Computing (with) Modular Forms

Gabor Wiese

Institut für Experimentelle Mathematik

Universität Duisburg-Essen

27 March 2009

Plan

(I) Arithmetic of coefficient fields of families of modular forms. Introduction.

(II) Calculations (by Marcel Mohyla) and questions.

(III) Modular forms algorithms and implementations - a wiki.

Coefficient fields

Let $f = \sum_{n=1}^{\infty} a_n \, q^n$ be a newform (today mostly of prime level).

Coefficient field of f: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$.

Coefficient fields

Let $f = \sum_{n=1}^{\infty} a_n \, q^n$ be a newform (today mostly of prime level).

Coefficient field of f: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$.

- $\mathbb{Q}_f$ is a number field.

Coefficient fields

Let $f = \sum_{n=1}^{\infty} a_n \, q^n$ be a newform (today mostly of prime level).

Coefficient field of f: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$.

- $\mathbb{Q}_f$ is a number field.
- If the weight of f is 2, let A_f be the abelian variety attached to f (by Shimura).
  Then $\mathbb{Q}_f = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\mathbb{Q}}(A_f)$.

Coefficient fields

Let $f = \sum_{n=1}^{\infty} a_n \, q^n$ be a newform (today mostly of prime level).

Coefficient field of f: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$.

- $\mathbb{Q}_f$ is a number field.
- If the weight of f is 2, let A_f be the abelian variety attached to f (by Shimura).
  Then $\mathbb{Q}_f = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\mathbb{Q}}(A_f)$.

What about the arithmetic of $\mathbb{Q}_f$?

Coefficient fields

What is the arithmetic of: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$?

We consider the *coefficient field of f mod p:*

$$\mathbb{F}_{p,f} = \mathbb{F}_p(\overline{a_n}; n \in \mathbb{N})$$

for a choice of $\overline{\mathbb{Z}} \overset{x \mapsto \overline{x}}{\twoheadrightarrow} \overline{\mathbb{F}}_p$ with a prime p.

Coefficient fields

What is the arithmetic of: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$?

We consider the *coefficient field of* f *mod* p*:*

$$\mathbb{F}_{p,f} = \mathbb{F}_p(\overline{a_n}; n \in \mathbb{N})$$

for a choice of $\overline{\mathbb{Z}} \overset{x \mapsto \overline{x}}{\twoheadrightarrow} \overline{\mathbb{F}}_p$ with a prime p.

- If $p \nmid$ index of $\mathbb{Z}[a_n \mid n \in \mathbb{N}]$ in the integers of $\mathbb{Q}_f$, then $\mathbb{F}_{p,f}$ is just a residue field of f for a prime above p.

Coefficient fields

What is the arithmetic of: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$?

We consider the *coefficient field of f mod p:*

$$\mathbb{F}_{p,f} = \mathbb{F}_p(\overline{a_n}; n \in \mathbb{N})$$

for a choice of $\overline{\mathbb{Z}} \overset{x \mapsto \overline{x}}{\twoheadrightarrow} \overline{\mathbb{F}}_p$ with a prime p.

- If $p \nmid$ index of $\mathbb{Z}[a_n \mid n \in \mathbb{N}]$ in the integers of $\mathbb{Q}_f$, then $\mathbb{F}_{p,f}$ is just a residue field of f for a prime above p.
- $\mathbb{F}_{p,f}$ only depends on the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy class $[f]$ of f. Write $\mathbb{F}_{p,[f]}$.

Coefficient fields

What is the arithmetic of: $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$?

We consider the *coefficient field of f mod p:*

$$\mathbb{F}_{p,f} = \mathbb{F}_p(\overline{a_n}; n \in \mathbb{N})$$

for a choice of $\overline{\mathbb{Z}} \overset{x \mapsto \overline{x}}{\twoheadrightarrow} \overline{\mathbb{F}}_p$ with a prime p.

- If $p \nmid$ index of $\mathbb{Z}[a_n \mid n \in \mathbb{N}]$ in the integers of $\mathbb{Q}_f$, then $\mathbb{F}_{p,f}$ is just a residue field of f for a prime above p.
- $\mathbb{F}_{p,f}$ only depends on the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy class $[f]$ of f. Write $\mathbb{F}_{p,[f]}$.

Why is $\mathbb{F}_{p,[f]}$ important?

Coefficient fields mod p

Why is $\mathbb{F}_{p,[f]}$ important?

- Shimura/Deligne: There is an odd Galois representation

$$\rho_{[f]} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_{p,[f]})$$

whose arithmetic is encoded in $[f]$.

Coefficient fields mod p

Why is $\mathbb{F}_{p,[f]}$ important?

- Ribet: If f has no CM, then for almost all p there is a totally imaginary field $K_{f,p}$ with $\mathrm{Gal}(K_{f,p}/\mathbb{Q})$ equal to $\mathrm{PSL}_2(\mathbb{F}_{p,[f]})$ or $\mathrm{PGL}_2(\mathbb{F}_{p,[f]})$.

  The arithmetic of $K_{f,p}$ is encoded in $[f]$.

Coefficient fields mod p

Why is $\mathbb{F}_{p,[f]}$ important?

- Ribet: If f has no CM, then for almost all p there is a totally imaginary field $K_{f,p}$ with $\mathrm{Gal}(K_{f,p}/\mathbb{Q})$ equal to $\mathrm{PSL}_2(\mathbb{F}_{p,[f]})$ or $\mathrm{PGL}_2(\mathbb{F}_{p,[f]})$.

  The arithmetic of $K_{f,p}$ is encoded in $[f]$.

- Serre's modularity conjecture (Theorem of Khare, Wintenberger, Kisin):

  Every totally imaginary number field with Galois group $\mathrm{PSL}_2(\mathbb{F})$ or $\mathrm{PGL}_2(\mathbb{F})$ for any finite field $\mathbb{F}$ arises in this way.

Coefficient fields mod p

What do we know about $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$?

- In concrete cases: easy to compute $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$.

Coefficient fields mod p

What do we know about $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$?

- In concrete cases: easy to compute $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$.
- Not directly related to the level and the weight of f:

  Just from level and weight, one cannot say much about $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$.

Coefficient fields mod p

What do we know about $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$?

- In concrete cases: easy to compute $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$.
- Not directly related to the level and the weight of f:

  Just from level and weight, one cannot say much about $\mathbb{Q}_f$ and $\mathbb{F}_{p,[f]}$.

Can one say something 'asymptotic', when varying f?

Coefficient fields mod p

Can one say something 'asymptotic', when varying f?

We will study:

- Sum of degrees $[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$ for all $[f]$ in a given level and weight.

  Degeneration of mod p Hecke algebras.

Coefficient fields mod p

Can one say something 'asymptotic', when varying f?

We will study:

- Sum of degrees $[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$ for all $[f]$ in a given level and weight.

  Degeneration of mod p Hecke algebras.

- Average degree $[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$ for all $[f]$ in a given level and weight.

Coefficient fields mod p

Can one say something 'asymptotic', when varying f?

We will study:

- Sum of degrees $[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$ for all $[f]$ in a given level and weight.

  Degeneration of mod p Hecke algebras.
- Average degree $[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$ for all $[f]$ in a given level and weight.
- Maximum degree $[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$ among all $[f]$ in a given level and weight.

Degeneration mod p

We fix a (prime) level N and a weight k.

Define

$$\dim_k(N) = (\text{number of newforms of level } N \text{ and weight } k).$$

Degeneration mod p

We fix a (prime) level N and a weight k.

Define

$$\dim_k(N) = (\text{number of newforms of level } N \text{ and weight } k).$$

Consider the sum of residue degrees

$$\deg_k^{(p)}(N) = \sum_{[f]} [\mathbb{F}_{p,[f]} : \mathbb{F}_p]$$

where $[f]$ runs through the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy classes of newforms of level N and weight k.

Degeneration mod p

Theorem. $\dim_k(N) = \deg_k^{(p)}(N) \overset{\text{def}}{=} \sum_{[f]} [\mathbb{F}_{p,[f]} : \mathbb{F}_p]$

(the mod p Hecke algebra is non-degenerate) $\Leftrightarrow$

Degeneration mod p

Theorem. $\dim_k(N) = \deg_k^{(p)}(N) \stackrel{\text{def}}{=} \sum_{[f]} [\mathbb{F}_{p,[f]} : \mathbb{F}_p]$

(the mod p Hecke algebra is non-degenerate) $\Leftrightarrow$

- there is no congruence modulo p between two newforms of level N and weight k and

Degeneration mod p

Theorem. $\dim_k(N) = \deg_k^{(p)}(N) \stackrel{\text{def}}{=} \sum_{[f]} [\mathbb{F}_{p,[f]} : \mathbb{F}_p]$

(the mod p Hecke algebra is non-degenerate) $\Leftrightarrow$

- there is no congruence modulo p between two newforms of level N and weight k and
- the coefficient fields $\mathbb{Q}_f$ are unramified at p for all newforms f of level N and weight k and

Degeneration mod p

Theorem. $\dim_k(N) = \deg_k^{(p)}(N) \stackrel{\text{def}}{=} \sum_{[f]} [\mathbb{F}_{p,[f]} : \mathbb{F}_p]$

(the mod p Hecke algebra is non-degenerate) $\Leftrightarrow$

- there is no congruence modulo p between two newforms of level N and weight k and
- the coefficient fields $\mathbb{Q}_f$ are unramified at p for all newforms f of level N and weight k and
- $p \nmid$ index $\mathbb{Z}_f = \mathbb{Z}[a_n(f) \mid n \in \mathbb{N}]$ in integers of $\mathbb{Q}_f$ for all newforms f of level N and weight k.

Degeneration mod p

Theorem. $\dim_k(N) = \deg_k^{(p)}(N) \stackrel{\text{def}}{=} \sum_{[f]} [\mathbb{F}_{p,[f]} : \mathbb{F}_p]$

(the mod p Hecke algebra is non-degenerate) $\Leftrightarrow$

- there is no congruence modulo p between two newforms of level N and weight k and
- the coefficient fields $\mathbb{Q}_f$ are unramified at p for all newforms f of level N and weight k and
- $p \nmid$ index $\mathbb{Z}_f = \mathbb{Z}[a_n(f) \mid n \in \mathbb{N}]$ in integers of $\mathbb{Q}_f$ for all newforms f of level N and weight k.

One could expect that strict inequality $\dim_k(N) > \deg_k^{(p)}(N)$ (degeneration modulo p) is a rare phenomenon.

Is that true?

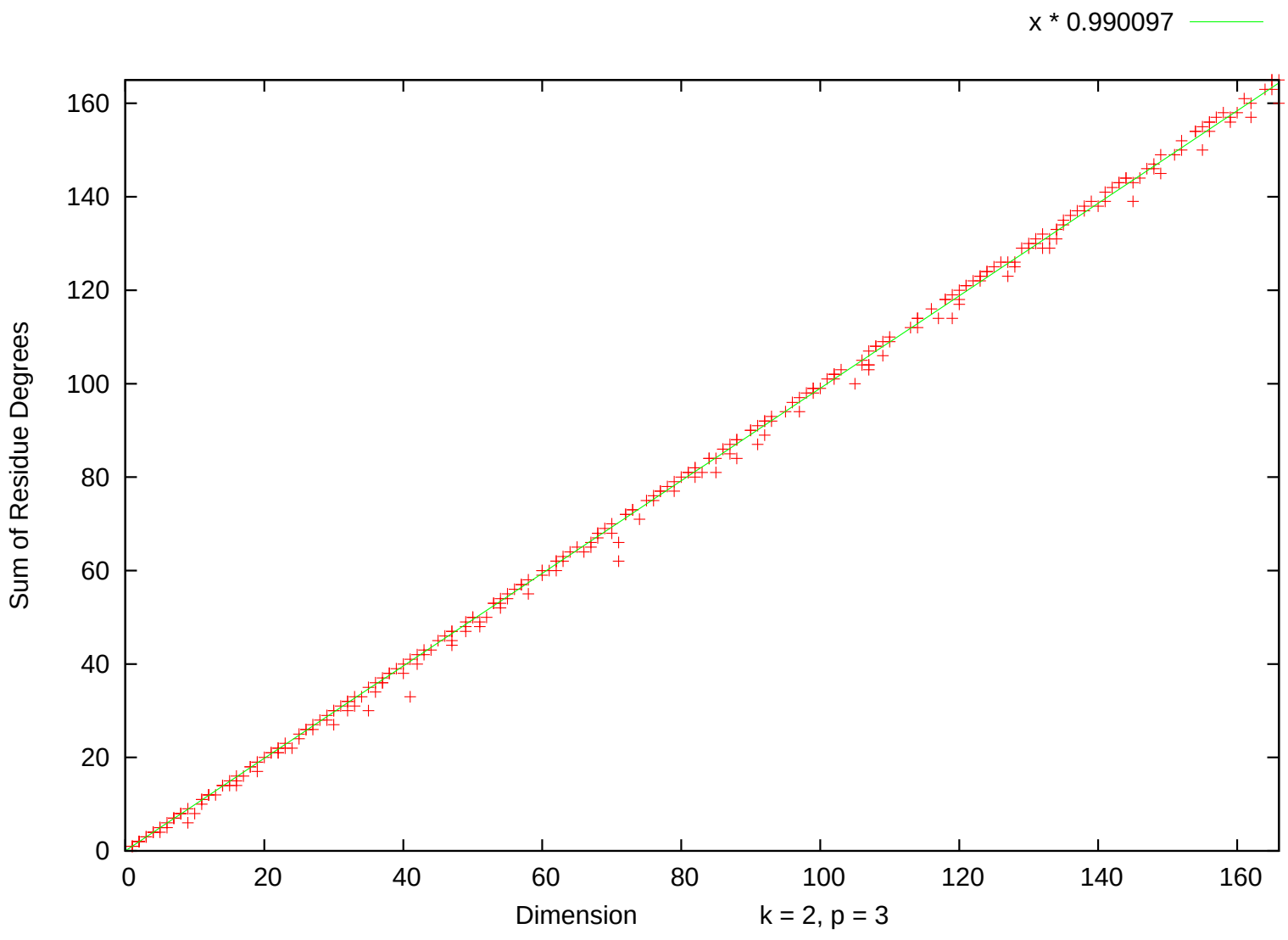
Degeneration mod p

Let us fix the prime p and the weight k.

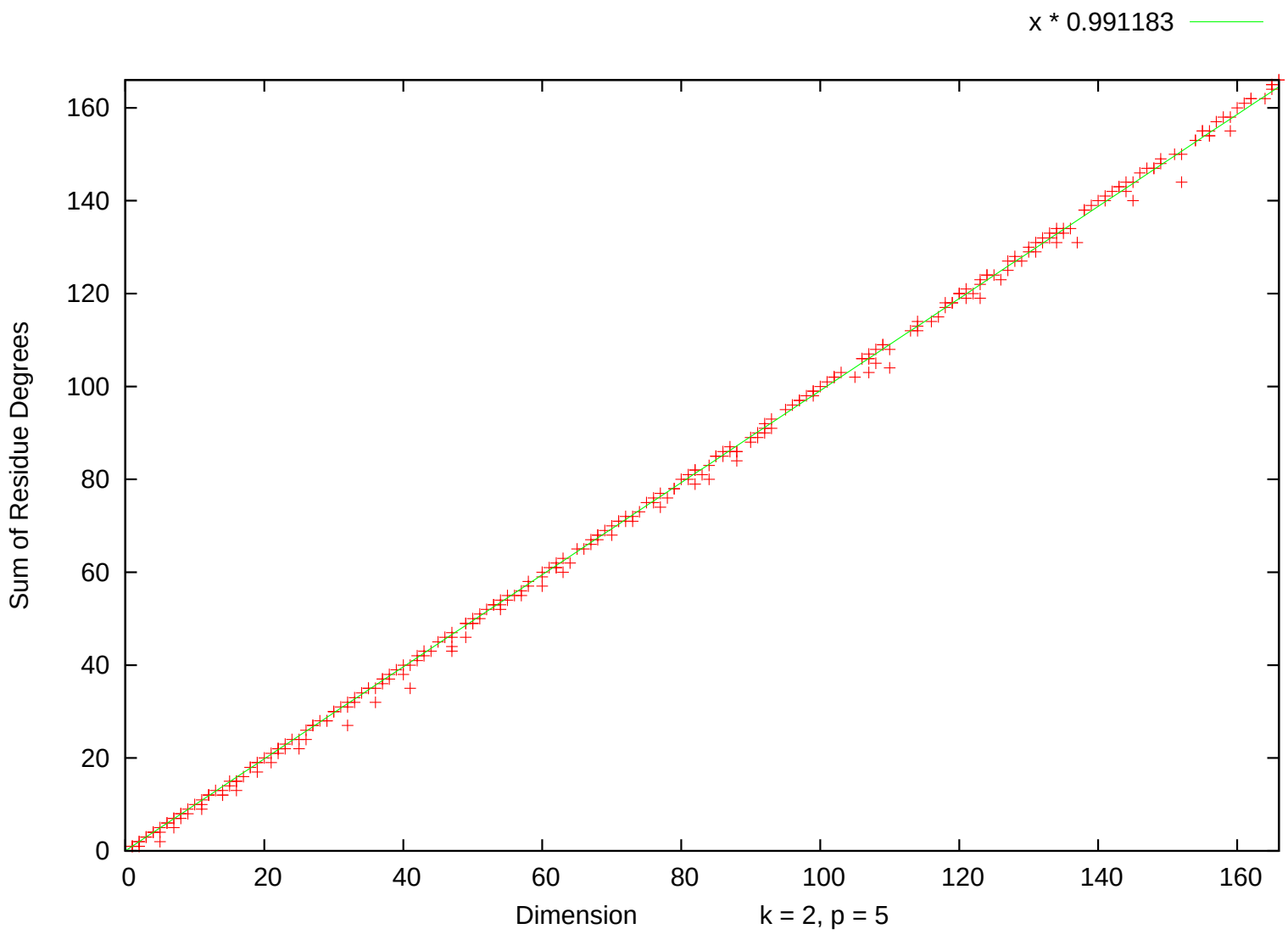
Plot $\deg_k^{(p)}(N)$ as a function of $\dim_k(N)$ for all prime levels $N \leq 2000$ (for $k = 2$).

First, let p be odd.

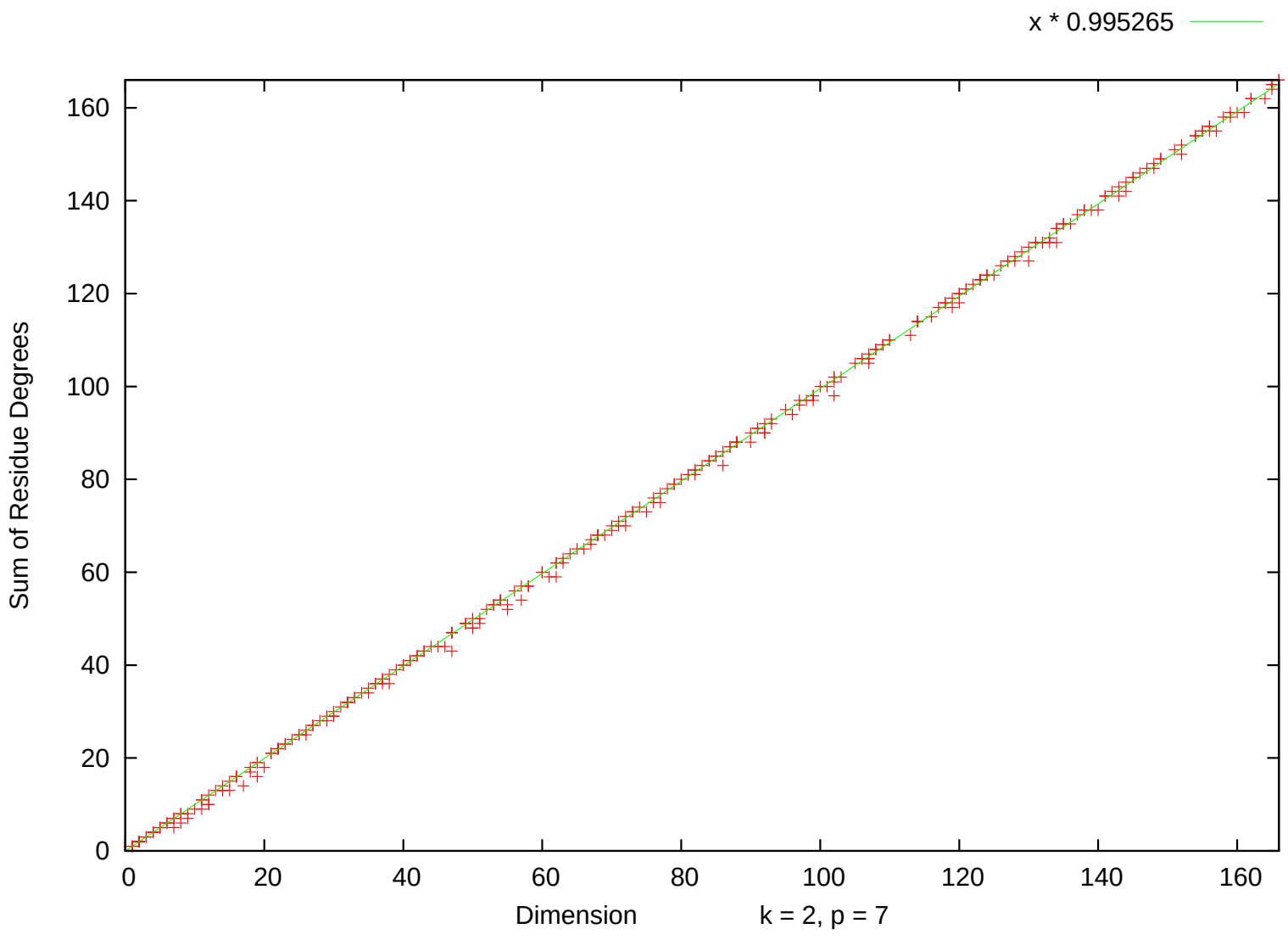
Degeneration mod p



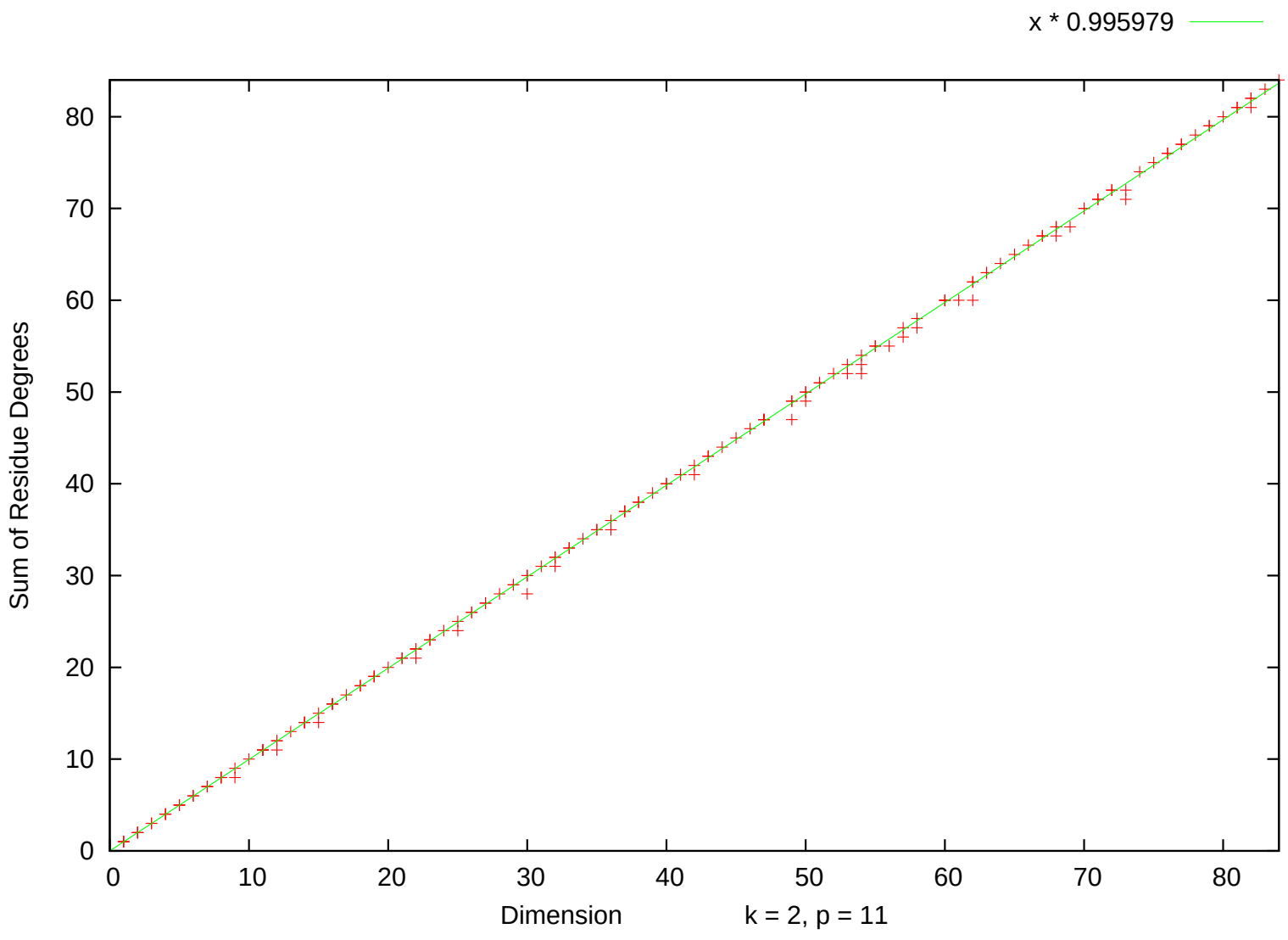
Degeneration mod p



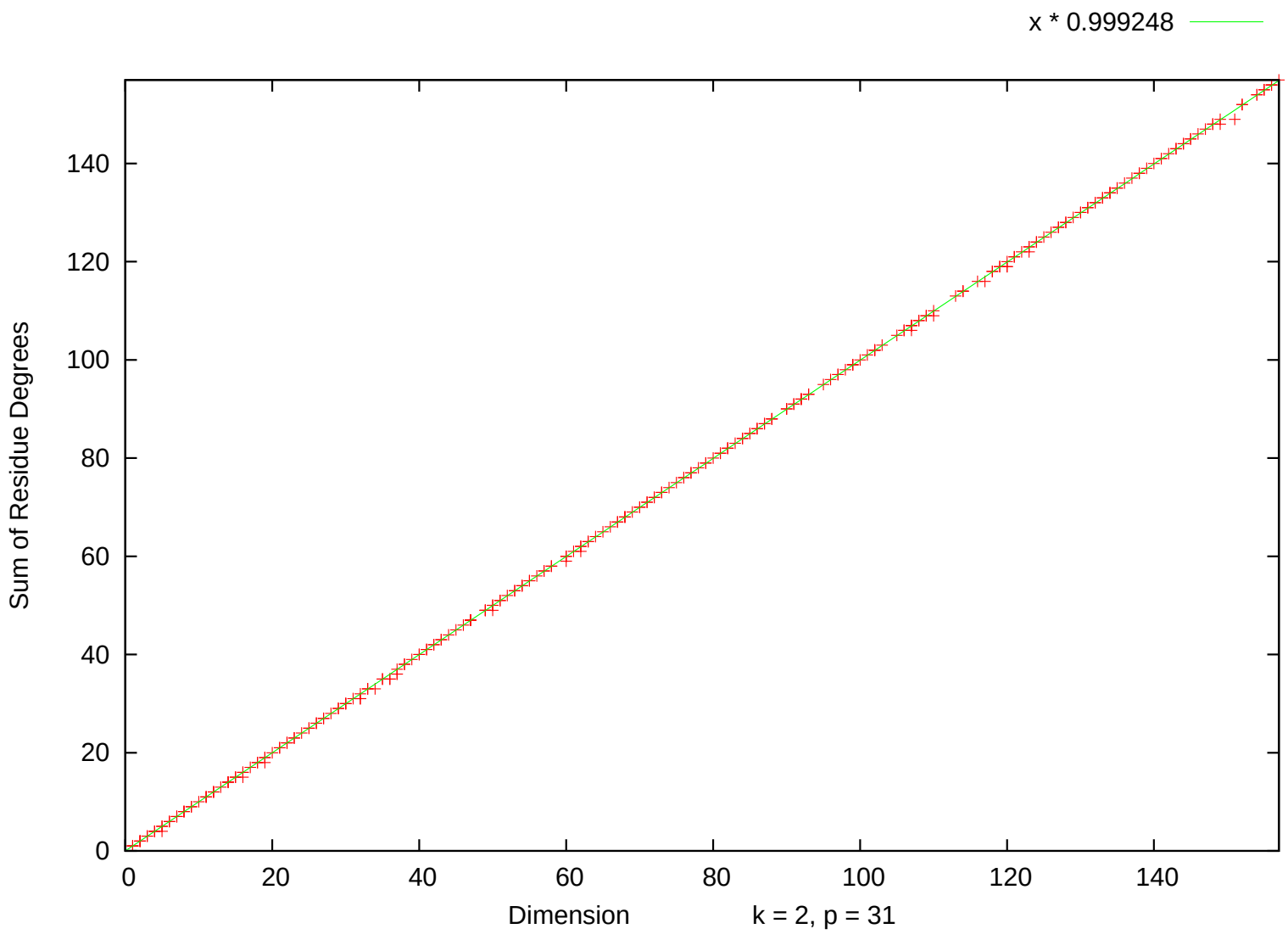
Degeneration mod p



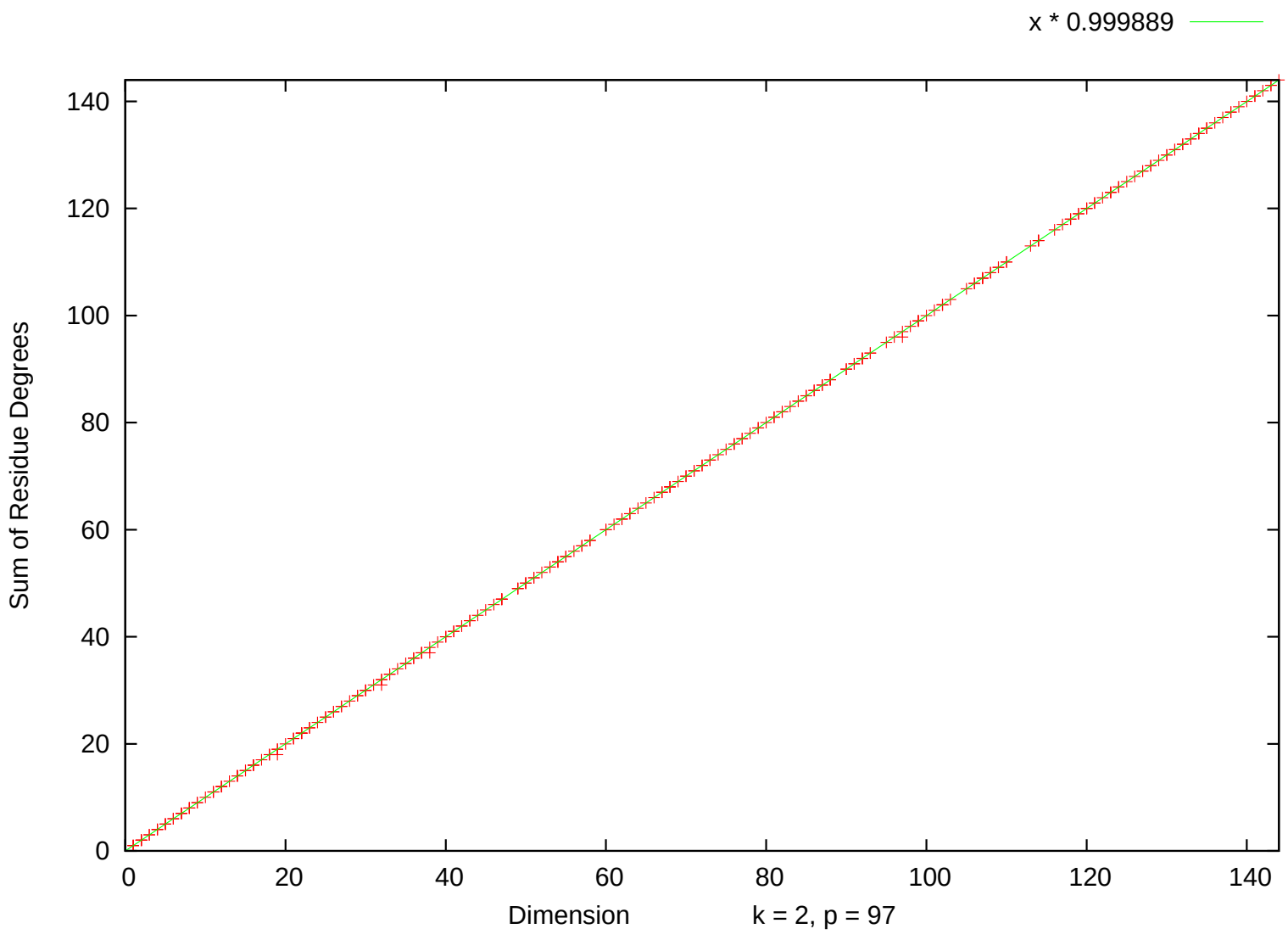
Degeneration mod p



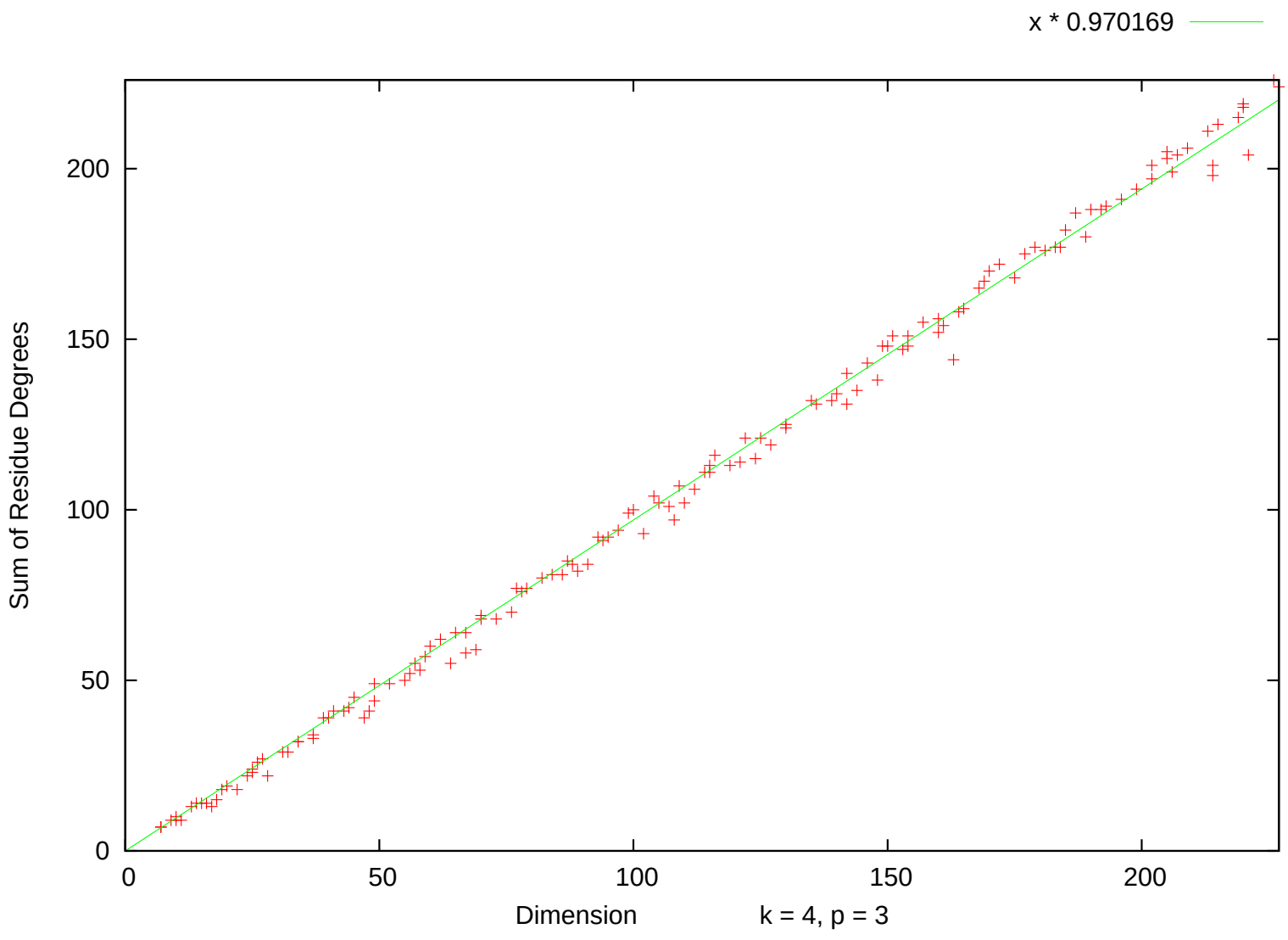
Degeneration mod p



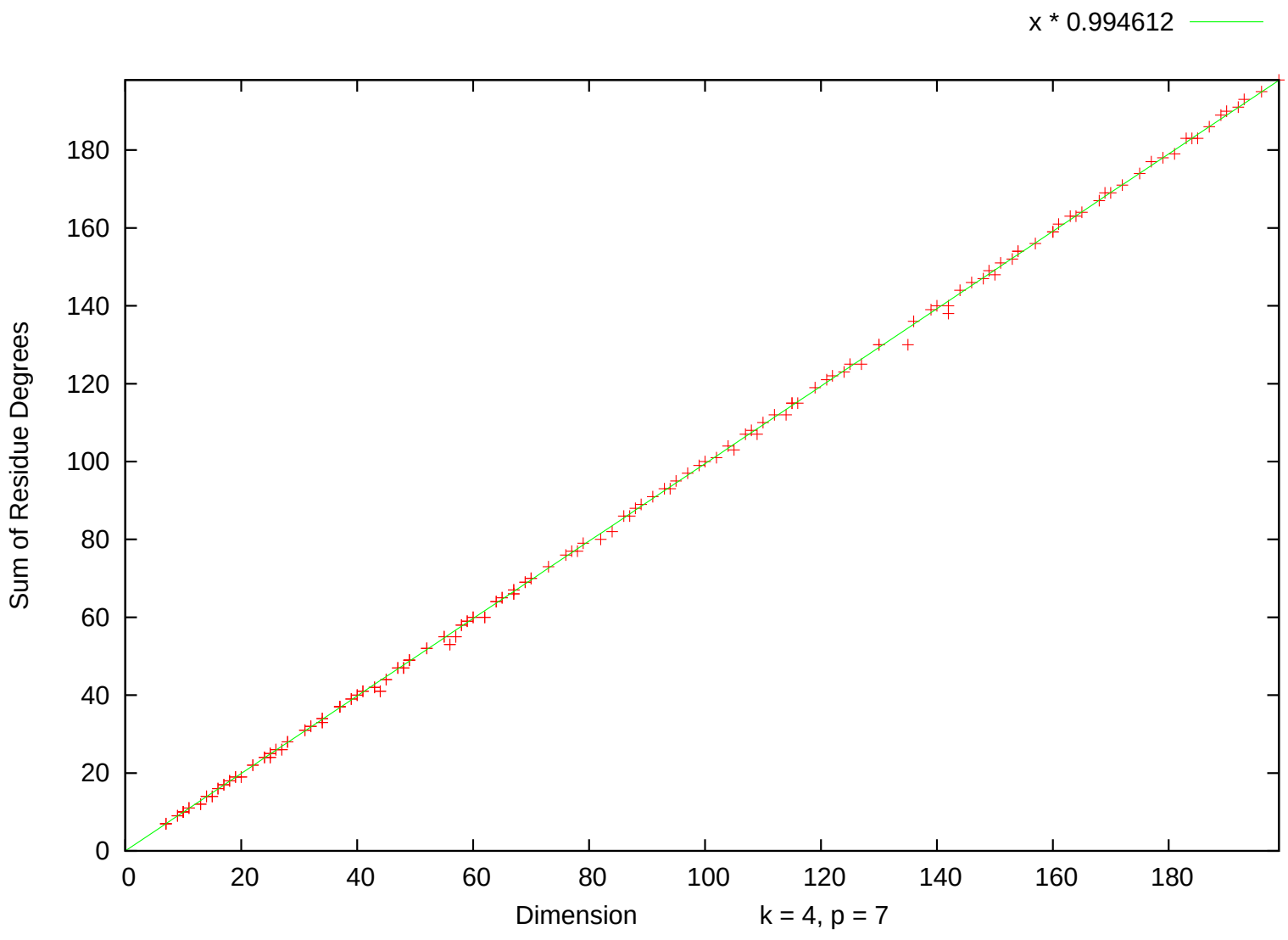
Degeneration mod p



Degeneration mod p



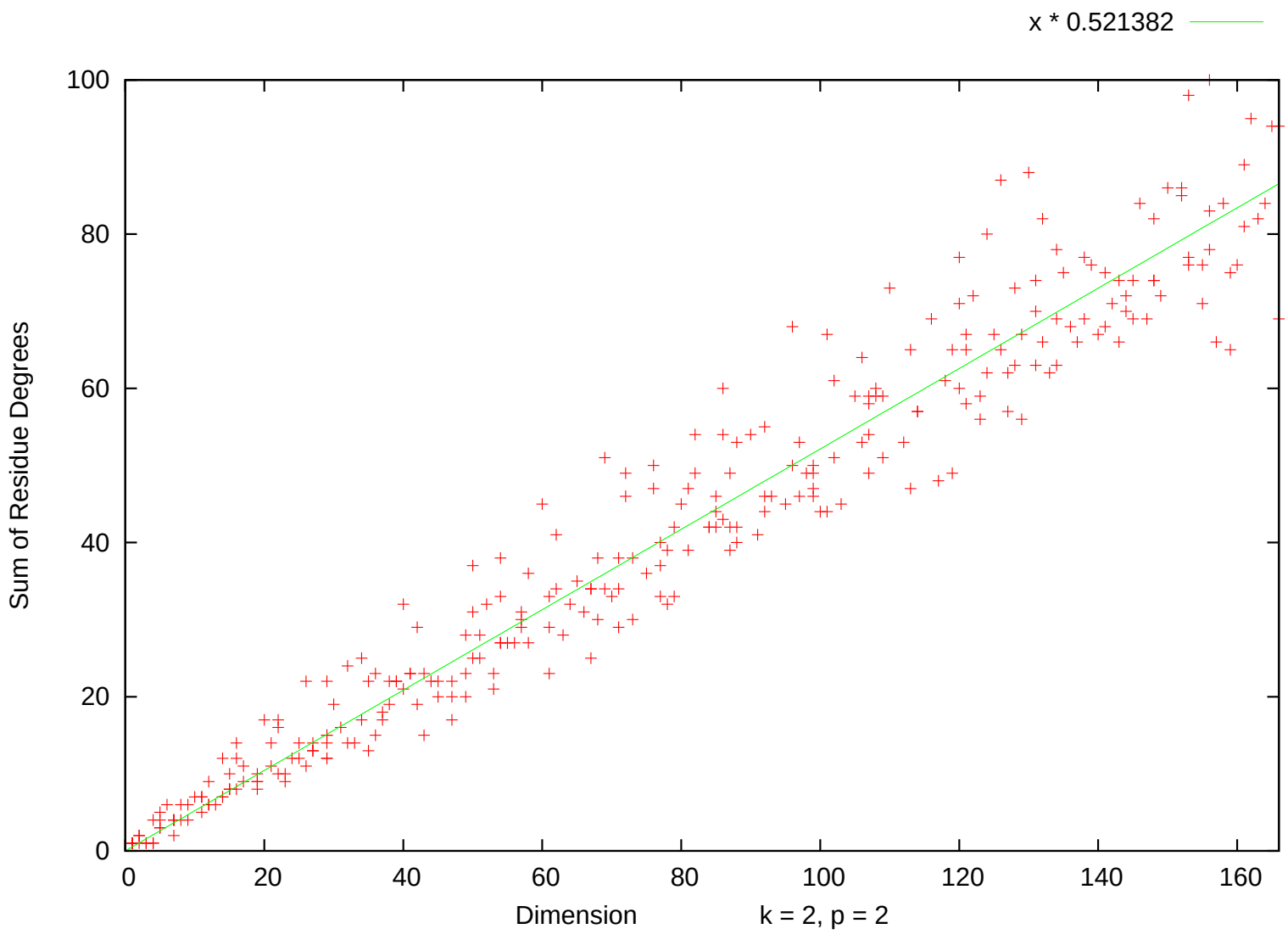
Degeneration mod p



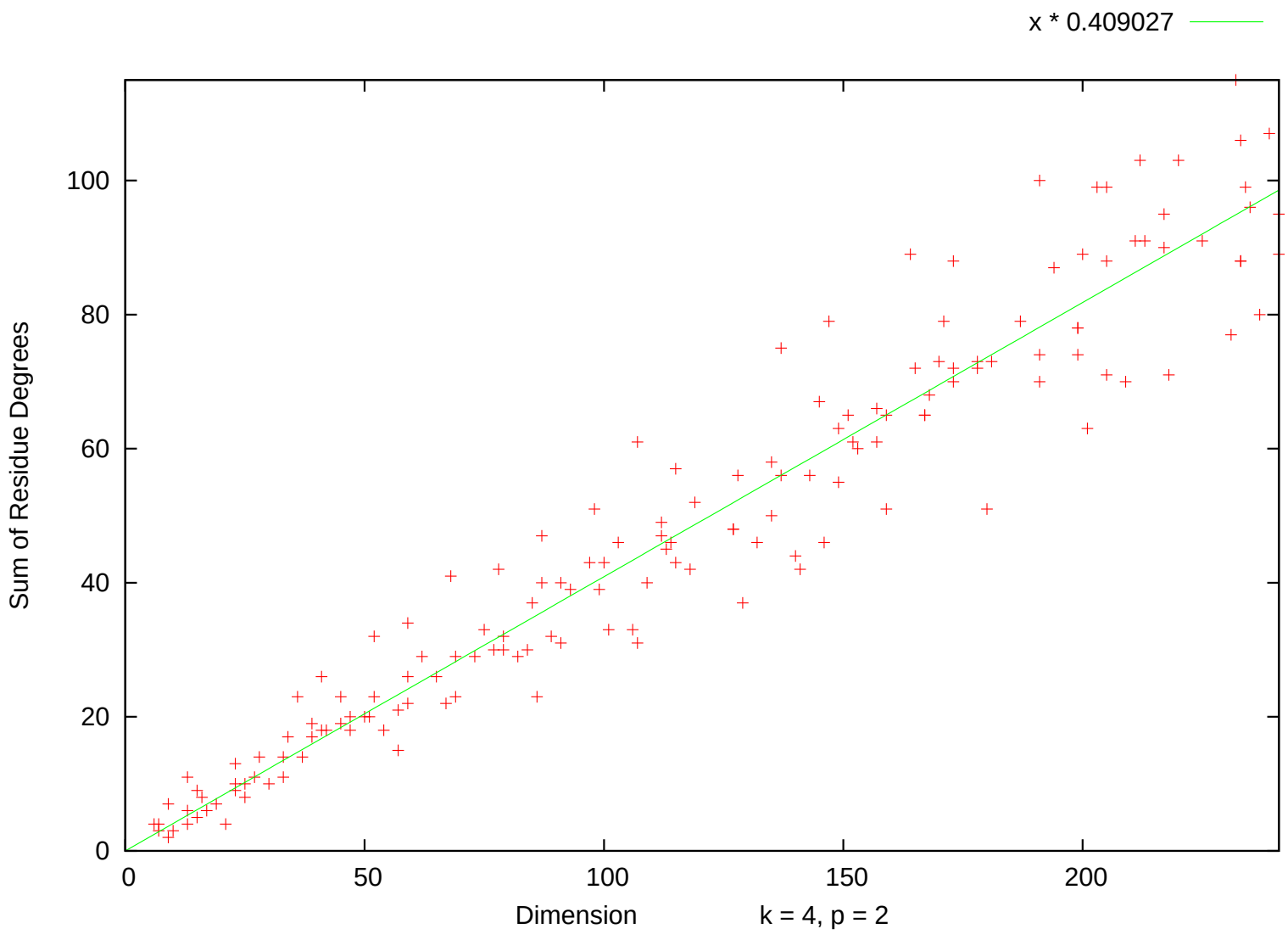
Degeneration mod p

Now $p = 2$.

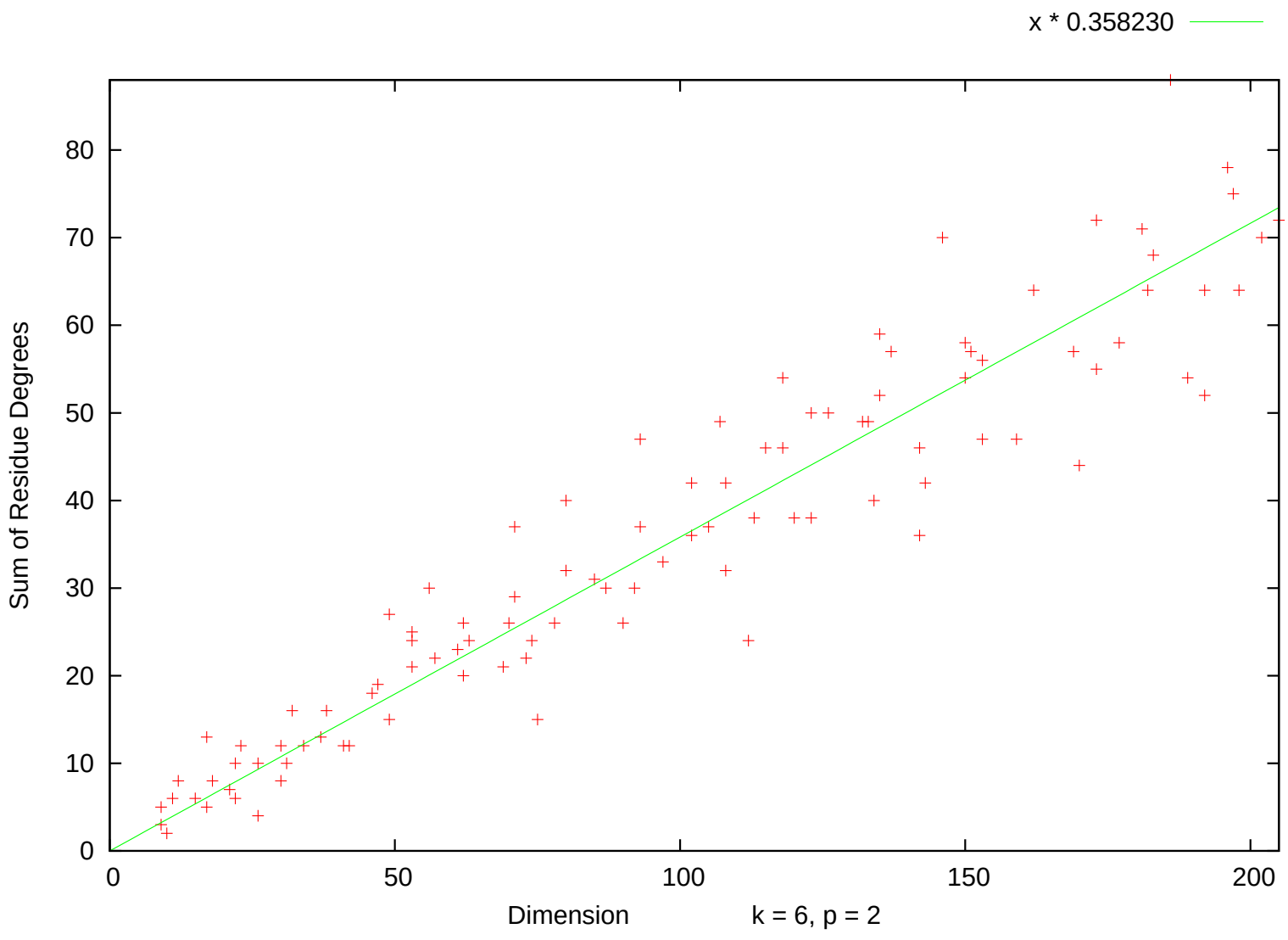
Degeneration mod p



Degeneration mod p



Degeneration mod p



Degeneration mod p

Question: *Fix a prime* $p > 2$ *and a weight* $k \geq 2$*.*

Are there $0 < \alpha \leq 1$ *and* $C > 0$ *s.t.*

$$\deg_k^{(p)}(N) \geq \alpha \dim_k(N) - C \quad ?$$

Degeneration mod p

Question: *Fix a prime* $p > 2$ *and a weight* $k \geq 2$.

Are there $0 < \alpha \leq 1$ *and* $C > 0$ *s.t.*

$$\deg_k^{(p)}(N) \geq \alpha \dim_k(N) - C \quad ?$$

Question: *Fix a prime* $p > 2$ *and a weight* $k \geq 2$.

Are there $0 < \alpha \leq \beta < 1$ *and* $C, D > 0$ *s.t.*

$$\beta \dim_k(N) + D \geq \deg_k^{(2)}(N) \geq \alpha \dim_k(N) - C \quad ?$$

Degrees of coefficient fields

Theorem (Serre). *Suppose* $N_m + k_m \to \infty$ *for* $m \to \infty$*.*

Then the set

$$\{[\mathbb{Q}_f : \mathbb{Q}] \mid f \text{ newform of level } N_m, \text{ weight } k_m \text{ some } m\}$$

is unbounded.

Degrees of coefficient fields

Theorem (Serre). *Suppose* $N_m + k_m \to \infty$ *for* $m \to \infty$*.*

Then the set

$$\{[\mathbb{Q}_f : \mathbb{Q}] \mid f \text{ newform of level } N_m, \text{ weight } k_m \text{ some } m\}$$

is unbounded.

In general, I do not know if the set

$$\{[\mathbb{F}_{p,[f]} : \mathbb{F}_p] \mid f \text{ newform of level } N_m, \text{ weight } k_m \text{ some } m\}$$

is bounded. The cases when the N_m contain big enough prime powers can be treated via ramification.

Degrees of coefficient fields

Theorem (Serre). *Suppose* $N_m + k_m \to \infty$ *for* $m \to \infty$*.*

Then the set

$$\{[\mathbb{Q}_f : \mathbb{Q}] \mid f \text{ newform of level } N_m, \text{ weight } k_m \text{ some } m\}$$

is unbounded.

In general, I do not know if the set

$$\{[\mathbb{F}_{p,[f]} : \mathbb{F}_p] \mid f \text{ newform of level } N_m, \text{ weight } k_m \text{ some } m\}$$

is bounded. The cases when the N_m contain big enough prime powers can be treated via ramification.

How do the $[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$ behave when k is fixed and N runs through the primes ?

Degrees of coefficient fields

Define:

- $\mathrm{average}_k^{(p)}(N) := \frac{\sum_{[f]}[\mathbb{F}_{p,[f]}:\mathbb{F}_p]}{\sum_{[f]} 1}$

  average degree of the coefficient fields mod p,

- $\max_k^{(p)}(N) := \max_{[f]}[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$

  maximum degree of the coefficient fields mod p.

Here, $[f]$ runs through the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy classes of newforms in level N and weight k.

Degrees of coefficient fields

Define:

- $\mathrm{average}_k^{(p)}(N) := \frac{\sum_{[f]}[\mathbb{F}_{p,[f]}:\mathbb{F}_p]}{\sum_{[f]} 1}$

  average degree of the coefficient fields mod p,

- $\max_k^{(p)}(N) := \max_{[f]}[\mathbb{F}_{p,[f]} : \mathbb{F}_p]$

  maximum degree of the coefficient fields mod p.

Here, $[f]$ runs through the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy classes of newforms in level N and weight k.

Can $\mathrm{average}_k^{(p)}(N)$ and $\max_k^{(p)}(N)$ be bounded by functions of $\dim_k(N)$?

Degrees of coefficient fields

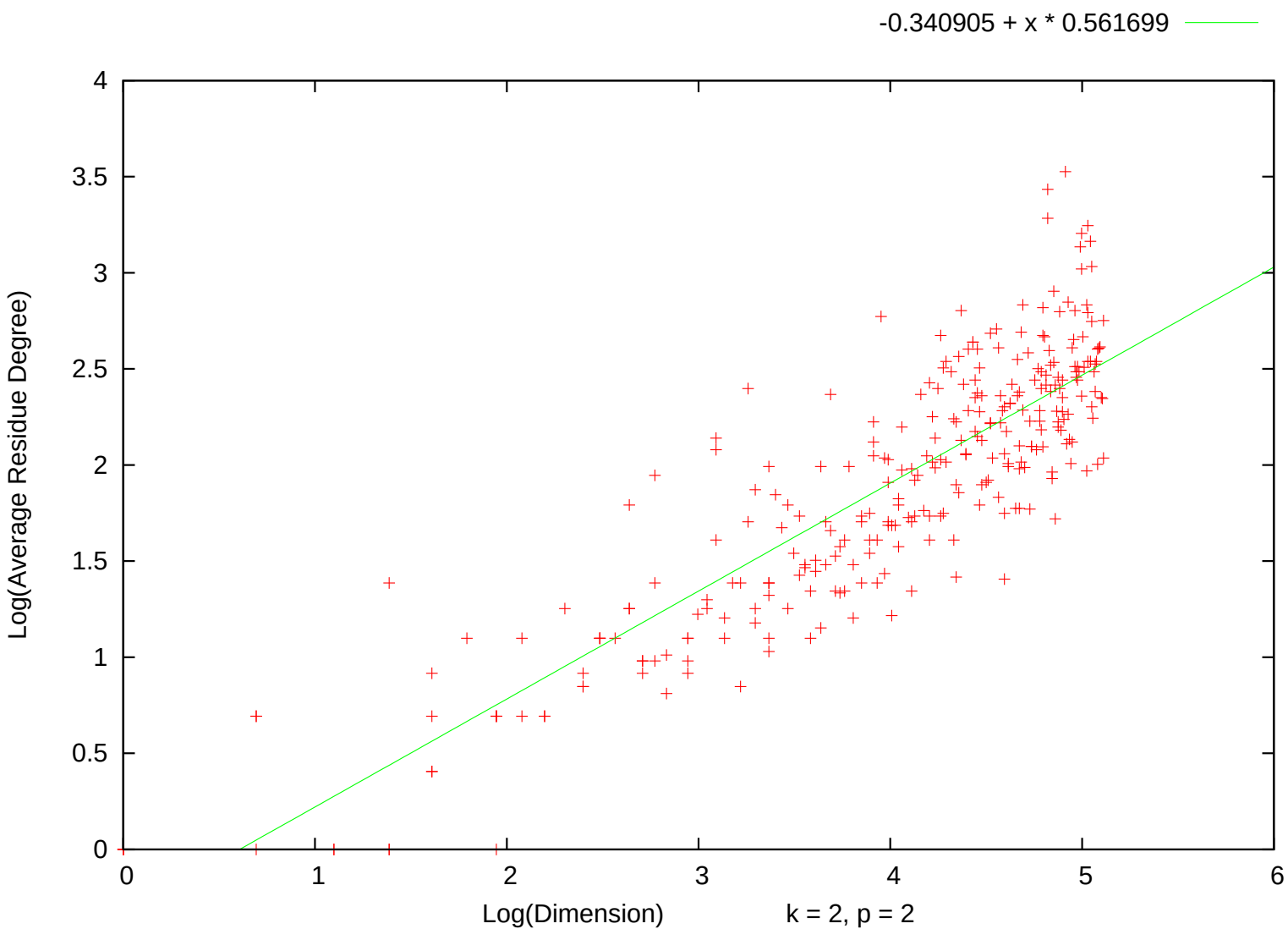
Fix p and $k = 2$.

Guess a dependence of the form

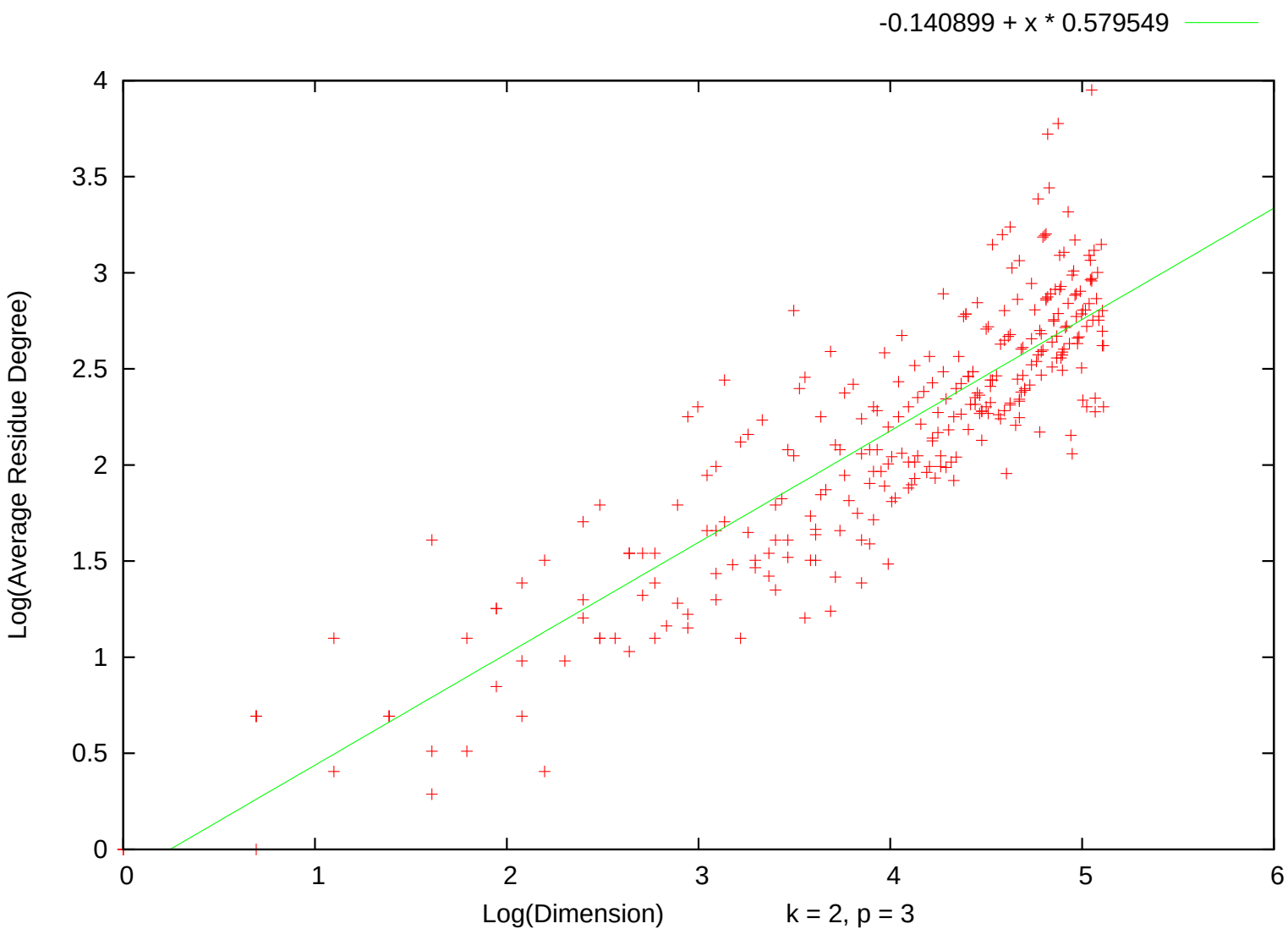
$$\mathrm{average}_k^{(p)}(N) \sim C\big(\dim_k(N)\big)^{\alpha}.$$

Plot $\log(\mathrm{average}_k^{(p)}(N))$ as a function of $\log(\dim_k(N))$ for the primes $N \leq 2000$.

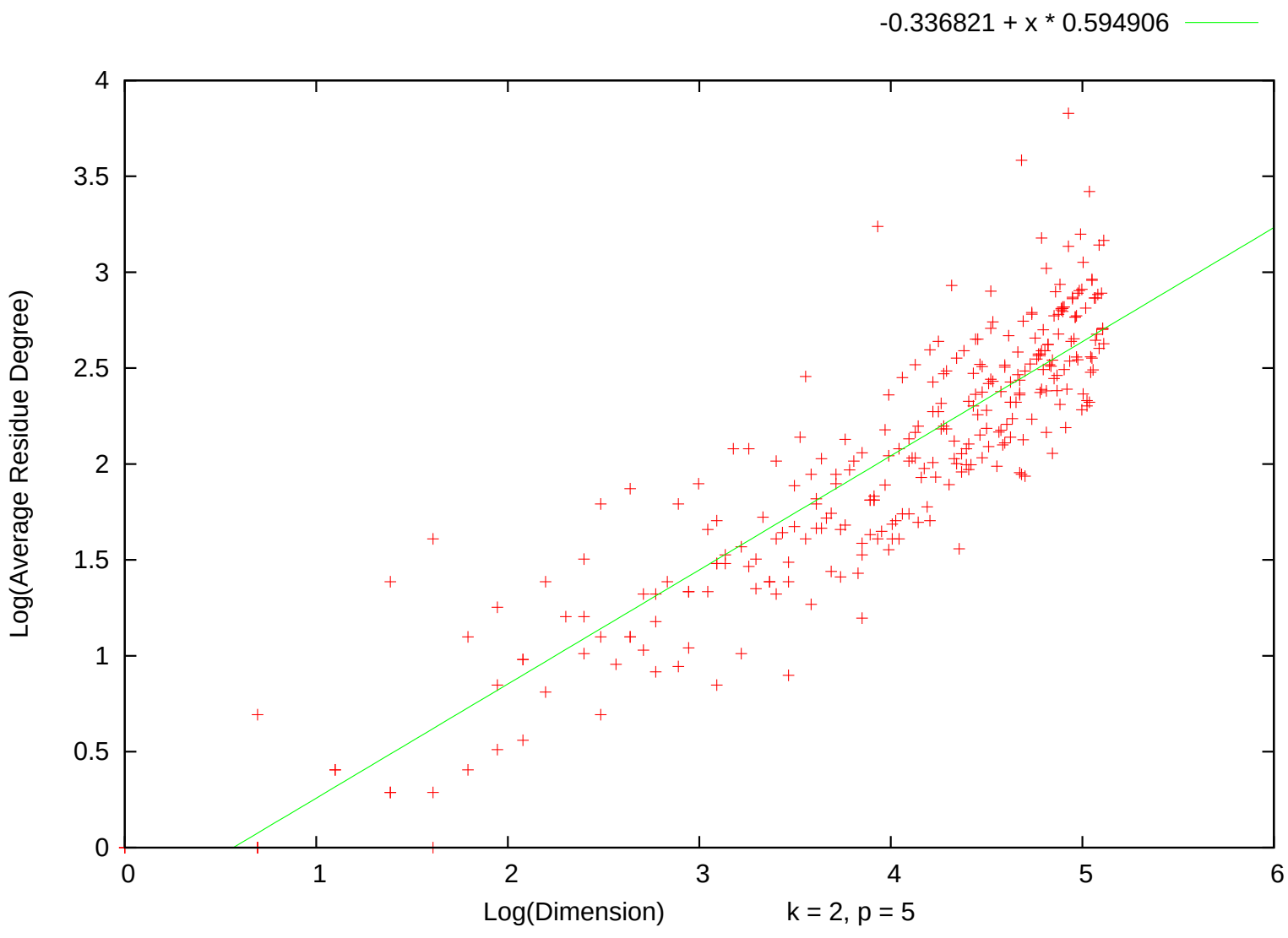
Degrees of coefficient fields



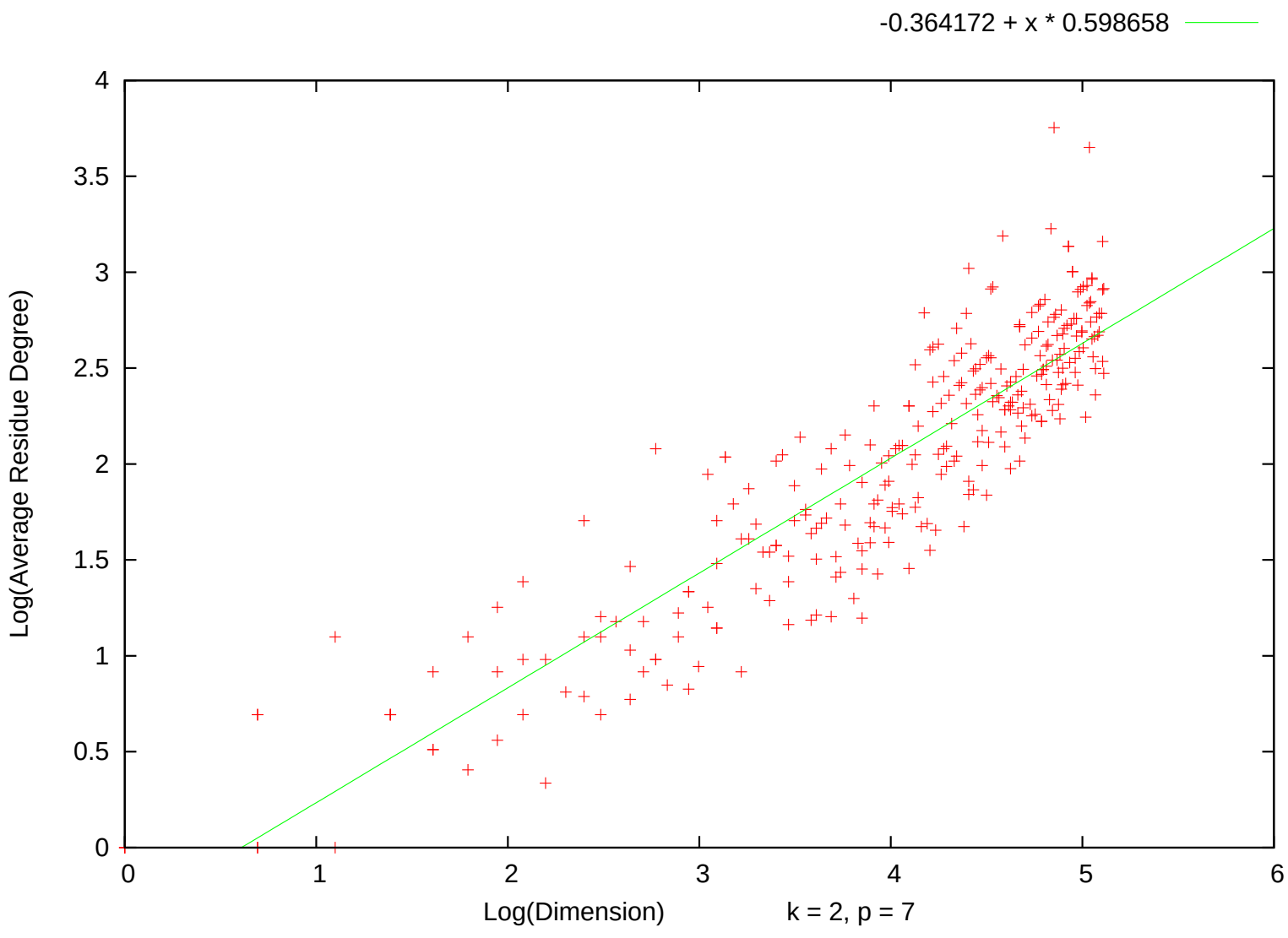
Degrees of coefficient fields



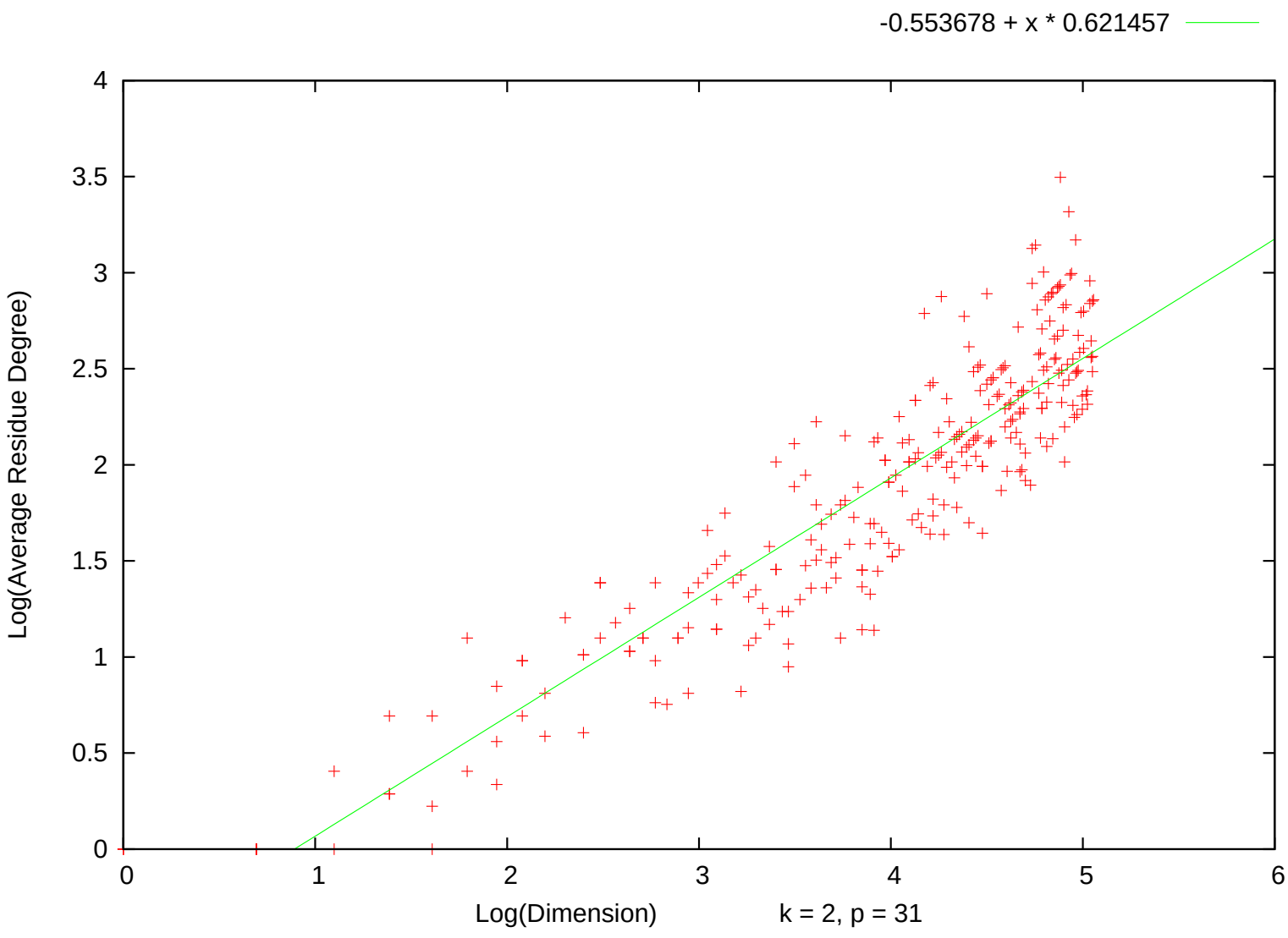
Degrees of coefficient fields



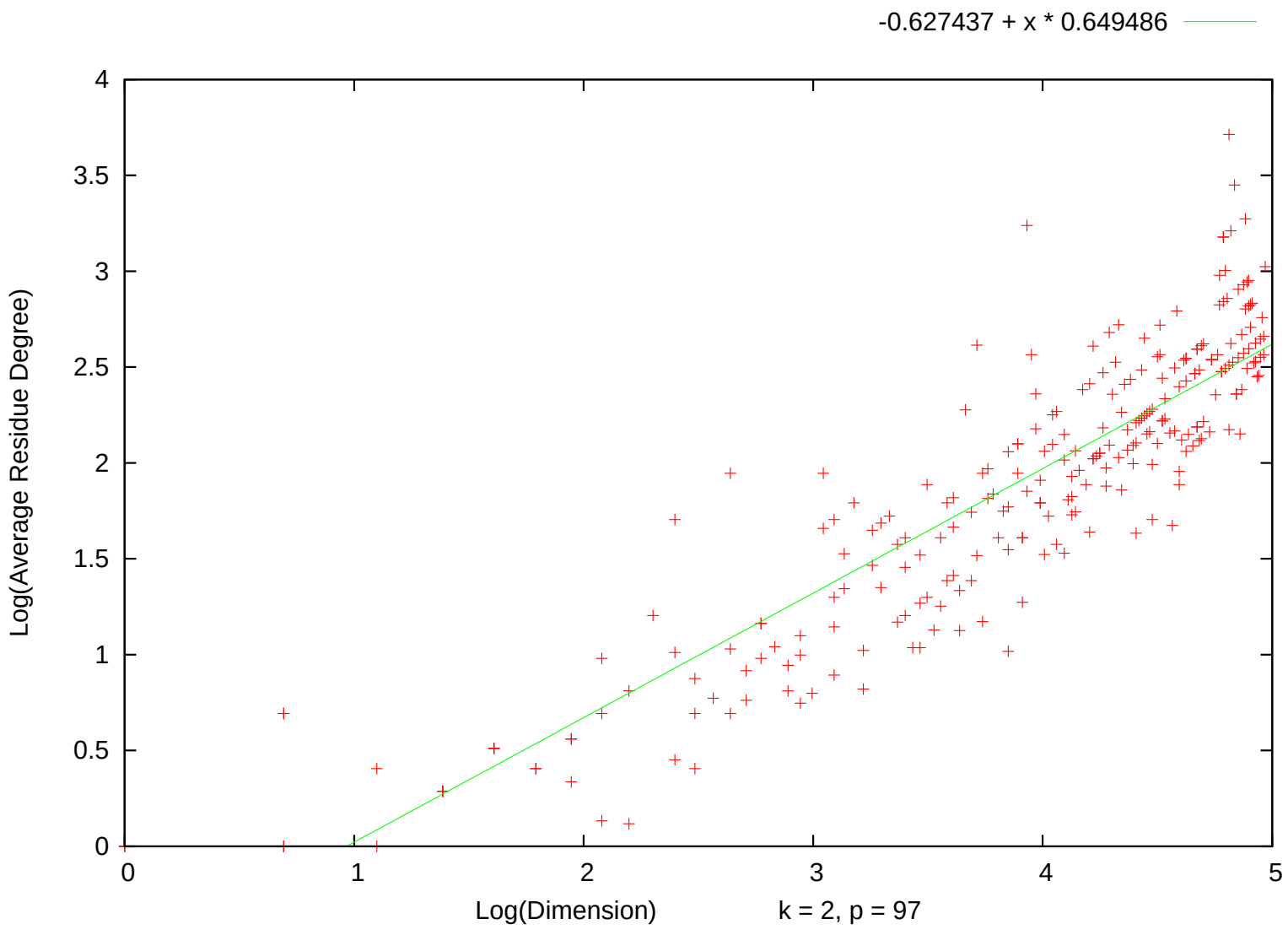
Degrees of coefficient fields



Degrees of coefficient fields



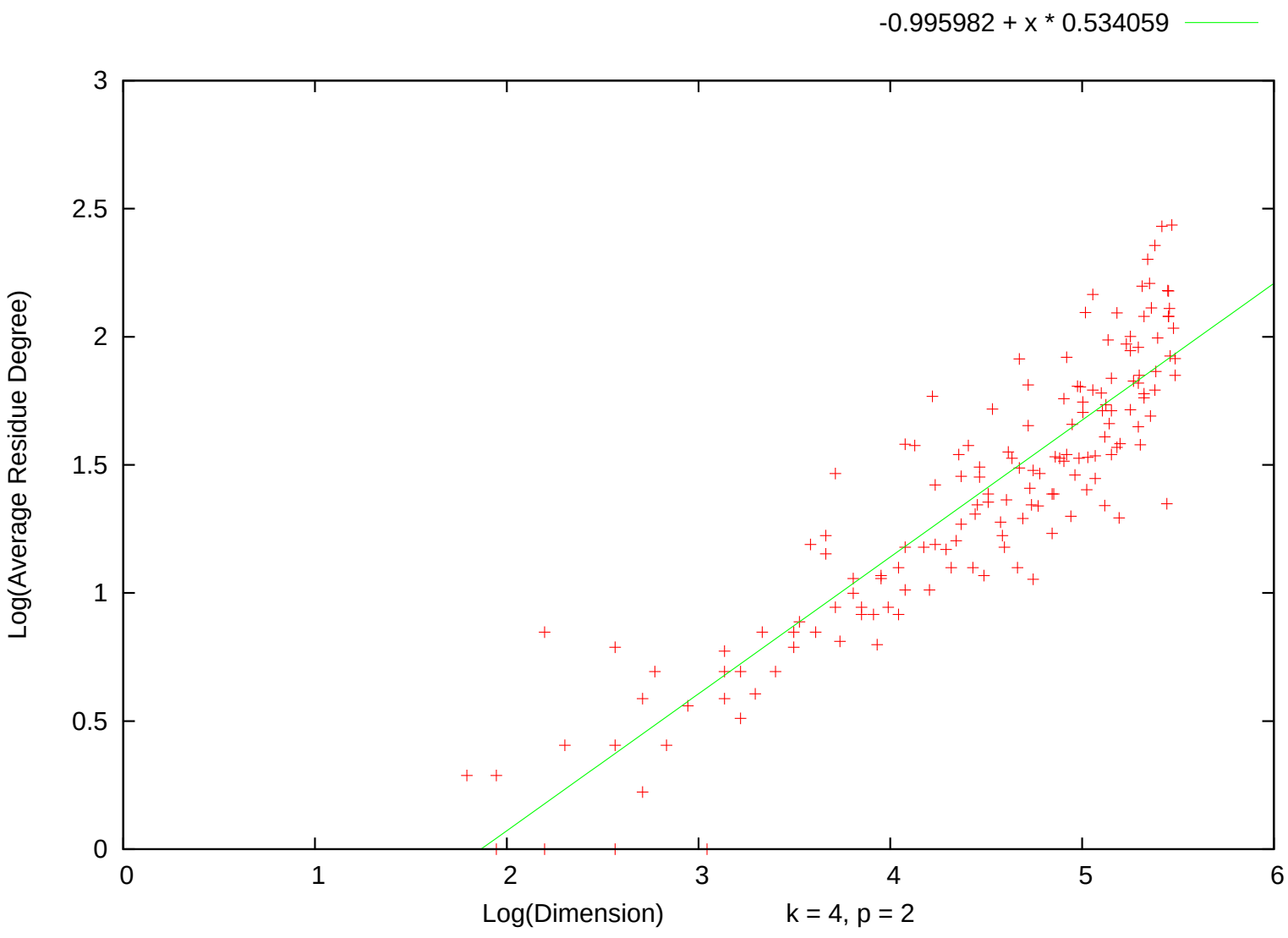
Degrees of coefficient fields



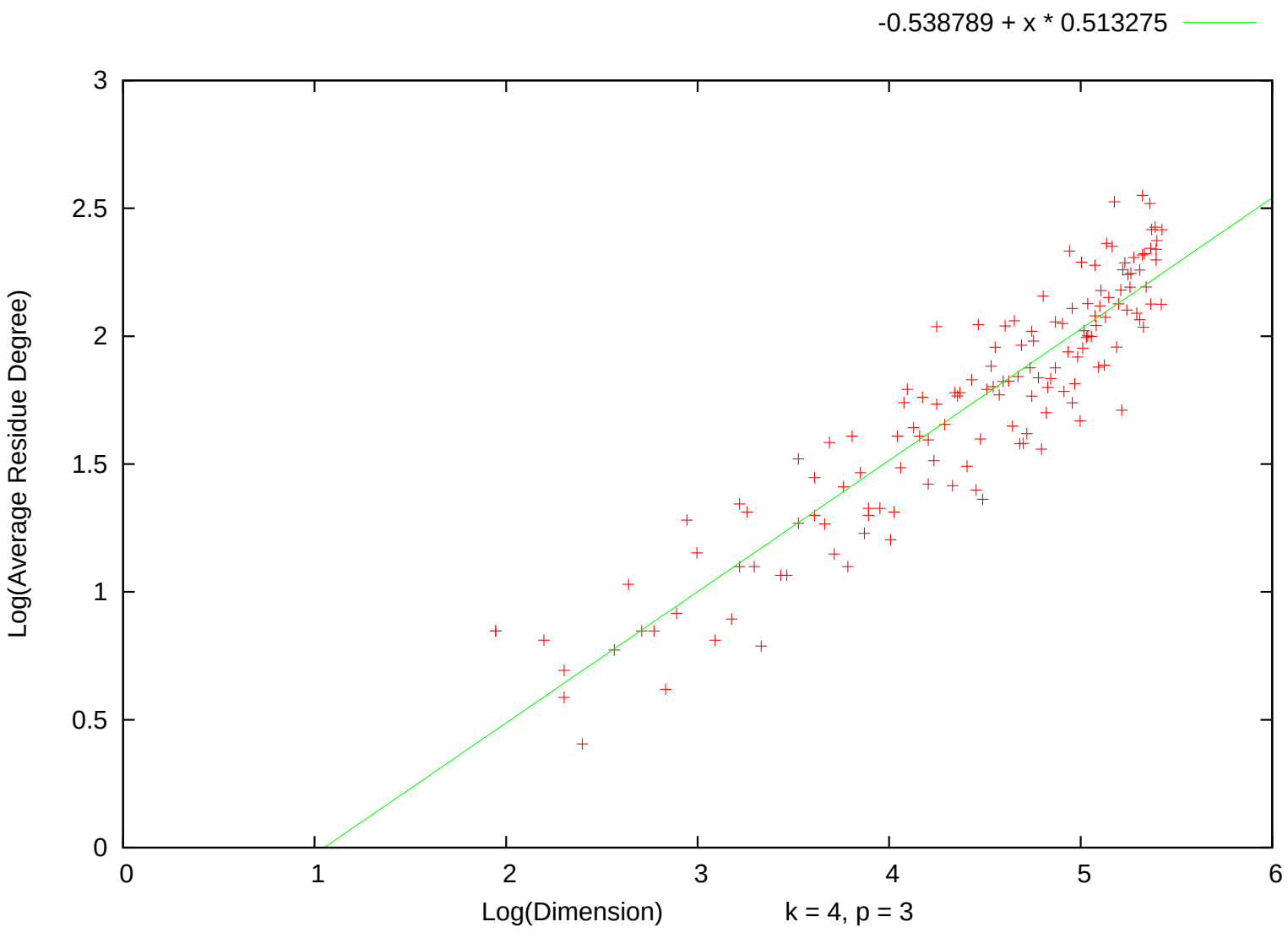
Degrees of coefficient fields

Now $k = 4$.

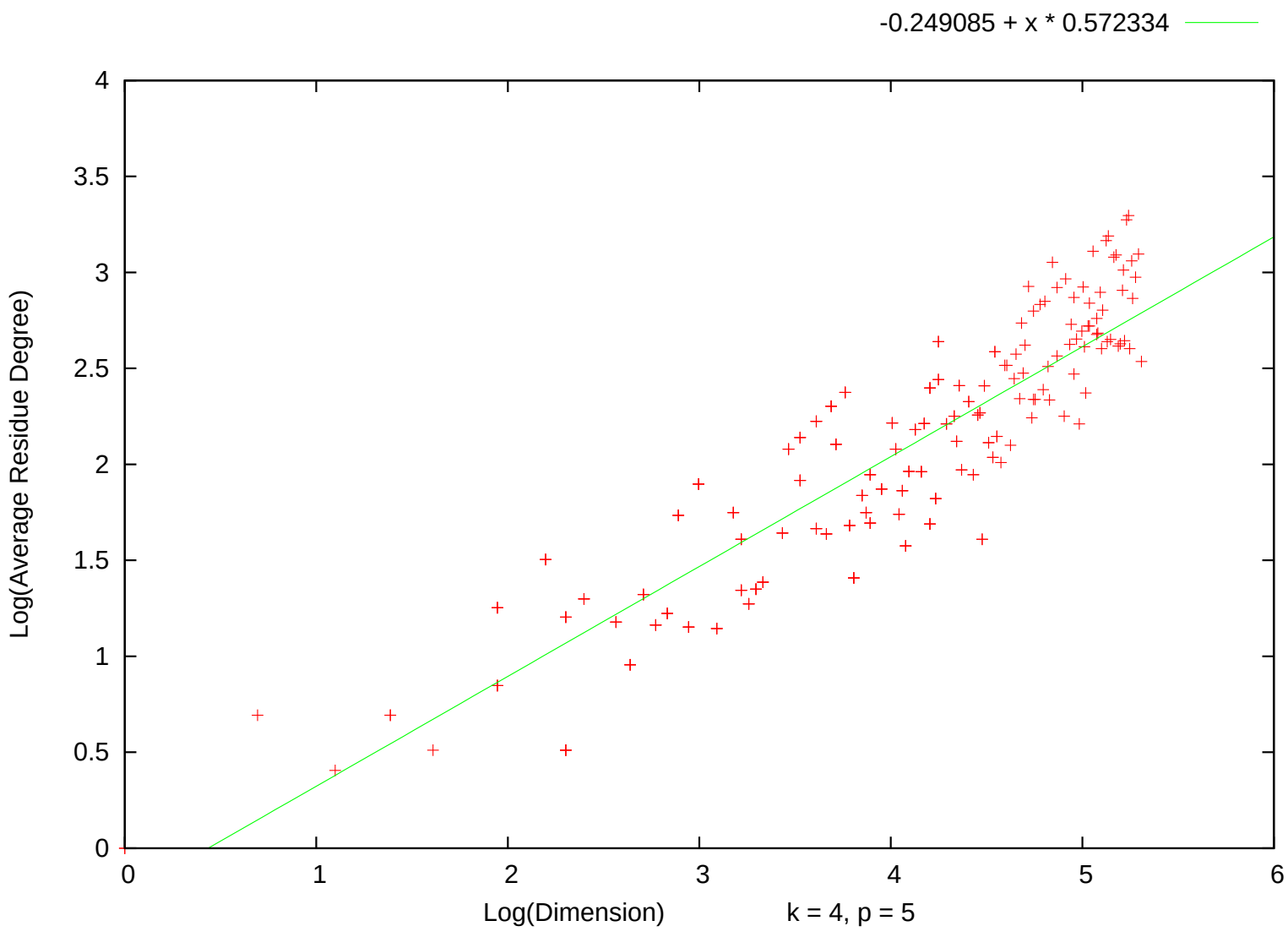
Degrees of coefficient fields



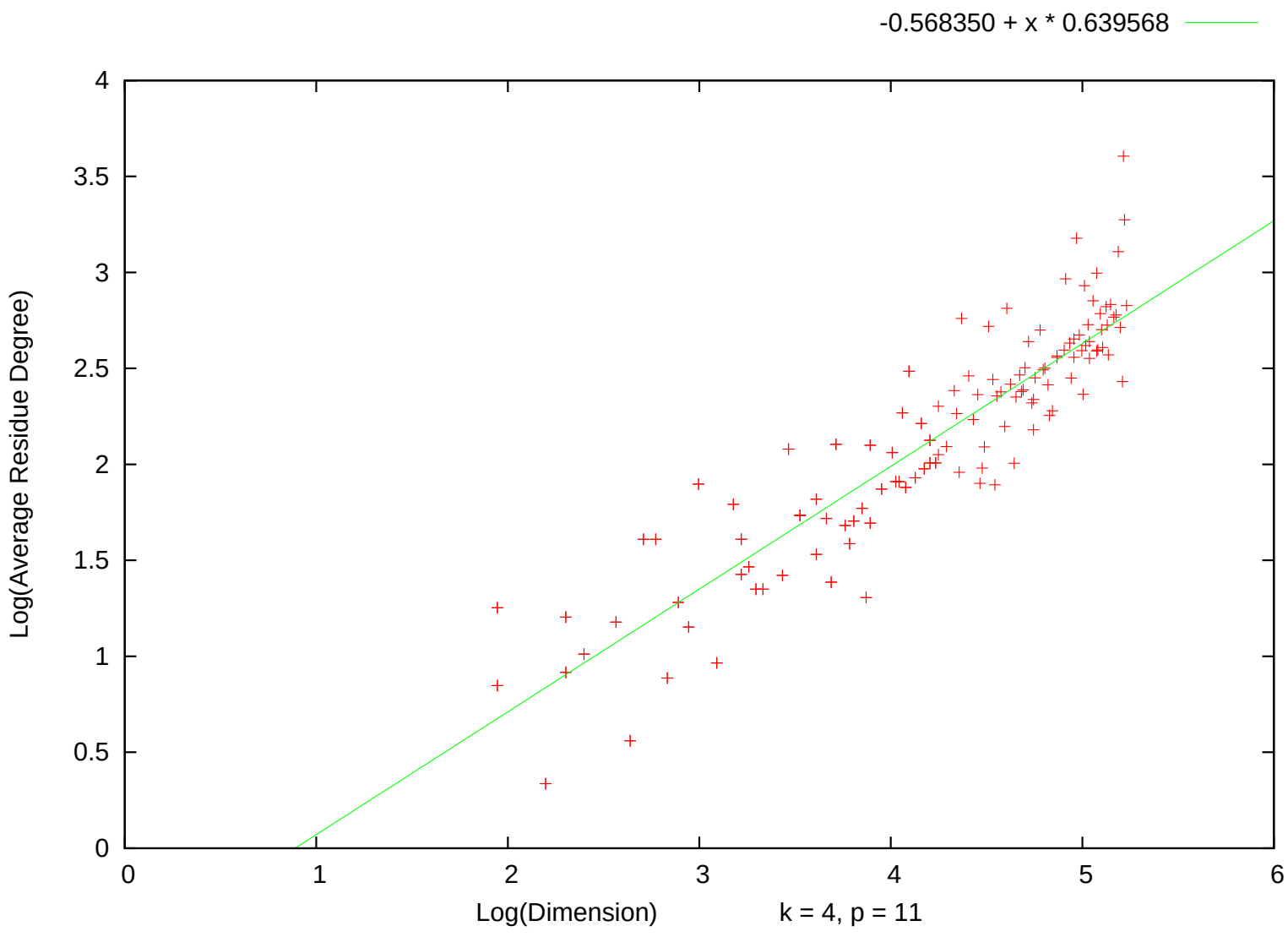
Degrees of coefficient fields



Degrees of coefficient fields



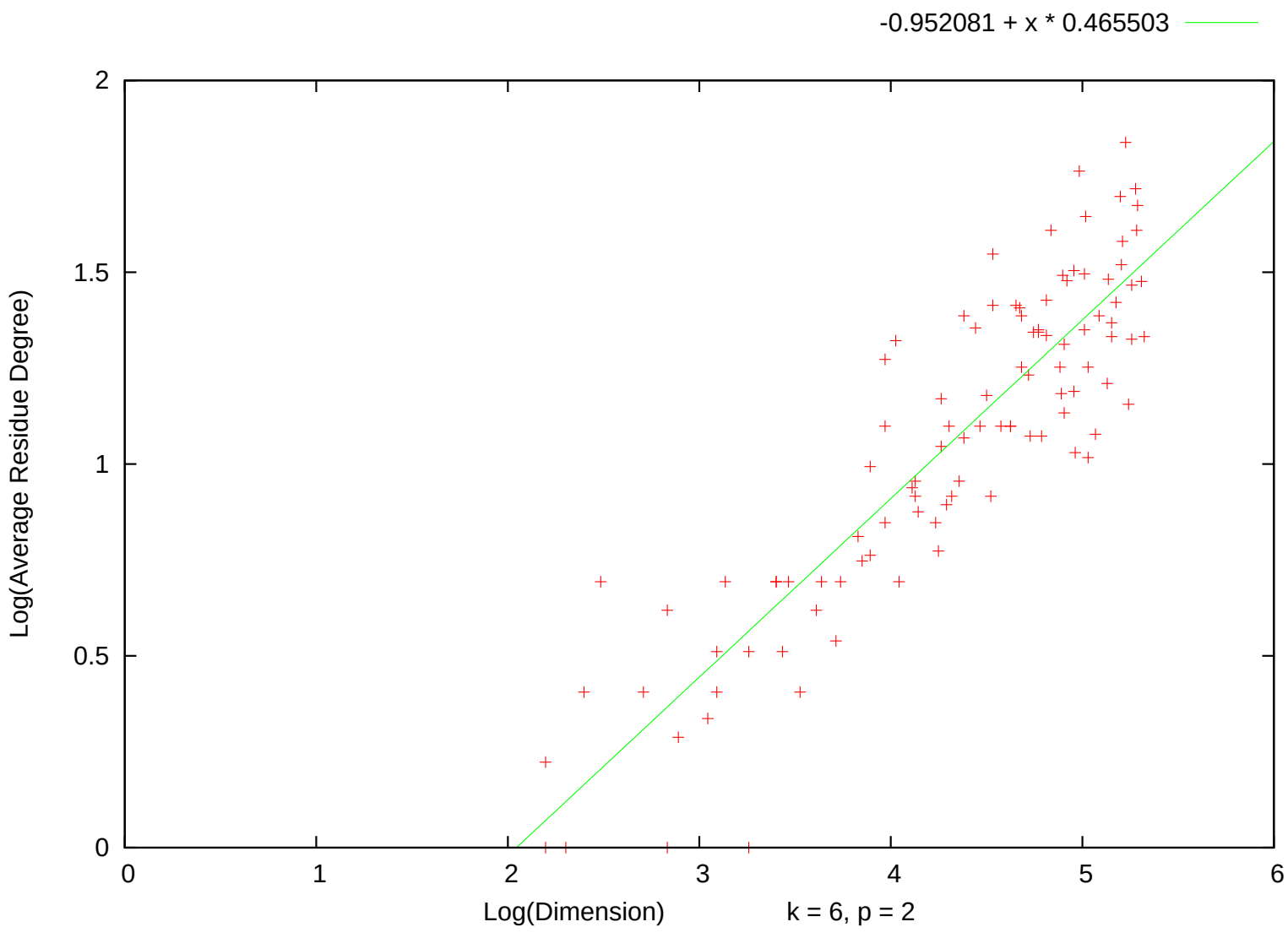
Degrees of coefficient fields



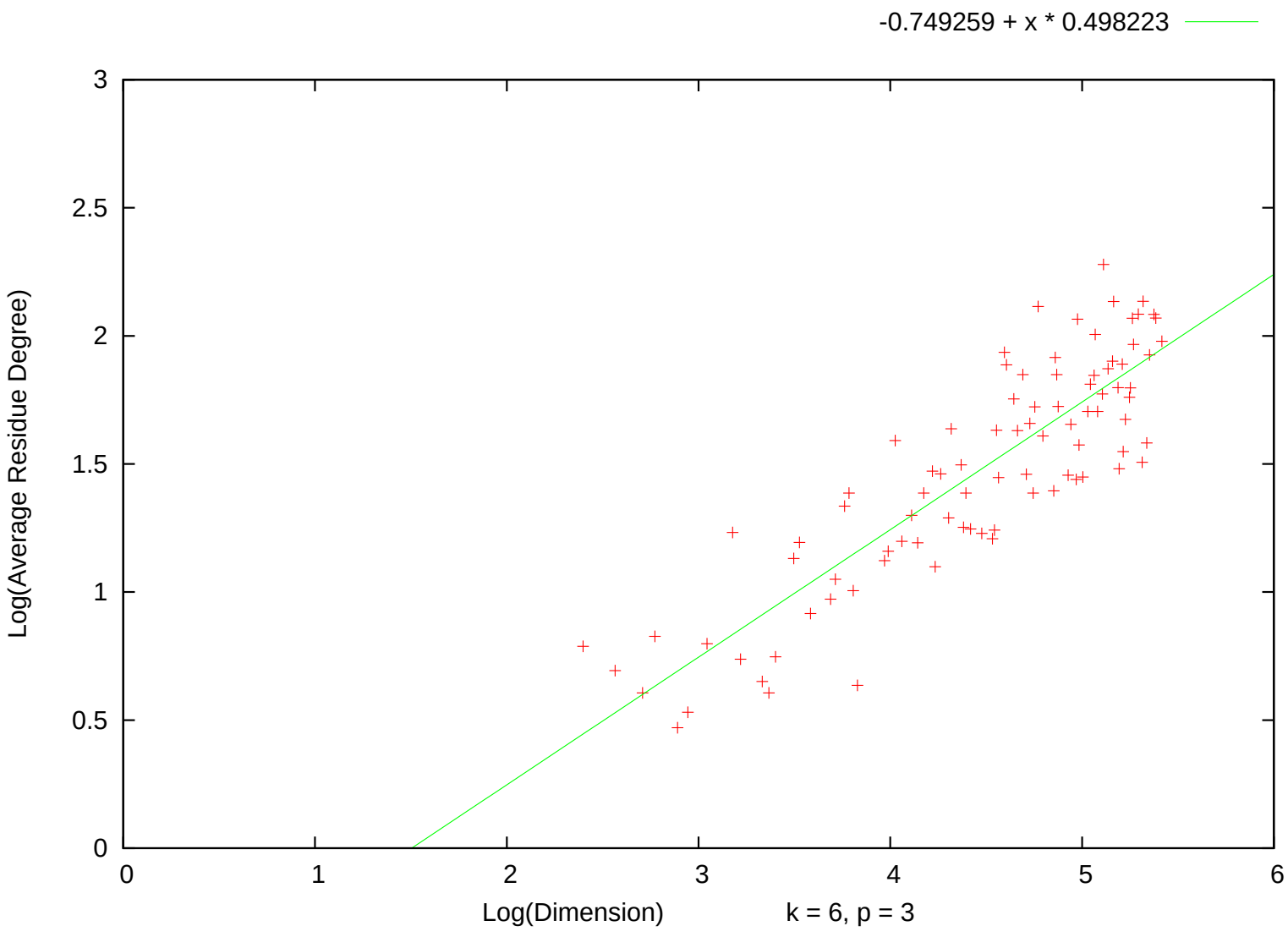
Degrees of coefficient fields

Now $k = 6$.

Degrees of coefficient fields



Degrees of coefficient fields



Degrees of coefficient fields

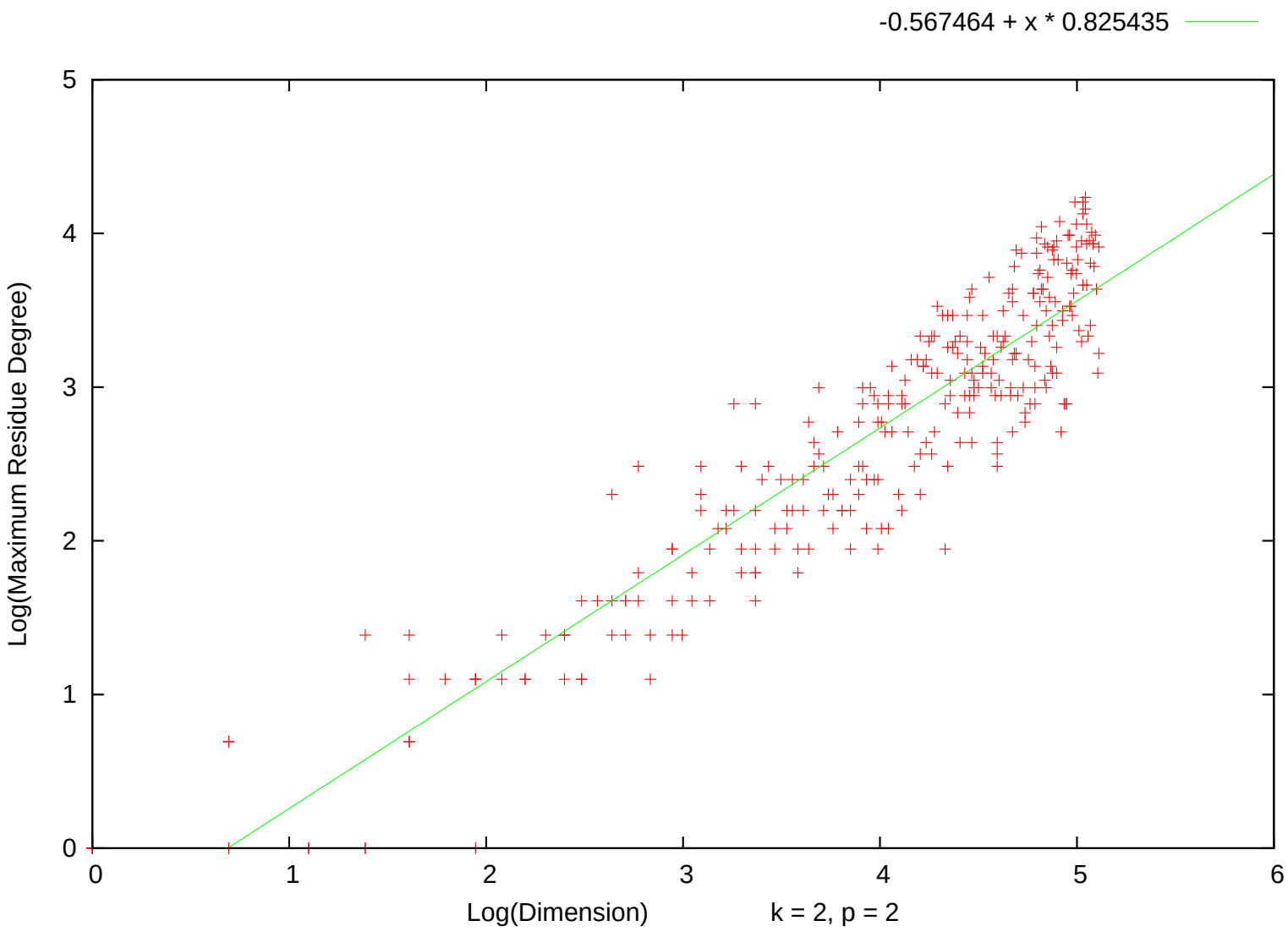
Fix p and $k = 2$.

Guess a dependence of the form

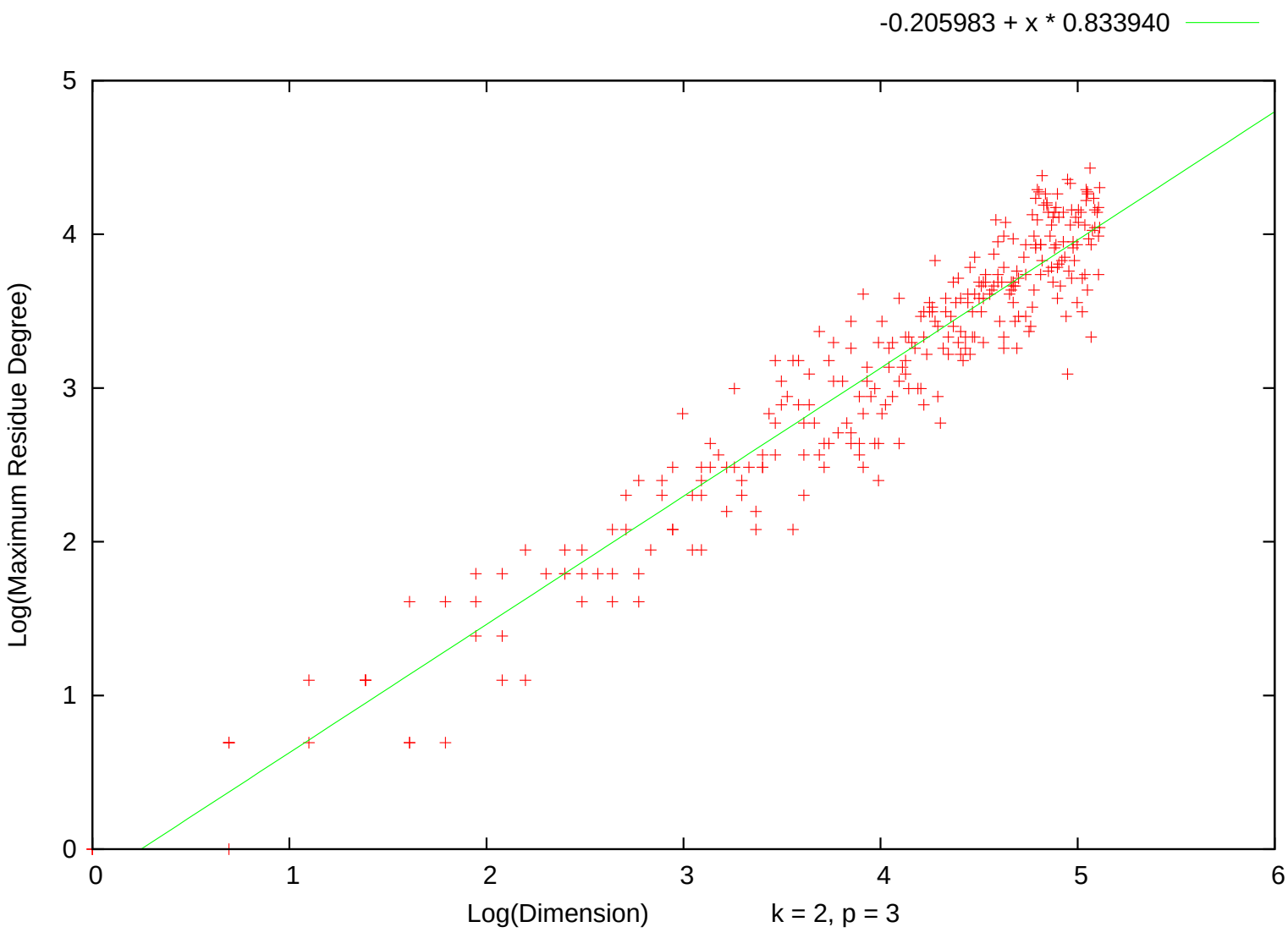
$$\max_k^{(p)}(N) \sim C\big(\dim_k(N)\big)^{\alpha}.$$

Plot $\log(\max_k^{(p)}(N))$ as a function of $\log(\dim_k(N))$ for the primes $N \leq 2000$.

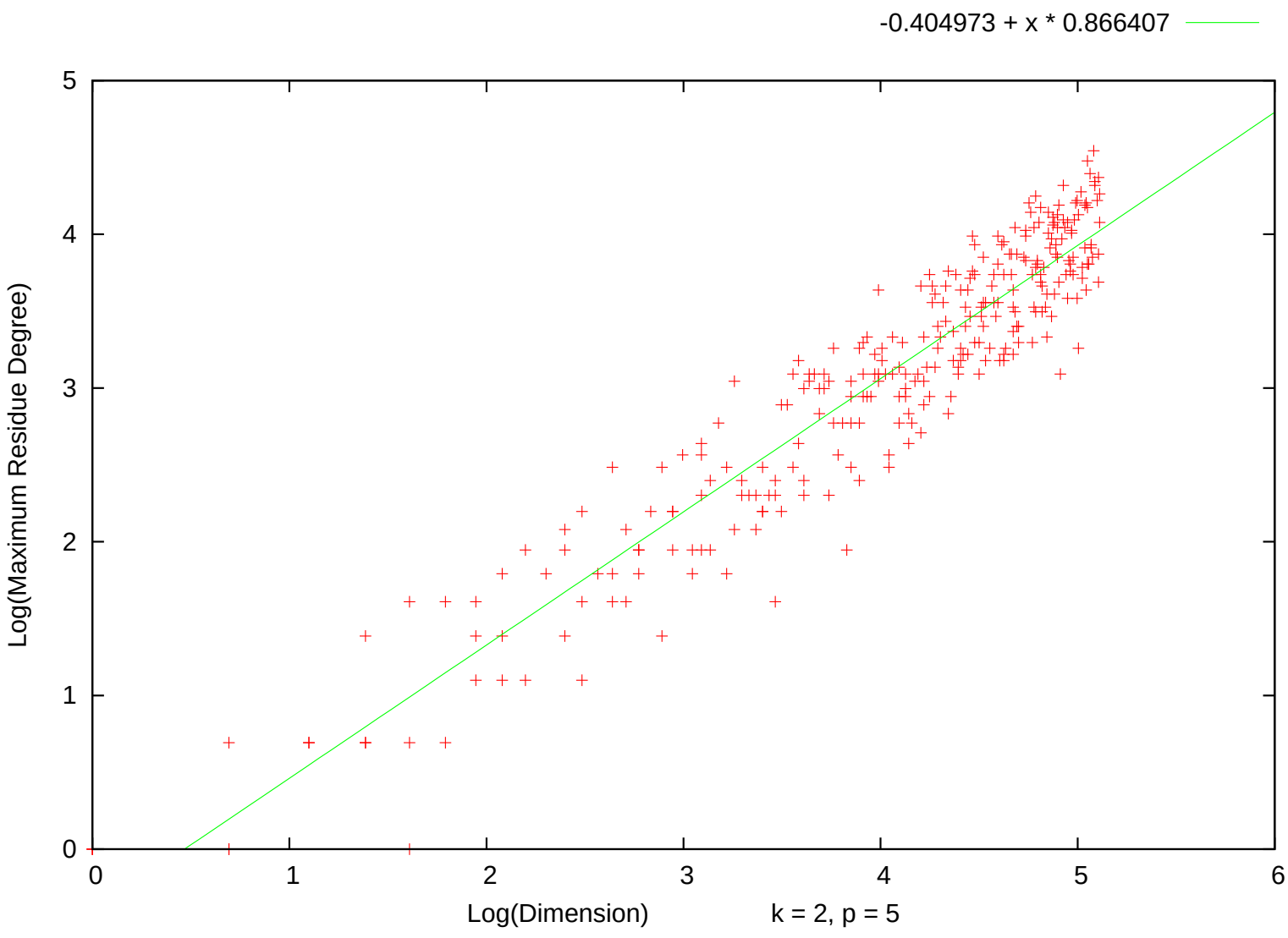
Degrees of coefficient fields



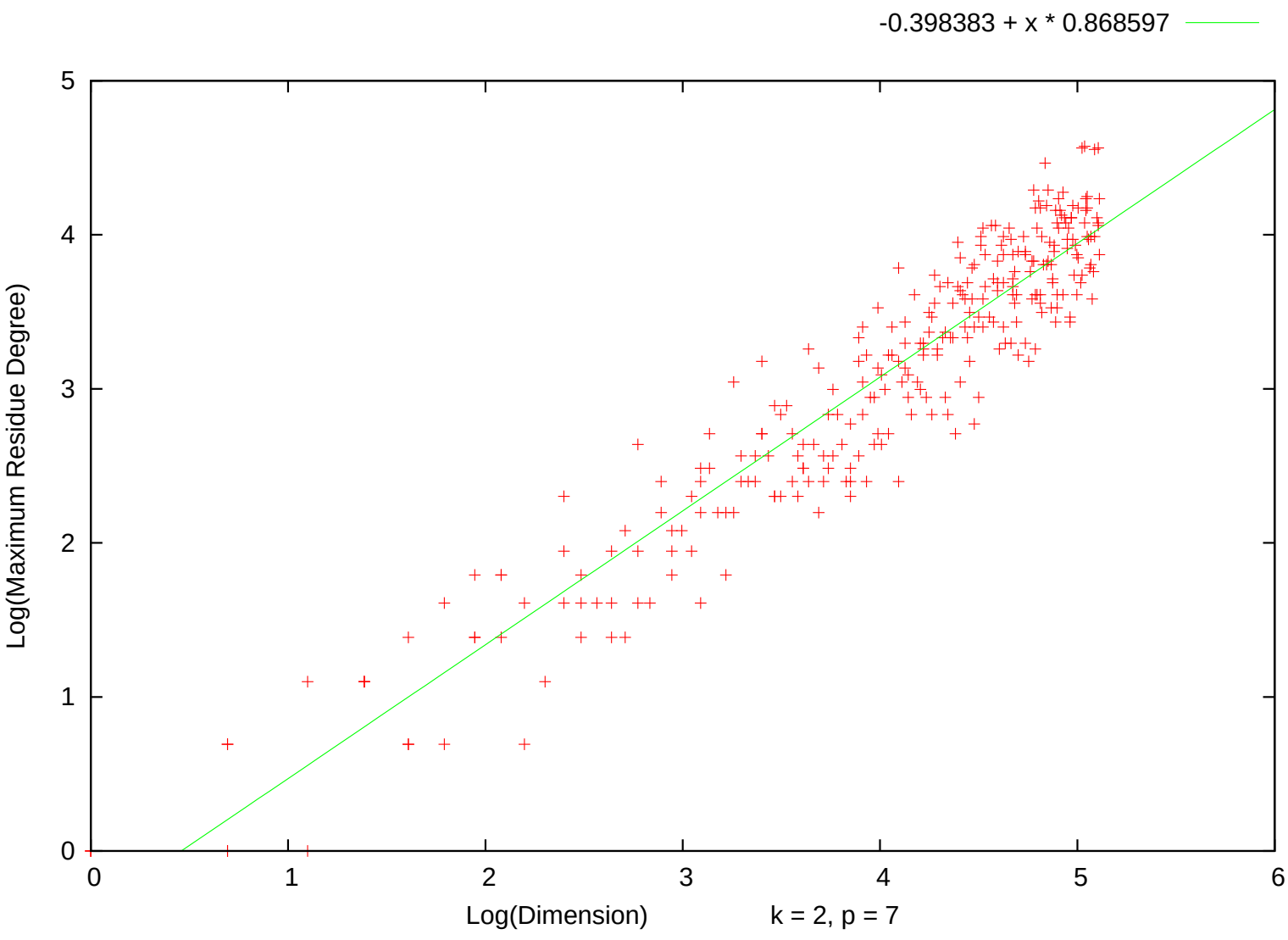
Degrees of coefficient fields



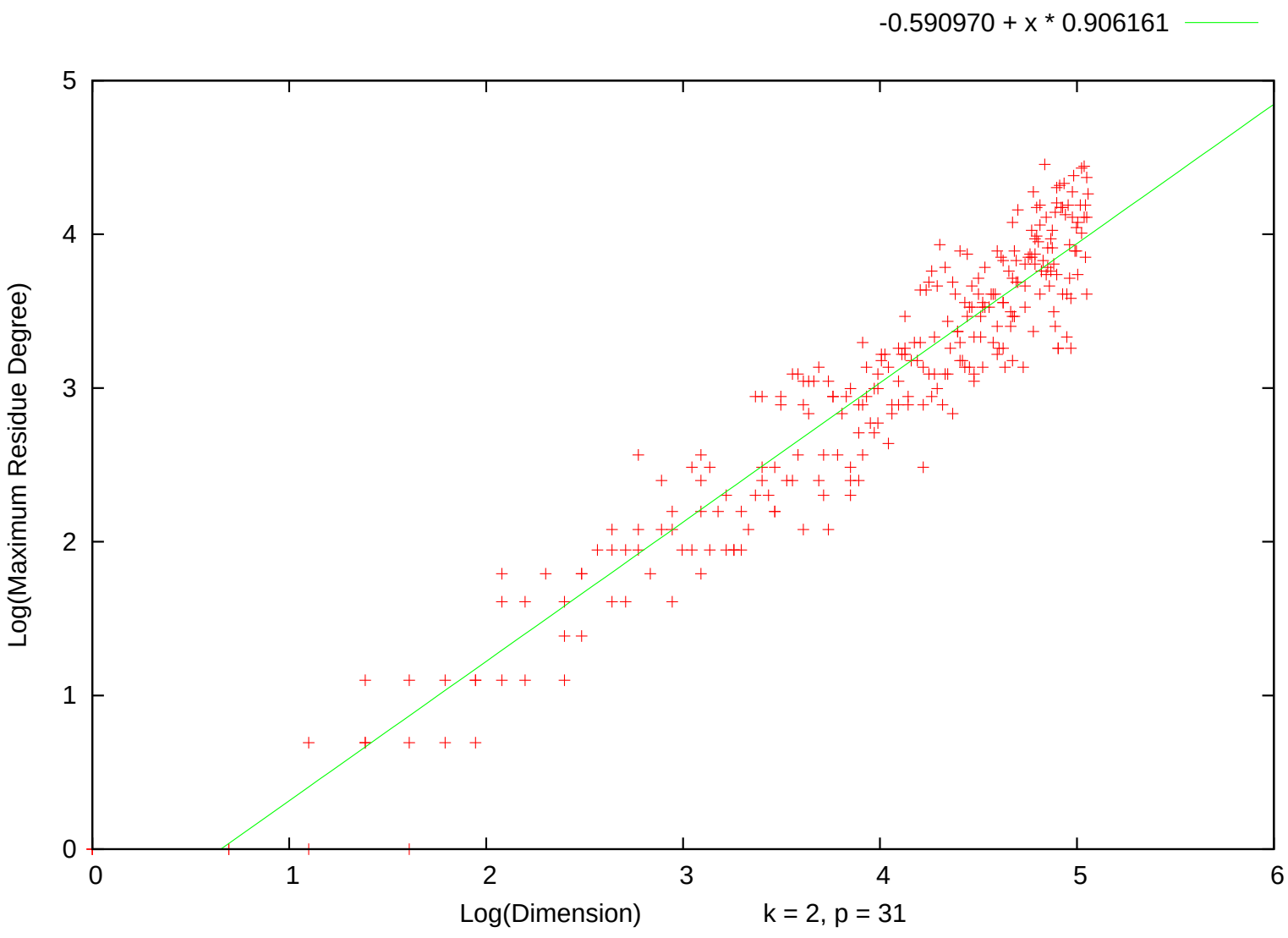
Degrees of coefficient fields



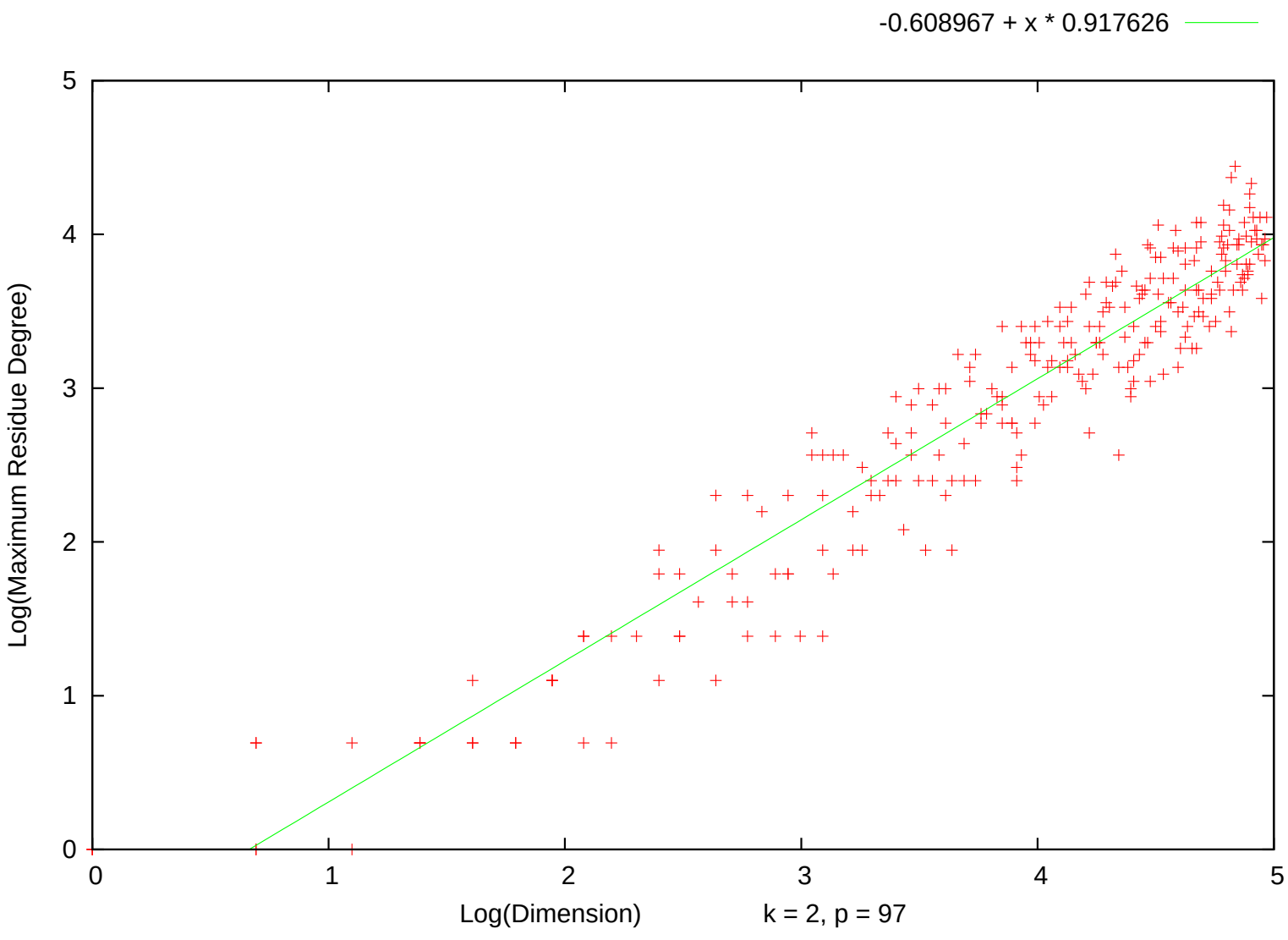
Degrees of coefficient fields



Degrees of coefficient fields



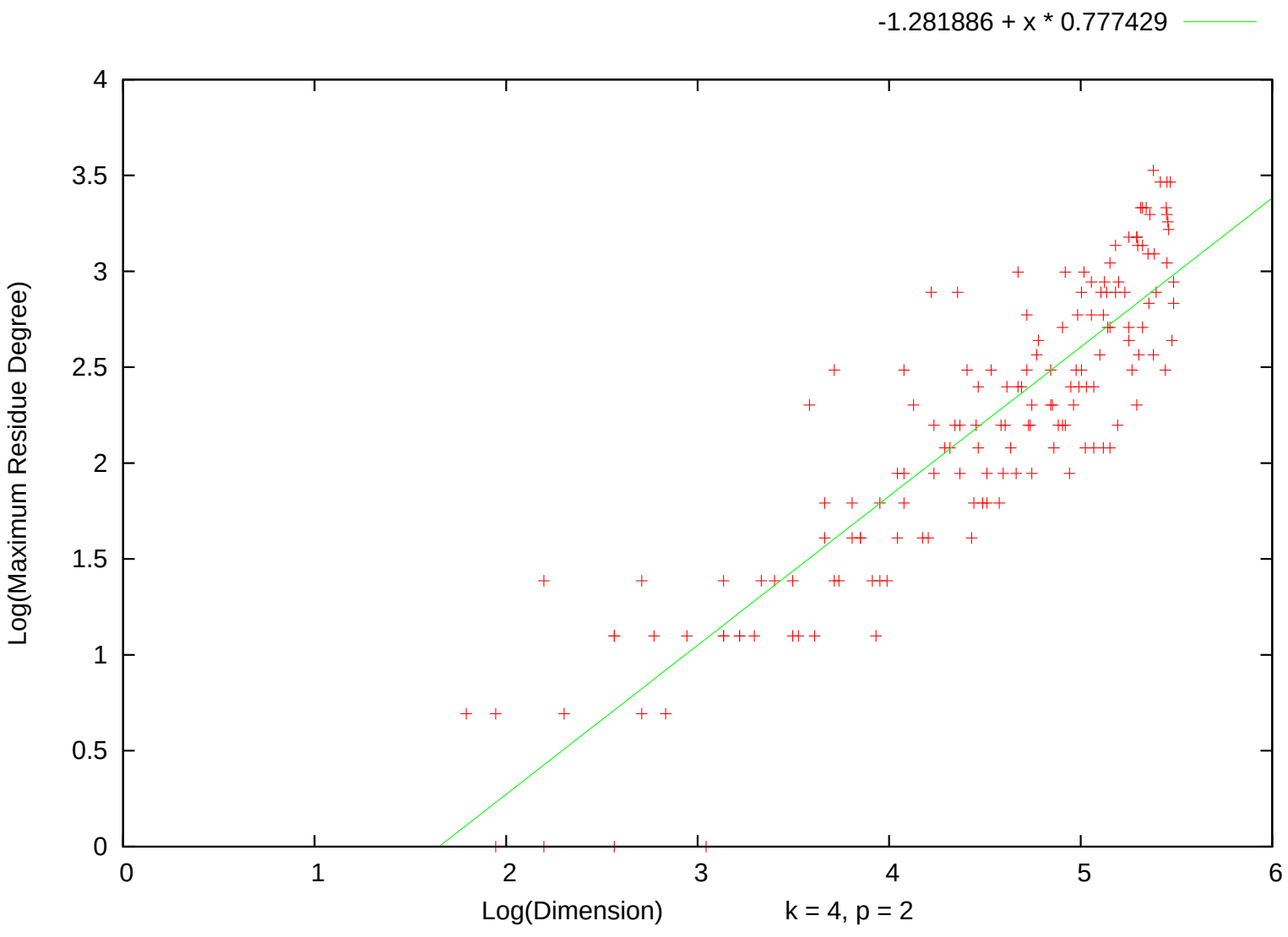
Degrees of coefficient fields



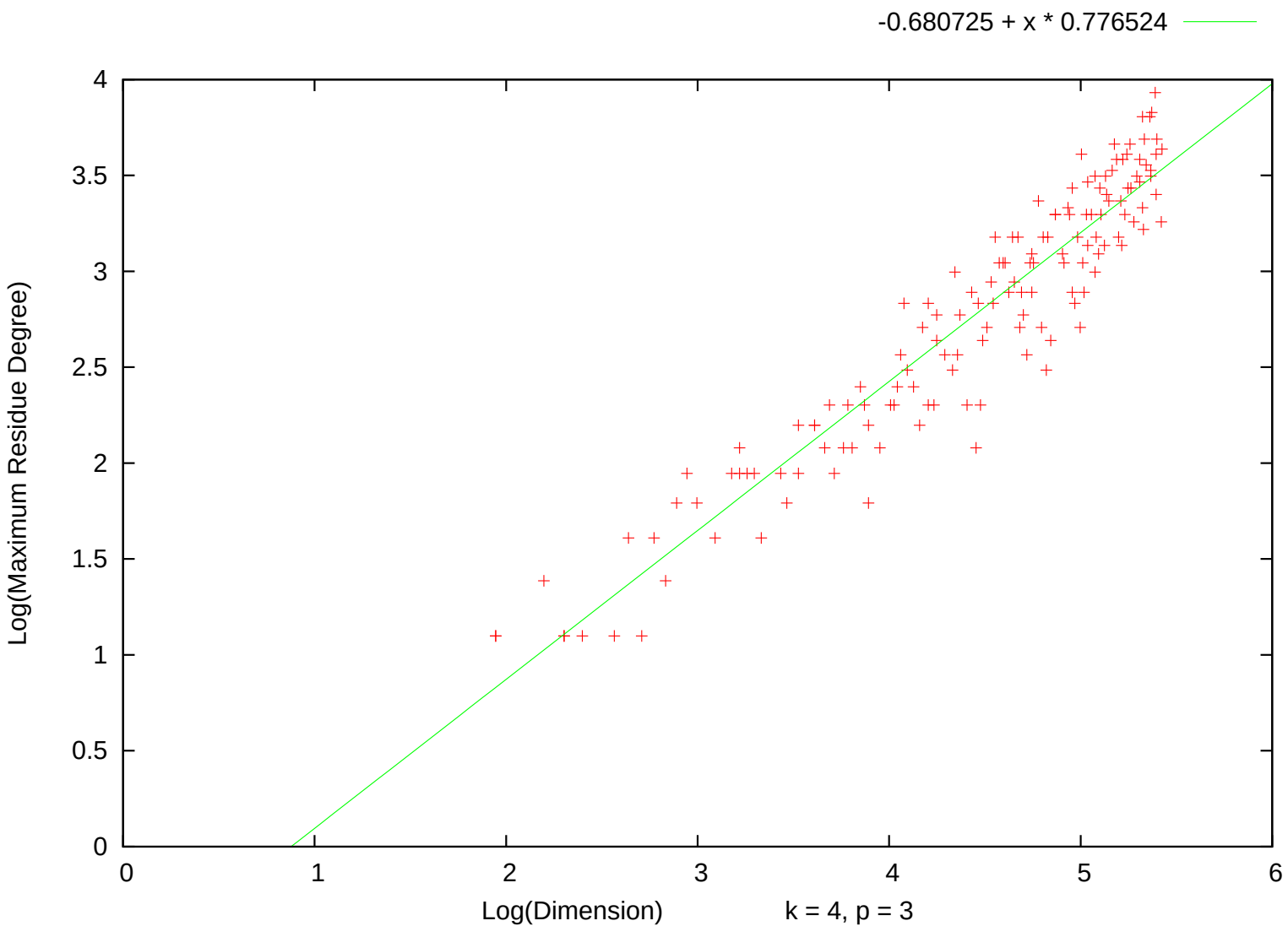
Degrees of coefficient fields

Now $k = 4$.

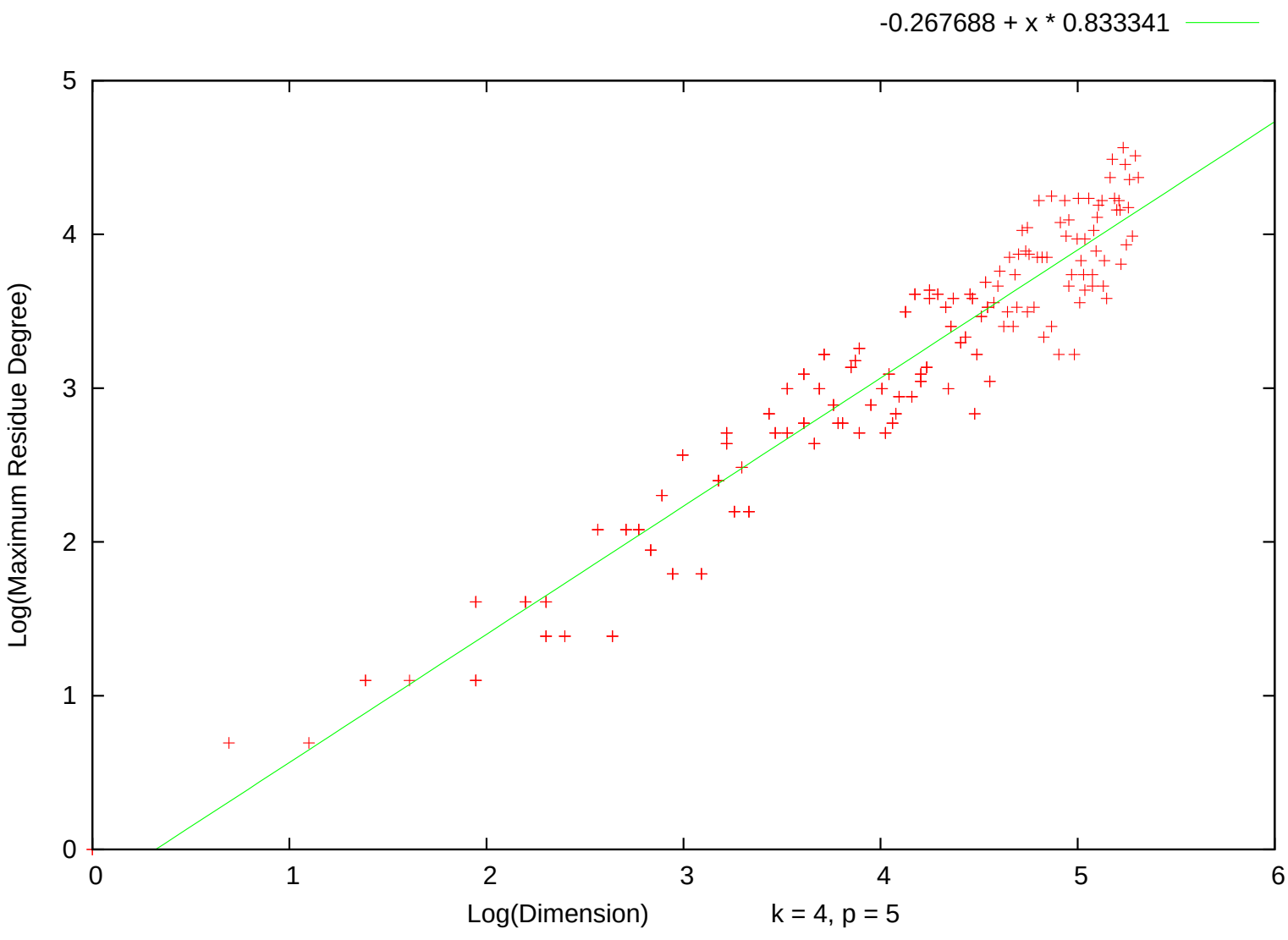
Degrees of coefficient fields



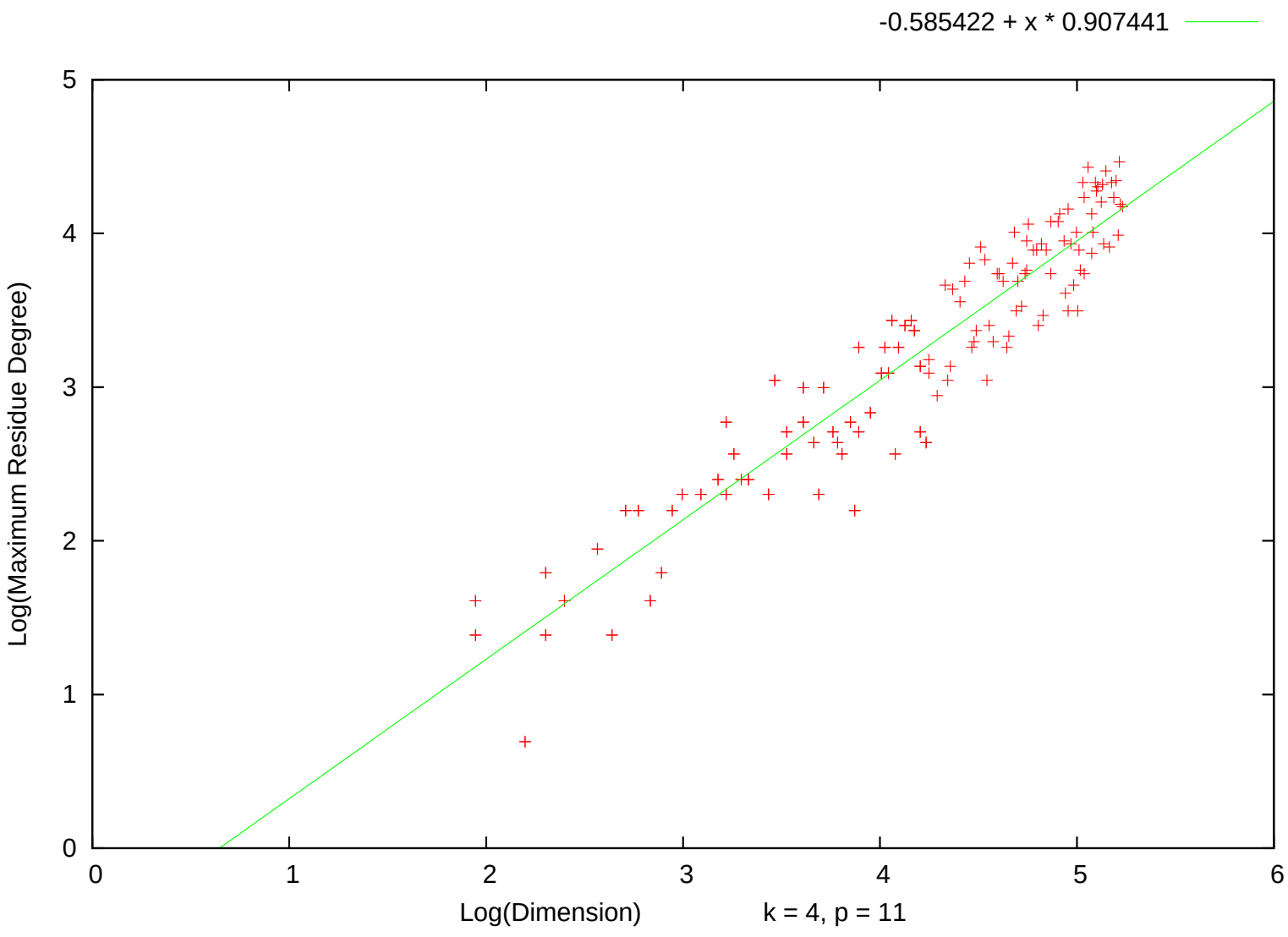
Degrees of coefficient fields



Degrees of coefficient fields



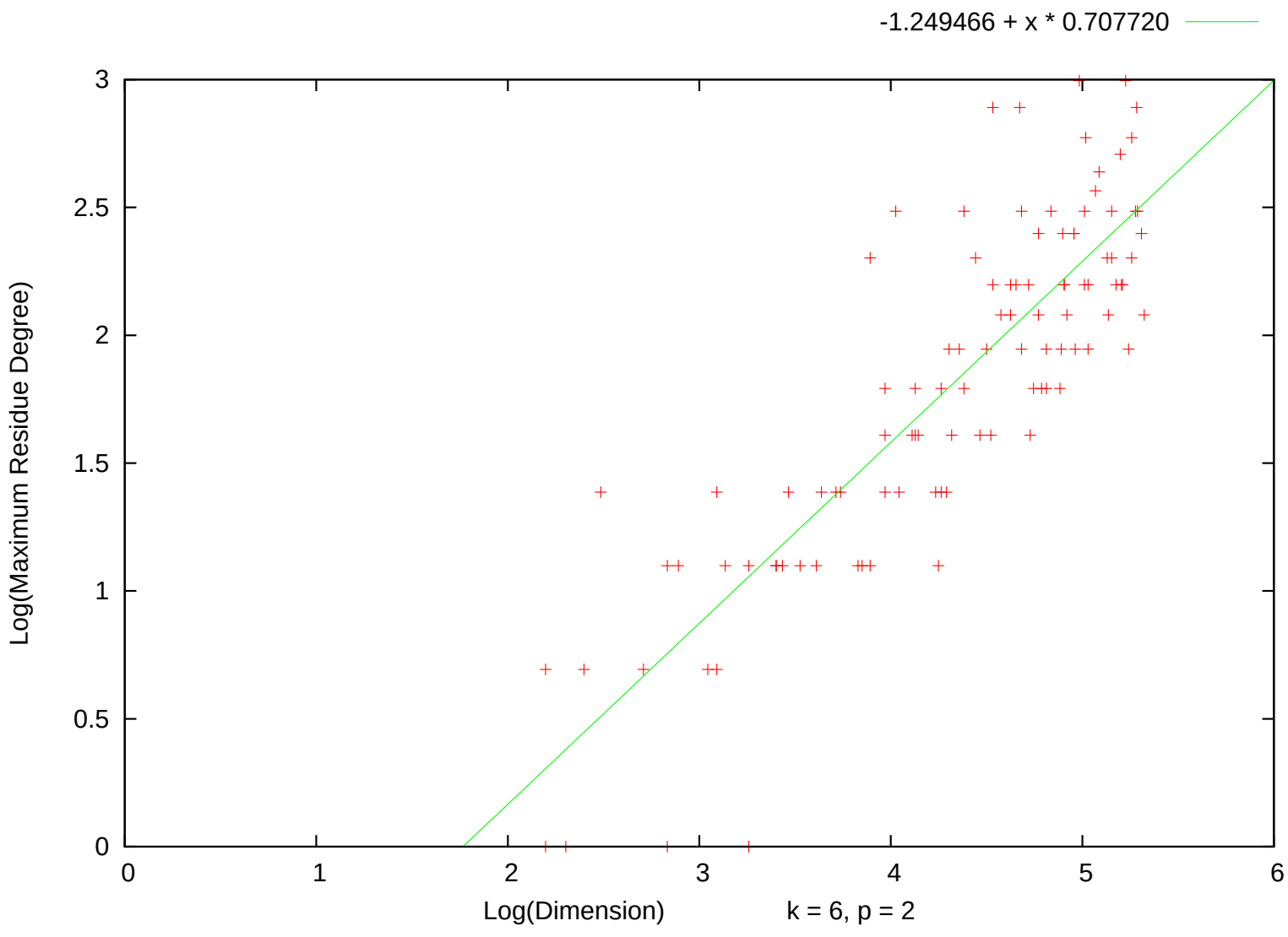
Degrees of coefficient fields



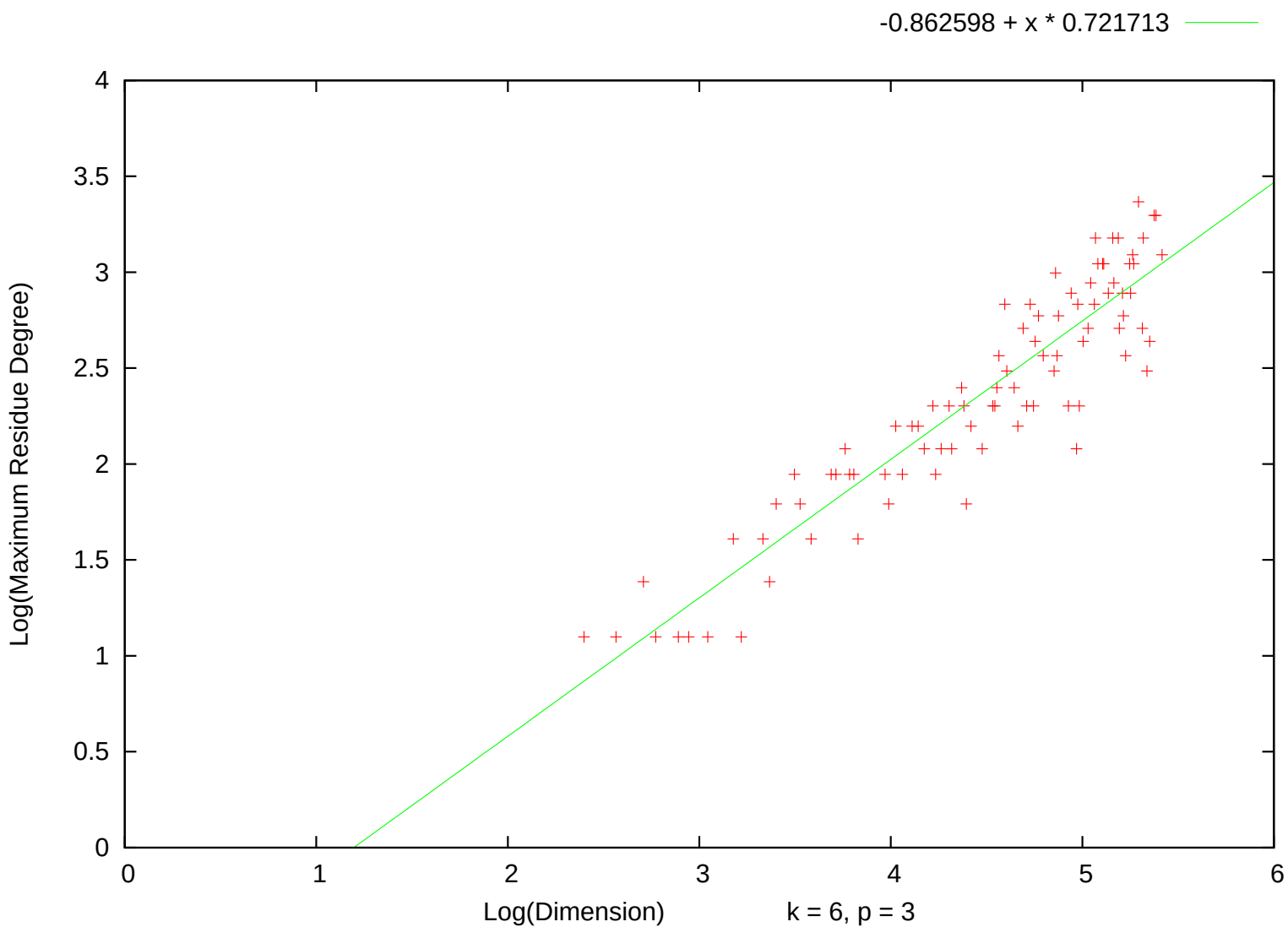
Degrees of coefficient fields

Now $k = 6$.

Degrees of coefficient fields



Degrees of coefficient fields



Degrees of coefficient fields

Question: *Fix p and the weight $k \geq 2$.*

Are there $0 < \alpha \leq \beta < 1$ and $C, D > 0$ s.t.

$$D \dim_k(N)^\beta \geq \text{average}_k^{(p)}(N) \geq C \dim_k(N)^\alpha \quad ?$$

Degrees of coefficient fields

Question: *Fix p and the weight $k \geq 2$.*

Are there $0 < \alpha \leq \beta < 1$ and $C, D > 0$ s.t.

$$D \dim_k(N)^\beta \geq \text{average}_k^{(p)}(N) \geq C \dim_k(N)^\alpha \quad ?$$

Question: *Fix p and the weight $k \geq 2$.*

Are there $0 < \alpha \leq \beta < 1$ and $C, D > 0$ s.t.

$$D \dim_k(N)^\beta \geq \max_k^{(p)}(N) \geq C \dim_k(N)^\alpha \quad ?$$

Now the Wiki!