mathbb{T}_k(N) \otimes \mathbb{Q}$ and $\widehat{\mathbb{T}}_k(N)_\eta$ are semisimple.*

The principal result of this section is the following proposition on the structure of the residual Hecke algebra. We assume the notation laid out in Section 2, in particular, we work with a general congruence subgroup Γ .

Proposition 3.3. — *Assume that $\widehat{\mathbb{T}}_\eta$ is semisimple (see, e.g., Corollary 3.2), i.e.*

$$\widehat{\mathbb{T}}_\eta \cong \prod_{\mathfrak{p} \in \text{MinSpec}(\widehat{\mathbb{T}})} L_{\mathfrak{p}}.$$

Then the residual Hecke algebra $\overline{\mathbb{T}}$ is semisimple if and only if all of the following three conditions are satisfied:

- (i) *No two $\mathfrak{p}_1, \mathfrak{p}_2 \in \text{MinSpec}(\widehat{\mathbb{T}})$ are congruent.*
- (ii) *None of the $\mathfrak{p} \in \text{MinSpec}(\widehat{\mathbb{T}})$ is ramified.*
- (iii) *For all $\mathfrak{p} \in \text{MinSpec}(\widehat{\mathbb{T}})$, the index $i_{\mathfrak{p}} = 1$.*

Proof. — We first prove that (i), (ii) and (iii) imply the semisimplicity of $\overline{\mathbb{T}}$.

The fact that there is no congruence means that in every $\mathfrak{m} \in \text{MaxSpec}(\widehat{\mathbb{T}})$ there is a unique $\mathfrak{p} \in \text{MinSpec}(\widehat{\mathbb{T}}_{\mathfrak{m}})$. As $\widehat{\mathbb{T}}_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong L_{\mathfrak{p}}$, it follows that $\widehat{\mathbb{T}}_{\mathfrak{m}}$ is a subring of $L_{\mathfrak{p}}$. Due to (iii), $\widehat{\mathbb{T}}_{\mathfrak{m}}$ is the ring of integers of $L_{\mathfrak{p}}$. Since by (ii) $L_{\mathfrak{p}}$ is unramified, we get that $\overline{\mathbb{T}}_{\mathfrak{m}}$ is the residue field of the integers of $L_{\mathfrak{p}}$. This shows that $\overline{\mathbb{T}}$ is a product of finite fields, i.e. semisimple.

Now we prove the converse direction and assume that $\overline{\mathbb{T}}$ is semisimple. Let $\mathfrak{m} \in \text{MaxSpec}(\widehat{\mathbb{T}})$. Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m \in \text{MinSpec}(\widehat{\mathbb{T}})$ be the distinct minimal primes contained in \mathfrak{m} . Then $\widehat{\mathbb{T}}_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong L_{\mathfrak{p}_1} \times \dots \times L_{\mathfrak{p}_m}$. Due to the non-degeneration $\overline{\mathbb{T}}_{\mathfrak{m}} \cong \widehat{\mathbb{T}}_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} \mathbb{F}_p \cong \mathbb{F}_{p^n}$ for some n . Since $\dim_{\mathbb{Q}_p} \widehat{\mathbb{T}}_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = n$, we have $[L_{\mathfrak{p}_i} : \mathbb{Q}_p] \leq n$ for $i = 1, \dots, m$.

Let \mathcal{O}_i be the ring of integers of $L_{\mathfrak{p}_i}$ for $i = 1, \dots, m$. It contains $\widehat{\mathbb{T}}_{\mathfrak{m}}/\mathfrak{p}_i$ with index $i_{\mathfrak{p}_i}$. Tensoring the exact sequence of \mathbb{Z}_p -modules

$$0 \rightarrow \widehat{\mathbb{T}}_{\mathfrak{m}}/\mathfrak{p}_i \rightarrow \mathcal{O}_i \rightarrow \mathcal{O}_i/(\widehat{\mathbb{T}}_{\mathfrak{m}}/\mathfrak{p}_i) \rightarrow 0$$

with \mathbb{F}_p over \mathbb{Z}_p we obtain the exact sequence of \mathbb{F}_p -vector spaces:

$$\mathbb{F}_{p^n} \rightarrow \mathcal{O}_i \otimes_{\mathbb{Z}_p} \mathbb{F}_p \rightarrow (\mathcal{O}_i/(\widehat{\mathbb{T}}_{\mathfrak{m}}/\mathfrak{p}_i)) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \rightarrow 0.$$

Since the map on the left is a ring homomorphism, it is injective. Now $\dim_{\mathbb{F}_p} \mathcal{O}_i \otimes_{\mathbb{Z}_p} \mathbb{F}_p \leq n$ implies that \mathcal{O}_i is unramified and that $i_{\mathfrak{p}_i} = 1$. Thus $[L_{\mathfrak{p}_i} : \mathbb{Q}_p] = n$ for $i = 1, \dots, m$ and, hence, $m = 1$, concluding the proof. \square

4. Observations and Questions

In this section, we explain and expose our computer experiments and we ask some questions suggested by our studies. All computer calculations were performed using MAGMA (see [BCP]).

4.1. Semisimplicity of the residual Hecke algebra. — A local finite-dimensional commutative \mathbb{F}_p -algebra A is semisimple if and only if it is simple, which is equivalent to A being field. We take the dimension of the maximal ideal \mathfrak{m} of A as a measure for the deviation of A from being semisimple. In particular, A is a field if and only if \mathfrak{m} has dimension 0.

For given prime p , level N and weight k we study the *sum of the residue degrees* of all prime ideals:

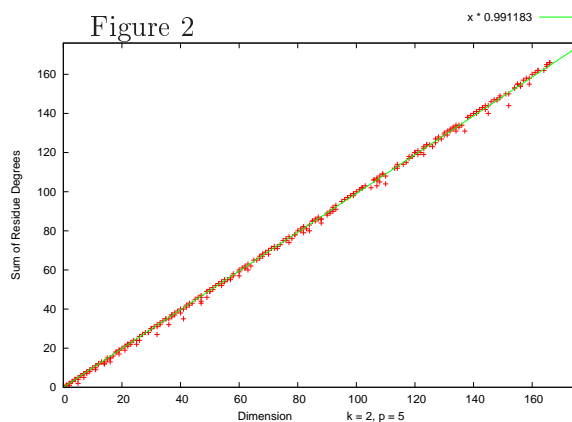
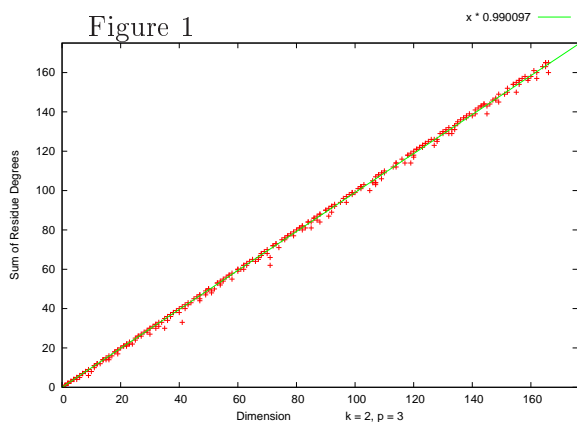
$$a_{N,k}^{(p)} = \sum_{\mathfrak{m} \in \text{Spec}(\overline{\mathbb{T}}_k(N))} [\mathbb{F}_{\mathfrak{m}} : \mathbb{F}_p].$$

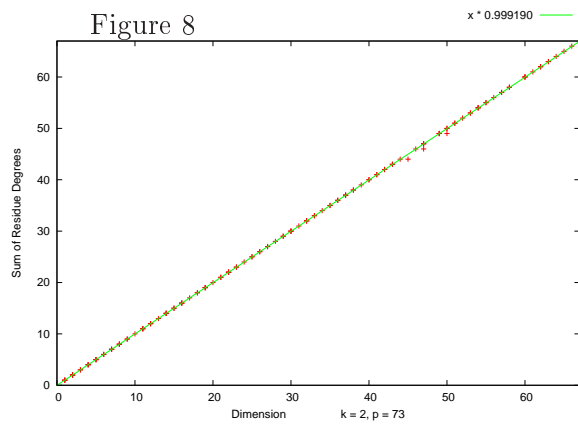
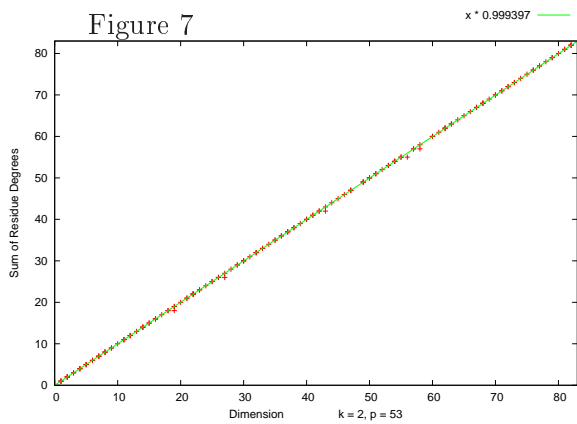
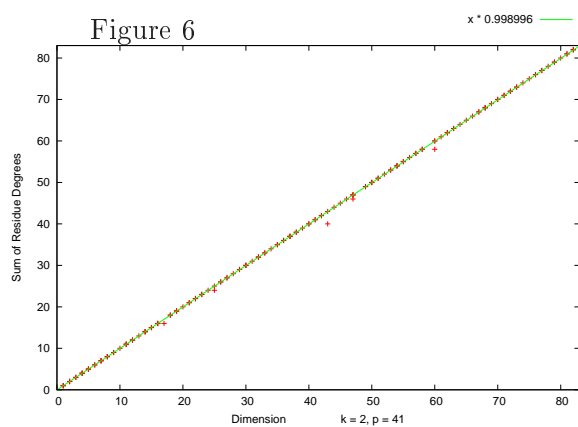
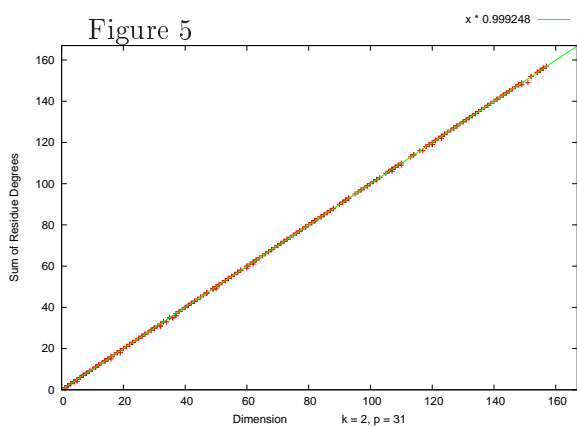
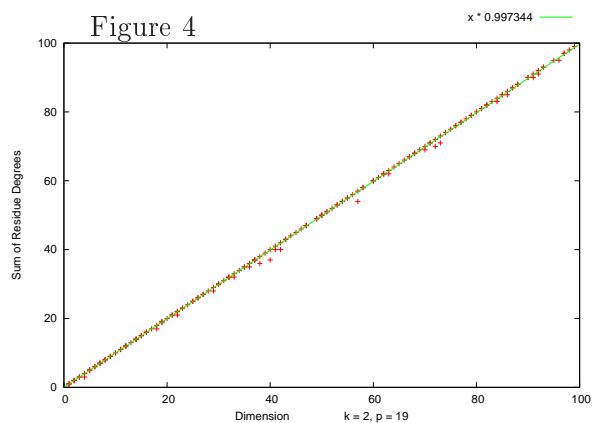
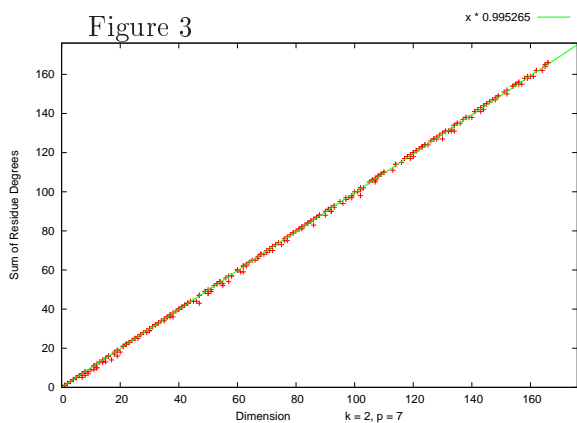
Clearly, $a_{N,k}^{(p)}$ is less than or equal to the $\overline{\mathbb{F}}_p$ -dimension of $S_k(N; \overline{\mathbb{F}}_p)$. Hence, $\overline{\mathbb{T}}_k(N)$ is semisimple if and only if $a_{N,k}^{(p)}$ is equal to this dimension.

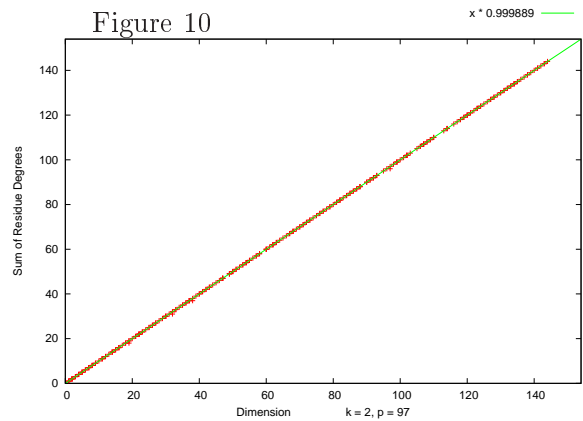
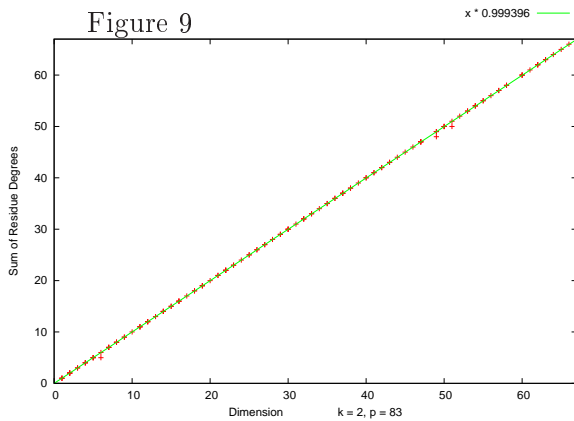
We intend to study the asymptotic behaviour of the function $a_{N,k}^{(p)}$ for a fixed prime p and fixed weight k as a function of the level N . For simplicity, we let N run through the prime numbers only in order to avoid contributions from lower levels via the degeneracy maps. We should point out that there can be contributions from lower weights: an eigenform in $S_k(N; \overline{\mathbb{F}}_p)$ also lives in $S_{k+n(p-1)}(N; \overline{\mathbb{F}}_p)$ for all $n \geq 0$ by multiplication by the Hasse invariant. Note that for $p > 2$ and $k = 2$, as well as for $p > 3$ and $k = 4$ there is no such contribution.

Our computational findings are best illustrated by plotting graphs. In each of the following plots, the prime p and the weight k are fixed and on the x -axis we plot $d(N) := \dim_{\overline{\mathbb{F}}_p} S_k(N; \overline{\mathbb{F}}_p)$ and on the y -axis the function $a_{N,k}^{(p)}$ as a function of N , i.e. each N gives rise to a dot at the appropriate place. The straight line in the graphs was determined as the linear function $\alpha \cdot d(N)$ which best fits the data (according to gnuplot and the least squares method).

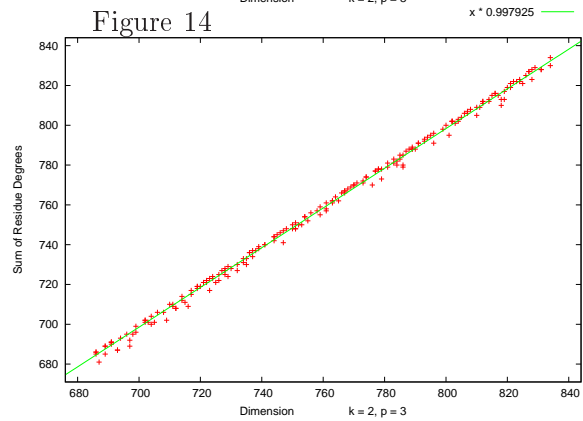
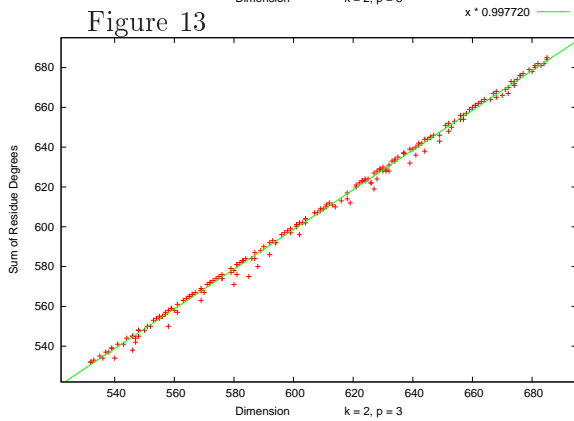
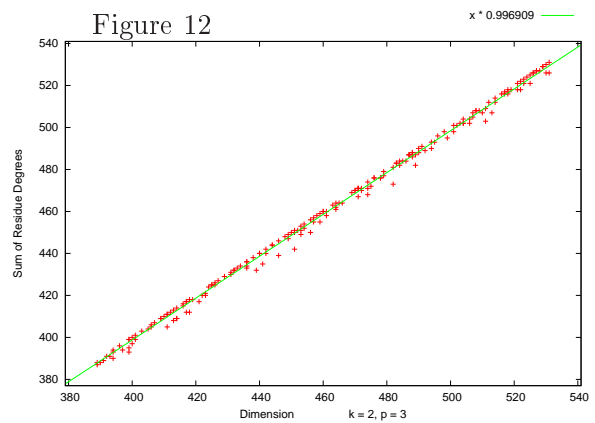
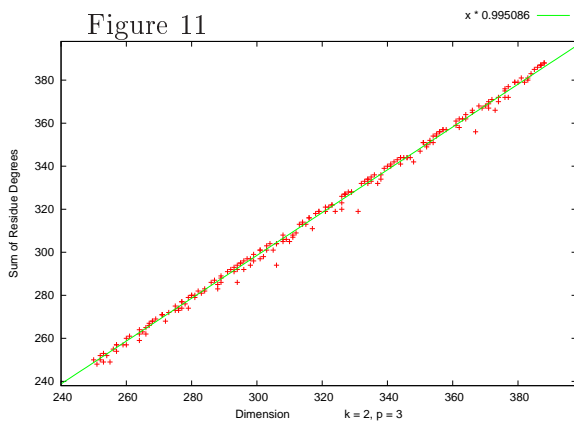
In the weights that we considered we observed a behaviour for $p = 2$ which seems to be completely different from the behaviour at all other primes. We made plots for all odd primes less than 100 and weight 2 and present a selection here. The graphs that we leave out look very similar.

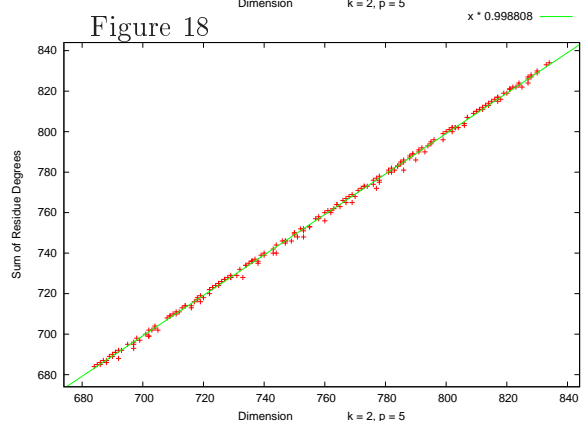
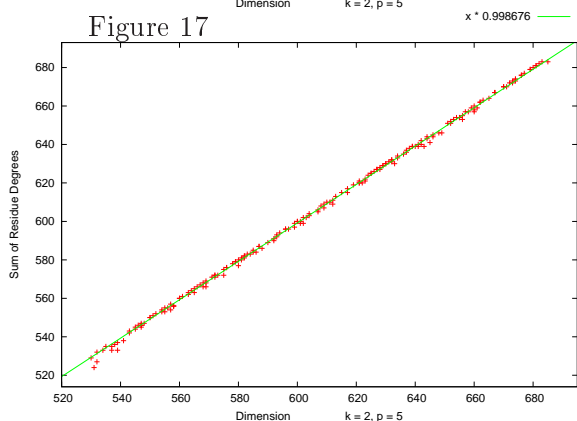
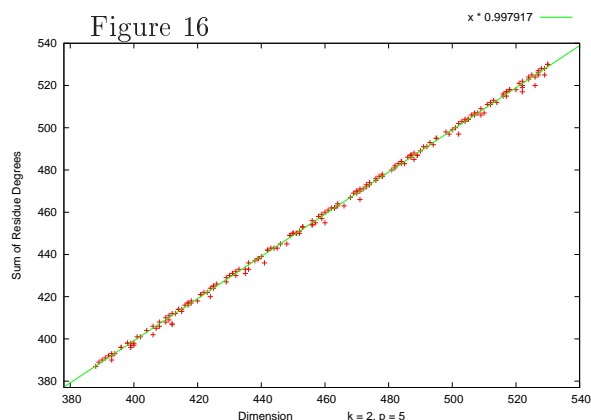
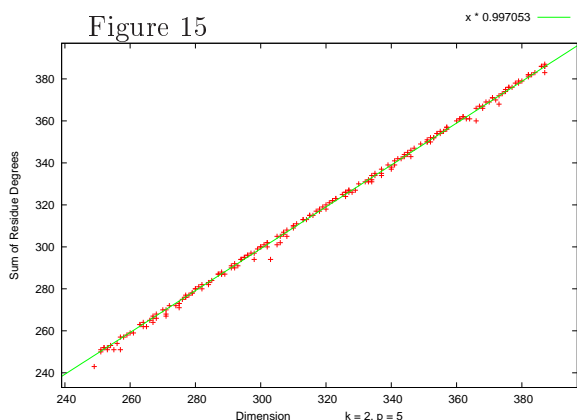




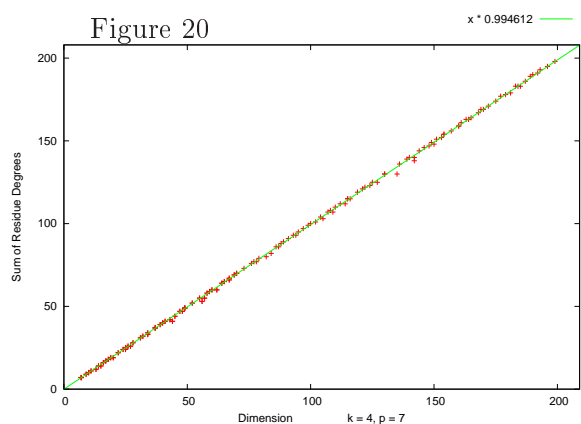
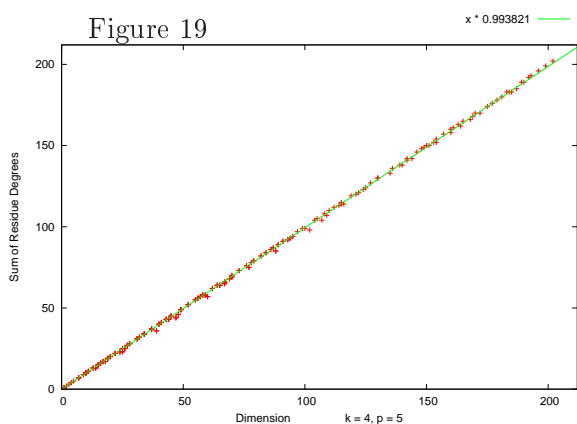


In Figures 1–10 the levels range over all primes up to a certain bound (which is not the same for all p). We observe that non-semisimplicity seems to be a rather rare phenomenon which becomes rarer for growing p , as one might have guessed. In the next figures, we analyse the cases $p = 3, 5$ still for weight 2 more closely by letting the levels range through all primes between 3000 and 10009 subdivided into four consecutive intervals.





One can observe that the slope of the best fitting line through the origin seems to be increasing with growing dimension. Although we only computed relatively little data, we include two examples for weight 4. They do not suggest any significant difference to the weight 2 case.



We are led to ask the following question.

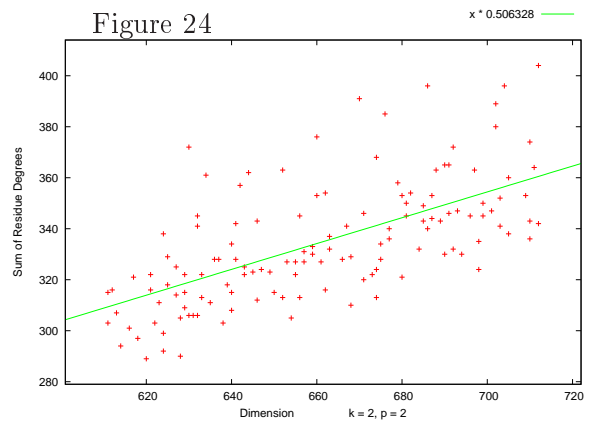
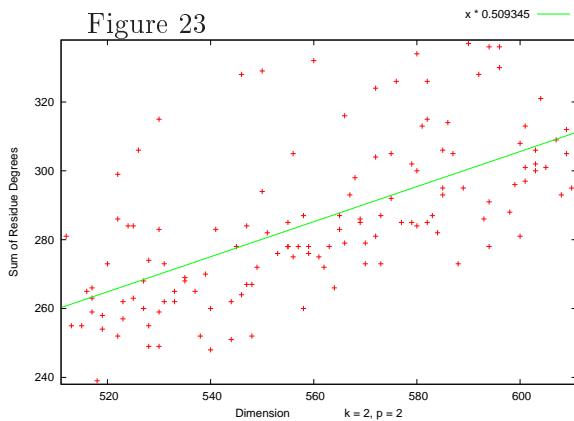
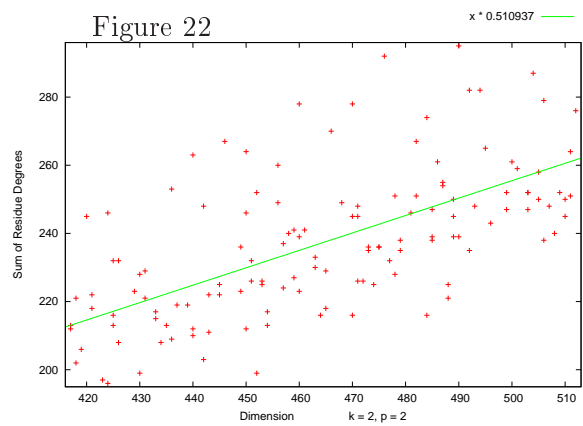
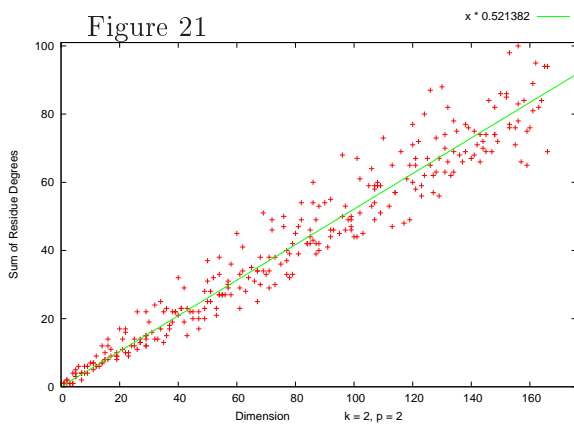
Question 4.1. — Fix an odd prime p and an even $k \geq 2$. Let $a(N) := a_{k,N}^{(p)}$ and $d(N) := \dim_{\overline{\mathbb{F}}_p} S_k(N; \overline{\mathbb{F}}_p)$. Does the following statement hold?

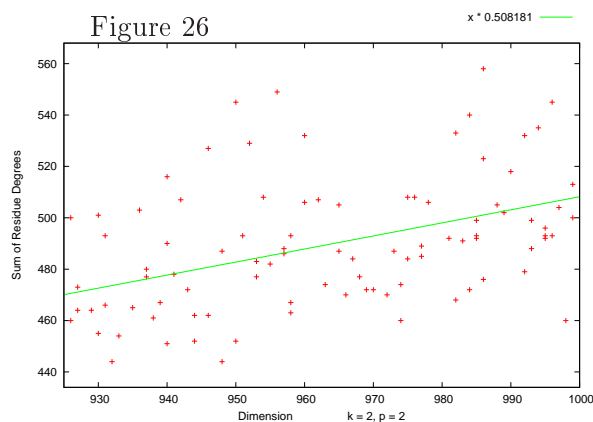
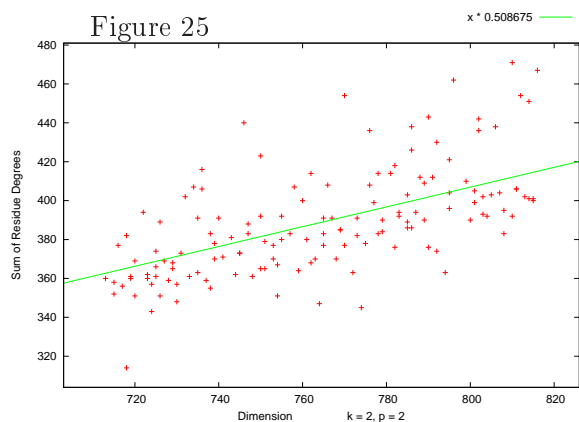
For all $\epsilon > 0$ there is $C_\epsilon > 0$ such that for all primes N the inequality

$$a(N) > (1 - \epsilon)d(N) - C_\epsilon$$

holds.

We contrast the situation, which seems very similar for every odd prime, with the one for $p = 2$ and $k = 2$. We do not consider any higher weights due to the contributions from weight 2, which would ‘disturb’ the situation. The following plots take prime numbers N into account that lie in six different intervals up to 12000.





In spite of the very irregular behaviour, it is remarkable that the slope of the best fitting line through the origin is always just a little bigger than $\frac{1}{2}$.

At the moment we cannot fully explain this behaviour. Contributions from weight one play some role. However, probably more important are congruences of forms having Atkin-Lehner eigenvalue $+1$ with forms having eigenvalue -1 . As Johan Bosman observes in a remark in [B], it follows from the connectedness of the spectrum of the Hecke algebra ([M], 10.6) for $k = 2$ and prime levels that there is always at least one such congruence for $p = 2$, whenever the $+1$ - and the -1 -eigenspace are nonempty.

We are led to ask the following question.

Question 4.2. — Fix an even weight $k \geq 2$. Let $a(N) := a_{k,N}^{(2)}$ and $d(N) := \dim_{\mathbb{F}_2} S_k(N; \overline{\mathbb{F}}_2)$. Are there $1 > \alpha \geq \beta > 0$ and constants $C, D > 0$ such that the inequality

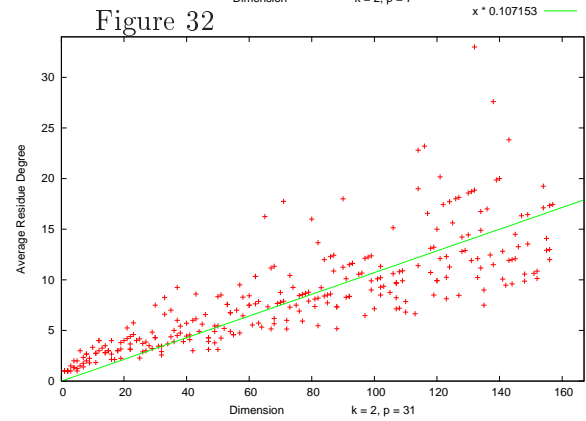
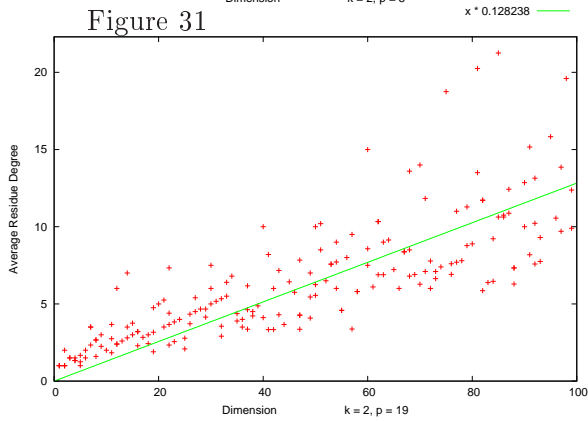
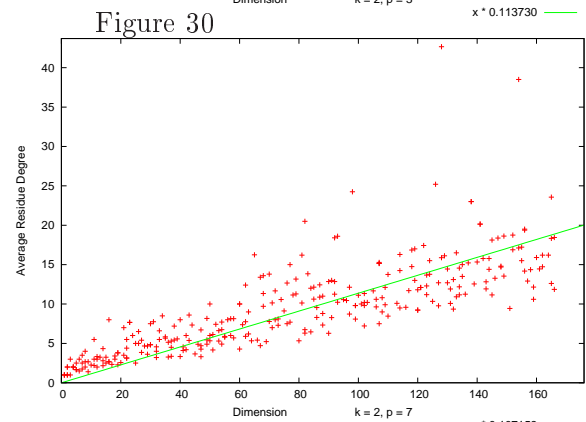
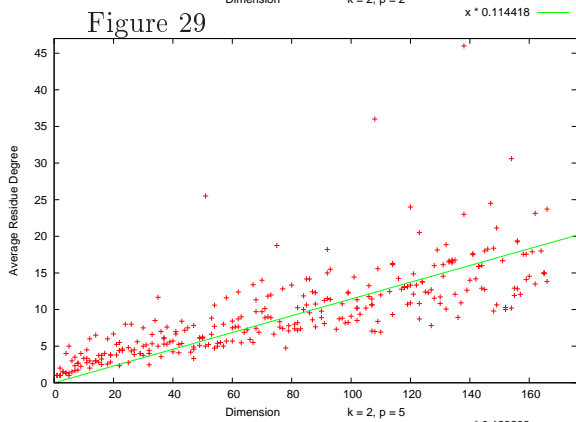
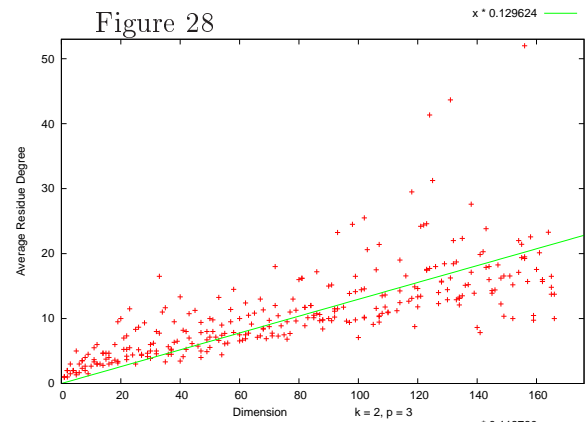
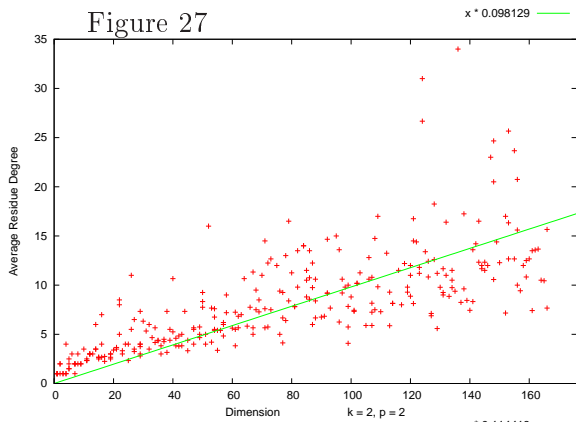
$$\alpha \cdot d(N) + C > a(N) > \beta \cdot d(N) - D$$

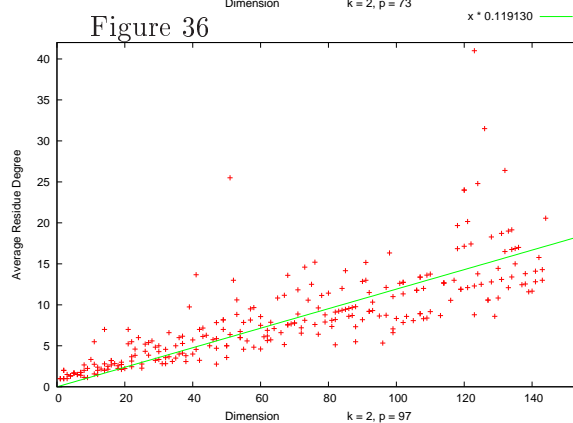
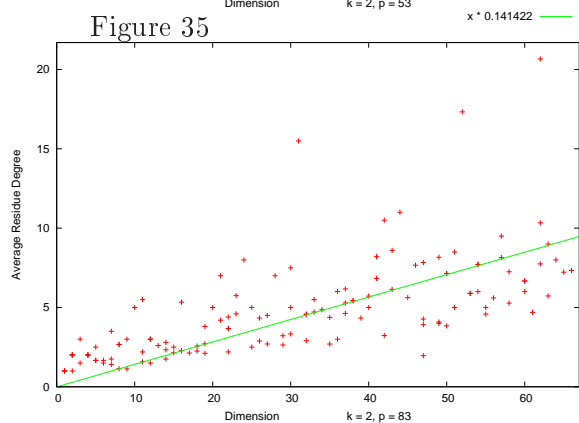
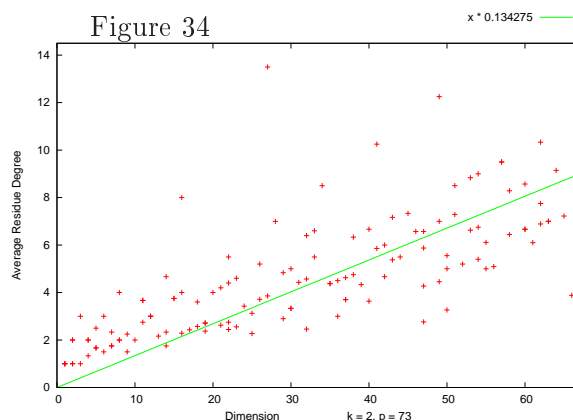
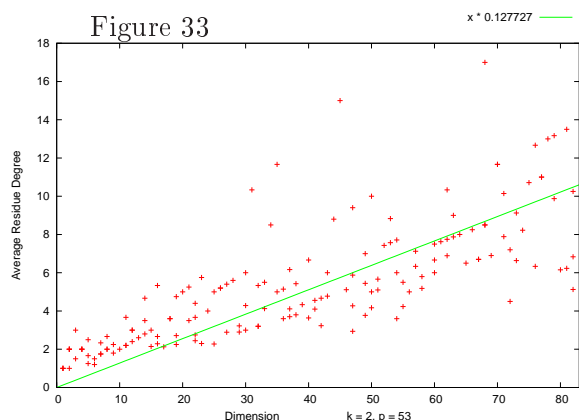
holds?

4.2. Average Residue Degree. — We now study the *average residue degree*, which we define for given level N , weight k and prime p as

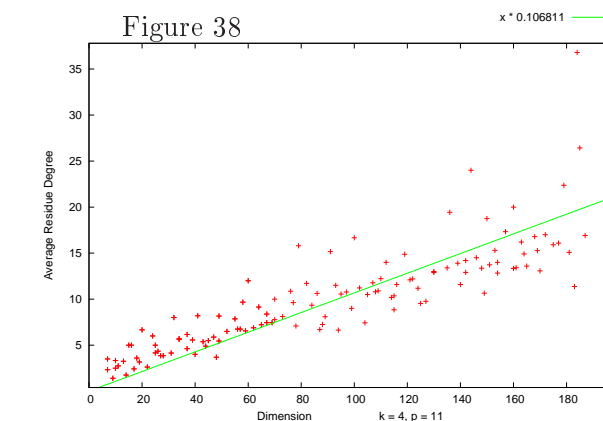
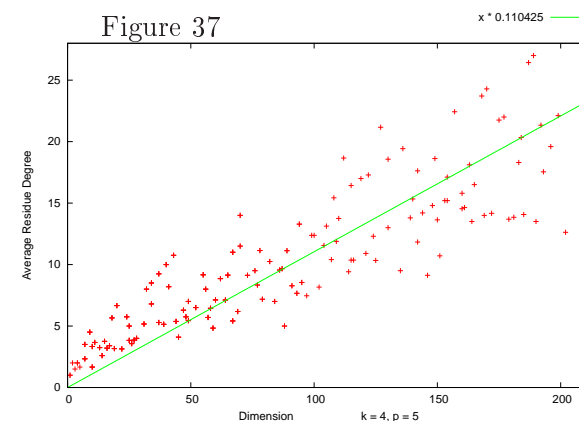
$$b_{N,k}^{(p)} = \frac{1}{\#\text{Spec}(\overline{\mathbb{T}}_k(N))} \sum_{\mathfrak{m} \in \text{Spec}(\overline{\mathbb{T}}_k(N))} [\mathbb{F}_{\mathfrak{m}} : \mathbb{F}_p] = \frac{a_{N,k}^{(p)}}{\#\text{Spec}(\overline{\mathbb{T}}_k(N))}.$$

We made computations for weight 2 and all primes p less than 100, where N runs through the same ranges as previously. We again plot the dimension $d(N)$ on the x -axis and the function $b_{N,k}^{(p)}$ on the y -axis and the straight line is again the best fitting function $\alpha \cdot d(N)$, although we believe that this is not the right function to take (see below). We again present a selection of prime numbers as before, however, including $p = 2$ from the beginning. The graphs that we leave out have very similar shapes.

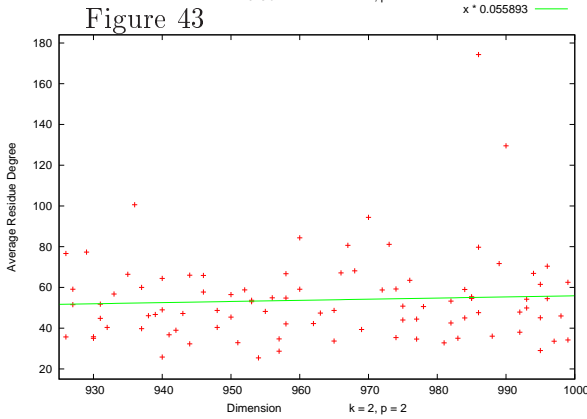
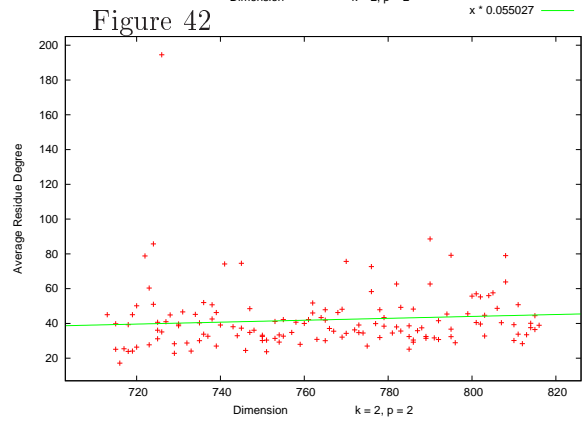
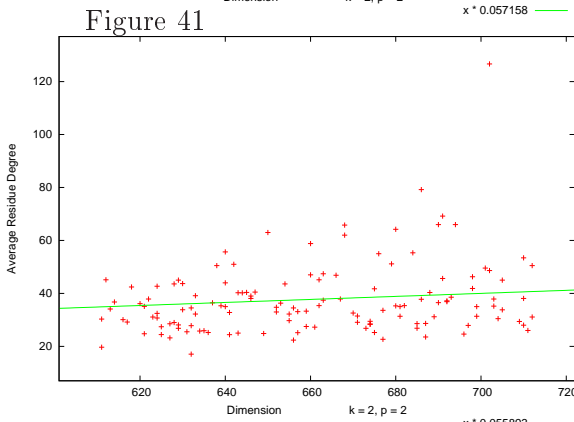
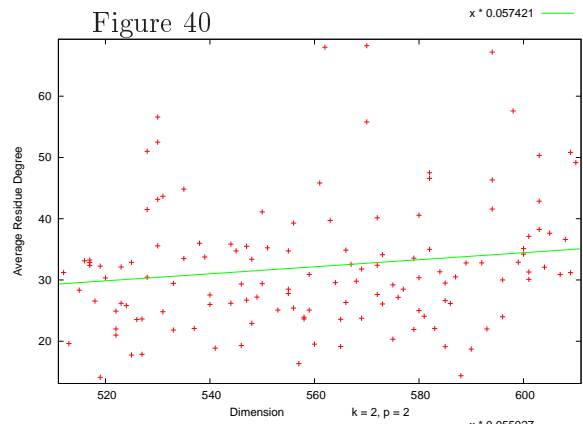
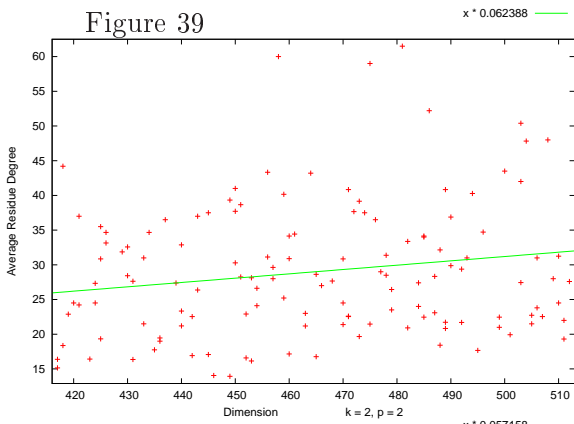




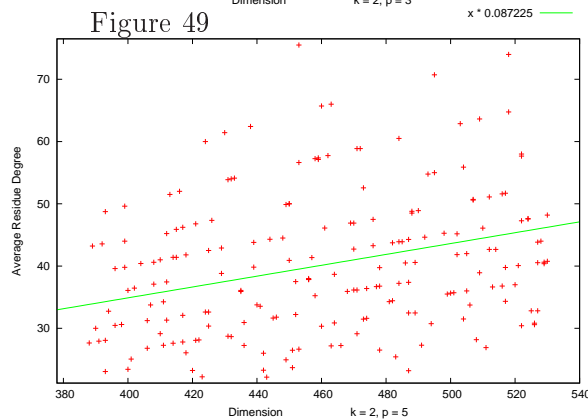
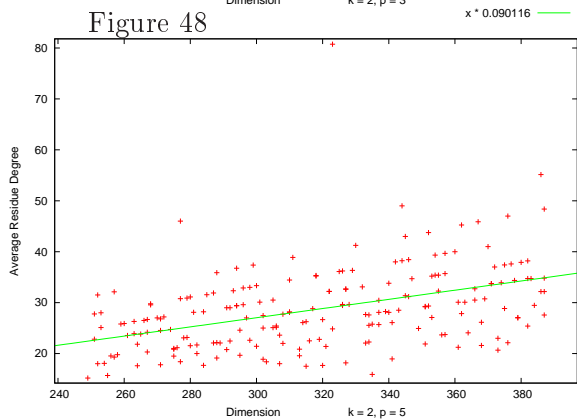
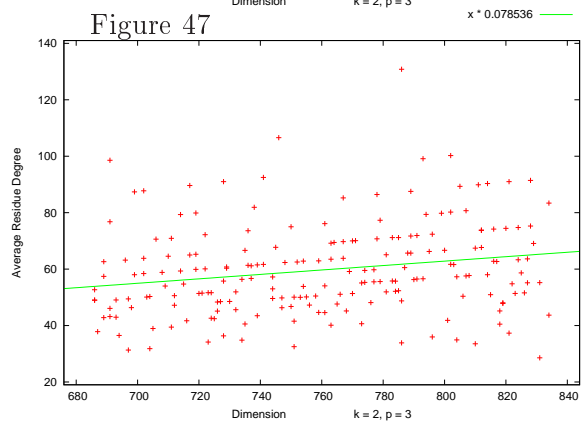
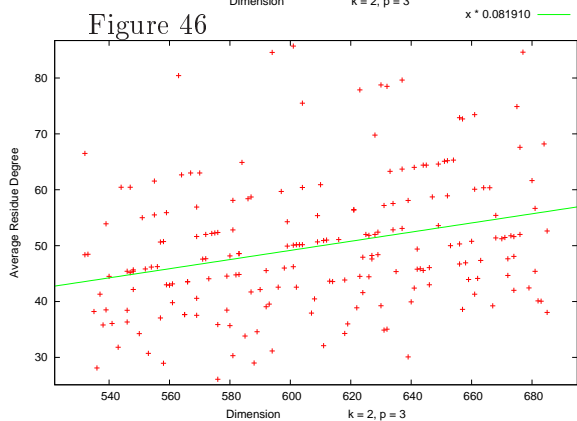
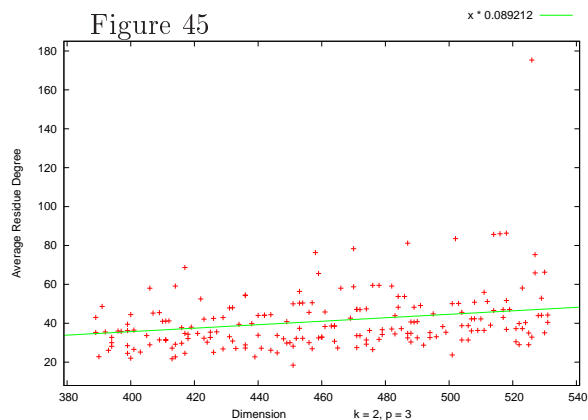
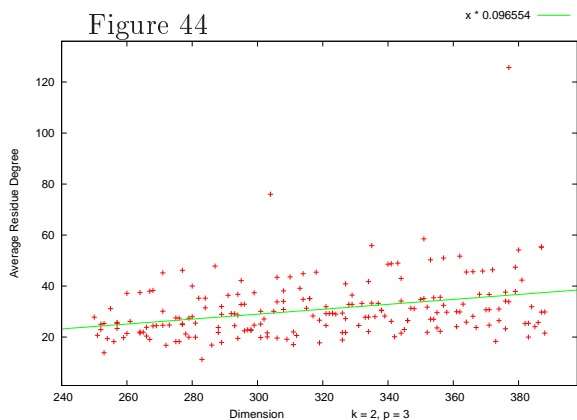
Here are again two examples for weight 4.

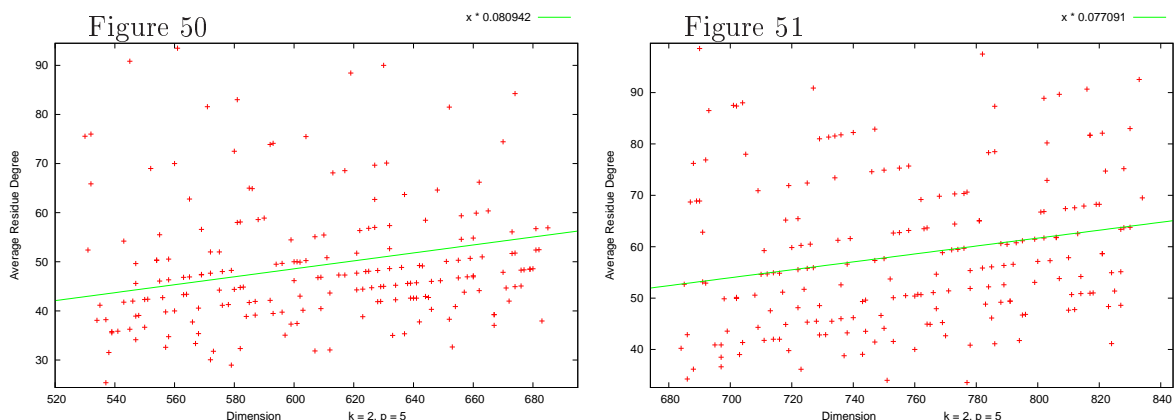


Very roughly speaking the data suggest that the average residue degree grows with the dimension, as is certainly to be expected. We also conducted a closer analysis for the primes 2, 3 and 5. For $p = 2$ we used all primes in different intervals up to 12000 and obtained these plots:



Here are the plots for $p = 3, 5$ and the primes between 3000 and 10009 subdivided into four intervals.





We observe that the slope of the best fitting line goes slightly down with the dimension. This strongly suggests that taking a straight line does not seem to be quite correct. We also made logarithmic plots, which we do not reproduce here; they seemed to suggest to us that a behaviour of the form $b_{N,k}^{(p)} \sim \text{const} \cdot d(N)^\alpha$ is not quite correct either (the best choice of α seems to be close to 1 in accordance with the previous discussion).

These computations suggest the following question.

Question 4.3. — Fix a prime p and an even weight $k \geq 2$. Let $b(N) := b_{k,N}^{(p)}$ and $d(N) := \dim_{\overline{\mathbb{F}}_p} S_k(N; \overline{\mathbb{F}}_p)$. Do there exist constants C_1, C_2 and $0 < \alpha \leq \beta < 1$ such that the inequality

$$C_1 + \alpha \frac{d(N)}{\log(d(N))} \leq b(N) \leq C_2 + \beta \cdot d(N)$$

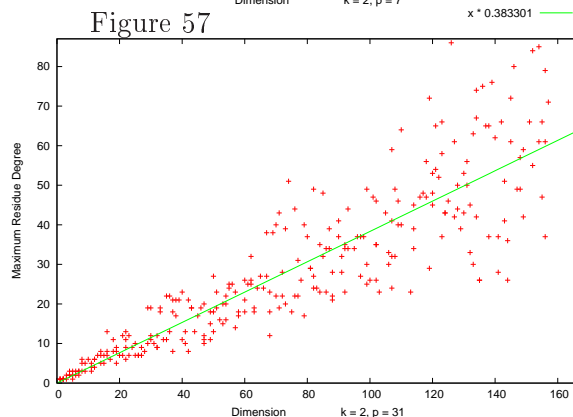
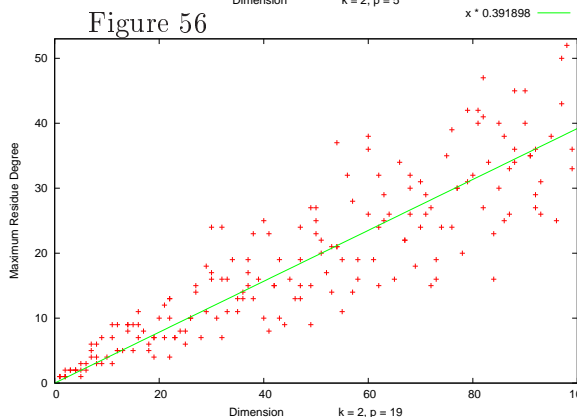
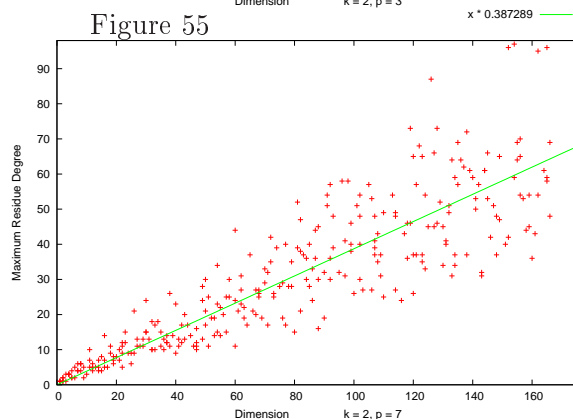
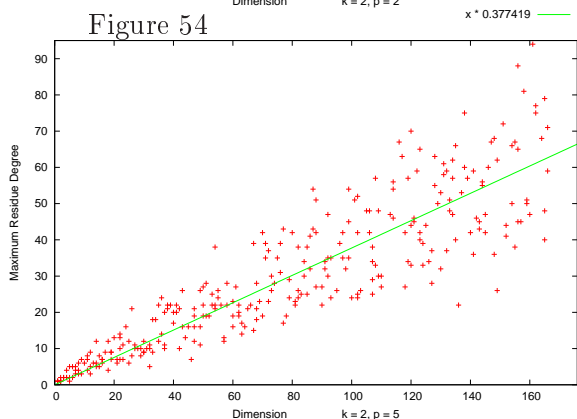
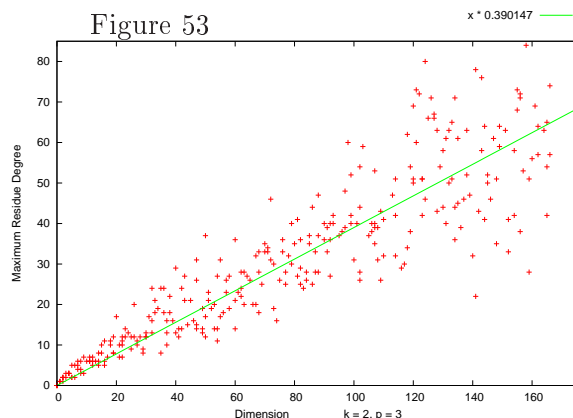
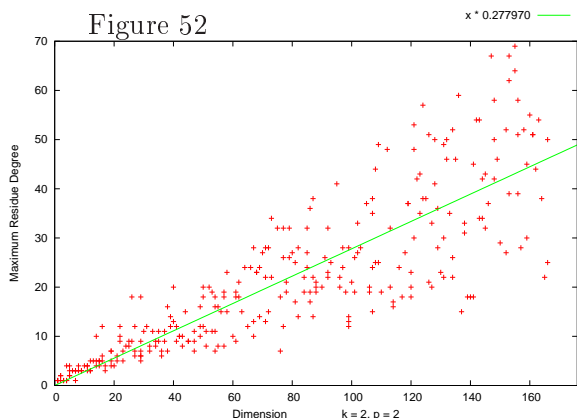
holds?

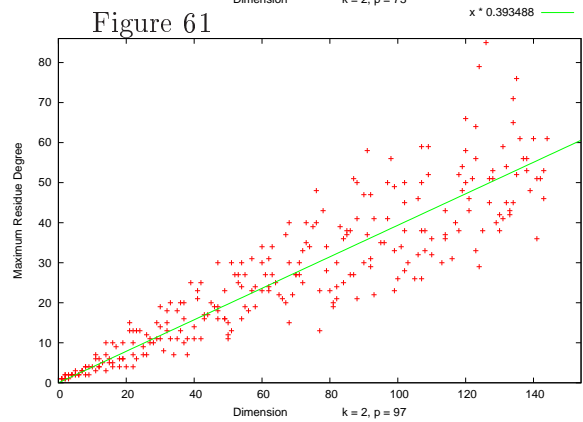
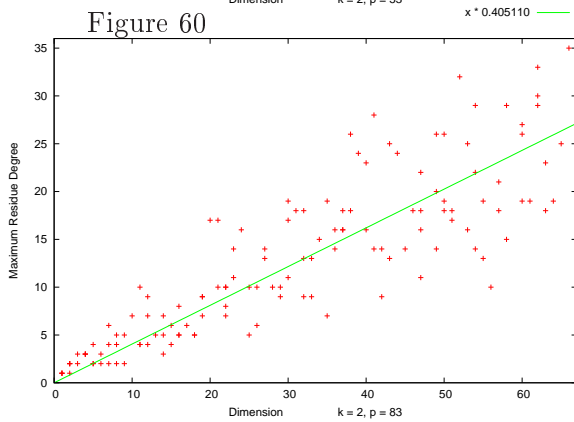
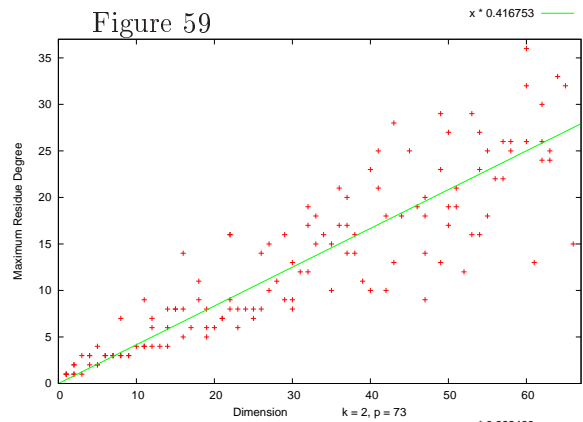
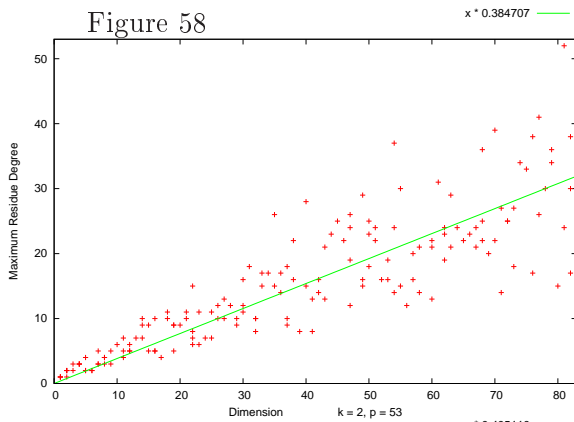
We remark that if $a_{N,k}^{(p)}$ behaves like $d(N)$, as suggested by Question 4.1, then Question 4.3 is equivalent to asking that $\#\text{Spec}(\overline{\mathbb{T}}_k(N))$ does not grow faster than a constant times $\log(d(N))$. The phenomenon that for odd primes p most of the dots in the diagrams seem to lie on or very close to certain distinguished lines through the origin is natural in view of Question 4.1: the slope of the line on or close to which a dot lies is just $\frac{1}{\#\text{Spec}(\overline{\mathbb{T}}_k(N))}$.

4.3. Maximum Residue Degree. — Now we turn our attention to the *maximum residue degree*, which we define for given level N , weight k and prime p as

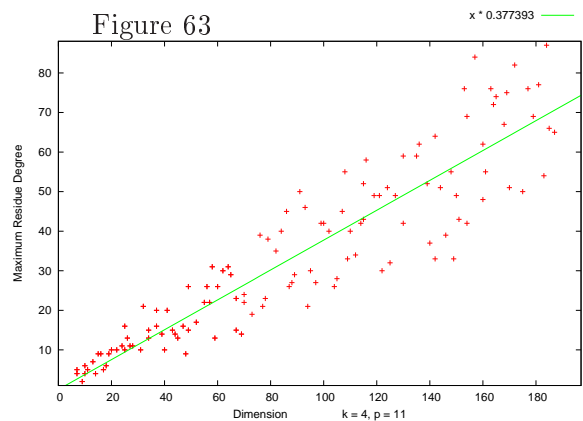
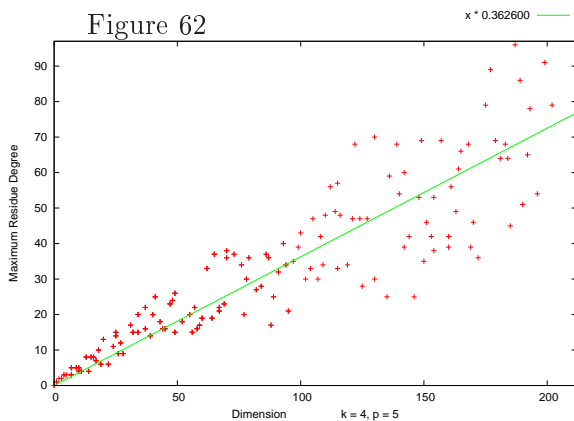
$$c_{N,k}^{(p)} = \max\{[\mathbb{F}_{\mathfrak{m}} : \mathbb{F}_p] \mid \mathfrak{m} \in \text{Spec}(\overline{\mathbb{T}}_k(N))\}.$$

We made computations for weight 2 and all primes p less than 100, where N runs through the same ranges as previously. We again plot the dimension $d(N)$ on the x -axis and the function $c_{N,k}^{(p)}$ on the y -axis and the straight line is again the best fitting function $\alpha \cdot d(N)$. This time we believe that this might be the right function to take. Here is again a selection of the plots that we obtained.

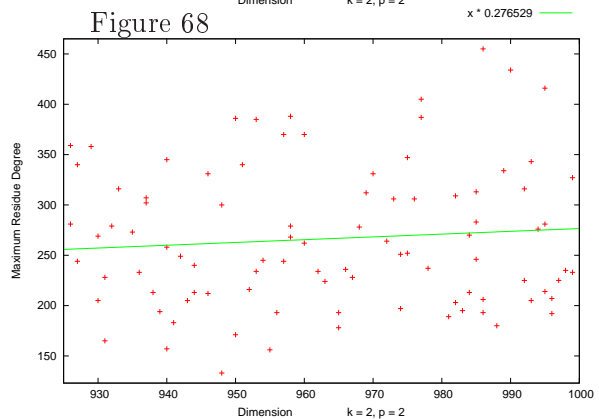
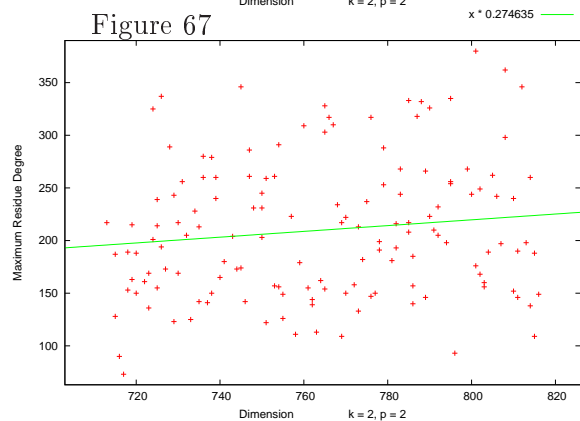
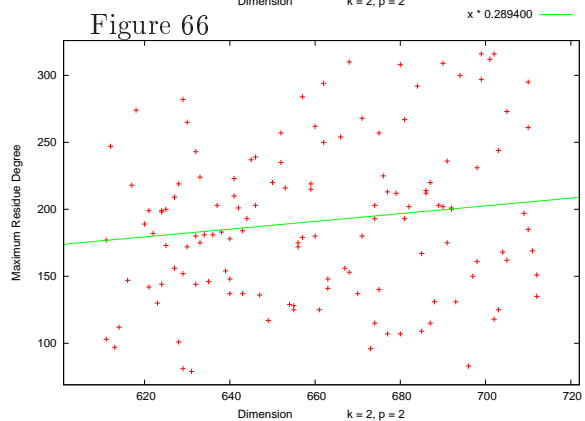
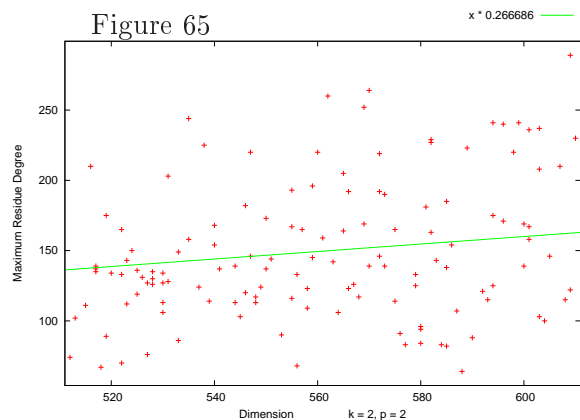
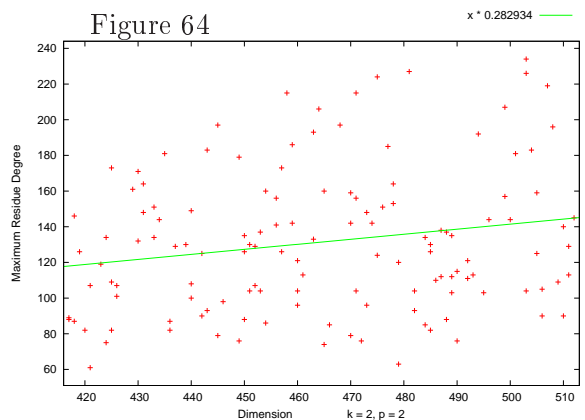




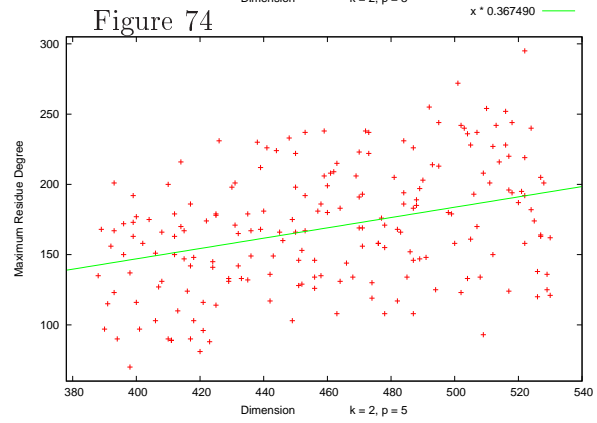
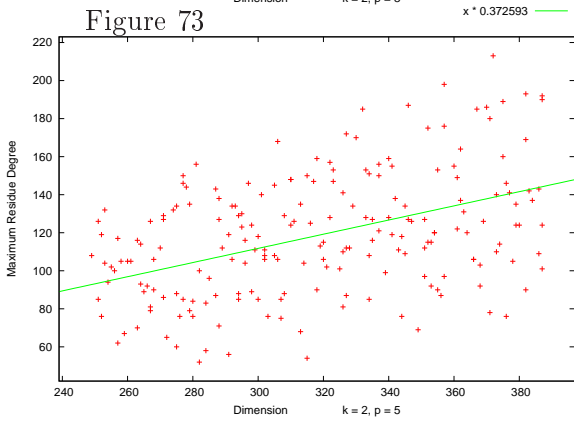
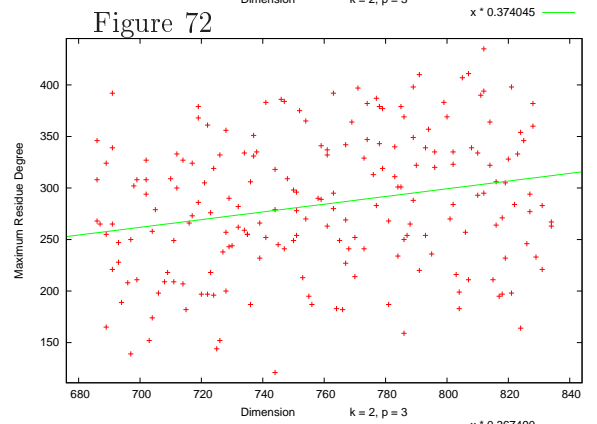
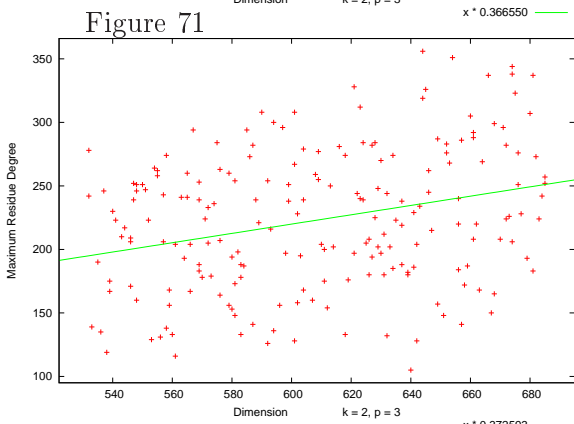
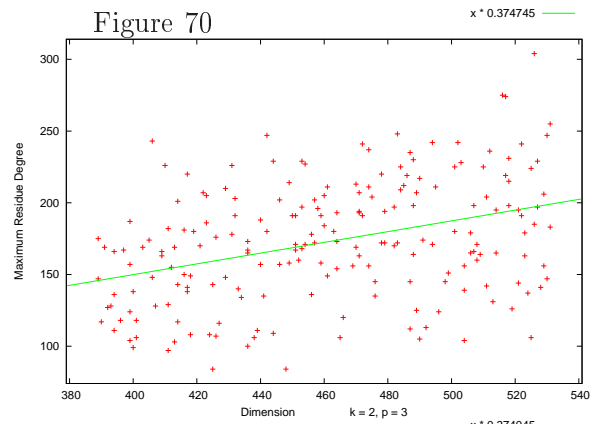
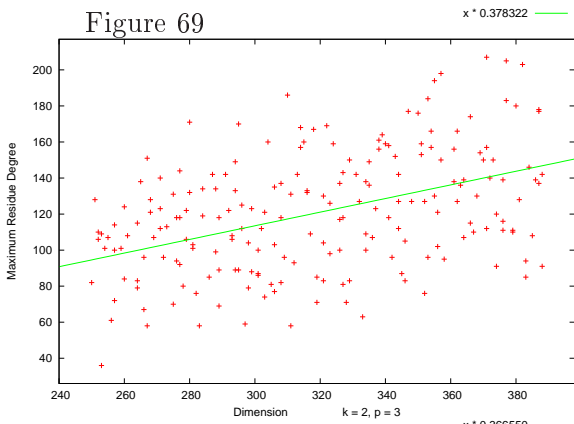
Here are again two examples for weight 4.

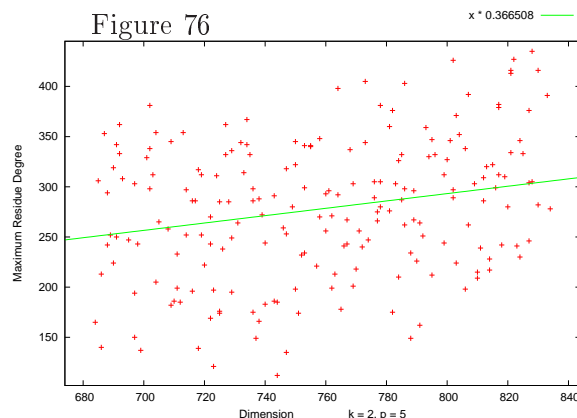
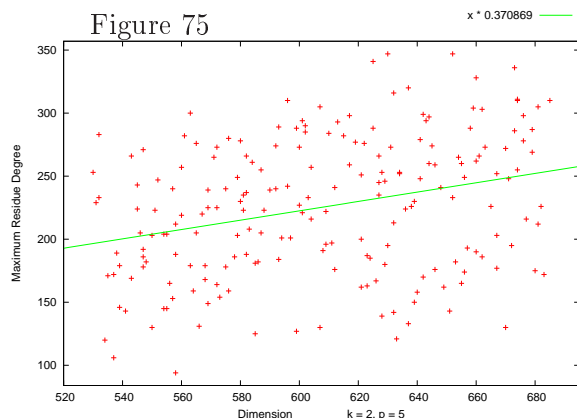


The data certainly suggest that the maximum residue degree grows with the dimension. It is remarkable to see that the slopes of the best fitting lines all seem to be very close to each other – with the single exception of the case $p = 2$, which might be caused by the same phenomenon as earlier. Also in this case we conducted a closer analysis for the primes 2, 3 and 5. For $p = 2$ we used all primes in different intervals up to 12000 and obtained these plots:



Here are the plots for $p = 3, 5$ and the primes between 3000 and 1009 subdivided into four intervals.





We observe that, although the best fitting lines were computed using different intervals, their slopes are very close to each other. These computations suggest the following question.

Question 4.4. — Fix a prime p and an even weight $k \geq 2$. Let $c(N) := c_{k,N}^{(p)}$ and $d(N) := \dim_{\mathbb{F}_p} S_k(N; \overline{\mathbb{F}_p})$. Do there exist constants C_1, C_2 and $0 < \alpha \leq \beta < 1$ such that the inequality

$$C_1 + \alpha \cdot d(N) \leq c(N) \leq C_2 + \beta \cdot d(N)$$

holds?

References

- [BLGHT] T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor. *A family of Calabi-Yau varieties and potential automorphy II*. To appear in P.R.I.M.S.
- [BCP] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system I: The user language*. J. Symb. Comp. **24(3–4)** (1997), 235–265.
- [B] J. Bosman. *Modular forms applied to the computational inverse Galois problem*. Preprint, 2010.
- [CHT] L. Clozel, M. Harris and R. Taylor. *Automorphy for some l -adic lifts of automorphic mod l representations*. Pub. Math. IHES **108** (2008), 1–181.
- [CE] Coleman, Robert F.; Edixhoven, Bas. *On the semi-simplicity of the U_p -operator on modular forms*. Math. Ann. **310** (1998), no. 1, 119–127.
- [DiWi] L. Dieulefait, G. Wiese. *On Modular Forms and the Inverse Galois Problem*. Accepted for publication in the Transactions of the AMS.
- [DS] Deligne, Pierre; Serre, Jean-Pierre. *Formes modulaires de poids 1*. Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530.
- [DI] F. Diamond and J. Im. *Modular forms and modular curves*, in *Seminar on Fermat’s Last Theorem (Toronto, ON, 1993–1994)*, 39–133, Amer. Math. Soc., Providence, RI, 1995.
- [HSHT] M. Harris, N. Shepherd-Barron and R. Taylor. *A family of Calabi-Yau varieties and potential automorphy*. Annals of Math. **171** (2010), 779–813.
- [M] B. Mazur. *Modular curves and the Eisenstein ideal*. Inst. Hautes Études Sci. Publ. Math. No. **47** (1977), 33–186 (1978).
- [S] J.-P. Serre. *Répartition asymptotique des valeurs propres de l’opérateur de Hecke T_p* . J. American Mathematical Society **10(1)**, 1997, 75–102.

- [T] R. Taylor. *Automorphy for some l -adic lifts of automorphic mod l representations. II* Pub. Math. IHES **108** (2008), 183–239.
- [W] G. Wiese. *On projective linear groups over finite fields as Galois groups over the rational numbers*. In: 'Modular Forms on Schiermonnikoog' edited by Bas Edixhoven, Gerard van der Geer and Ben Moonen. Cambridge University Press, 2008, 343–350.

23 octobre 2010

MARCEL MOHYLA, Universität Duisburg-Essen, Institut für Experimentelle Mathematik, Ellernstraße 29,
45326 Essen, Germany

GABOR WIESE, Universität Duisburg-Essen, Institut für Experimentelle Mathematik, Ellernstraße 29, 45326
Essen, Germany • *E-mail* : `gabor.wiese@uni-due.de`