Galois groups in generalisation of Maedas conjecture

This note is a continuation and suggested improvement concerning the student projects under the name *Galois groups in generalisation of Maeda's conjencture* written by Valnea Skansi and Lucija Calic.

1 Improvement on the range of primes

First of all, we would like to improve the bound we previously set (10 000) and determine how many prime numbers we have to test until we find cycles of the required type. A word on notation: we will use the notation $(2, odd)$-cycles to represent the factorisation that consists of one transposition and all the other cycles are of odd order. Let us recall, in order to verify we have a symmetric group we must find a $(2, odd)$-cycle and an $(n-1)$-cycle. The *Chebotarev's density theorem* tells us that the factorisation types are equidistributed. This means that we know that there are m k-cycles in S_n, we expect to find a k-cycle every $\frac{n!}{m}$-th time, i.e. if we test a primes, we expect to encounter $(a \cdot \frac{m}{n!})$ k-cycles.

So, let us first look at how many $(n-1)$-cycles are there in S_n. The answer is $n \cdot (n-2)!$, as we have n choices of the missing element, and for each of those choices, there are $(n-2)!$ different $(n-1)$-cycles. Thus, the proportion of $(n-1)$-cycles is $\frac{n \cdot (n-2)!}{n!} = \frac{1}{n-1}$.

The calculation is a little bit more difficult for the case of $(2, odd)$-cycles. We know that we can form a transposition in exactly $\frac{n \cdot (n-1)}{2}$ ways. In order to calculate the number of permutations of the set $\{1, ..., n-2\}$ that have cycles of odd length we will use generating functions.

Let $a_C(n)$ denote the number of permutations in S_n whose cycles have lengths in some set C. The following formula holds:

$$\sum_{n=1}^{\infty} a_C(n) \frac{x^n}{n!} = exp\left(\sum_{m \in C} \frac{x^m}{m}\right)$$

If we let C be the set of all odd positive integers, the expression now reads:

$$\sum_{n=1}^{\infty} a_C(n)\frac{x^n}{n!} = exp\left(\sum_{m=0}^{\infty}\frac{x^{2m+1}}{2m+1}\right)$$

Now from that we get:

$$exp\left(\sum_{m=0}^{\infty}\frac{x^{2m+1}}{2m+1}\right) = exp\left(\sum_{m=1}^{\infty}\frac{x^m}{m} - \sum_{m=1}^{\infty}\frac{x^{2m}}{2m}\right)$$

$$= exp\left(\sum_{m=1}^{\infty}\frac{x^m}{m} - \frac{1}{2}\sum_{m=1}^{\infty}\frac{(x^2)^m}{m}\right)$$

$$= exp\left(-log(1-x)) + \frac{1}{2}log(1-x^2)\right) = \frac{1}{1-x}\cdot\left(1-x^2\right)^{\frac{1}{2}}$$

$$= \frac{1}{1-x}\cdot\left(1-x^2\right)^{\frac{1}{2}}\cdot\frac{1+x}{1+x} = \frac{1+x}{\sqrt{1-x^2}}$$

$$= (1+x)\cdot(arcsin(x))' = (1+x)\cdot\left(\sum_{n=0}^{\infty}\frac{(2n)!}{4^n\cdot(n!)^2\cdot(2n+1)}x^{2n+1}\right)'$$

$$= (1+x)\cdot\sum_{n=0}^{\infty}\frac{(2n)!}{4^n\cdot(n!)^2}x^{2n} = \sum_{n=0}^{\infty}\frac{(2n)!}{4^n\cdot(n!)^2}(x^{2n}+x^{2n+1})$$

$$= \sum_{n=0}^{\infty}\frac{((2n)!)^2}{4^n\cdot(n!)^2}\frac{x^{2n}}{(2n)!} + \frac{(2n)!\cdot(2n+1)!}{4^n\cdot(n!)^2}\frac{x^{2n+1}}{(2n+1)!}$$

From this it follows that the a_k we were looking for is $\frac{((k)!)^2}{2^k\cdot((k/2)!)^2}$ for even k and $\frac{(k-1)!\cdot(k)!}{2^{(k-1)}\cdot(((k-1)/2)!)^2}$ for odd k.

Since we are trying to find a bound for the number of primes, we will take the smaller value, and that is the value for even k so from now on we will use that expression. Because of the two elements from the set $\{1,...,n\}$ form a transposition, we are actually looking for the expression :

$$a_{n-2} = \frac{((n-2)!)^2}{2^{n-2}\cdot((n-2)/2)!)^2}$$

Finally, the number of $(2, odd)$-cycles in S_n is

$$\frac{((n-2)!)^2}{2^{n-2}\cdot((n-2)/2)!)^2}\cdot\frac{n(n-1)}{2}$$

$$= \frac{(n-2)!n!}{2^{n-1} \cdot ((n-2)/2)!)^2},$$

so the proportion of $(2, odd)$-cycles is

$$\frac{(n-2)!}{2^{n-1} \cdot ((n-2)/2)!)^2}.$$

Now, for every n we encounter as a polynomial degree, we will calculate a value denoted in our code as y, which is the maximum between the inverses of proportion of $(n-1)$-cycles and the proportion of $(2, odd)$-cycles. Then, for the value R that is input (or 0.1 by default), we compute for how many prime numbers we have to take into consideration in order to be able to claim that the conjecture is false, with varying confidence, in case the required cycle types are not found.The number of primes we do the calculations for is determined as $q = \frac{100}{R} \cdot \lceil y \rceil$. We then input that value into a function that returns the q-th prime and obtain the range of integers r we will go through.

Remark: in the code, the symbol q was not used explicitly.

2 Results and graphic representation

There is a table of the square-free levels up to 100 and the maximum weights found by our program. As it is visible from the table, as the level increases, the weight gets smaller. Our algorithm stops looking for the maximum weight if $k > 20$ and there are no polynomials generated by the programme.

N	1	2	3	5	6	7	10	11	13	14	15	17	19
k	434	434	386	236	166	100	100	100	88	100	100	72	66

N	21	22	23	26	29	30	31	33	34	35	37	38	39	41-97
k	58	58	56	56	46	92	40	40	40	40	38	38	38	10

Furthermore, we have graphically presented our findings for the maximum, minimum and average primes, where the x-axis represents the degree of the polynomial and the y-axis is max/min/average prime for that degree. Also, we present the graphs of sample sizes, i.e. for a certain degree, the number of primes that generate result 'true' for a polynomial of that degree we encountered. The term 'first prime' represents the prime for which the (n-1)-cycle was found and the term 'second prime' is the prime for which a (2,odd)-cycle was found. The results are the following:

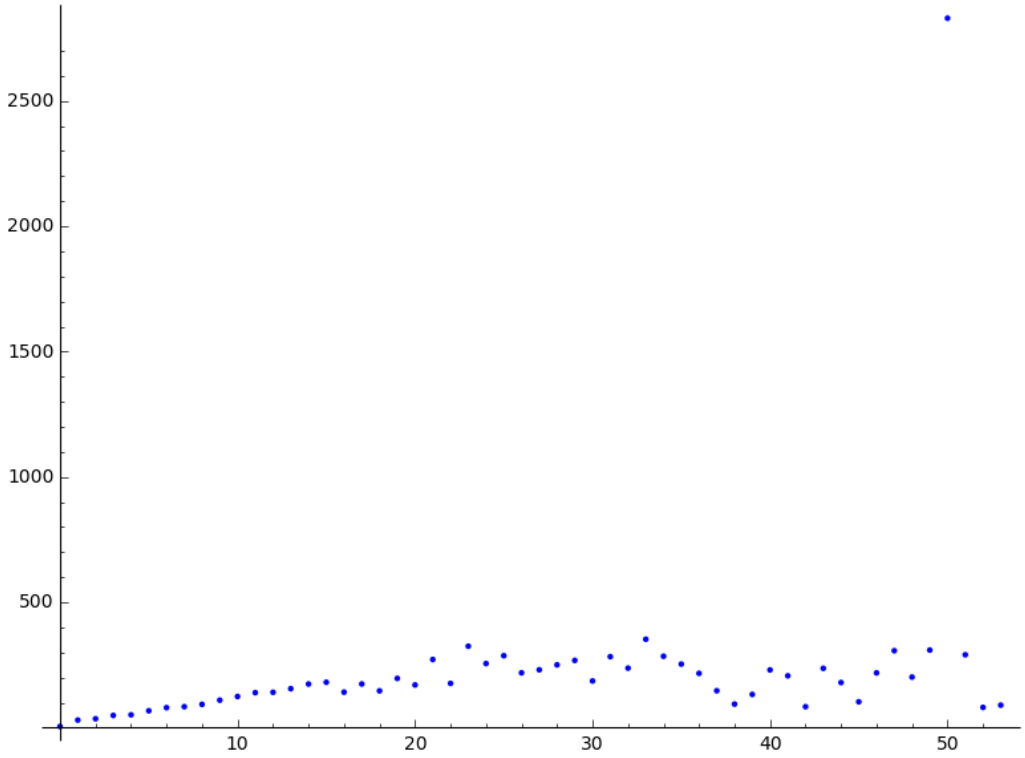

Figure 1: Average of the primes

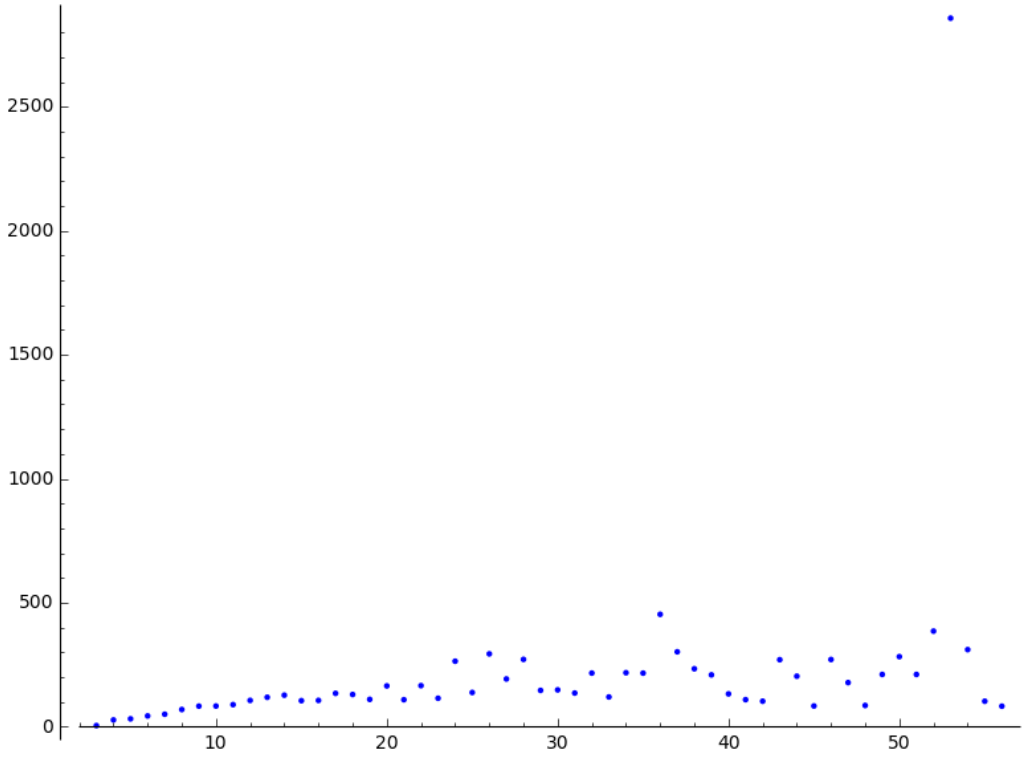

Figure 2: Average of the first primes

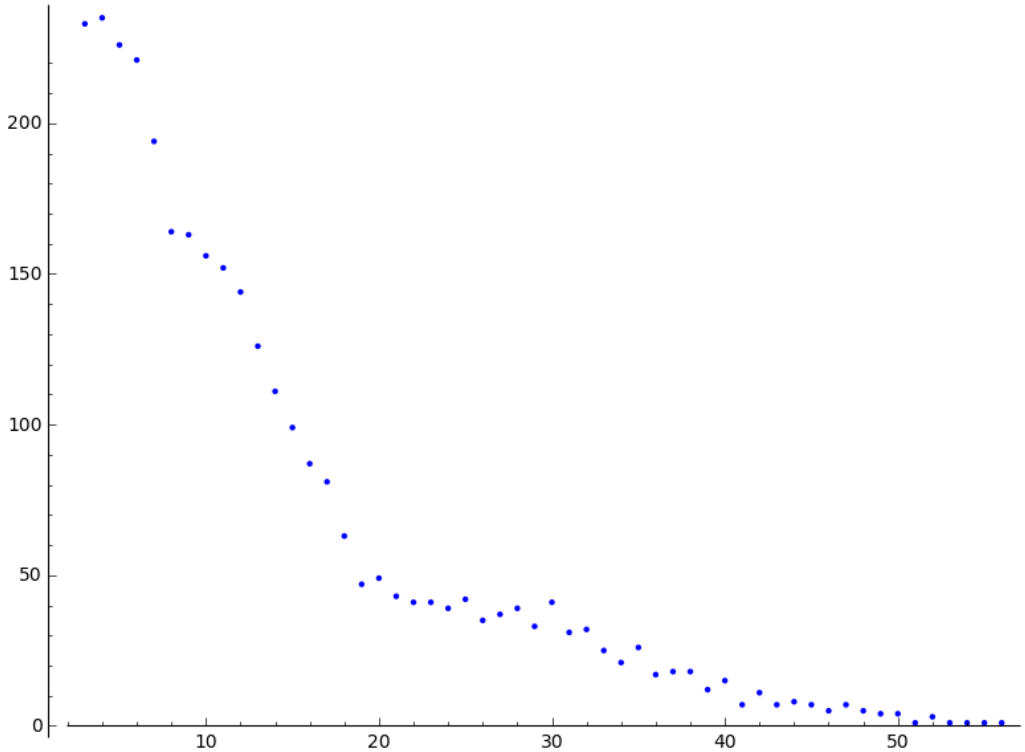

Figure 3: Sample size of the first primes for different degres

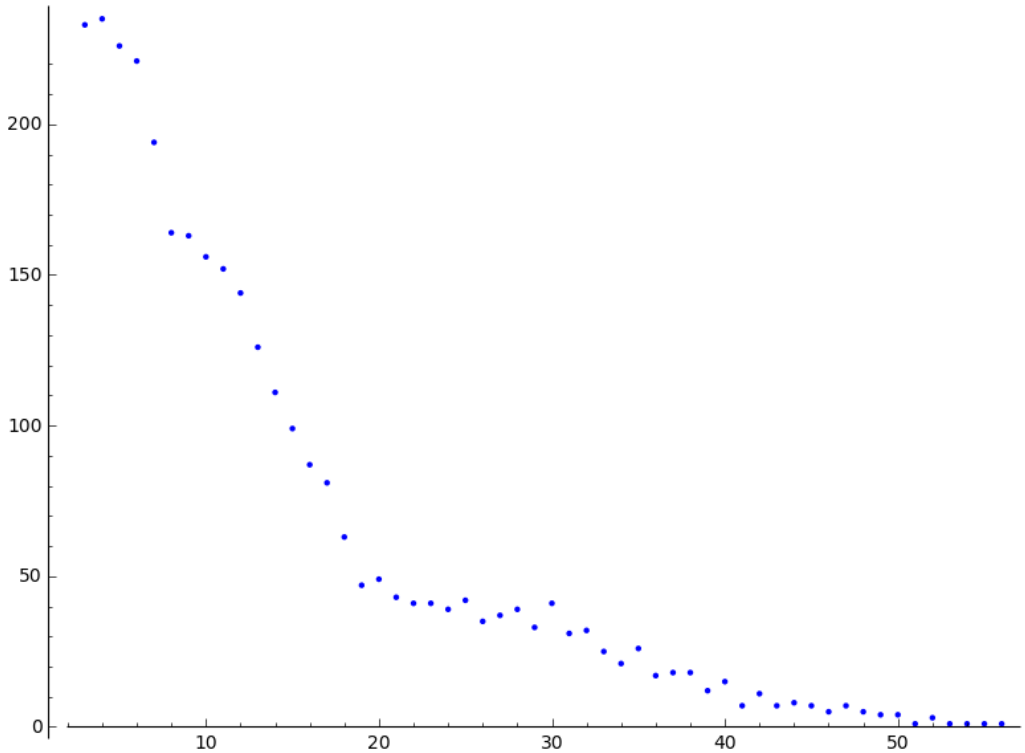

Figure 4: Sample size of the second primes for different degres

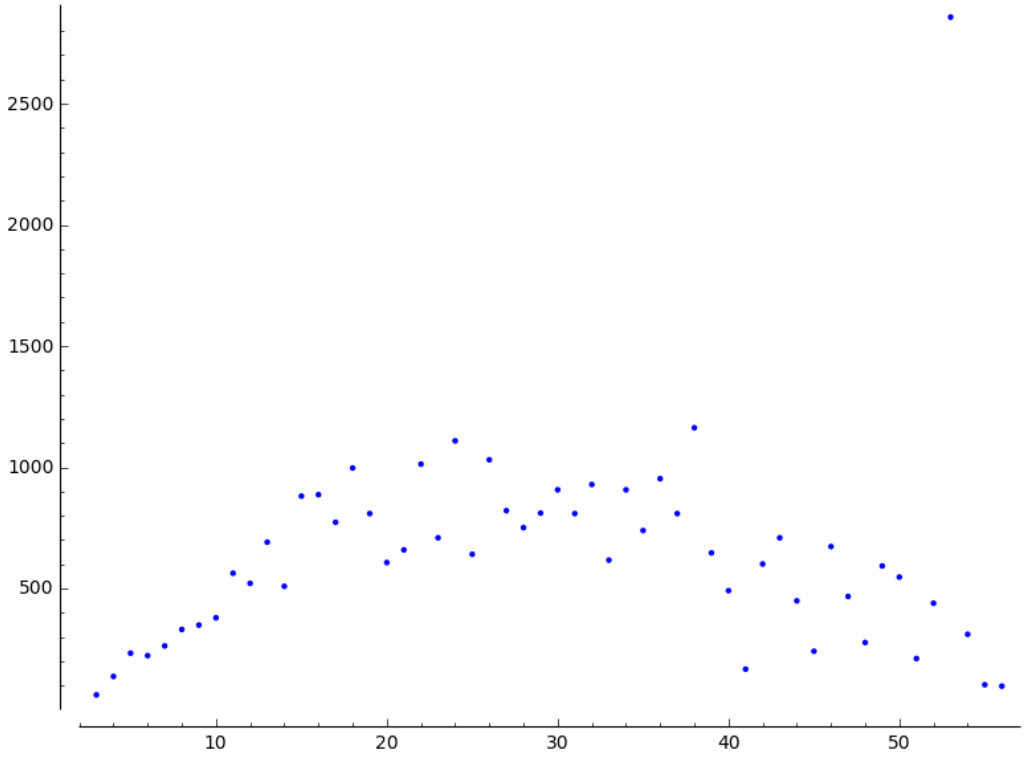

Figure 5: The maximum of primes for different degrees

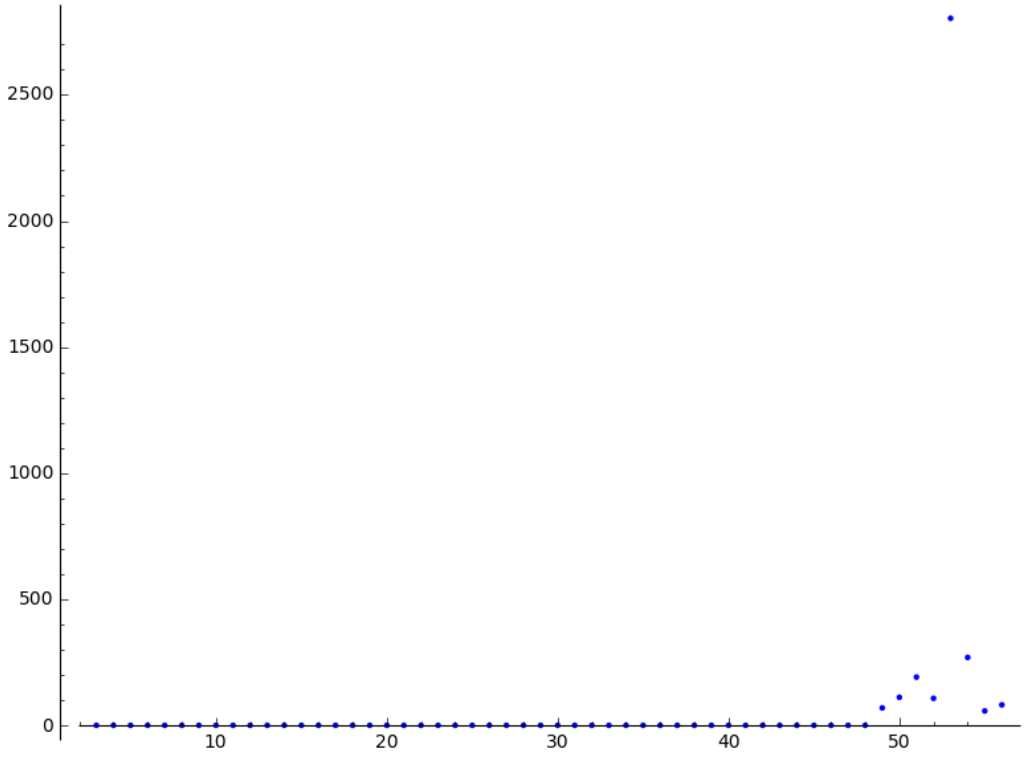

Figure 6: The minimum of primes for different degrees

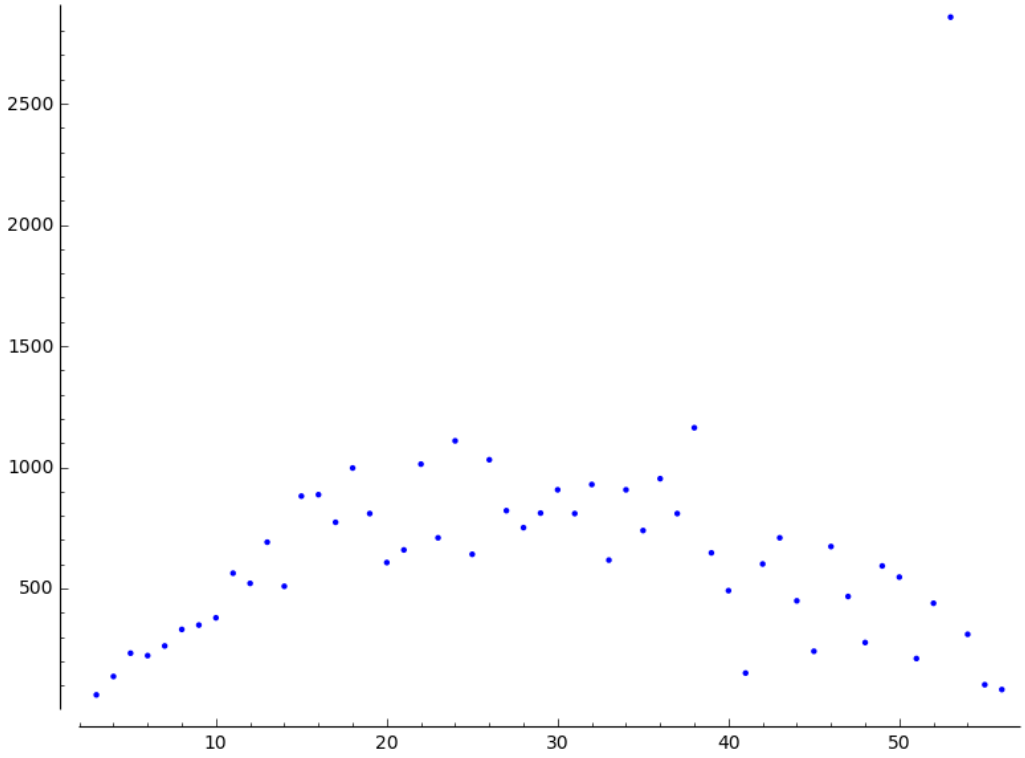

Figure 7: The maximum of first primes for different degrees

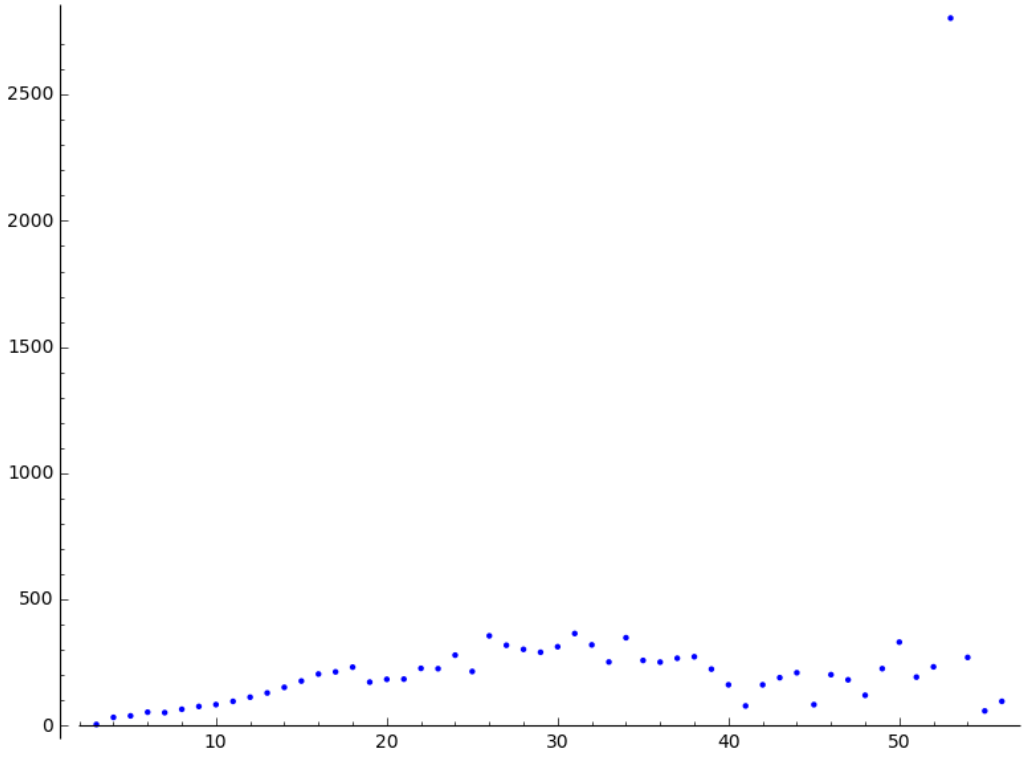

Figure 8: Average of the second primes

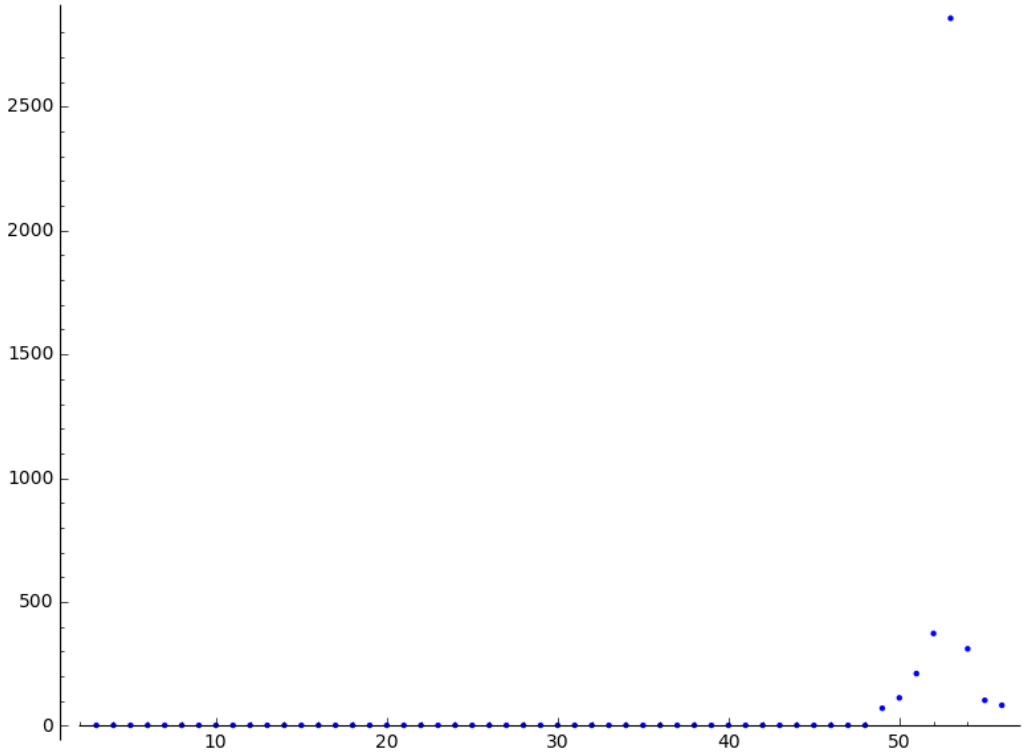

Figure 9: The minimum of first primes for different degrees

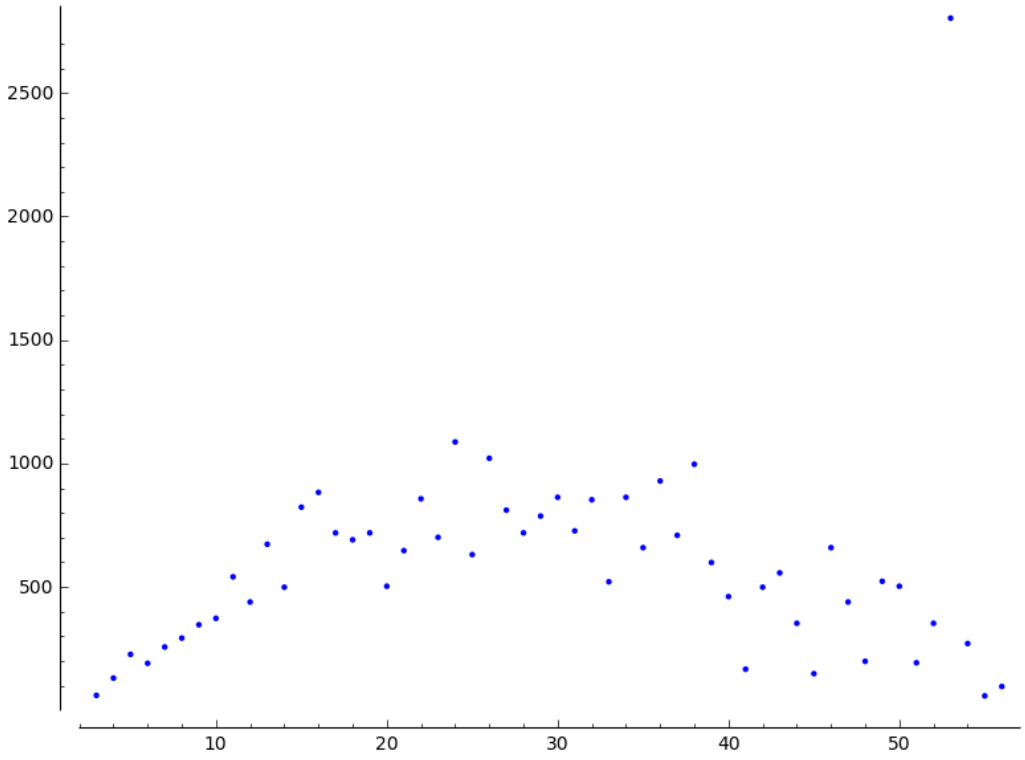

Figure 10: The maximum of second primes for different degrees

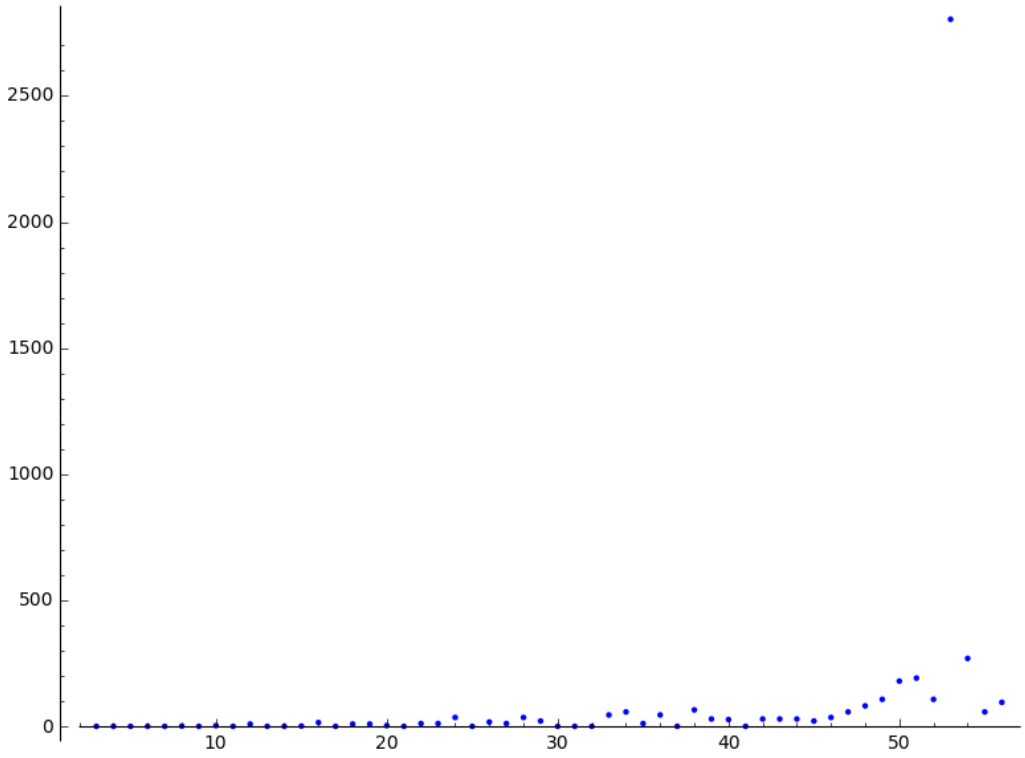

Figure 11: The minimum of second primes for different degrees

3 Testing for Arbitrary Coefficient Field

Modifications have been made on our program in order to be able to test the conjecture for more general cases. The core of the program stayed unchanged (as the theorem about criteria for the symmetrical group is the same in arbitrary field). The difference is that now, we had to factor with respect to prime ideals in the coefficient field. Due to the fact that we are not dealing simply with prime numbers, we have not been able to produce tables that resemble the previous ones (describing the average/minimum/maximum primes that were computed for polynomials of the certain degree). Also, we have used a fixed range of primes (which we then correlated to prime ideals), in particular 10 000.

This time, however, we have found many cases in which the conjecture was false. The following table shows on which levels it has failed for free-square levels N and the highest k we managed to get in a reasonable time. The ϵ value represents a Dirichlet character. The higher we were going for levels and weights the longer it took to verify the conjecture. Eventually we managed to reach a quite low level in comparison to the previous results. For all the other levels up to 15 we have tested, the conjecture holds true.

N	k	ϵ	result
3	15	-1	FALSE
3	17	-1	FALSE
3	19	-1	FALSE
3	21	-1	FALSE
3	23	-1	FALSE
3	25	-1	FALSE
3	27	-1	FALSE
3	29	-1	FALSE
6	11	-1	FALSE
6	13	-1	FALSE
6	15	-1	FALSE
6	17	-1	FALSE
6	19	-1	FALSE
6	21	-1	FALSE
6	23	-1	FALSE
6	25	-1	FALSE
6	27	-1	FALSE
6	29	-1	FALSE
6	31	-1	FALSE
14	9	zeta6	FALSE
14	11	zeta6	FALSE
15	9	(1,zeta4)	FALSE
15	11	(1,zeta4)	FALSE