Regular polygons

J. Mainik

February 12, 2025

Abstract

The construction of regular polygons with a compass and straightedge is a well-known task and this problem has interested mathematicians for a long time. In particular, for a long time they could not answer the question of whether is it possible to construct a regular 17gon with a compass and straightedge. C. F. Gauss solved this problem in 1796. He proved later that it is possible to construct with a compass and straightedge the regular polygons with $n = 2^m n_1 \cdots n_l$ sides, where n_1, \cdots, n_l are different prime numbers of the form $n_k = 2^{2^{\nu_k}} + 1$. P. Wantzel proved in 1837 that only these regular polygons can be constructed. Essential is here the construction of the regular polygons with $n_k = 2^{2^{\nu_k}} + 1$ sides. The currently known prime numbers of the form $n = 2^{2^{\nu}} + 1$ are 3, 5, 17, 257 and 65537.

In the paper we present a new approach for solving this task. Among other things we analyze in detail the case of n = 65537. J. G. Hermes announced in 1894 that he had a full description of the construction of the 65537-gon. This was the result of 10 years of work, but his text was too extensive and was never published. We show exactly and without gaps how the regular 65537-gon can be constructed.

Keywords: polygon, regular n-gon, compass, straightedge

1 Introduction

The construction of regular polygons with a compass and straightedge is a well-known task which has engaged mathematicians for a long time. Particularly interesting was the question of whether is it possible to construct with a compass and straightedge the regular 17-gon. This task, which is immediately understandable and can be formulated so simply, could not be solved for more than 2000 years. C. F. Gauss solved this problem in 1796, [1,2].

Gauss proved later that it is possible to construct with a compass and straightedge the regular polygons with $n = 2^m n_1 \cdots n_l$ sides, where n_1, \cdots, n_l are different prime numbers of the form $n_k = 2^{2^{\nu_k}} + 1$. Gauss came to the solution by his research in the area of number theory, namely that for the prime number n it is possible to find a number g for which g^k modulo n, $1 \le k \le n-1$, give all numbers $1, 2, 3, \cdots, n-1$. This number g is known as primitive root. The numbers

$$z^{\frac{2\pi r_k}{n}}, 1 \le k \le 16,$$

are arranged so that $r_k = g^k \mod n$. The set of elements arranged in this way will be split into two smaller parts so that the elements will be added to the parts alternately. The smaller parts will be split again in the same way. Gauss noticed that this gives rise to sets for which the values can be calculated with the help of quadratic equations.

Gauss knew also that only these regular polygons can be constructed with a compass and straightedge but did not prove it. P. Wantzel completed the result of Gauss and proved it in 1837 with the help of ideas and methods of Galois theory. The intersection points for a straight line and a circle or for two circles are determined as roots of quadratic equations and the construction with a compass and straightedge therefore corresponds to the extension of the rational numbers with the help of square roots.

The prime numbers of the form $n = 2^{2^{\nu}} + 1$ are known as Fermat primes as Fermat thought that the numbers of this form are prime numbers. That is not true, the only prime numbers of this form currently known are 3, 5, 17, 257 and 65537.

It is here decisive to construct the regular polygons with $n_k = 2^{2^{\nu_k}} + 1$ corners, as it is easy to increase the number of sides with the help of products or with doublings. For understandable reasons we do not analyze the cases n = 3 and n = 5. These cases are simple, and we are focused on the cases n = 17, n = 257 and n = 65537. We present an approach that differs from the method of Gauss. In particular we take a closer look at the case of n = 65537.

There is a nearly infinite list of publications on this subject. We show only a few of them, [1-16], but this list confirms very well that work is being carried out on this task continuously. This is so because the search is still going on for shorter and prettier constructions of the regular polygons.

One of the first geometric constructions of the 17-gon was presented by M. G. Paucker in 1819 and published in 1822, [4]. A simpler construction of the 17-gon was found by H. W. Richmond in 1893, [6]. Other constructions of the 17-gon were presented by Daniele and L. Gérard at the end of the 19th century.

Paucker proposed the first description of the construction for the 257gon in 1822. In 1825 J. Erchinger proposed an another construction, and this construction was discussed by Gauss himself in Göttingischen Gelehrten Anzeigen, [3]. In 1832 the same construction was once again presented by F. J. Richelot, [5]. D. W. DeTemple in the year 1991, M. Trott in 1995 and C. Gottlieb in 1999 published other constructions of the 257-gon, [9-11].

It took a long time until a construction of the regular 65537-gon was presented. In the year 1894, nearly 100 years after the publication of C. F. Gauss, J. Hermes announced that he had finished his work and had a full and accurate construction of the 65537-gon. This was the result of 10 years of work, but the paper of Hermes was too extensive and was never published. This paper is kept in the library of the University of Goettingen, is very complicated and was probably never checked strictly. Hermes was able to publish only a 17 page summary in 1895, [15]. In the publication of Duane DeTemple, [9], a simpler construction should be presented.

It is clear that the construction of regular polygons with a compass and straightedge has not the highest practical relevance. The author doesn't believe either that the 65537-gon should in fact be practically constructed.

But the interest of mathematicians and non-mathematicians for this task is still present. That has to do with the elegance of the regular n-gons and the simplicity of the question but even more with the need for solutions of such understandable tasks.

In this paper we present precisely and without gaps the construction of the regular 65537-gon.

The author hopes that the new approach to constructing the regular polygons and the full description of the construction for the 65537-gon will find interest and understanding.

2 Denominations and remarks

In the following n is equal to 17, 257 or 65537. If we confine ourselves to one of these values, we will always formulate it clearly.

For $z = e^{2\pi i/n}$ we have

$$z^n - 1 = 0 \tag{1}$$

and the the values z^k for $k = 0, 1, \dots, n-1$ are the solutions of this equation. The points $z^k = e^{k \cdot 2\pi i/n}$, $0 \le k \le n-1$, are lying on the circle with the radius 1 and represent the vertices of the regular *n*-gon. We have the radius 1 of this circle and therefore the point $z^0 = 1$. It applies

$$z^{n} - 1 = (z - 1)(z^{n-1} + z^{n-2} + \dots + z + 1)$$

and the values $z^k = e^{k \cdot 2\pi i/n}$, $1 \le k \le n-1$, which we need also, are the solutions of the equation

$$z^{n-1} + z^{n-2} + \dots + z + 1 = 0 \tag{2}$$

In order to construct the regular n-gon we have thus to determine the solutions of this algebraic equation, and these solutions should be constructed with a compass and straightedge.

In this context we summarize a few simple facts. For the solution of the equation $x^2 + px + q = 0$ we have

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

and we can construct them with a compass and straightedge, if we have the segments with the lengths p und q. For these constructions we need in addition to the segments with the lengths p und q the segment of the lengths 1, but this segment is already present. This is the radius of the circle, on which the vertices of the regular n-gon positioned.

It may be worth making here a remark about the square root. The value \sqrt{D} can be drawn as follows: draw the semicircle with diameter D + 1 and the perpendicular to this diameter at the point that splits the diameter into segments of the length D and 1. The perpendicular line from this point to the semicircle has the length \sqrt{D} .

By constructing with a compass and straightedge we are, in certain sense, limited to solutions of quadratic equations. It is known, for example, that the solution of the simple cubic equation

$$x^3 - 3x - 1 = 0$$

that appears by trisection of the 60-degree angle and even the value $\sqrt[3]{2}$ that you need for doubling the cube cannot be drawn with a compass and straightedge.

Mathematicians refer here to field extensions of rational numbers with square roots. In order to determine the solution of a more complicated equation we have to come repeatedly to quadratic equations and draw the solutions for them.

To determine the quadratic equations themselves the following is relevant. The quadratic equations with the solutions x_1 and x_2 can be determined by Vieta's theorem. It holds

$$(x - x_1)(x - x_2) = x^2 - (x_1 + x_2) \cdot x + (x_1 \cdot x_2) = 0$$

an the appropriate quadratic equation is determined by the sum $x_1 + x_2$ and the product $x_1 \cdot x_2$.

In the following we will always divide a complicated value so that all terms of the complicated value will be distributed between the two parts. The sum of the parts is therefore automatically equal to the divided value and we always just have to determine the product of the parts. For the fairly complicated equation (2) for example we must therefore several times split the sum S

$$S = z^{n-1} + z^{n-2} + \dots + z \tag{3}$$

into smaller parts in such a way that we can determine the products of these parts. Then we can draw the parts with a compass and straightedge.

To assign the solutions of the quadratic equation to the geometrical objects correctly we have to know which of the values is to calculate with the sign "+" and which is to calculate with the sign "-" before the determinant. I.e. we have to know which of them is bigger.

If F_1 and F_2 are parts of S, it holds $F_1 + F_2 = S$, and we have to choose F_1 and F_2 so that we can determine the product $F_1 \cdot F_2$. We know the value S, and it holds S = -1, but we don't know any parts of S. It is therefore naturally to choose the parts F_1 and F_2 so that in the product $F_1 \cdot F_2$ all terms z^k , $1 \le k \le n-1$, of S appears an equal amount of times. Then $F_1 \cdot F_2$ provides an even coverage of S, and if $F_1 \cdot F_2$ covers $S \mid \mu$ times, it holds $F_1 \cdot F_2 = \mu \cdot S + \nu$. The constant summand ν must be here the number of elements z^k in F_1 for which the inverse elements z^{n-k} belong to F_2 . We obtain so the necessary information to determine the relevant quadratic equation for the Parts F_1 and F_2 .

3 Parts of S and invariant sets

From (1) we see that $z^{n+m} = z^m$, and therefore we get

$$z^{k} \cdot S = z^{k} \cdot (z + \dots + z^{n-1-k} + z^{n-k} + z^{n+1-k} + \dots + z^{n-1})$$

= $z + z^{2} + \dots + z^{k-1} + z^{k+1} + \dots + z^{n-1} + 1$

so that

$$z^k + z^k \cdot S = S + 1 \tag{4}$$

If we add up in (4) over all values z^k that belong to F_1 , we obtain

$$F_1 + F_1 \cdot S = \mu(F_1) \cdot S + \mu(F_1)$$
(5)

where $\mu(F_1)$ denotes the number of elements of F_1 . Due to $S = F_1 + F_2$ we have thus

$$F_1 + F_1 \cdot (F_1 + F_2) = \mu(F_1) \cdot S + \mu(F_1)$$

and therefore

$$(F_1 + F_1^2) + F_1 \cdot F_2 = \mu(F_1) \cdot S + \mu(F_1)$$
(6)

From the last equality we can see that $F_1 \cdot F_2$ provides an even coverage of S if and only if $F_1 + F_1^2$ provides an even coverage of S. It is naturally, in this context, to take a closer look to the squares of elements of the part F_1 .

In the following we always designate the terms $z^k = e^{k \cdot 2\pi i/n}$, $1 \le k \le n-1$, as elements.

Proposition 1. Let F_1 be so that $F_1 + F_1^2$ provides an even coverage of S. Then with $z^k \in F_1$ it also holds $z^{2k} \in F_1$.

Proof. At first we notice that $z_1^2 \neq z_2^2$ if z_1 and z_2 are different terms in $S, z_1 \neq z_2$. This property is obvious.

Let be $z_1 \in F_1$ and $z_1^2 \notin F_1$. The element z_1^2 will then obviously have an odd coverage with $F_1 + F_1^2$: once as the element z_1^2 in F_1^2 and in addition possibly an even number of times by products $2z_l \cdot z_m$ of different elements z_l and z_m of F_1 by the calculation of F_1^2 . It follows immediately that for each element z_k of F_1 the square z_k^2 cannot belong to F_1 . It has to be so because otherwise the element z_k^2 , $z_k^2 \in F_1$, will be covered with $F_1 + F_1^2$ an even number of times. As $F_1 + F_1^2$ provides an even coverage, all elements of S must have this odd coverage. This means that in $F_1 + F_1^2$ each element of F_2 appears exactly once as z_k^2 for $z_k \in F_1$. We see so that F_1 and F_2 must have the same number $\frac{n-1}{2}$ of elements and the function $f(z) = z^2$ provides a one-to-one mapping F_1 to F_2 .

We see in (6) at once that together with $F_1 + F_1^2$ the product $F_1 \cdot F_2$ provides an odd coverage of S. The product $F_1 \cdot F_2$ has $(\frac{n-1}{2})^2 - r$ elements, where r is the number of elements z^k in F_1 for which the inverse elements z^{n-k} belong to F_2 . It holds here obviously $0 \le r \le \frac{(n-1)}{2}$. As $F_1 \cdot F_2$ provides an even coverage of S n-1 is a divisor of $(\frac{n-1}{2})^2 - r$ and this is possible only if r = 0. So we see that the coverage μ for $F_1 \cdot F_2$ is $\mu = \frac{n-1}{4}$. We come to a contradiction as $\frac{n-1}{4}$ is an even number.

Corollary. As a corollary of the proved proposition one sees that with each element z^k of F_1 all elements $z^{2k}, z^{4k}, z^{8k}, \cdots$ belong to F_1 also.

Definition. We denote a set of elements G an invarian set if with each element z^k of G the element z^{2k} also belongs to G: $z^k \in G \Longrightarrow z^{2k} \in G$. The order of elements of an invariant set, where the next element is the square of the previous one, we denote a natural order.

Now we want to analyze the invariant sets more precisely. We begin, at first, with the element $z = e^{\frac{2\pi i}{n}}$, where $n = 2^{2^{\nu}} + 1$. Instead of calculating the squares $z_1 = z, z_2 = z^2, z_3 = z^4, \cdots$ it is easier to work with the degrees $1, 2, 4, \cdots$ of these elements. These degrees will be repeatedly doubled and the condition $z^n = 1$ means that for the degrees it must be calculated modulo n. The degree of z_k is 2^{k-1} modulo n and we obtain so by the calculations modulo n the numbers

$$1, 2, 4, \cdots, 2^{2^{\nu}-1}, n-1, n-2, n-4, \cdots, n-2^{2^{\nu}-1}$$
 (7)

We use here the equalities: $2^{2^{\nu}} = n - 1$, $2^{2^{\nu}+1} = 2 \cdot (n-1) = n - 2$ modulo n, $2^{2^{\nu}+2} = 2 \cdot (n-2) = n - 4$ modulo n, \dots , and

$$2^{2^{\nu+1}-1} = 2^{2\cdot 2^{\nu}-1} = 2^{2^{\nu}}2^{2^{\nu}-1} = (n-1)2^{2^{\nu}-1} = n - 2^{2^{\nu}-1} \text{ modulo } n$$

By the next doubling we come again back to 1:

$$2 \cdot (n - 2^{2^{\nu} - 1}) = 2n - 2^{2^{\nu}} = 2n - (n - 1) = 1 modulo n$$

This means that we have an invariant set of $2^{\nu+1}$ different elements. We denote this set in the following G_1 .

Proposition 2. Every invariant set consists of $2^{\nu+1}$ different elements. By natural order the *m*-th element, $1 \le m \le 2^{\nu}$, of the invariant set is inverse to the $(2^{\nu} + m)$ -th element of the set.

Proof. We have already seen that the invariant set G_1 consists of $2^{\nu+1}$ different elements. We can also immediately see, (7), that for G_1 the *m*-th element is inverse to the $(2^{\nu} + m)$ -th element. We want to show this for any invariant set.

Any invariant set with natural order is determined as follows. Starting with a chosen initial element we get the next elements as the square of the previous one. One must take here into account that $z^n = 1$.

If we begin not with the starting element z of G_1 but with the element z^k , 1 < k < n, which does not belong to G_1 , we will get again $2^{\nu+1}$ different elements and come analog to the case G_1 back to the starting element z^k . We can see this because the degrees of the elements here are k times higher than the degrees of elements in G_1 .

Indeed, by calculation modulo n for the degrees of the elements we have

 $k \cdot 2^m = k \mod n \Leftrightarrow k \cdot (2^m - 1) = 0 \mod n$

As k is not a divisor of the prime number n it must apply $2^m = 1 \mod n$, and we have seen by calculation of the invariant set G_1 that this happens first by $m = 2^{\nu+1}$. This means that any invariant set has $2^{\nu+1}$ elements and these elements are different.

The degree of the *m*-th element of the invariant set with the starting element z^k is equal to $k \cdot 2^{m-1}$ and the degree of the $(2^{\nu} + m)$ -th element is $k \cdot 2^{2^{\nu}+m-1}$. We obtain therefore by calculation modulo n

$$k \cdot 2^{m-1} + k \cdot 2^{2^{\nu} + m - 1} = k \cdot 2^{m-1} \cdot (2^{2^{\nu}} + 1) = k \cdot 2^{m-1} \cdot n = 0$$

This means that the mentioned elements are inverse. \blacksquare

It is clear that the invariant sets cannot overlap. From the overlapping point they will coincide and due to the coming back to the starting element they should be the same. This means that the $2^{2^{\nu}}$ elements of S distributed between $2^{2^{\nu}}/2^{\nu+1} = 2^{2^{\nu}-(\nu+1)}$ invariant sets.

In the case $n = 2^{2^2} + 1 = 17$ there are only 2 invariant sets with 8 elements each, in the case $n = 2^{2^3} + 1 = 257$ there are 16 invariant sets with 16 elements each and in the case $n = 2^{2^4} + 1 = 65537$ there are $2^{11} = 2048$ invariant sets each with 32 elements.

We can obviously formulate the Proposition 1 others as follows: By the split of S the invariant sets must be distributed between F_1 and F_2 , an invariant set must not be torn.

As shown in Proposition 2 each two inverse elements z^k and z^{n-k} belong to the same invariant set. It follows then that for the appropriate parts F_1 and F_2 the constant summand ν in the product $F_1 \cdot F_2$ is equal to 0 and it holds thus $F_1 \cdot F_2 = \mu S$.

Each invariant set consists of pairs of inverse elements, and it is naturally to unite these inverse pairs and do not separate them. There are two reasons for this. At first, by the work with the pairs we are dealing with real values

$$p_k = z^k + z^{n-k} = 2\cos\frac{2k\pi}{n}$$

and we are particularly interested in the value $p_1 = 2\cos\frac{2\pi}{n}$. If we determine this value, we can very simply construct the polygon completely. The second reason for the work with pairs is that we will have twice less values. In the case n = 17 we have 2 invariant sets with 4 pairs each, in the case n = 257we have 16 invariant sets with 8 pairs, and in the case n = 65537 we have 2048 invariant sets each with 16 pairs.

We have assumed above that for the pair $p_k = z^k + z^{n-k}$ the number k is chosen as min(k, n-k) and therefore the numbers k of the pairs are in the range $1 \le k \le \frac{n-1}{2}$. So we get a unique numbering of the pairs. One can also represent the pair p_k as $p_k = z^k + z^{-k}$, and this form can be more appropriate for some calculations.

To work with pairs we have to know how we can multiply them. At first, let $p_k = z^k + z^{-k}$, $1 \le k \le \frac{n-1}{2}$, and $p_m = z^m + z^{-m}$, $1 \le m \le \frac{n-1}{2}$, be different. Then we have

$$p_k \cdot p_m = (z^k + z^{-k})(z^m + z^{-m}) = z^{k+m} + z^{-(k+m)} + z^{k-m} + z^{m-k}$$

and we see that the product of two different pairs is the sum of two pairs. We had not determined in advance which of the numbers k or m is bigger and in addition the sum m + k can become bigger then $\frac{n-1}{2}$, but we must have a number between 1 and $\frac{n-1}{2}$. Taking into account that $z^n = 1$ the product $p_k \cdot p_m$ can be presented as follows

$$p_k \cdot p_m = p_{|k-m|} + p_{min(k+m,n-(k+m))} \tag{8}$$

For the square of the pair p_k we obtain

$$p_k^2 = (z^k + z^{-k})^2 = z^{2k} + z^{-2k} + 2$$

The square of a pair is so a sum of a pair and the constant 2. The constant substitutes here the second pair. To get the number between 1 and $\frac{n-1}{2}$ the result must be represented as follows

$$p_k^2 = p_{\min(2k,n-2k)} + 2 \tag{9}$$

4 Regular 17-gon

The results of the Propositions 1 and 2 are sufficient to construct the regular 17-gon. In this case we have only two invariant sets, which we denote G_1 and G_2 . The invariant set G_1 consists of the pairs p_1 , p_2 , p_4 and p_8 and G_2 consists of the pairs p_3 , p_6 , p_5 and p_7 : $G_1 = p_1 + p_2 + p_4 + p_8$, $G_2 = p_3 + p_6 + p_5 + p_7$. For these pairs here is chosen the natural order and that's why we come with the square from one pair to the next one: $p_1^2 = p_2 + 2$, $p_2^2 = p_4 + 2$, \cdots . It holds also $p_8^2 = p_1 + 2$ so that we have for the pairs a certain circular property. The same is also true for the pairs in G_2 .

According to the Proposition 1 S must be splitted into invariant sets. For the sum $G_1 + G_2$ we have immediately $G_1 + G_2 = S = -1$, and only the product $G_1 \cdot G_2$ must be calculated. We obtain via direct calculation

$$G_1 \cdot G_2 = (p_1 + p_2 + p_4 + p_8) \cdot (p_3 + p_6 + p_5 + p_7)$$

= $4(p_1 + p_2 + p_3 + p_4 + p_5 + p_6 + p_7 + p_8) = 4S = -4$

and the corresponding quadratic equation is thus

$$x^2 + x - 4 = 0. (10)$$

It holds here $G_1 > G_2$, and we obtain therefore

$$G_1 = -\frac{1}{2} + \sqrt{\frac{1}{4} + 4} = \frac{-1 + \sqrt{17}}{2}, \quad G_2 = -\frac{1}{2} - \sqrt{\frac{1}{4} + 4} = -\frac{1 + \sqrt{17}}{2}$$

and these values can be constructed with a compass and straightedge.

We have calculated the product $G_1 \cdot G_2$ directly. We could do it another way. It applies

$$2G_1 \cdot G_2 = (G_1 + G_2)^2 - (G_1^2 + G_2^2) = S^2 - (G_1^2 + G_2^2)$$

and by the calculation of the squares of the invariant sets we can use the obvious property that for G_k the sum of the squares of the appropriate pairs is equal to $G_k + 2 \cdot pair(G_k)$, where $pair(G_k)$ is the number of pairs in G_k . The products of different pairs in G_1 and in G_2 must be calculated here also, but there are fewer of them. We will show later that this calculation can be done even easier.

We want to get the pair p_1 , and it is thus naturally to split the invariant set $G_1 = p_1 + p_2 + p_4 + p_8$. The sum of the corresponding parts P_1 and P_2 is known immediately

$$P_1 + P_2 = G_1.$$

As we know only G_1 and G_2 (S is also the sum of G_1 and G_2), we have to choose the parts P_1 and P_2 so that we can calculate the product $P_1 \cdot P_2$ on the basis of G_1 and G_2 . There are not too many possibilities to split G_1 , and we can check them individually. The splitting of G_1 so that one part has 1 pair and the other has 3 pairs doesn't fit. We have then in product 6 pairs, wich cannot be distributed evenly between G_1 and G_2 as they have 4 pairs each. If we consider the parts with 2 pairs in each of them, we see simply that the splittings into $P_1 = p_1 + p_2$ and $P_2 = p_4 + p_8$, or into $P_1 = p_1 + p_8$ and $P_2 = p_2 + p_4$ are not fit. Thus, it can be only the splitting of G_1 into $P_1 = p_1 + p_4$ and $P_2 = p_2 + p_8$.

If we calculate $P_1 \cdot P_2$ for this split directly, we gain

$$P_1 \cdot P_2 = (p_1 + p_4)(p_2 + p_8) = p_1 + p_3 + p_7 + p_8 + p_2 + p_6 + p_4 + p_5 = S$$

Thus, the appropriate quadratic equation is here

$$x^2 - G_1 \cdot x - 1 = 0 \tag{11}$$

and as $P_1 > P_2$, we obtain

$$P_1 = \frac{G_1 + \sqrt{G_1^2 + 4}}{2}, \quad P_2 = \frac{G_1 - \sqrt{G_1^2 + 4}}{2}$$

and these values can be constructed with a compass and straightedge.

It is possible to calculate here the product $P_1 \cdot P_2$ for the split of G_1 with the help of squares. It applies

$$2P_1 \cdot P_2 = G_1^2 - (P_1^2 + P_2^2) = G_1^2 - ((p_1 + p_4)^2 + (p_2 + p_8)^2)$$

= $G_1^2 - (p_1^2 + p_2^2 + p_4^2 + p_8^2) - 2(p_3 + p_5 + p_6 + p_7) = G_1^2 - G_1 - 8 - 2G_2$
= $G_1^2 + G_1 - 8 - 2(G_1 + G_2) = G_1^2 + G_1 - 8 - 2S = G_1^2 + G_1 - 6$

We could use already this value with the square G_1^2 and determine the corresponding quadratic equation. But we can also notice that G_1 is the solution of the equation (10) so that it applies

$$G_1^2 + G_1 = 4$$

and we obtain therefore for $P_1 \cdot P_2$ the known value

$$P_1 \cdot P_2 = \frac{1}{2}(G_1^2 + G_1 - 6) = \frac{1}{2}(4 - 6) = -1$$

In any case we can notice here that it is appropriate to split the invariant set so that the pairs are taken over one. Then we can easier calculate the squares of the relevant parts.

Now we have the value $p_1 + p_4$ and due to $p_4 = p_2^2 - 2$ and $p_2 = p_1^2 - 2$ we can go to an equation of 4th degree and analyze it. But it is not pleasant to solve equations of 4th degree and we need quadratic equations. Therefore it is naturally to split $P_1 = p_1 + p_4$. We can choose here as parts only p_1 and p_4 . The sum is already known, $p_1 + p_4 = P_1$, and we have to calculate $p_1 \cdot p_4$. If we calculate the product $p_1 \cdot p_4$ directly, we obtain

$$p_1 \cdot p_4 = p_3 + p_5$$

The value $p_3 + p_5$ presents a part of G_2 and to determine this value we have to split G_2 . It can also be seen that the parts for $G_2 = p_3 + p_6 + p_5 + p_7$ should be $p_3 + p_5$ and $p_6 + p_7$ and for these parts the pairs should be again chosen over one. We could really easy do it, but we want to get by without that. We want to use the squares. It applies obviously

$$2p_1 \cdot p_4 = (p_1 + p_4)^2 - (p_1^2 + p_4^2) = P_1^2 - (p_2 + p_8 + 4) = P_1^2 - P_2 - 4$$

and therefore

$$p_1 \cdot p_4 = \frac{P_1^2 - P_2 - 4}{2}$$

The quadratic equation for p_1 and p_4 is hence

$$x^2 - P_1 \cdot x + \frac{P_1^2 - P_2 - 4}{2} = 0$$

and because of $p_1 > p_4$ we obtain

$$p_1 = \frac{P_1}{2} + \sqrt{\frac{P_1^2}{4} - \frac{P_1^2 - P_2 - 4}{2}} = \frac{P_1 + \sqrt{2P_2 - P_1^2 + 8}}{2}$$

Thus we can construct with a compass and straightedge the value $p_1 = 2\cos\frac{2\pi}{17}$ and therefore the complete regular 17-gon.

5 Building of invariant sets

The case of regular 17-gon is completed, and in the following we will focus on the cases n = 257 and n = 65537.

Until now we have presented in detail only one invariant set, namely the set G_1 . Now we present an approach that helps us to build all invariant sets and establish a special order of the invariant sets.

As noticed earlier, we can instead of elements z^k use the degrees k and if we work with degrees, we have to calculate *modulo* n to take into account the property $z^n = 1$. We want to work here with the degrees. For an unvariant set G we denote in the following \hat{G} the set of the degrees of the elements z^k in G and the order of the degrees in \hat{G} correspons here the natural order of the elements in G.

For G_1 the appropriate degrees in natural order \hat{G}_1 are shown in (7). The next invariant set G_2 we build so that the starting number in \hat{G}_2 is 3, i.e. a number three times bigger than the starting number of \hat{G}_1 , and the other numbers in \hat{G}_2 are being calculated with the help of doublings

$$\hat{G}_2 = \left\{3, \ 3 \cdot 2, \ 3 \cdot 4, \cdots, 3 \cdot 2^{2^{\nu+1}-1}\right\}$$

wherein the calculation is *modulo* n so that we obtain numbers between 1 and n-1. The doubling corresponds here to the calculation of square of the elements.

For the following sets $\hat{G}_3, \hat{G}_4, \cdots$ the starting number will be always calculated so that it is three times bigger than the starting number of the previous set. The other numbers in these sets are calculated after that with the help of doublings. For the set \hat{G}_k we have so

$$\hat{G}_k = \left\{ 3^{k-1}, \ 3^{k-1} \cdot 2, 3^{k-1} \cdot 4, \cdots, 3^{k-1} \cdot 2^{2^{\nu+1}-1} \right\}$$

Here the calculation is *modulo* n and we obtain numbers between 1 and n-1.

Remark 1. We don't show in the denominations G_k and \hat{G}_k the parameter n so as not to overload them. G_k and \hat{G}_k depend on number n and must

be calculated separately for the relevant n. It will in the following allways be clear which number n we consider.

Remark 2. The factor 3, by which the starting numbers increase, is in the approach of Gauss known as primitive root. The author came to this factor via a completely different way and doesn't use this factor to determine all elements of S.

Looking at the split of S into parts F_1 and F_2 we have seen that we have to get an even coverage with the help of $F_1 + F_1^2$. Due to Proposition 1 we came to the squares of invariant sets. If we look at the square of G_1 , we will see that G_1^2 contains the value $3G_1$, the threefold of G_1 itself, and the fourfold of an another invariant set, and it is the invariant set with the starting element z^3 . Analogous it is also for other invariant sets. The sum $G_1 + G_1^2$ has therefore automatically the fourfold of G_1 and we choose the factor 3 for building of the set \hat{G}_2 for the next invariant set G_2 in order to get a certain symmetry in the coverage for the invariant sets. The order of the invariant sets should be so that the sum $G_i + G_i^2$ delivers the value $4G_i$ for the invariant set itself and the value $4G_{i+1}$ for the next invariant set G_{i+1} . The invariant sets G_i and G_{i+1} should be distributed to different parts F_1 and F_2 . This was the idea of building and ordering the invariant sets.

The factor 3, as we will see, fits quite well. Later we will see that not the factor itself but other properties are responsible for ensuring that the necessary calculations can be done. We will analyze the choice of this factor later.

Proposition 3. With the help of the presented approach all invariant sets will be built.

Proof. If the starting numbers of \hat{G}_k are defined, the sets \hat{G}_k are builded with the help of doublings and they are indeed corresponds to invariant sets G_k and can't overlap. We have thus only to show that the sets \hat{G}_k , $1 \leq k \leq 2^{2^{\nu}-(\nu+1)}$, all different.

First we consider the case n = 257. We have to calculate *modulo* 257 and to show that the 16 sets \hat{G}_k , $1 \le k \le 16$, are different.

We can build the set \hat{G}_k for any number $k \ge 1$. The starting numbers of the sets \hat{G}_2 , \hat{G}_3 , \hat{G}_4 , \hat{G}_5 are equal to 3, 9, 27 and 81 respectively. As these numbers do not belong to \hat{G}_1 the sets are not equal to \hat{G}_1 . For the step from \hat{G}_1 to \hat{G}_5 we had to increase the starting number with the factor 81. If we go from \hat{G}_5 to \hat{G}_9 , we have to increase the starting number again with the factor 81 and calculate *modulo* 257. The starting number of \hat{G}_9 is therefore equal to $rest(81 \cdot 81, 257) = 136$. The number 136 doesn't belong to \hat{G}_1 and the sets \hat{G}_9 and \hat{G}_1 are different, $\hat{G}_9 \neq \hat{G}_1$. We came from \hat{G}_1 to \hat{G}_9 with the help of the factor 136 and therefore we come from \hat{G}_9 to \hat{G}_{17} with the same factor 136. The starting number of \hat{G}_{17} is thus equal to $rest(136 \cdot 136, 257) = 249$. The number 249 = 257 - 8 belongs to \hat{G}_1 , and we see thus that $\hat{G}_{17} = \hat{G}_1$

Let not all sets \hat{G}_k , $1 \leq k \leq 16$, be different, and let m, m > 0, be the smallest number so that for any number $k \geq 1$ it holds $\hat{G}_{k+m} = \hat{G}_k$. Then we have here $1 \leq m < 16$.

From the equality $\hat{G}_{k+m} = \hat{G}_k$ it follows obviously that $3^m = 2^j \mod n$. But with the help of the equality $3^m = 2^j \mod n$ we obtain simply that $\hat{G}_{1+m} = G_1$, $\hat{G}_{1+2m} = \hat{G}_{1+m}, \cdots$, and this means that \hat{G}_1 repeats with the period $m, 1 \leq m < 16$. We have seen that $\hat{G}_{17} = \hat{G}_1$, and therefore m should be a divisor of 16. This means that m is equal to 8 or is a divisor of 8. In any case we have $\hat{G}_9 = \hat{G}_1$ and come to a contradiction.

In the case n = 65537 the proof can be easy adjusted. We have to calculate modulo 65537 and to show that the sets \hat{G}_k , $1 \le k \le 2048$, are different. In the calculation of the starting number for the set \hat{G}_9 here we don't need to calculate modulo 65537 and obtain the number $81^2 = 6561$. This number dosn't belong to \hat{G}_1 so that $\hat{G}_9 \neq \hat{G}_1$. If here we analogous to the case n = 257 double the steps, we obtain the starting numbers for the sets \hat{G}_{17} , \hat{G}_{33} , \hat{G}_{65} , \hat{G}_{129} , \hat{G}_{257} , \hat{G}_{513} , \hat{G}_{1025} and \hat{G}_{2049} . The starting number of the next sets is here the square of the previous starting number calculated modulo 65537. We obtain so the starting numbers 11088, 3668, 19139, 15028, 282, 13987, 8224 and 8 respectively. Only one number of them, namely 8, belongs to \hat{G}_1 so that only \hat{G}_{2049} is equal to \hat{G}_1 . As $\hat{G}_{1025} \neq \hat{G}_1$ we can analogous to the previous come to a contradiction.

We denote in the following the number of all invariant sets ng, $ng = 2^{2^{\nu}-(\nu+1)}$. For the invariant set with presented building and order we have found a pretty circle property: when we run through all invariant sets we come back to the first invariant set so that $G_{ng+k} = G_k$.

In the following we will understand G_k as the sum of their elements. As all elements z^k of the sum S are unique distributed between the invariant sets it holds for S the representation

$$S = G_1 + G_2 + \dots + G_{ng}$$

The invariant sets consist of pairs of inverse elements. We want to show here that one can perform the presented building of invariant sets on the basis of pairs. For the invariant set G_k we will get this way an naturally odered set of the pais in G_k and a corresponding odered set \bar{G}_k of the numbers of these pairs. We deenote in the following $q_{k,m}$ the *m*-th number in \hat{G}_k and $r_{k,m}$ the *m*-th number in \bar{G}_k end want to show, that $r_{k,m} = \min(q_{k,m}, n - q_{k,m})$.

First we show it for the starting numbers in \hat{G}_k and in \bar{G}_k . This is so for \hat{G}_1 and \bar{G}_1 . The first number in \hat{G}_1 is $q_{1,1} = 1$, (7), and this is the number of

the first pair in G_1 also, so that $r_{1,1} = 1 = \min(q_{1,1}, n - q_{1,1})$. For k > 1 we calculate the first number $q_{k,1}$ in \hat{G}_k with the help of the first number $q_{k-1,1}$ in \hat{G}_{k-1} as $q_{k,1} = 3s_{k-1} \mod n$. To get the first number $r_{k,1}$ in \bar{G}_k on the basis of $r_{k-1,1}$ we have to calculate the value $j = 3r_{k-1,1} \mod n$ and then the number of the corresponding pair, i.e. $r_{k,1} = \min(j, n-j)$. In the case $r_{k-1,1} = q_{k-1,1}$ we simply have here

$$j = 3r_{k-1,1} \mod n = 3q_{k-1,1} \mod n = q_{k,1}$$

and therefore automatically $r_{k,1} = min(q_{k,1}, n - q_{k,1})$. In the case $r_{k-1,1} = n - q_{k-1,1}$ we have

$$j = 3r_{k-1,1} \mod n = 3(n - q_{k-1,1}) \mod n$$

and the value j and the number $q_{k,1}$ are grades of inverse elements in a pair. Indeed, we get here easy

$$(j+q_{k,1}) \mod n = 3(n-q_{k-1,1}+q_{k-1,1}) \mod n = 0$$

and it follows immediately that $r_{k,1} = min(q_{k,1}, n - q_{k,1})$.

Next we will show that this property remains active if we calculate the values $q_{k,m+1}$ in \hat{G}_k and $r_{k,m+1}$ in \bar{G}_k with the help of doublings. We have here $q_{k,m+1} = 2q_{k,m} \mod lo n$. To get the number $r_{k,m+1}$ we have to calculate the value $j = 2r_{k,m} \mod lo n$ and then the number of the corresponding pair $r_{k,m+1} = \min(j, n-j)$. In the case $r_{k,m} = q_{k,m}$ we simply get here $j = 2r_{k,m} \mod lo n = q_{k,m+1}$ and therefore $r_{k,m+1} = \min(q_{k,m+1}, n-q_{k,m+1})$. In the case $r_{k,m} = n - q_{k,m}$ we have $j = 2(n - r_{k,m}) \mod lo n$ and get simply for the sum $j + q_{k,m+1}$

$$(j + q_{k,m+1}) \mod n = 2(n - r_{k,m} + r_{k,m}) \mod n = 0$$

We see so that j and $q_{k,m+1}$ are grades of inverse elements in a pair and it follows therefore simply that $r_{k,m+1} = min(q_{k,m+1}, n - q_{k,m+1})$.

According to Proposition 2 in an invariant set with natural order the inverse elements of the first 2^{ν} elements are under the final 2^{ν} elements. This means that in the work with pairs the first 2^{ν} numbers in \overline{G}_k will be different, they are the numbers of the pairs in the set G_k . The first element and the $(2^{\nu} + 1)$ -th element in G_k are inverse and if we work with pairs we come after the 2^{ν} -th number in \overline{G}_k back to the first number in \overline{G}_k . Due to this circle property for the numbers in \overline{G}_k we have the prety circle property for the pairs in G_k : starting with the first pair of the invariant set we run by the doublings through all 2^{ν} pairs of the set and come from the last pair back to the starting pair.

If we work with pairs, we have to calculate only 2^{ν} numbers of pairs. If we work with elements, we have to calculate $2^{\nu+1}$ numbers of elements.

In the case n = 257 the pairs in the 16 invariant sets with natural order are the follows:

$$\begin{array}{rcl} G_1 &= \{1,\,2,\,4,\,8,\,16,\,32\,,64,\,128\} \\ \bar{G}_2 &= \{3,\,6,\,12,\,24,\,48,\,96,\,65,\,127\} \\ \bar{G}_3 &= \{9,\,18\,;36,\,72,\,113,\,31,\,62,\,124\} \\ \bar{G}_4 &= \{27,\,54\,;108,\,41,\,82,\,93,\,71,\,115\} \\ \bar{G}_5 &= \{81,\,95\,;67,\,123,\,11,\,22,\,44,\,88\} \\ \bar{G}_6 &= \{14,\,28\,;56,\,112,\,33,\,66,\,125,\,7\} \\ \bar{G}_7 &= \{42,\,84\,;89,\,79,\,99,\,59,\,118,\,21\} \\ \bar{G}_8 &= \{126,\,5\,;10,\,20,\,40,\,80,\,97,\,63\} \\ \bar{G}_9 &= \{121,\,15\,;30,\,60,\,120,\,17,\,34,\,68\} \\ \bar{G}_{10} &= \{106,\,45\,;90,\,77,\,103,\,51,\,102,\,53\} \\ \bar{G}_{11} &= \{61,\,122\,;13,\,26,\,52,\,104,\,49,\,98\} \\ \bar{G}_{12} &= \{74,\,109\,;39,\,78,\,101,\,55,\,110,\,37\} \\ \bar{G}_{13} &= \{35,70,117,23,46,92,73,11\} \\ \bar{G}_{14} &= \{105,\,47\,;94,\,69,\,119,\,19,\,38,\,76\} \\ \bar{G}_{15} &= \{58,\,116\,;25,\,50,\,100,\,57,\,114,\,29\} \\ \bar{G}_{16} &= \{83,\,91\,;75,\,107,\,43,\,86,\,85,\,87\} \end{array}$$

In the case n = 65537 the 2048 invariant sets consist of 16 pairs and the list is too big and cannot be so simply presented.

6 Multiplication of invariant sets

Next we analyze what we will get as product of invariant sets. This is a natural question. If, for example, we split S into invariant sets, we have to calculate the product of the parts. Thus we come to the product of invariant sets.

Proposition 4. The product of two different invariant sets is the sum of $2^{\nu+1}$ invariant sets.

Proof. An invariant set, as we have seen, can be built as follows. We start with one element and add all other elements calculating repeatedly the square of the previous element. From the last element of the invariant set we come this way back to the starting element. If we work in the building of the invariant set with degrees of the elements, we have to use doublings

and calculate *modulo* n to take into account that $z^n = 1$. In the following calculations we will work with degrees and use, without discussing the small transformations every time, the well known properties of the calculation *modulo* n.

We denote the invariant sets that we want to multiply G and H and the product $G \cdot H$. We assume that these invariant sets are different, $G \neq H$. Let $\hat{G} = \{k_1, k_2, \cdots, k_{2^{\nu+1}}\}$ be the degrees of the elements in G and $\hat{H} = \{m_1, m_2, \cdots, m_{2^{\nu+1}}\}$ be the degrees of the elements in H.

The product $z^{k_i} \cdot z^{m_j}$ of elements with the degrees k_i and m_j is equal to $z^{k_i+m_j}$, and this means that we have to calculate the sum $k_i + m_j$ of the degrees k_i and m_j . We have to calculate here *modulo* n.

First let's consider the products of the first element z^{k_1} in G with all elements $z^{m_1}, z^{m_2}, \cdots, z^{m_{2^{\nu+1}}}$ in H. We obtain so the numbers

$$k_1 + m_1, k_1 + m_2, \cdots, k_1 + m_{2^{\nu+1}}$$
 (12)

For the product of the second element z^{k_2} in G with all elements in H we obtain the numbers

$$k_2 + m_1, k_2 + m_2, \cdots, k_2 + m_{2^{\nu+1}}$$
 (13)

and due to $k_2 = 2k_1$ and $m_j = 2m_{j-1}$ for $2 \le j \le 2^{\nu+1}$ they are the values

$$2k_1 + m_1, 2(k_1 + m_1), \cdots, 2(k_1 + m_{2^{\nu+1}-1})$$
(14)

Thus, for $2 \leq j \leq 2^{\nu+1}$ we get the numbers $m_2 + k_j$ by doubling of $m_1 + k_{j-1}$ exactly the same way as by the building of degrees for invariant sets.

But we have not compared the last number $k_1 + m_{2^{\nu+1}}$ in (12) and the first number $k_2 + m_1$ in (14). If we double the first of them, we gain

$$2(k_1 + m_{2^{\nu+1}}) = k_2 + m_{2^{\nu+1}+1} = k_2 + m_1$$

because we come in the set \hat{H} from $m_{2^{\nu+1}}$ back to m_1 .

So we see that we obtain all numbers in (13) with doubling of (12). We will obviously have so a doubling at each next increase for the degrees of the elements in G. There is no need to repeat the proof. Each element in the invariant set G can be selected as the starting element, and we can simply say that it is the element with the number m_2, m_3, \cdots .

We obtain so for the set of numbers (12) consequent $2^{\nu+1} - 1$ doublings. With these doublings each of the $2^{\nu+1}$ numbers in (12), will run through all degrees of elements of an invariant set if we take into account the starting number itself. It is exactly the way of building the set of degrees for an invariant set. The product $G \cdot H$ is thus the sum of $2^{\nu+1}$ invariant sets. In practical calculations with the help of elements we choose the degree of one element in one of the invariant sets and calculate the sums of this number and the degrees of all elements in the other invariant set (we have to calculate here *modulo* n) and for so defined $2^{\nu+1}$ numbers we have to find to which invariant sets they belong.

The multiplication of invariant sets is obviously commutative and we can choose from which of them we will use all elements and from which only one. We can also freely select which of the single element should be considered fixed.

In the case n = 257 the product of two different invariant sets is the sum of $16 = 2^4$ invariant sets and in the case n = 65537 this is the sum of $32 = 2^5$ invariant sets. The summands in product don't necessarily have to be different.

If we calculate the same way the square G^2 of the invariant set G, we find among the numbers

$$k_1 + k_1, k_1 + k_2, \cdots, k_1 + k_{2^{\nu+1}}$$

the value 0, because it holds $k_{2^{\nu}+1} = n - k_1$. The number 0 doesn't belong to any invariant set, but yields $z^0 = 1$. The same occurs if we use as first summand $k_2, \dots, k_{2^{\nu+1}}$. So we can see that the square of an invariant set is the sum of $2^{\nu+1}-1$ invariant sets and the constant $2^{\nu+1}$. The constant $2^{\nu+1}$ replaces the missing invariant set.

As it is preferable to work with pairs than with elements, we will schow that we can calculate the product $G \cdot H$ with the help of pairs. We limit ourselves first to the case $G \neq H$. We select again one pair in G and use all pairs in H. Let be k_1 the number of the selected pair in G and m_j , $1 \leq j \leq 2^{\nu}$, be the numbers of all pairs in H. It holds here $1 \leq k_1 \leq (n-1)/2$ and $1 \leq m_j \leq (n-1)/2$ for $1 \leq j \leq 2^{\nu}$.

In the work with pairs we have to calculate the products of the single selected pair in G with all pairs in H and find to which invariant set each of the two pairs in these products belongs. We come so, as we know, to the pairs with the numbers $min(k_1 + m_j, n - (k_1 + m_j)), 1 \le m_j \le (n-1)/2$, and the numbers $|k_1 - m_j|, 1 \le m_j \le (n-1)/2$.

It is appropriate to make here a simple remark. The inverse elements belong to the same invariant set and we can consider the numbers of pairs as numbers of elements and determine the corresponding invariant sets with the help of numbers of elements.

We want to schow that if we work with pairs we come to the same invariant sets as if we work with elements and use from G the element with the number k_1 and in H all elements. The numbers of all elements in H obviously the numbers m_j , $1 \leq j \leq 2^{\nu}$, and the numbers $n - m_j$, $1 \leq j \leq 2^{\nu}$. If we work with elements we have to calculate therefore the numbers $k_1 + m_j$, $1 \leq j \leq 2^{\nu}$, and $k_1 + (n - m_j)$, $1 \leq j \leq 2^{\nu}$, and determine the corresponding invariant sets for these numbers. It holds here $1 \leq k_1 + m_j < n$, so that $k_1 + m_j$ is a number of an element. The sum $k_1 + (n - m_j)$ can be bigger than n and we have, if necessary, calculate *modulo* n.

First we consider a number $min(k_1 + m_j, n - (k_1 + m_j))$ in the work with pairs. It applies here $1 \le k_1 + m_j < n$ and $1 \le n - (k_1 + m_j) < n$ so that $k_1 + m_j$ and $n - (k_1 + m_j)$ are the numbers of inverse elements. These elements belong to the same invariant set and we get for $min(k_1 + m_j, n - (k_1 + m_j))$ the same invariant set as for $k_1 + m_j$ in the work with elements.

For a number $|k_1 - m_j|$ we consider first the case $m_j > k_1$. It applies then $|k_1 - m_j| = m_j - k_1$ and $1 \le m_j - k_1 \le \frac{n-1}{2}$. Due to $1 \le m_j - k_1 \le \frac{n-1}{2}$ it also applies $1 \le n - (m_j - k_1) \le \frac{n-1}{2}$. But we have here $n - (m_j - k_1) = k_1 + (n - m_j)$ and thus $|k_1 - m_j|$ and $k_1 + (n - m_j)$ are the numbers of inverse elements. Therefore we get in the work with pairs for the number $|k_1 - m_j|$ the same invariant set as in the work with elements for $k_1 + (n - m_j)$.

In the case $k_1 > m_j$ it applies $|k_1 - m_j| = k_1 - m_j$ and we have in the work with pairs to determine the corresponding invariant set for the pair with the number $k_1 - m_j$. As noticesd above, we can here understand $k_1 - m_j$ as a number of an element and determine the corresponding invarian set for this element. Due to $z^n = 1$ the element with the number $k_1 - m_j$ is the same element as with the number $n + (k_1 - m_j)$ and we come, if we work with pairs, again for the number $|k_1 - m_j|$ to the same corresponding invariant set as for the number $k_1 + (n - m_j)$ in the work with elements.

We see so that in the case $G \neq H$ we come in the work with pairs and in the work with elements to the same corresponding invariant sets and therefore to the same result for the product $G \cdot H$. It is clear that we can work with pairs in the case G = H also.

In the work with pairs we are free to choose for which invariant set we will use all pairs and for which only one pair. We can also freely select the fixed pair. For the square of an invariant set the result is analogous.

In the case n = 257 we have, for example,

$$G_1 \cdot G_5 = 2G_2 + G_3 + G_4 + G_6 + 2G_7 + 2G_8 + G_9 + G_{10}$$
(15)
+G_{11} + G_{13} + G_{14} + 2G_{16}

 $G_1G_9 = 2G_1 + 2G_3 + G_5 + 2G_6 + G_7 + 2G_9 + 2G_{11} + G_{13} + 2G_{14} + G_{15} (16)$ and

$$G_1^2 = 16 + 3G_1 + 4G_2 + 2(G_3 + G_6 + G_8 + G_9)$$
(17)

In the case n = 65537 we have

$$G_1^2 = 32 + 3G_1 + 4G_2 + 2 \cdot (G_3 + G_{778} + G_{801} + G_{1025} + G_{1100} \quad (18) + G_{1117} + G_{1179} + G_{1264} + G_{1266} + G_{1900} + G_{1956} + G_{1957})$$

and

$$G_{1} \cdot G_{1025} = 2 \cdot (G_{1} + G_{1025}) + (G_{24} + G_{1048}) + 2 \cdot (G_{155} + G_{1179})$$
(19)
+(G_{185} + G_{1209}) + (G_{309} + G_{1333}) + (G_{360} + G_{1384}) + (G_{531} + G_{1555})
+(G_{667} + G_{1691}) + (G_{719} + G_{1743}) + (G_{734} + G_{1758})
+2 \cdot (G_{778} + G_{1802}) + (G_{841} + G_{1865}) + (G_{946} + G_{1970})

7 Shift property

Now we want to show a property of the product of invariant sets which we denote in the following as shift property. This property is connected with the chosen order of the invariant sets and will be very helpful in the calculations for the following splits.

Let G_p be the invariant set with the number p and G_q the invariant set with the number q, $G_p \neq G_q$, and let be correct the following representation for the product

$$G_p \cdot G_q = G_{l_1} + G_{l_2} + \dots + G_{l_{2^{\nu+1}}}$$
(20)

We want to calculate the product $G_{p+s} \cdot G_{q+s}$. The numbers of both new invariant sets here are bigger by the same amount s > 0. We speak about a shift in the product, denote the value s > 0 as the height of the shift and write shift = s.

Let k_1 be the number of an element in the invariant set G_p and $m_1, m_2, \dots, m_{2^{\nu+1}}$ be the numbers of all elements in G_q . As shown above, we have to consider for calculation of $G_p \cdot G_q$ the following sum of numbers

$$k_1 + m_1, k_1 + m_2, \cdots, k_1 + m_{2^{\nu+1}}$$
 (21)

and find to which invariant sets the elements with these numbers belong. The values in (21) are calculated *modulo* n and they are between 1 and n-1. It follows from (20) that $G_{l_1}, G_{l_2}, \cdots, G_{l_{2^{\nu+1}}}$ are exactly the $2^{\nu+1}$ corresponding invariant sets.

If we go from G_p to the invariant set G_{p+1} we obtain for G_{p+1} an element with the number $3k_1$. That is true even if p is the biggest number of invariant sets $ng = 2^{2^{\nu}-(n+1)}$. Due to the circle property for the invariant

sets we come in this case from the number of an element in the set G_{ng} by multiplication with the factor 3 to a number of an element in G_1 . We have here to understand the invariant set G_{ng+1} as G_1 .

For the invariant set G_{q+1} we have obviously the numbers of elements $3m_1, 3m_2, \dots, 3m_{2^{\nu+1}}$. The number $3k_1$ for G_{p+1} and $3m_1, 3m_2, \dots, 3m_{2^{\nu+1}}$ for G_{q+1} must be calculated *modulo* n.

In any case we gain for the sum of the new numbers of elements the following values

$$3(k_1 + m_1), 3(k_1 + m_2), \cdots, 3(k_1 + m_{2^{\nu+1}})$$
 (22)

These values must be calculated *modulo* n but it is clear that these numbers belong to invariant sets, which follow the invariant sets we used by calculating $G_p \cdot G_q$. Instead of (20) it holds thus for the product of G_{p+1} and G_{q+1}

$$G_{p+1} \cdot G_{q+1} = G_{l_1+1} + G_{l_2+1} + \dots + G_{l_{2\nu+1}+1}$$
(23)

If in (20) $l_k = ng$ is the biggest number of a invariant set, then in (23) the set G_{l_k+1} is to understand as G_1 . The next invariant set is built here in the same way as we have built all invariant sets, i.e. with increasing the starting number by the factor 3.

We have, in fact, shown that at the step to $G_{p+1} \cdot G_{q+1}$ the numbers of the invariant sets in $G_p \cdot G_q$ must be simply increased by the value 1 and the new numbers must be adjusted if they exceed the number ng. We can understand the adjusting of the numbers of invariant sets as rotation with the step 1, if all numbers $1, \dots, ng$ of invariant sets positioned on the circle. It is clear that by any shift with shift = s the result is analogous.

We calculate the function $\rho(k, m)$ for natural values k and m as follows:

$$\rho(k,m) = \begin{cases} m, & \text{if } k = k_0 \cdot m \\ rest(k,m), & \text{otherwise} \end{cases} \tag{24}$$

For any shift with the height shift = s it applies obviously

$$G_{p+s}G_{q+s} = G_{\rho(l_1+s,ng)} + G_{\rho(l_2+s,ng)} + \dots + G_{\rho(l_2\nu+1}+s,ng)$$
(25)

It is clear that for the square of an invariant set the result is completely analogous. The constant doesn't change and for the numbers of the invariant sets in the sum we have to make the appropriate shifts. For example, it would be very simply on the basis of (16 - 18) to calculate the product $S_5 \cdot S_{13}$ or the squares G_9^2 and G_{1025}^2 .

8 Splitting method

In the following we will at first, starting with S,

$$S = G_1 + G_2 + G_2 + G_3 + G_4 + \dots + G_{ng-1} + G_{ng}$$

build consequent smaller parts so that they consist of invariant sets. We will take here for the following parts every second invariant set from the previous part, starting with the first or second invariant set in the part we want to split.

For S we consider the parts F(1,2) and F(2,2). F(1,2) is here the sum of every second invariant set starting with G_1 in S, and F(2,2) is the sum of every second invariant set starting with G_2 in S,

$$F(1,2) = G_1 + G_3 + G_5 + \dots + G_{ng-1}$$
(26)

$$F(2,2) = G_2 + G_4 + G_6 + \dots + G_{ng}$$
(27)

For F(1,2) and F(2,2) the splitting will be continued. We split F(1,2) into the parts F(1,4) and F(3,4) and split F(2,2) into F(2,4) and F(4,4). We gain so

$$F(1,4) = G_1 + G_5 + G_9 + \dots + G_{ng-3}$$

$$F(3,4) = G_3 + G_7 + G_{11} + \dots + G_{ng-1}$$

$$F(2,4) = G_2 + G_6 + G_{10} + \dots + G_{ng-2}$$

$$F(4,4) = G_4 + G_8 + G_{12} + \dots + G_{ng}$$

On the basis of $F(j, 2^k)$, $1 \leq j \leq 2^k$, we define analogous $F(j, 2^{k+1})$ and $F(j+2^k, 2^{k+1})$. It holds here obviously always the equality

$$F(j, 2^{k+1}) + F(j+2^k, 2^{k+1}) = F(j, 2^k)$$

These splittings should be continued until we come to single invariant sets.

In the notation $F(j, 2^m)$ the first parameter j is the number of the invariant set with which the sum begins, and the second parameter 2^m shows by what amount the numbers of invariant sets grow.

For the following it is important to note here that the invariant set G_l belongs to the part $F(\rho(l, 2^m), 2^m)$.

We will later frequently have the shift with the height shift = s for all invariant sets in the part

$$F(k, 2^m) = G_k + G_{k+2^m} + \dots + G_{k+nq-2^m}$$

i.e. in all summands $G_k, G_{k+2^m}, \cdots, G_{k+ng-2^m}$. For this shift the distance 2^m between the numbers of the invariant sets doesn't change but instead

of the smallest number k we come obviously to the new smallest number $\rho(k+s, 2^m)$, as this number is between 1 and 2^m . This means that we come with the shift with the height shift = s from $F(k, 2^m)$ to $F(\rho(k+s, 2^m), 2^m)$.

The splitting of the invariant sets itself we will do analogous. The invariant set G_k with the natural order of its 2^{ν} pairs will be consequently splitted into parts $G_k(j, 2^m)$, $1 \leq j \leq 2^m$, formed as follows.

 $G_k(1,2)$ begins with the first pair in G_k and contains from G_k every second pair after the previous one. $G_k(2,2)$ begins with the second pair in G_k and contains from G_k every second pair after the previous one. Analogous $G_k(j, 2^m)$ will be splitted into $G_k(j, 2^{m+1})$ and $G_k(j + 2^m, 2^{m+1})$.

In notation $G_k(j, 2^m)$ the parameter j indicates the j-th pair in G_k in natural order of the pairs in G_k , and this is not the number of this pair itself. For G_1 is p_1 , in fact, the first and p_2 the second pair and $G_1(1, 2^m)$ begins therefore with p_1 and $G_1(2, 2^m)$ begins with p_2 . But for G_2 the first pair is p_3 and $G_2(1, 2^m)$ begins with p_3 and $G_2(2, 2^m)$ begins with p_6 , as p_6 is the second pair of G_2 in natural order.

It is important to understand how the numbers of the pairs in $G_k(j, 2^m)$ change, if we go from one pair to the next one. For $G_k(1, 2)$, starting with the first pair, we select always the second pair in natural order. As we come in G_k to the next pair with doubling of the number, the number of the next pair in $G_k(1, 2)$ must be four times bigger than the number of the previous pair. These numbers will be here calculated *modulo* n and, if necessary, changed from the number of an element to the number of a pair. For $G_k(2, 2)$ it is also the same. For $G_k(j, 4)$ the number of the next pair increases by the factor 16. For $G_k(j, 2^m)$ this factor is obviously 2^{2^m} .

In the case n = 17 we did the splittings of invariant sets exactly this way. We had in this case only a few possible splittings and could quickly understand that only this variant is possible.

Remark. The presented splittings corresponds to the splittings for Gaussian periods. The author was at first engaged in the construction of regular polygons just for fun and did consciously not study the publications on this subject. He knew only the result of Gauss but not his solution method. This is how he came to the splitting approach in a completely different way on the basis of invariant sets.

In the following the splittings, which belong to the same level of splitting, are united in steps. For the $2^{2^{\nu}}$ elements we need $2^{\nu} - 1$ steps to come to the single pair p_1 . In the first $2^{\nu} - \nu - 1$ steps we work with invariant sets, then with pairs in invariant sets. In step 1 we split S into F(1,2) and F(2,2), in step $m, 2 \leq m \leq 2^{\nu} - \nu - 1$, we split the values $F(j, 2^{m-1}), 1 \leq j \leq 2^{m-1}$. To come to the starting pair in an invariant set we need the next ν steps.

Proposition 5. The product $F(j, 2^{m+1}) \cdot F(j+2^m, 2^{m+1})$ can be represented and constructed on the basis of the values $F(k, 2^m)$, $1 \le k \le 2^m$.

Proof. We consider at first the product $2F(1, 2^{m+1}) \cdot F(1 + 2^m, 2^{m+1})$. It holds obviously

$$2F(1, 2^{m+1}) \cdot F(1 + 2^m, 2^{m+1}) =$$

$$(28)$$

$$(G_1G_{1+2^m} + G_1G_{1+2^m+2^{m+1}} + \dots + G_1G_{1+ng-2^m})$$

$$+(G_{1+2^m}G_{1+2^{m+1}} + G_{1+2^m}G_{1+2^m+2^{m+1}} + \dots + G_{1+2^m}G_{1+ng})$$

$$+(G_{1+2^{m+1}}G_{1+2^{m+2}} + G_{1+2^{m+1}}G_{1+2^{m+2}} + \dots + G_{1+2^{m+1}}G_{1+ng+2^m})$$

$$+(G_{1+2^m+2^{m+1}}G_{1+ng+2^{m+1}})$$

$$+\dots$$

$$+(G_{1+ng-2^{m+1}}G_{1+ng-2^m} + G_{1+ng-2^m+1}G_{1+ng+2^m} + \dots + G_{1+ng-2^m}G_{1+2\cdot ng-2^{m+1}})$$

$$+(G_{1+ng-2^m}G_{1+ng} + G_{1+ng-2^m}G_{1+ng+2^{m+1}} + \dots + G_{1+ng-2^m}G_{1+2\cdot ng-2^{m+1}})$$

The first factor inside the brackets in (28) is chosen alternating from $F(1, 2^{m+1})$ and $F(1 + 2^m, 2^{m+1})$ and does not change within the brackets.

The second factor changes. The number of the invariant set for the second factor is bigger than for the first factor and can also be bigger than ng. In the first brackets with the products G_1G_j the number j of the second factor grows by the amount 2^{m+1} from $1+2^m$ to $1+ng-2^m$. In the second brackets with the products $G_{1+2^m}G_j$ the number j grows by the amount 2^{m+1} from $1+2^{m+1}$ to 1+ng. We take here into account that $G_{ng+1} = G_1$ and therefore we have $G_{1+2^m}G_{1+ng} = G_{1+2^m}G_1$. In the third brackets with the products $G_{1+2^m+1}G_j$ the number j grows by the amount 2^{m+1} from $1+2^m+2^{m+1}$ to $1+ng+2^m$ and we have here $G_{1+2^m+2^{m+1}}G_{1+ng+2^m} = G_{1+2^m+2^{m+1}}G_{1+2^m}$. This continues until we come in the last brackets to the products $G_{1+ng-2^m}G_j$. We obtain so certainly all relevant products twice.

One sees immediately that we obtain the summands in the next brackets with the shift of summands in the previous brackets with height $shift = 2^m$.

If we shift any invariant set with the height $shift = 2^m$, we obtain obviously an invariant set in the same part $F(k, 2^m)$, and if we repeat the shifts $2^m - 1$ times, the rusult will properly run through $F(k, 2^m)$. This means that the product $2F(1, 2^{m+1}) \cdot F(1 + 2^m, 2^{m+1})$ is a sum of values $F(k, 2^m)$, and they can be determined as follows. We have to consider the invariant sets in sum of the products in the first brackets

$$G_1G_{1+2^m} + G_1G_{1+2^m+2^{m+1}} + \dots + G_1G_{1+nq-2^m}$$
(29)

i.e. the sum of products G_1 with all other invariant sets in $F(1 + 2^m, 2^{m+1})$, and determine to which part $F(k, 2^m)$, $1 \le k \le 2^m$, they belong. If then $\gamma(k, 2^m)$ is the amount of these invariant sets in $F(k, 2^m)$, $1 \le k \le 2^m$, it holds

$$2F(1,2^{m+1}) \cdot F(1+2^m,2^{m+1}) = \sum_{k=1}^{2^m} \gamma(k,2^m) F(k,2^m)$$
(30)

In (29) the summands, which stand symmetrical to the mid, have the same amount of invariant sets in $F(k, 2^m)$, $1 \leq k \leq 2^m$. Indeed, we come from $G_1G_{1+2^m+k\cdot 2^{m+1}}$ to $G_1G_{1+ng-2^m-k\cdot 2^{m+1}}$ if we perform a shift with the height $shift = ng - 2^m - k \cdot 2^{m+1}$. By this shift G_1 goes to $G_{1+ng-2^m-k\cdot 2^{m+1}}$ and $G_{1+2^m+k\cdot 2^{m+1}}$ becomes $G_{1+ng} = G_1$. As the multiplication of invariant sets is commutative we obtain from the first product the second. But if we shift an invariant set with the height $shift = ng - 2^m - k \cdot 2^{m+1}$, we obtain an invariant set which belongs to the same part $F(k, 2^m)$. We can therefore instead of the complete sum in (29) consider the half of this sum and determine the amount $\mu(k, 2^m)$ of invariant sets in $F(k, 2^m)$, $1 \leq k \leq 2^m$, for this half

$$G_1G_{1+2^m} + G_1G_{1+2^m+2^{m+1}} + \dots + G_1G_{1+ng/2-2^m}$$
(31)

It applies then

$$F(1, 2^{m+1}) \cdot F(1 + 2^m, 2^{m+1}) = \sum_{k=1}^{2^m} \mu(k, 2^m) F(k, 2^m)$$
(32)

To come from $F(1, 2^{m+1}) \cdot F(1+2^m, 2^{m+1})$ to $F(j, 2^{m+1}) \cdot F(j+2^m, 2^{m+1})$ we have to perform in (32) a shift with the height shift = j - 1 for the starting invariant set G_k of $F(k, 2^m)$ and with this shift $F(k, 2^m)$ goes to $F(\rho(k+j-1, 2^m), 2^m)$. It applies thus

$$F(j, 2^{m+1}) \cdot F(j+2^m, 2^{m+1}) = \sum_{k=1}^{2^m} \mu(k, 2^m) F(\rho(k+j-1, 2^m), 2^m) \quad (33)$$

We have presented the product $F(j, 2^{m+1}) \cdot F(j + 2^m, 2^{m+1})$ as a linear combination of the values $F(k, 2^m)$ with integer coefficients and this presentation certainly can be constructed with a compass and straightedge if these values are given.

Remark 1. To make the formulas more understandable we showed in (28) and (29) more summands of $F(1, 2^m)$. It is clear that the approach is analogous also in the cases that $F(1, 2^m)$ has only of 2 or 4 summands.

Remark 2. The approach can be used for splitting S into F(1,2) and F(2,2) and we achieve in this case a very pretty result. In (31) we have in this case $\frac{ng}{4}$ products which yield $\frac{ng}{4} \cdot 2^{\nu+1} = \frac{(n-1)}{4}$ invariant sets. For these invariant sets we have a shift with the height shift = 1, and each of them properly runs through S. In this case we obtain thus simply

$$F(1,2) \cdot F(2,2) = (n-1)/4 \cdot S = -(n-1)/4$$
(34)

In the case n = 257 we can also easy show that $F(1,4) \cdot F(3,4)$ is an integer. In this case, as we know, we have to consider the sum $G_1G_3 + G_1G_7$ and determine the amount of invariant sets from F(1,2) and F(2,2) in this sum. The two necessary products in the sum can be calculated trivially. So we obtain in the case n = 257 that $\mu(1,2) = \mu(2,2) = 16$ and therefore

$$F(1,4) \cdot F(3,4) = 16 \cdot (F(1,2) + F(2,2)) = 16 \cdot S = -16$$

Significant is here obviously that $\mu(1,2)$ and $\mu(2,2)$ are equal.

We wont to calculate $F(1,4) \cdot F(3,4)$ even in the case n = 65537. First we show here that the values $\mu(1,2)$ and $\mu(2,2)$ are equal, and then we can easily calculate them. $\mu(1,2)$ and $\mu(2,2)$ are integer numbers, they are the amount of invariant sets with odd and even numbers respectively in the sum

$$G_1G_3 + G_1G_7 + G_1G_{11} + \dots + G_1G_{1023}$$

This sum has 256 products and therefore in total $256 \cdot 32 = (n-1)/8$ invariant sets. It applies therefore $\mu(1,2) + \mu(2,2) = (n-1)/8$, and we want to show that $\mu(1,2) = \mu(2,2) = (n-1)/16 = 4096$.

The simple numerical calculation for the sum of the corresponding values $cos(2k\pi/n)$ shows that it applies approximately: $F(1,2) \approx 127,501$, $F(2,2) \approx -128,501$, $F(1,4) \approx -26,58292$ and $F(3,4) \approx 154,0839$. With the help of these results we gain immediately that $F(1,4) \cdot F(3,4) \approx -4095,9999987$ and $F(1,2) - F(2,2) \approx 256,002$.

Let be $\mu(1,2) = \frac{(n-1)}{16} + k$ and $\mu(2,2) = \frac{(n-1)}{16} - k$, where k obviously has to be an integer between -(n-1)/16 and (n-1)/16. It applies then

$$F(1,4) \cdot F(3,4) = 4096 \cdot (F(1,2) + F(2,2)) + k \cdot (F(1,2) - F(2,2))$$

= 4096 \cdot S + k \cdot (F(1,2) - F(2,2))

and therefore

$$-4096 + k \cdot 256,002 \approx -4095,9999987$$

The calculation accuracy certainly allows just the only possibility that this approximative equality is correct, it must be k = 0. Then we have here $\mu(1,2) = \mu(2,2) = (n-1)/16$ and therefore

$$F(1,4) \cdot F(3,4) = -(n-1)/16 \tag{35}$$

It follows obviously that the product $F(2, 4) \cdot F(4, 4)$ is here the same integer, $F(2, 4) \cdot F(4, 4) = -(n-1)/16.$

We can calculate the product $2F(1, 2^{m+1}) \cdot F(1+2^m, 2^{m+1})$ a different way with the help of squares, and this can be advantageous in the case n = 65537. It applies obviously

$$2F(1, 2^{m+1}) \cdot F(1 + 2^m, 2^{m+1}) = \left(F(1, 2^{m+1}) + F(1 + 2^m, 2^{m+1})\right)^2 - F^2(1, 2^{m+1}) - F^2(1 + 2^m, 2^{m+1}) = F^2(1, 2^m) - Q_1 - Pr_1$$

where Q_1 is the sum of the squares of the invariant sets in $F(1, 2^{m+1})$ and in $F(1 + 2^m, 2^{m+1})$ and Pr_1 is the twice sum of products of different invariant sets in $F(1, 2^{m+1})$ and in $F(1 + 2^m, 2^{m+1})$.

 Q_1 is obviously the sum of the squares of all invariant sets in $F(1, 2^m)$

$$Q_1 = G_1^2 + G_{1+2^m}^2 + G_{1+2^{m+1}}^2 + \dots + G_{1+ng-2^{m+1}}^2 + G_{1+ng-2^m}^2$$

and this sum can be easily calculated. Indeed, for every step from one square to the next one in this sum we have for these squares a shift with the height $shift = 2^m$. At these shifts with $shift = 2^m$ an invariant set remains in the same part $F(k, 2^m)$. We have $ng/2^m$ squares, and it means that each invariant set in the first square G_1^2 will properly run through the corresponding part $F(k, 2^m)$. We can therefore calculate Q_1 as follows. We consider all invariant sets in the first square G_1^2 and determine for these invariant sets the amount $\gamma_1(k, 2^m)$ of invariant sets which belong to $F(k, 2^m)$, $1 \le k \le 2^m$. The sum Q_1 has then the following presentation

$$Q_1 = (n-1)/2^m + \sum_{k=1}^{2^m} \gamma_1(k, 2^m) \cdot F(k, 2^m)$$

We obtain here the constant $(n-1)/2^m = 32 \cdot ng/2^m$ as the sum of the constants for the $ng/2^m$ invariant sets. The square G_1^2 is already calculated, (18), and we can simply determine the necessary numbers $\gamma_1(k, 2^m)$.

For Pr_1 , the twice sum of products of different invariant sets in the part $F(1, 2^{m+1})$ and in the part $F(1 + 2^m, 2^{m+1})$, we come analogously to (28) to the following presentation

$$Pr_{1} = (G_{1}G_{1+2^{m+1}} + G_{1}G_{1+2^{m+2}} + \dots + G_{1}G_{1+ng-2^{m+1}})$$
(36)
+($G_{1+2^{m}}G_{1+2^{m}+2^{m+1}} + G_{1+2^{m}}G_{1+2^{m}+2^{m+2}} + \dots + G_{1+2^{m}}G_{1+ng+2^{m}})$
+($G_{1+2^{m+1}}G_{1+2^{m+2}} + G_{1+2^{m+1}}G_{1+2^{m+3}} + \dots + G_{1+2^{m+1}}G_{1+ng})$
+($G_{1+2^{m}+2^{m+1}}G_{1+2^{m}+2^{m+2}} + G_{1+2^{m}+2^{m+1}}G_{1+2^{m}+2^{m+3}} + \dots)$
+...

In this presentation the first factor is chosen alternately from $F(1, 2^{m+1})$ and $F(1 + 2^m, 2^{m+1})$ and is multiplied by the other invariant sets of the same part. The number of the second factor is bigger than the number of the first factor and can be bigger than ng.

For the so formed sum we have a shift with the height $shift = 2^m$ and to calculate Pr_1 we have therefore to consider the sum in the first brackets

$$G_1 G_{1+2^{m+1}} + G_1 G_{1+2^{m+2}} + \dots + G_1 G_{1+ng-2^{n+2}} + G_1 G_{1+ng-2^{m+1}}$$
(37)

and determine for this sum the amount $\gamma_2(k, 2^m)$ of invariant sets in $F(k, 2^m)$, $1 \le k \le 2^m$. Thus we obtain

$$Pr_1 = \sum_{k=1}^{2^m} \gamma_2(k, 2^m) F(k, 2^m).$$

In (37) the pairs, which stand symmetrical to the mid, have the same amount of invariant sets in $F(k, 2^m)$, but the mid itself has not a symmetrical pair. For the calculation of $\gamma_2(k, 2^m)$ we have to take the amount of pairs from $F(k, 2^m)$ in

$$G_1G_{1+2^{m+1}} + G_1G_{1+2^{m+2}} + \dots + G_1G_{1+ng/2-2^{m+1}}$$

twice and for the invariant sets from $G_1G_{1+ng/2}$ only once.

The new presentation of $F(1, 2^{m+1}) \cdot F(1 + 2^m, 2^{m+1})$ can obviously also be constructed with a compass and straightedge.

The advantage if this slightly more complicated approach is that in the case n = 65537 we have for m = 2 to consider here the 128 products $G_1 \cdot G_9, G_1 \cdot G_{17}, \dots, G_1 \cdot G_{1025}$ and the square G_1^2 . For $m \ge 3$ we have to consider smaller and smaller parts of these products. If we use the first (slightly simpler) approach we need in total 256 products $G_1 \cdot G_5, G_1 \cdot G_9, \dots, G_1 \cdot G_{1025}$.

Next we consider the splitting of invariant sets itself. As above we denote ng the number of all invariant sets, and np denotes here the number of all pairs in S, np = (n - 1)/2.

Proposition 6. The product $G_k(s, 2^{m+1}) \cdot G_k(s+2^m, 2^{m+1})$ can be calculated and constructed with a compass and straightedge on the basis of the values $G_i(l, 2^m)$, $1 \leq j \leq ng$, $1 \leq l \leq 2^m$.

Proof. We consider first the product $G_1(1, 2^{m+1}) \cdot G_1(1+2^m, 2^{m+1})$. To make the following presentations simpler we denote here M the value 2^{2^m} , $M = 2^{2^m}$. Then it applies obviously

$$G_1(1,2^m) = p_1 + p_M + p_{M^2} + p_{M^3} + p_{M^4} + \dots + p_{(n-1)/(M^2)} + p_{(n-1)/M^2}$$

This presentation fits in the case m = 0 too. In this case we have here $G_1(1,1) = G_1$ and M = 2.

The number of pairs always increase here by the factor M and because of $M \cdot (n-1)/M = n-1$ and $\min(n-1, n-(n-1)) = 1$ we come from the last pair $p_{(n-1)/M}$ back to the starting pair p_1 . It applies then

$$G(1, 2^{m+1}) = p_1 + p_{M^2} + p_{M^4} + \dots + p_{(n-1)/M^2}$$

and

$$G_1(1+2^m, 2^{m+1}) = p_M + p_{M^3} + p_{M^5} + \dots + p_{(n-1)/M}$$

The sum of the parts is known, $G_1(1, 2^{m+1}) + G_1(1 + 2^m, 2^{m+1}) = G_1(1, 2^m)$, and the product $G_1(1, 2^{m+1}) \cdot G_1(1 + 2^m, 2^{m+1})$ we calculate with the help of squares. It applies

$$2G_1(1, 2^{m+1}) \cdot G_1(1+2^m, 2^{m+1}) = \left(G_1(1, 2^{m+1}) + G_1(1+2^m, 2^{m+1})\right)^2 -G_1^2(1, 2^{m+1}) - G_1^2(1+2^m, 2^{m+1}) = G_1^2(1, 2^m) - Q - Pr$$

where Q is the sum of the squares of all pairs in $G_1(1, 2^{m+1})$ and in $G_1(1+2^m, 2^{m+1})$, and Pr is the twice sum of the products of different pairs in $G_1(1, 2^{m+1})$ and in $G_1(1+2^m, 2^{m+1})$.

Q is obviously the sum of squares of all pairs in $G_1(1, 2^m)$ and it holds

$$Q = p_1^2 + p_M^2 + p_{M^2}^2 + p_{M^3}^2 + \dots + p_{(n-1)/M}^2$$

= $(p_2 + p_{2M} + p_{2M^2} + p_{2M^3} + \dots + p_{2(n-1)/M}) + 2 \cdot 2^{\nu}/2^m$
= $G_1(2, 2^m) + 2^{\nu+1-m}$

We get here the constant $2 \cdot 2^{\nu}/2^m = 2^{\nu+1-m}$ because $G_1(1, 2^m)$ has $2^{\nu}/2^m$ pairs and the square of every pair provides the constant 2. The equality

$$p_2 + p_{2M} + p_{2M^2} + p_{2M^3} + \dots + p_{2(n-1)/M} = G_1(2, 2^m)$$

is obvious because we come with the increase of the number of each pair by the factor 2 from $G_1(1, 2^m)$ to $G_1(2, 2^m)$.

It applies thus

$$2G_1(1,2^{m+1}) \cdot G_1(1+2^m,2^{m+1}) = G_1^2(1,2^m) - G_1(2,2^m) - 2^{\nu+1-m} - Pr \quad (38)$$

and for the twice sum of different pairs in $G_1(1, 2^{m+1})$ and in $G_1(1+2^m, 2^{m+1})$

we have the following presentation

$$Pr = (p_{1}p_{M^{2}} + p_{1}p_{M^{4}} + \dots + p_{1}p_{(n-1)/M^{2}}))$$

$$+ (p_{M}p_{M^{3}} + p_{M}p_{M^{5}} + \dots + p_{M}p_{(n-1)/M})$$

$$+ (p_{M^{2}}p_{M^{4}} + p_{M^{2}}p_{M^{6}} + \dots + p_{M^{2}}p_{(n-1)})$$

$$+ (p_{M^{3}}p_{M^{5}} + p_{M^{3}}p_{M^{7}} + \dots + p_{M^{3}}p_{(n-1)\cdot M})$$

$$+ \dots$$

$$+ (p_{(n-1)/M^{2}}p_{(n-1)} + p_{(n-1)/M^{2}}p_{(n-1)M^{2}} + \dots + p_{(n-1)/M^{2}}p_{(n-1)^{2}/M^{4}})$$

$$+ (p_{(n-1)/M}p_{(n-1)M} + p_{(n-1)/M}p_{(n-1)M^{3}} + \dots + p_{(n-1)/M}p_{(n-1)^{2}/M^{3}}).$$
(39)

In the brackets the first factor is chosen alternately from $G_1(1, 2^{m+1})$ and $G_1(1 + 2^m, 2^{m+1})$ and this factor doesn't change within the brackets. The number of the second factor is bigger than the number of the first one and can be bigger than np. We use here the circle property for the pairs. In the third brackets we have, for example, $p_{M^2}p_{(n-1)} = p_{M^2}p_1$ an in the fourth brackets we have $p_{M^3}p_{(n-1)M} = p_{M^3}p_M$. In the last brackets we have $p_{(n-1)/M}p_{(n-1)M} = p_{(n-1)/M}p_{(n-1)M^3} = p_{(n-1)/M}p_{M^3}$ and $p_{(n-1)/M}p_{(n-1)^2/M^3} = p_{(n-1)/M}p_{(n-1)/M^3}$. So we certainly obtain all corresponding products of pairs twice.

For the chosen representation we can see that if we go from one pair of brackets to the next pair of brackets the number of the first factor always gets M times higher: we have $p_1, p_M, p_{M^2}, p_{M^3}, \cdots$. For the numbers of the second pairs inside the brackets we have the same, they also get M times bigger if we go to the next pair of brackets. Inside the first brackets we have, for example, $p_{M^2}, p_{M^4}, \cdots, p_{(n-1)/M^2}$ and inside the second pair we have $p_{M^3}, p_{M^5}, \cdots, p_{(n-1)/M}$.

But if both numbers of pairs in product get M times bigger, then the numbers of the pairs in the result of the product also will be M times bigger. We have here, of course, to calculate *modulo* n and change, if necessary, from the number of an element to a number of a pair. If we take any starting pair and calculate then again and again pairs with M times bigger numbers, the pairs remain in the same part $G_j(l, 2^m)$ to which the starting pair belongs. These pairs will obviously properly run through the part $G_j(l, 2^m)$ if we calculate $2^{\nu}/2^m$ pairs. This is exactly how the parts $G_j(l, 2^m)$ are built.

So we see that Pr is equal to the sum of values $G_j(l, 2^m)$, and these $G_j(l, 2^m)$ are the parts to which belong the pairs from the sum in the first brackets

$$p_1 p_{M^2} + p_1 p_{M^4} + \dots + p_1 p_{(n-1)/M^4} + p_1 p_{(n-1)/M^2}$$

$$\tag{40}$$

This sum consists of the products of the first pair in $G_1(1, 2^{m+1})$ with the other pairs in $G_1(1, 2^{m+1})$. It follows therefore from (38-39) that we have for

the product $G_1(1, 2^{m+1}) \cdot G_1(1 + 2^m, 2^{m+1})$ a presentation on the basis of a constant and the values $G_j(l, 2^m)$.

Pr must be calculated only if $2 \leq 2^{m+1} \leq 2^{\nu-2}$. In the case $2^{m+1} = 2^{\nu-1}$ the value Pr disappears, because in (40) no product remains.

We want to look closely at the products which stand in (40) symmetrically to the mid. These are the products $p_1 p_{M^{2k}}$ and $p_1 p_{(n-1)/M^{2k}}$ and the numbers of the pairs in the results of the products are $M^{2k} - 1$ and $M^{2k} + 1$ as well as $(n-1)/M^{2k} - 1$ and $(n-1)/M^{2k} + 1$. If we multiply the numbers for the first product by the factor $(n-1)/M^{2k}$, we obtain obviously elements which belong to the same part $G_i(l, 2^m)$. But it applies

$$(M^{2k} - 1) \cdot (n - 1)/M^{2k} = n - 1 - (n - 1)/M^{2k} = n - (1 + (n - 1)/M^{2k})$$

and due to $1+(n-1)/M^{2k} < (n-1)/2$ it holds $n-(1+(n-1)/M^{2k}) > (n-1)/2$ and therefore the corresponding number of pair is here $1+(n-1)/M^{2k}$. It applies analogously

$$(M^{2k}+1) \cdot (n-1)/M^{2k} = n-1 + M^{2k} = n - (M^{2k}-1)$$

and the corresponding number of the pair is $M^{2k} - 1$. We see so that the pairs for the products which stand symmetrically to the mid belong to the same parts $G_j(l, 2^m)$ and yield the same input to Pr.

We denote in the following the input for the products in the front of the mid in (40) as Pr_L . In this denomination L schould poin out that we use products left regarding the mid. If we have only 4 summands in $G_1(1, 2^m)$, we have in (40) only 1 product, i.e. the product in the mid, and Pr_L disappears, $Pr_L = 0$.

The input for the product in the mid of (40) we denote Pr_M . He is not present, i.e. $Pr_M = 0$, if we have in $G_1(1, 2^m)$ only 2 pairs and therefore no products in (40).

We can calculate Pr_M exactly. In the case n = 257 we have in the mid of (40). the product p_1p_{16} and it applies $p_1p_{16} = p_{15} + p_{17}$. The pair p_{15} is here the 2th and p_{17} is the 6th pair G_9 . In the case $2^{m+1} = 2$ they provide together the input $Pr_M = 2G_9$, and in the case $2^{m+1} = 4$ they provide together the input $Pr_M = 2G_9(2, 2)$.

In the case n = 65537 we have in the mid of (40). the product p_1p_{256} and it applies $p_1p_{256} = p_{255} + p_{257}$. The pair p_{255} is here the 4th and p_{257} is the 12th pair in G_{1025} . The common input of these pairs is here the follows: in the case $2^{m+1} = 2$ he is $Pr_M = 2G_{1025}$, in the case $2^{m+1} = 4$ he is $Pr_M = 2G_{1025}(2, 2)$, and in the case $2^{m+1} = 8$ he is $Pr_M = 2G_{1025}(4, 4)$.

So we can calculate the value Pr easier as $Pr = P_M + 2 \cdot Pr_L$. We don't have to calculate some unnecessary products of pairs and to determine the corresponding parts $G_j(l, 2^m)$. We could analogously to the previous derive a presentation for the product $G_k(1, 2^{m+1}) \cdot G_k(1 + 2^m, 2^{m+1})$. But it is easier to notice that in $G_k(1, 2^{m+1})$ and in $G_k(1 + 2^m, 2^{m+1})$ the numbers of pairs by the factor 3^{k-1} higher than in $G_1(1, 2^{m+1})$ and $G_1(1 + 2^m, 2^{m+1})$ respectively. It follows therefore immediately that in the product $G_k(1, 2^{m+1}) \cdot G_k(1 + 2^m, 2^{m+1})$ the numbers of pairs must be 3^{k-1} times higher than in $G_1(1, 2^{m+1}) \cdot G_1(1 + 2^m, 2^{m+1})$. This means that we obtain $G_k(1, 2^{m+1}) \cdot G_k(1 + 2^m, 2^{m+1})$ on the basis of $G_1(1, 2^{m+1}) \cdot G_1(1 + 2^m, 2^{m+1})$ with the shift with the height shift = k - 1 for the numbers of invariant sets. This shift must be done for the number j for every summand $G_j(l, 2^m)$ of the product $G_1(1, 2^{m+1}) \cdot G_1(1 + 2^m, 2^{m+1})$, and due to the circle property for the invariant sets we come here from $G_j(l, 2^m)$ to $G_{\rho(j+k-1,ng)}(l, 2^m)$.

The product $G_k(s, 2^{m+1}) \cdot G_k(s + 2^m, 2^{m+1})$ can be simply obtained on the basis of $G_k(1, 2^{m+1}) \cdot G_k(1 + 2^m, 2^{m+1})$. Indeed, in $G_k(s, 2^{m+1})$ and $G_k(s + 2^m, 2^{m+1})$ the numbers of pairs are by the factor 2^{s-1} higher than in $G_k(1, 2^{m+1})$ and in $G_k(1 + 2^m, 2^{m+1})$ respectively. Therefore the numbers of pairs in product $G_k(s, 2^{m+1}) \cdot G_k(s+2^m, 2^{m+1})$ also by the factor 2^{s-1} higher than for pairs in $G_k(1, 2^{m+1}) \cdot G_k(1+2^m, 2^{m+1})$. This means that we come from the product $G_k(1, 2^{m+1}) \cdot G_k(1 + 2^m, 2^{m+1})$ to $G_k(s, 2^{m+1}) \cdot G_k(s + 2^m, 2^{m+1})$ with the help of the shift in the numbers of the starting pairs with the height shift = s - 1. This shift must be done for the starting number j for all summands $G_j(l, 2^m)$ of the product $G_k(1, 2^{m+1}) \cdot G_k(1 + 2^m, 2^{m+1})$. Due to the circle property for the pairs we come with this shift from $G_j(l, 2^m)$ to $G_j(\rho(l+s-1, 2^m), 2^m)$.

The values $G_k(s, 2^{m+1}) \cdot G_k(s+2^m, 2^{m+1})$ certainly can be constructed with a compass and straightedge.

Remark 1. In the denomination of Pr, Pr_L and Pr_M we have no reference for the value 2^m , but it is always clear which value exactly is meant. Due to $G_j(1,1) = G_j$ we obtain for the product $G_k(1,2) \cdot G_k(2,2)$ a presentation on the basis of invariant sets.

Remark 2. We could obviously derive a simpler presentation for $G_k(j, 2^{m+1}) \cdot G_k(j + 2^m, 2^{m+1})$ without the help of squares. But it results in more products and, as we have seen for the 17-gon, in more splittings.

9 Regular 257-gon

In the case n = 257 we have 16 invariant sets, each with 8 pairs.

Step 1. First of all we split S into F(1,2) and F(2,2).

The sum and the product are known here: F(1,2) + F(2,2) = S = -1and $F(1,2) \cdot F(2,2) = -(n-1)/4 = -64$. Therefore F(1,2) and F(2,2) are the solutions of the the quadratic equation

$$x^2 + x - 64 = 0 \tag{41}$$

and due to F(1,2) > F(2,2) we have

$$F(1,2) == \frac{-1 + \sqrt{257}}{2}, \quad F(2,2) = \frac{-1 - \sqrt{257}}{2}$$
(42)

Step 2. We split F(j, 2) into F(j, 4) and F(2 + j, 4), $1 \le j \le 2$.

The sum and the product are known here:

F(j,4) + F(2+j,4) = F(j,2) and $F(j,4) \cdot F(2+j,4) = -(n-1)/16 = -16$. Therefore we can calculate F(j,4) and F(2+j,4) on the basis of the quadratic equation

$$x^2 - F(j,2)x - 16 = 0$$

Due to F(1,4) > F(3,4) and F(2,4) > F(4,4) we obtain for $1 \le j \le 2$

$$F(j,4) = \frac{F(j,2)}{2} + \sqrt{\frac{F^2(j,2)}{4} + 16} = \frac{F(j,2) + \sqrt{F^2(j,2) + 64}}{2}$$
$$F(2+j,4) = \frac{F(j,2)}{2} - \sqrt{\frac{F^2(j,2)}{4} + 16} = \frac{F(j,2) - \sqrt{F^2(j,2) + 64}}{2}$$

It is possible to reform these formulas so that $F^2(j, 2)$ disappears. Indeed, as shown in step 1, (41), we have for F(j, 2) the equality

$$F^2(j,2) + F(j,2) - 64 = 0$$

and can replace $F^2(j,2)$ by 64 - F(j,2). It follows thus for $1 \le j \le 2$

$$F(j,4) = \frac{F(j,2) + \sqrt{128 - F(j,2)}}{2}$$
(43)

$$F(2+j,4) = \frac{F(j,2) - \sqrt{128 - F(j,2)}}{2}$$
(44)

Step 3. We consider at first the split of $F(1, 4) = G_1 + G_5 + G_9 + G_{13}$ into $F(1, 8) = G_1 + G_9$ and $F(5, 8) = G_5 + G_{13}$.

For the sum we have F(1,8) + F(5,8) = F(1,4), and to calculate the product $F(1,8) \cdot F(5,8)$ we have to determine the amount $\mu(k,4)$ of invariant sets from F(k,4), $1 \leq k \leq 4$, in G_1G_5 . The product G_1G_5 was already calculated, (15), and we have here

$$\mu(1,4) = 2, \ \mu(2,4) = 5, \ \mu(3,4) = 4, \ \mu(4,4) = 5.$$

Thus we obtain

$$F(1,8) \cdot F(5,8) = 2F(1,4) + 5F(2,4) + 4F(3,4) + 5F(4,4)$$

= 5S - 3F(1,4) - F(3,4) = -5 - 3F(1,4) - F(3,4)

and it follows therefore for F(j, 8) and F(4 + j, 8), $1 \le j \le 4$,

$$F(j,8) + F(4+j,8) = F(j,4)$$

$$F(j,8) \cdot F(4+j,8) = -5 - 3F(j,4) - F(\rho(2+j,4),4)$$

The values F(j, 8) and F(4+j, 8), $1 \le j \le 4$, definitely can then be calculated and constructed on the basis of the relevant quadratic equation provided that

$$F(1,8) > F(5,8), F(2,8) < F(6,8), F(3,8) > F(7,8), F(4,8) < F(8,8).$$

We do not make here the possible transformations of the solutions so that the square $F^2(j, 4)$ disappears. This is not absolutely necessary as the square can be constructed with a compass and straightedge.

Step 4. We consider at first the split of $F(1,8) = G_1 + G_9$ into $F(1,16) = G_1$ and $F(9,16) = G_9$.

For the sum we have $G_1 + G_9 = F(1, 8)$. One could calculate the product $G_1 \cdot G_9$ analogous to the previous step. But it is already calculated, (16), and we use this result and make only a simple transformation:

$$G_1 \cdot G_9 = 2F(1,8) + 2F(3,8) + F(5,8) + 2F(6,8) + F(7,8)$$

= -2 - F(5,8) - F(7,8)

For G_j and G_{8+j} , $1 \le j \le 8$, we have therefore

$$G_j + G_{8+j} = F(j,8)$$

$$G_j \cdot G_{8+j} = -2 - F(\rho(4+j,8),8) - F(\rho(6+j,8),8)$$

For the solutions of the relevant quadratic equations it must be kept in mind that

$$G_1 > G_8, G_2 > G_{10}, G_3 > G_{11}, G_4 > G_{12}, G_5 > G_{13}, G_6 > G_{14}, G_7 < G_{15}.$$

From here on we consider the steps with the splittings of invariant sets into pairs and we consider these steps in reverse order. Duo to the special interest in the value p_1 , we consider the steps so that we come to p_1 without unneeded calculations. As p_1 belongs to G_1 we start with the split of G_1 . Step 7. The last split to obtain p_1 is the split of $G_1(1,4) = p_1 + p_{16}$ into p_1 and p_{16} . For the sum it holds $p_1 + p_{16} = G_1(1,4)$, and for the product $2p_1 \cdot p_{16}$ we have, (38-39),

$$2p_1 \cdot p_{16} = G_1^2(1,4) - G_1(2,4) - 4$$

The term Pr is absent here. For p_1 and p_{16} it applies thus

$$p_1 + p_{16} = G_1(1,4)$$

$$p_1 \cdot p_{16} = \frac{G_1^2(1,4) - G_1(2,4)}{2} - 2$$

The values p_1 and p_{16} can be clearly calculated on the basis of the relevant quadratic equation provided that $p_1 > p_{16}$.

For the calculations in step 7 we need in any case the values $G_1(1, 4)$ and $G_1(2, 4)$, and it is necessary to get them in step 6 at the splitting of $G_1(1, 2)$ and $G_1(2, 2)$.

Step 6. We split at first $G_1(1,2) = p_1 + p_4 + p_{16} + p_{64}$ into $G_1(1,4) = p_1 + p_{16}$ and $G_1(3,4) = p_4 + p_{64}$.

The sum is known, $G_1(1,4) + G_1(3,4) = G_1(1,2)$, and for the product $2G_1(1,4) \cdot G_1(3,4)$ it holds, (38-39),

$$2G_1(1,4) \cdot G_1(3,4) = G_1^2(1,2) - G_1(2,2) - 8 - Pr_M$$

The part Pr_L is absent here and the part Pr_M is known, $Pr_M = 2G_9(2,2)$. For $G_1(1,4)$ and $G_1(3,4)$ we have therefore

$$G_1(1,4) + G_1(3,4) = G_1(1,2)$$

$$G_1(1,4) \cdot G_1(3,4) = \frac{G_1^2(1,2) - G_1(2,2)}{2} - 4 - G_9(2,2)$$

and in the calculation of $G_1(1,4)$ and $G_1(3,4)$ on the basis of the relevant quadratic equation it is to consider that $G_1(1,4) > G_1(3,4)$.

For step 7 we need $G_1(2,4)$ also, and therefore we split $G_1(2,2)$ into $G_1(2,4)$ and $G_1(4,4)$. Compared to $G_1(1,4)$ and $G_1(3,4)$ we have here a shift with the height *shift* = 1 for the starting pair. For $G_1(2,4)$ and $G_1(4,4)$ we get therefore

$$G_1(2,4) + G_1(2,4) = G_1(2,2)$$

$$G_1(2,4) \cdot G_1(4,4) = \frac{G_1^2(2,2) - G_1(1,2)}{2} - 4 - G_9(1,2)$$

and in the calculation of $G_1(2,4)$ and $G_1(4,4)$ on the basis of the relevant quadratic equation it is to consider that $G_1(2,4) > G_1(4,4)$.

It remains only to notice that we need for the calculations in this step the values $G_1(1,2)$, $G_1(2,2)$ as well as $G_9(1,2)$ and $G_9(2,2)$. It is necessary to get them in step 5.

Step 5. We split at first $G_1 = p_1 + p_2 + p_4 + p_8 + p_{16} + p_{32} + p_{64} + p_{128}$ into $G_1(1,2) = p_1 + p_4 + p_{16} + p_{64}$ and $G_1(2,2) = p_2 + p_8 + p_{32} + p_{128}$.

The sum is known, $G_1(1,2) + G_1(2,2) = G_1$, and due to (38-39) it holds

$$2G_1(1,2) \cdot G_1(2,2) = G_1^2 - G_1 - Pr$$

The part Pr_M for $= p_1p_{16}$ is known, $Pr_M = 2G_9$, and the part Pr_L for p_1p_4 we have to calculate.

We have here $p_1p_4 = p_3 + p_5$. The pair p_3 belongs to G_2 and the pair p_5 belongs to G_8 , so that $Pr_L = G_2 + G_8$. It follows that $Pr = 2(G_2 + G_8) + 2G_9$ and we have therefore for $G_1(1, 2)$ and $G_1(2, 2)$

$$G_1(1,2) + G_1(2,2) = G_1$$

$$G_1(1,2) \cdot G_1(2,2) = \frac{G_1^2 - G_1}{2} - 8 - (G_2 + G_8 + G_9)$$

It is easy to calculate $G_1(1,2)$ and $G_1(2,2)$ on the basis of the relevant quadratic equation with consideration that $G_1(1,2) > G_1(2,2)$.

To get $G_9(1,2)$ and $G_9(2,2)$ we have to split G_9 and, as we know, we get the equations for $G_9(1,2)$ and $G_9(2,2)$ on the basis of the equations for $G_1(1,2)$ and $G_1(2,2)$ with the shift with the height shift = 9 - 1 = 8 in the number of invariant sets. We get so for $G_9(1,2)$ and $G_9(2,2)$

$$G_{9}(1,2) + G_{9}(2,2) = G_{9}$$

$$G_{9}(1,2) \cdot G_{9}(2,2) = \frac{G_{9}^{2} - G_{9}}{2} - 8 - (G_{1} + G_{10} + G_{16})$$

and it is to consider in the calculation that $G_9(2,2) > G_9(1,2)$.

The calculations in this step show that to determine p_1 we need the invariant sets G_1 , G_2 , G_8 , G_9 , G_{10} and G_{16} . This information can be used to avoid unneeded splits. In step 4 it is necessary to split F(1,8), F(2,8) and F(8,8) only. To get the necessary values F(1,8), F(2,8) and F(8,8) we have to split only F(1,4), F(2,4) and F(4,4) in step 3. In step 2 it is necessary to calculate only these 3 values, we do not need the value F(3,4). That ends the case n = 257.

10 Regular 65537-gon

In the case n = 65537 we have 2048 invariant sets each with 16 pairs. We need here 15 steps to obtain p_1 . At first we split invariant sets into pairs. We consider the corresponding steps in reverse order to determine p_1 without unneeded calculations.

Step 15. In this step we have to split $G_1(1,8) = p_1 + p_{256}$ into p_1 and p_{256} . In the calculation of the product $2p_1 \cdot p_{256}$ the term Pr in (38) fails and we have here

$$2p_1 \cdot p_{256} = G_1^2(1,8) - G_1(2,8) - 4.$$

It follows hence for p_1 and p_{256}

$$p_1 + p_{256} = G_1(1,8)$$

$$p_1 \cdot p_{256} = \frac{G_1^2(1,8) - G_1(2,8)}{2} - 2$$

and these values can be calculated with the relevant quadratic equation taking into account that $p_1 > p_{256}$. For this calculation, as we see, we need definitely the values $G_1(1,8)$ and $G_1(2,8)$.

Step 14. In order to get $G_1(1,8)$ we have to split

$$G_1(1,4) = p_1 + p_{16} + p_{256} + p_{4096}$$

into $G_1(1,8) = p_1 + p_{256}$ and $G_1(5,8) = p_{16} + p_{4096}$. For the product $2G_1(1,8) \cdot G_1(5,8)$ we have

$$2G_1(1,8) \cdot G_1(5,8) = G_1^2(1,4) - G_1(2,4) - 8 - Pr_M$$

The part Pr_L is absent here and Pr_M is known, $Pr_M = 2G_{1025}(4, 4)$. For $G_1(1, 8)$ and $G_1(5, 8)$ we have thus

$$G_1(1,8) + G_1(5,8) = G_1(1,4)$$

$$G_1(1,8) \cdot G_1(5,8) = \frac{G_1^2(1,4) - G_1(2,4)}{2} - 4 - G_{1025}(4,4)$$

and we can determine these values as solutions of the relevant quadratic equation taking into account that $G_1(1,8) > G_1(5,8)$.

For $G_1(2,8)$ and $G_1(6,8)$ we have, compared with $G_1(1,8)$ and $G_1(5,8)$, a shift for the starting pair with the height shift = 1, therefore we come for $G_1(2,8)$ and $G_1(6,8)$ to the following equations

$$G_1(2,8) + G_1(6,8) = G_1(2,4)$$

$$G_1(2,8) \cdot G_1(6,8) = \frac{G_1^2(2,4) - G_1(3,4)}{2} - 4 - G_{1025}(1,4)$$

 $G_1(2,8)$ and $G_1(6,8)$ can then be calculated using the corresponding quadratic equation and taking into account that $G_1(2,8) > G_1(6,8)$.

To perform the calculations in this step we need obviously the values $G_1(1,4), G_1(2,4), G_1(3,4), G_{1025}(1,4)$ and $G_{1025}(4,4)$.

Step 13. We obtain the values $G_1(1, 4)$ and $G_1(3, 4)$, if we split $G_1(1, 2) = p_1 + p_4 + p_{16} + p_{64} + p_{256} + p_{1024} + p_{4096} + p_{16384}$ into $G_1(1, 4) = p_1 + p_{16} + p_{256} + p_{4096}$ and $G_1(3, 4) = p_4 + p_{64} + p_{1024} + p_{16384}$.

For the product $2G_1(1,4) \cdot G_1(3,4)$ we have

$$2G_1(1,4) \cdot G_1(3,4) = G^2(1,2) - G_1(2,2) - 16 - Pr$$

The part Pr_M is known, $Pr_M = 2G_{1025}(2,2)$, and Pr_L for p_1p_{16} we have to calculate. We have here $p_1p_{16} = p_{15} + p_{17}$. The pair p_{15} is the 6th pair in G_{1957} and p_{17} is the 12th pair in G_{1117} and therefore $Pr_L = G_{1957}(2,2) + G_{1117}(2,2)$.

For $G_1(1,4)$ and $G_1(3,4)$ we have therefore

$$G_{1}(1,4) + G_{1}(3,4) = G_{1}(1,2)$$

$$G_{1}(1,4) \cdot G_{1}(3,4) = \frac{G_{1}^{2}(1,2) - G_{1}(2,2)}{2} - 8$$

$$-G_{1025}(2,2) - G_{1117}(2,2) - G_{1957}(2,2)$$

and we can clearly calculate $G_1(1, 4)$ and $G_1(3, 4)$ using the relevant quadratic equation and taking into account that $G_1(1, 4) > G_1(3, 4)$.

With the help of the result for $G_1(1, 4)$ and $G_1(3, 4)$ we come to the result for $G_1(2, 4)$ and $G_1(4, 4)$ with the shift in the numbers of the starting pairs with the *shift* = 1. For $G_1(2, 4)$ and $G_1(4, 4)$ we obtain therefore

$$G_{1}(2,4) + G_{1}(4,4) = G_{1}(2,2)$$

$$G_{1}(2,4) \cdot G_{1}(4,4) = \frac{G_{1}^{2}(2,2) - G_{1}(1,2)}{2} - 8$$

$$-G_{1025}(1,2) - G_{1117}(1,2) - G_{1957}(1,2)$$

and we can calculate $G_1(2,4)$ and $G_1(4,4)$ with the help of the relevant quadratic equation taking into account that $G_1(2,4) > G_1(4,4)$.

The value $G_{1025}(1,4)$ can be determined, if we split of $G_{1025}(1,2)$ into $G_{1025}(1,4)$ and $G_{1025}(3,4)$. We come to the equations for $G_{1025}(1,4)$ and $G_{1025}(3,4)$ on the basis of the equations for $G_1(1,4)$ and $G_1(3,4)$ with shift with height shift = 1024 for the numbers of the invariant sets.

For the values $G_{1025}(1,4)$ and $G_{1025}(3,4)$ we obtain thus

$$G_{1025}(1,4) + G_{1025}(3,4) = G_{1025}(1,2)$$

$$G_{1025}(1,4) \cdot G_{1025}(3,4) = \frac{G_{1025}^2(1,2) - G_{1025}(2,2)}{2} - 8$$

$$-G_1(1,2) - G_{93}(1,2) - G_{933}(1,2)$$

and they can be determined by solving the relevant quadratic equation. Here we schould consider that $G_{1025}(1,4) > G_{1025}(3,4)$. We need only the value $G_{1025}(1,4)$ here.

The value $G_{1025}(4,4)$ can be determined, if we split of $G_{1025}(2,2)$ into $G_{1025}(2,4)$ and $G_{1025}(4,4)$. Corresponding to $G_{1025}(1,4)$ and $G_{1025}(3,4)$ we have a shift with the height shift = 1 in the numbers of starting pairs and obtain therefore for $G_{1025}(2,4)$ and $G_{1025}(4,4)$

$$G_{1025}(2,4) + G_{1025}(4,4) = G_{1025}(2,2)$$

$$G_{1025}(2,4) \cdot G_{1025}(4,4) = \frac{G_{1025}^2(2,2) - G_{1025}(1,2)}{2} - 8$$

$$-G_1(2,2) - G_{93}(2,2) - G_{933}(2,2)$$

These values can be clearly calculated by solving the relevant quadratic equation and taking into account that $G_{1025}(2,4) < G_{1025}(4,4)$. We need here only the value $G_{1025}(4,4)$.

The calculations in this step show that to realize all of them we need the values $G_1(1,2)$, $G_1(2,2)$, $G_{93}(1,2)$, $G_{93}(2,2)$, $G_{255}(1,2)$, $G_{255}(2,2)$, $G_{933}(1,2)$, $G_{933}(2,2)$, $G_{1025}(1,2)$, $G_{1025}(2,2)$, $G_{1117}(1,2)$, $G_{1117}(2,2)$, $G_{1957}(1,2)$ and $G_{1957}(2,2)$. In order to obtain them we have to split the invariant sets G_1 , G_{93} , G_{225} , G_{933} , G_{1025} , G_{1117} and G_{1957} .

Step 12. We split $G_1 = p_1 + p_2 + p_4 + \dots + p_{16384} + p_{32768}$ into $G_1(1,2) = p_1 + p_4 + p_{16} + p_{64} + p_{256} + p_{1024} + p_{4096} + p_{16384}$ and $G_1(2,2) = p_2 + p_8 + p_{32} + p_{128} + p_{512} + p_{2048} - p_{8192} + p_{32768}$

For the product $2G_1(1,2) \cdot G_1(2,2)$ we have here

$$2G_1(1,2) \cdot G_1(2,2) = G_1^2 - G_1 - 32 - Pr$$

The part Pr_M is known, $Pr_M = 2G_{1025}$, and Pr_L for $p_1p_4 + p_1p_{16} + p_1p_{64}$ we have to calculate. It applies here

$$p_1p_4 + p_1p_{16} + p_1p_{64} = p_3 + p_5 + p_{15} + p_{17} + p_{63} + p_{65}$$

We have seen in calculation of $G_1(1, 4) \cdot G_1(3, 4)$ that p_{15} belongs to G_{1957} and p_{17} belongs to G_{1117} . The new pairs are distributed as follows: p_3 belongs to G_2 , p_5 belongs to G_{1956} , p_{63} belongs to G_{1266} , and the pair p_{65} belongs to G_{1900} . So we have here $Pr_L = G_2 + G_{1117} + G_{1266} + G_{1900} + G_{1956} + G_{1957}$.

For $G_1(1,2)$ and $G_1(2,2)$ we obtain

$$G_{1}(1,2) + G_{1}(2,2) = G_{1}$$

$$G_{1}(1,2) \cdot G_{1}(2,2) = \frac{G_{1}^{2} - G_{1}}{2} - 16 - G_{2} - G_{1025} - G_{1117} - G_{1266}$$

$$-G_{1900} - G_{1956} - G_{1957}$$

and one can clearly calculate $G_1(1,2)$ and $G_1(2,2)$ with the help of the relevant quadratic equation taking into account that $G_1(1,2) > G_1(2,2)$.

To calculate $G_{93}(1,2)$ and $G_{93}(2,2)$ we have to split G_{93} . We get the equations for $G_{93}(1,2)$ and $G_{93}(2,2)$ with the help of the equations for $G_1(1,2)$ and $G_1(2,2)$ with the shift with the height shift = 92 in the number of invariant sets. We get so for $G_{93}(1,2)$ and $G_{93}(2,2)$

$$G_{93}(1,2) + G_{93}(2,2) = G_{93}$$

$$G_{93}(1,2) \cdot G_{93}(2,2) = \frac{G_{93}^2 - G_{93}}{2} - 16 - G_1 - G_{94} - G_{1117} - G_{1209}$$

$$-G_{1358} - G_{1992} - G_{2048}$$

One can clearly determine $G_{93}(1,2)$ and $G_{93}(2,2)$ by solving the relevant quadratic equation and taking into account that $G_{93}(1,2) < G_{93}(2,2)$.

For $G_{933}(1,2)$ and $G_{933}(2,2)$ we have, compared to $G_1(1,2)$ and $G_1(2,2)$, the shift with the height shift = 992 in the numbers of invariant sets. Therefore we get for $G_{933}(1,2)$ and $G_{933}(2,2)$

$$G_{933}(1,2) + G_{933}(2,2) = G_{933}$$

$$G_{933}(1,2) \cdot G_{933}(2,2) = \frac{G_{933}^2 - G_{933}}{2} - 16 - G_1 - G_{150} - G_{784}$$

$$-G_{840} - G_{841} - G_{934} - G_{1957}$$

and can clearly calculate $G_{993}(1,2)$ and $G_{933}(2,2)$ with the help of the relevant quadratic equation taking into account that $G_{933}(1,2) < G_{933}(2,2)$.

For $G_{1025}(1,2)$ and $G_{1025}(2,2)$ we have, compared to $G_1(1,2)$ and $G_1(2,2)$, the shift with the height shift = 1024 in the numbers of invariant sets. We get therefore for $G_{1025}(1,2)$ and $G_{1025}(2,2)$

$$G_{1025}(1,2) + G_{1025}(2,2) = G_{1025}$$

$$G_{1025}(1,2) \cdot G_{1025}(2,2) = \frac{G_{1025}^2 - G_{1025}}{2} - 16 - G_1 - G_{93} - G_{242}$$

$$-G_{876} - G_{932} - G_{933} - G_{1026}$$

and can clearly calculate $G_{1025}(1,2)$ and $G_{1025}(2,2)$ with solving the relevant quadratic equation and taking into account that $G_{1025}(1,2) < G_{1025}(2,2)$.

For $G_{1117}(1,2)$ and $G_{1117}(2,2)$ we have, compared to $G_1(1,2)$ and $G_1(2,2)$, the shift with the height shift = 1116 in the numbers of invariant sets. We get therefore for $G_{1117}(1,2)$ and $G_{1117}(2,2)$

$$G_{1117}(1,2) + G_{1117}(2,2) = G_{1117}$$

$$G_{1117}(1,2) \cdot G_{1117}(2,2) = \frac{G_{1117}^2 - G_{1117}}{2} - 16 - G_{93} - G_{185} - G_{334}$$

$$-G_{968} - G_{1024} - G_{1025} - G_{1118}$$

and can clearly calculate $G_{1117}(1,2)$ and $G_{1117}(2,2)$ with solving the relevant quadratic equation and taking into account that $G_{1117}(1,2) < G_{1117}(2,2)$.

At last, for $G_{1957}(1,2)$ and $G_{1957}(2,2)$ we have, compared to $G_1(1,2)$ and $G_1(2,2)$, the shift with the height shift = 1956 in the numbers of invariant sets. For $G_{1957}(1,2)$ and $G_{1957}(2,2)$ we obtain therefore

$$G_{1957}(1,2) + G_{1957}(2,2) = G_{1957}$$

$$G_{1957}(1,2) \cdot G_{1957}(2,2) = \frac{G_{1957}^2 - G_{1957}}{2} - 16 - G_{933} - G_{1025} - G_{1174}$$

$$-G_{1808} - G_{1864} - G_{1865} - G_{1958}$$

and we can clearly calculate them with the help of the relevant quadratic equation taking into account that $G_{1957}(1,2) < G_{1957}(2,2)$.

We have presented all splits in step 11 and can see that we need for these splits the invariant sets G_j and G_{j+1024} for the following 18 numbers j 1, 2, 93, 94, 150, 185, 242, 334, 784, 840, 841, 876, 932, 933, 934, 941, 968, 1024 (45)

The invariant sets G_j und G_{j+1624} are parts of F(j, 1024), and these 18 values F(j, 1024) we unconditionally have to split in step 11.

In step 11 we already split the values F(j, 1024). We consider this step in advance as we don't need any special calculation for these splits and the results of these splits will help to reduce the calculations in the other steps.

Step 11. We consider at first the split of $F(1, 1024) = G_1 + G_{1025}$ into $F(1, 2048) = G_1$ and $F(1025, 2048) = G_{1025}$.

The product $F(1, 2048) \cdot F(1025, 2048) = G_1 \cdot G_{1025}$ is known, (19),

$$F(1, 2048) \cdot F(1025, 2048) = 2F(1, 1024) + F(24, 1024)$$
(46)
+2F(155, 1024) + F(185, 1024) + F(309, 1024) + F(360, 1024)
+F(531, 1024) + F(667, 1024) + F(719, 1024) + F(734, 1024)
+2F(778, 1024) + F(841, 1024) + F(946, 1024)

and we get for F(j, 2048) and F(1024 + j, 2048), $1 \le j \le 1024$,

$$\begin{split} F(j,2048) + F(1024 + j,2048) &= F(j,1024) \\ F(j,2048) \cdot F(1024 + j,2048) &= 2F(j,1024) + F(\rho(23 + j,1024),1024) \\ + 2F(\rho(154 + j,1024),1024) + F(\rho(184 + j,1024),1024) \\ + F(\rho(308 + j,1024),1024) + F(\rho(359 + j,1024),1024) \\ + F(\rho(530 + j,1024),1024) + F(\rho(666 + j,1024),1024) \\ + F(\rho(718 + j,1024),1024) + F(\rho(733 + j,1024),1024) \\ + 2F(\rho(777 + j,1024),1024) + F(\rho(840 + j,1024),1024) \\ + F(\rho(945 + j,1024),1024) \end{split}$$

We don't need the calculations for all numbers $j, 1 \leq j \leq 1024$. We have seen in step 12 that we have to split only 18 values F(j, 1024) with the numbers j from the list (45). To clearly calculate the values $G_j = F(j, 2048)$ and $G_{1024+j} = F(1024 + j, 2048)$ we need the information which of them is bigger. In the following list are represented only those numbers j from the list of 18 numbers (45), for which it holds F(j, 2048) > F(1024 + j, 2048)

1, 2, 185, 334, 968, 1024

This information is doubtless sufficient to clearly calculate F(j, 2048) and F(1024 + j, 2048) with the help of the relevant quadratic equation.

Now we want to analyze which of the values F(j, 1024) we really need to perform the calculations in this step.

If we split F(j, 1024) for the 18 numbers j from the list (45), we need the appropriate values F(k, 1024) to represent $F(j, 2048) \cdot F(j+1024, 2048)$. For j = 1 we can see these numbers k in (46), and for the others 17 numbers j we can calculate them on this basis with the help of appropriate shifts. So we see that we need, in total, 213 values F(k, 1024) to perform the calculations in step 11. It is a lot of values but clearly less than 1024 possible values. The list of the 213 numbers j (we use instead of k our usual notation j) of the required values F(j, 1024) is the following

$$\begin{split} 1, 2, 6, 14, 15, 23, 24, 25, 28, 36, 43, 58, 62, 63, 64, 68, 71, 87, 92, 93, 94, 98, \\ 101, 106, 116, 117, 119, 124, 125, 128, 150, 154, 155, 156, 160, 163, 173, 175, \\ 176, 184, 185, 186, 208, 211, 216, 217, 218, 225, 242, 247, 248, 252, 255, 265, \\ 267, 268, 269, 276, 277, 278, 290, 303, 304, 308, 309, 310, 334, 339, 346, 347, \\ 357, 359, 360, 361, 369, 382, 396, 401, 402, 426, 438, 396, 401, 402, 426, 438, \\ 439, 440, 447, 452, 453, 458, 474, 478, 482, 483, 488, 493, 509, 518, 530, 531, \\ 532, 534, 535, 537, 544, 549, 550, 570, 574, 575, 576, 583, 585, 593, 594, 600, \\ 601, 610, 623, 624, 626, 627, 628, 629, 635, 641, 642, 643, 650, 656, 657, 662, \\ 666, 667, 668, 677, 680, 685, 686, 687, 692, 693, 694, 705, 715, 718, 719, 720, \\ 721, 733, 734, 735, 748, 749, 750, 757, 759, 760, 761, 762, 772, 777, 778, 779, \\ 784, 797, 807, 811, 812, 816, 826, 827, 840, 841, 842, 851, 853, 854, 855, 862, \\ 863, 864, 868, 870, 871, 876, 883, 889, 899, 903, 908, 918, 927, 932, 933, 934, \\ 938, 941, 945, 946, 947, 955, 956, 957, 960, 962, 964, 968, 975, 990, 991, 994, \\ 995, 1000, 1019, 1024 \end{split}$$

For 32 of these numbers, namely for the following numbers j

 $6, 23, 25, 58, 62, 63, 64, 71, 98, 116, 117, 150, 154, 155, 156, 173, 175, 208, 247, 248, 265, 267, 304, 339, 359, 396, 426, 452, 478, 482, 483, 488 \tag{47}$

there are present F(j, 1024) and F(j + 512, 1024). For these numbers j we obtain therefore these two necessary values, if we split F(j, 512). We have therefore to do only 181 splits in step 10.

From here on we consider the steps in natural order. Thereby we will use the already gained information about the required values F(j, 1024) to reduce the quantity of splits.

Step 1. We split S into F(1, 2) and F(2, 2).

The sum and the product are known here:

F(1,2) + F(2,2) = S = -1, $F(1,2) \cdot F(2,2) = -(n-1)/4 = -16384$, and F(1,2) and F(2,2) can be clearly calculated with the help of the quadratic equation

$$x^2 + x - 16384 = 0 \tag{48}$$

taking into account that F(1,2) > F(2,2).

Step 2. For the split F(j, 2) into F(j, 4) and F(2+j, 4) the sum and the product are known:

F(j,4)+F(2+j,4)=F(j,2) and $F(j,4)\cdot F(2+j,4)=-(n-1)/16=-4096$. Therefore F(j,4) and $F(2+j,4), 1 \leq j \leq 2$, can be clearly calculated with the help of the quadratic equation

$$x^2 - F(j,2)x - 4096 = 0$$

considering that $F(j,4) < F(2+j,4), 1 \le j \le 2$.

Step 3. First we look at the split of

$$F(1,4) = G_1 + G_5 + G_9 + G_{13} + \dots + G_{2041} + G_{2045}$$

into $F(1,8) = G_1 + G_9 + \dots + G_{2041}$ and $F(5,8) = G_5 + G_{13} + \dots + G_{2045}$

The sum is known, F(1,8) + F(5,8) = F(1,4), and to calculate the product $F(1,8) \cdot F(5,8)$ we can use the sum

$$G_1G_5 + G_1G_{13} + \dots + G_1G_{1013} + G_1G_{1021}$$

and determine $\mu(k, 4)$, the amont of invariant sets which belong to the part F(k, 4), $1 \le k \le 4$. We have here

$$\mu(1,4) = 992, \ \mu(2,4) = 1040, \ \mu(3,4) = 1024, \ \mu(4,4) = 1040,$$

and it holds therefore

$$F(1,8) \cdot F(5,8) = 992F(1,4) + 1040F(2,4) + 1024F(3,4) + 1040F(4,4)$$

= 1040 \cdot S - 48F(1,4) - 16F(3,4) = -1040 - 48F(1,4) - 16F(3,4)

For the parts F(j, 8) and F(4 + j, 8), $1 \le j \le 4$, we get then

$$F(j,8) + F(4+j,8) = F(j,4)$$

$$F(j,8) \cdot F(4+j,8) = -1040 - 48F(j,4) - 16F(\rho(2+j,4),4)$$

and these values can be clearly calculated taking into account that

$$F(1,8) < F(5,8), F(2,8) > F(6,8), F(3,8) > F(7,8), F(4,8) < F(8,8)$$

Step 4. First we look at the split of

$$F(1,8) = G_1 + G_9 + G_{17} + G_{25} + \dots + G_{2033} + G_{2041}$$

into $F(1, 16) = G_1 + G_{17} + \dots + G_{2033}$ and $F(9, 16) = G_9 + G_{25} + \dots + G_{2041}$

The sum is known, F(1, 16) + F(9, 16) = F(1, 8), and in calculation of the product $F(1, 16) \cdot F(9, 16)$ we come to the sum

$$G_1G_9 + G_1G_{25} + \dots + G_1G_{1017}$$

The amount $\mu(k, 8)$ of invariant sets which belong to F(k, 8), $1 \le k \le 8$, is in this sum the following

$$\mu(1,8) = 284, \ \mu(2,8) = 237, \ \mu(3,8) = 272, \ \mu(4,8) = 237, \ \mu(5,8) = 256, \ \mu(6,8) = 269, \ \mu(7,8) = 256, \ \mu(8,8) = 237$$

and we get therefore

$$F(1,16) \cdot F(9,16) = \sum_{k=1}^{8} \mu(k,8)F(k,8)$$

= -237 + 47F(1,8) + 35F(3,8) + 19F(5,8) + 32F(6,8) + 19F(7,8)

For F(j, 16) and F(8+j, 16), $1 \le j \le 8$, we obtain

$$F(j, 16) + F(8 + j, 16) = F(j, 8)$$

$$F(j, 16) \cdot F(8 + j, 16) = -237 + 47F(j, 8) + 35F(\rho(2 + j, 8), 8)$$

$$+19F(\rho(4 + j, 8), 8) + 32F(\rho(5 + j, 8), 8) + 19F(\rho(6 + j, 8), 8)$$

and these values can be clearly calculated considering that

$$\begin{split} F(1,16) &> F(9,16), \ F(2,16) > F(10,16), \ F(3,16) > F(11,16), \\ F(4,16) &< F(12,16), \ F(5,16) > F(13,16), \ F(6,16) < F(14,16), \\ F(7,16) &> F(15,16), \ F(8,16) < F(16,16). \end{split}$$

Step 5. First we look at the split of

$$F(1,16) = G_1 + G_{17} + G_{33} + G_{49} + \dots + G_{2017} + G_{2033}$$

into $F(1, 32) = G_1 + G_{33} + \dots + G_{2017}$ and $F(17, 32) = G_{17} + G_{49} + \dots + G_{2033}$ It holds F(1, 32) + F(17, 32) = F(1, 16), and in calculation of the product $F(1, 32) \cdot F(17, 32)$ we come to the sum $G_1G_{17} + G_1G_{49} + \dots + G_1G_{1009}$

The amount $\mu(k, 16)$ of invariant sets in this sum which belong to F(k, 16), $1 \le k \le 16$, is the following

$$\begin{split} \mu(1,16) &= 80, \ \mu(2,16) = 62, \ \mu(3,16) = 60, \ \mu(4,16) = 64, \\ \mu(5,16) &= 57, \ \mu(6,16) = 60, \ \mu(7,16) = 61, \ \mu(8,6) = 60, \\ \mu(9,16) &= 68, \ \mu(10,16) = 64, \ \mu(11,16) = 64, \ \mu(12,16) = 58, \\ \mu(13,16) &= 65, \ \mu(14,16) = 70, \ \mu(15,16) = 61, \ \mu(16,16) = 70 \end{split}$$

and therefore we obtain

$$\begin{split} F(1,32) \cdot F(17,32) &= \sum_{k=1}^{16} \mu(k,16) F(k,15) \\ &= -60 + 20 F(1,16) + 2 F(2,16) + 4 F(4,16) - 3 F(5,16) + F(7,16) \\ &\quad +8 F(9,16) + 4 F(10,16) + 4 F(11,16) - 2 F(12,16) + 5 F(13,16) \\ &\quad +10 F(14,16) + F(15,16) + 10 F(16,16) \end{split}$$

For F(j, 32) and F(16 + j, 32), $1 \le j \le 16$, we have therefore

$$\begin{split} F(j,32) + F(16+j,32) &= F(j,16) \\ F(j,32) \cdot F(16+j,32) &= -60 + 20F(j,16) + 2F(\rho(1+j,16),16) \\ &+ 4F(\rho(3+j,16),16) - 3F(\rho(4+j,16),16) + F(\rho(6+j,16),16) \\ &+ 8F(\rho(8+j,16),16) + 4F(\rho(9+j,16),16) + 4F(\rho(10+j,16),16) \\ &- 2F(\rho(11+j,16),16) + 5F(\rho(12+j,16),16) + 10F(\rho(13+j,16),16) \\ &+ F(\rho(14+j,16),16) + 10F(\rho(15+j,16),16) \end{split}$$

To calculate F(j, 32) and F(16 + j, 32), $1 \le j \le 16$, on the basis of the relevant quadratic equation we have to know which of them is bigger.

In order to summarize this information in short we present in the following list only the numbers $j, 1 \le j \le 16$, for which we have F(j, 32) > F(16+j, 32)

If any number $j, 1 \le j \le 16$, is not present in this list, it applies F(j, 32) < F(16 + j, 32). This information is obviously sufficient to clearly calculate the values F(j, 32) and F(16 + j, 32) with the help of the relevant quadratic equation.

Step 6. We consider at first the split of

$$F(1,32) = G_1 + G_{33} + G_{65} + G_{97} + \dots + G_{1985} + G_{2017}$$

into $F(1, 64) = G_1 + G_{65} + \dots + G_{1985}$ and $F(33, 64) = G_{33} + G_{97} + \dots + G_{2017}$

It holds F(1, 64) + F(33, 64) = F(1, 32), and in calculation of the product $F(1, 64) \cdot F(33, 64)$ we come to the sum

$$G_1G_{33} + G_1G_{97} + \dots + G_1G_{993}$$

The numbers $\mu(k, 32)$, $1 \le k \le 32$, for this sum here are the following

$$\begin{split} \mu(1,32) &= 4, \mu(2,32) = 12, \mu(3,32) = 20, \mu(4,32) = 13, \mu(5,32) = 20, \\ \mu(6,32) &= 18, \mu(7,32) = 16, \mu(8,32) = 19, \mu(9,32) = 19, \mu(10,32) = 22, \\ \mu(11,32) &= 12, \mu(12,32) = 22, \mu(13,32) = 13, \mu(14,32) = 13, \\ \mu(15,32) &= 11, \mu(16,32) = 22, \mu(17,32) = 20, \mu(18,32) = 15, \\ \mu(19,32) &= 25, \mu(20,32) = 12, \mu(21,32) = 16, \mu(22,32) = 12, \\ \mu(23,32) &= 16, \mu(24,32) = 17, \mu(25,32) = 29, \mu(26,32) = 16, \\ \mu(27,32) &= 7, \mu(28,32) = 17, \mu(29,32) = 13, \mu(30,32) = 17, \\ \mu(31,32) &= 13, \mu(32,32) = 11 \end{split}$$

The possible transformations of the representation for $F(1, 64) \cdot F(33, 64)$ do not give significant simplifications. Therefore we simply use the determined values $\mu(k, 32)$, $1 \le k \le 32$, without transformation.

For F(j, 64) and F(32 + j, 64), $1 \le j \le 32$, we have thus

$$F(j,64) + F(32+j,64) = F(j,32)$$

$$F(j,64) \cdot F(32+j,64) = \sum_{k=1}^{32} \mu(k,32) F(\rho(k+j-1,32),32)$$

In the following list we present the numbers $j, 1 \le j \le 32$, for which we have F(j, 64) > F(32+j, 64). If any number j is not present in this list, it applies F(j, 64) < F(32+j, 64),

1, 2, 4, 5, 9, 10, 11, 12, 21, 24, 28, 29, 31, 32

On the basis of this information F(j, 64) and F(32 + j, 64), $1 \le j \le 32$, can clearly be calculated with the help of the relevant quadratic equation.

Step 7. We consider at first the split of

$$F(1, 64) = G_1 + G_{65} + G_{129} + G_{193} + \dots + G_{1921} + G_{1985}$$

into $F(1, 128) = G_1 + G_{129} + \dots + G_{1921}$ and $F(65, 128) = G_{65} + G_{193} + \dots + G_{1985}$

The sum is known, F(1, 128) + F(65, 128) = F(1, 64), and in calculation of the product $F(1, 128) \cdot F(65, 128)$ we come to the sum

$$G_1G_{65} + G_1G_{193} + \dots + G_1G_{961}$$

The list of the numbers $\mu(k, 64)$, $1 \le k \le 64$, for this sum is very large, but numbers are between 0 and 10. In order to summarize this result we denote $\mathcal{K}(m, 64), 1 \le m \le 10$, the set of numbers k for which applies $\mu(k, 64) = m$. The set for the numbers k for which applies $\mu(k, 64) = 0$ is unnecessary. It holds here

$$\begin{split} \mathcal{K}(1,64) &= \{13,24,31,33,37,38\},\\ \mathcal{K}(2,64) &= \{3,7,9,21,36,46,56,57\}\\ \mathcal{K}(3,64) &= \{2,15,19,25,27,28,35,40,41,42,45,47,59,61,64\},\\ \mathcal{K}(4,64) &= \{29,32,43,48,51,52,58,60\},\\ \mathcal{K}(4,64) &= \{29,32,43,48,51,52,58,60\},\\ \mathcal{K}(5,64) &= \{4,5,6,8,11,16,20,22,23,30,53,62\},\\ \mathcal{K}(6,64) &= \{10,12,14,17,34,44,54\},\\ \mathcal{K}(7,64) &= \{39,49,50\},\\ \mathcal{K}(8,64) &= \{18,55,63\},\\ \mathcal{K}(9,64) &= \emptyset,\\ \mathcal{K}(10,64) &= \{26\} \end{split}$$

For F(j, 128) and F(64 + j, 128), $1 \le j \le 64$, we have therefore F(j, 128) + F(64 + j, 128) = F(j, 64) $F(j, 128) \cdot F(64 + j, 128) = \sum_{m=1}^{10} m \left(\sum_{k \in \mathcal{K}(m, 64)} F(\rho(k + j - 1, 64), 64) \right)$ In the following list we present the numbers $j, 1 \le j \le 64$, for which we have F(j, 128) > F(64 + j, 128):

1, 2, 3, 4, 6, 8, 10, 12, 16, 17, 18, 19, 20, 21, 24, 26, 27, 28, 29, 31, 32, 33, 34, 36, 37, 39, 40, 42, 45, 46, 48, 50, 51, 57, 58, 59, 62, 63

For the absent numbers j we have F(j, 128) < F(64 + j, 128). This information is sufficient to clearly calculate F(j, 128) and F(64 + j, 128) with the help of the relevant quadratic equation.

Step 8. We consider at first the split of

$$F(1, 128) = G_1 + G_{129} + G_{257} + \dots + G_{1793} + G_{1921}$$

into $F(1, 256) = G_1 + G_{257} + \dots + G_{1793}$ and $F(129, 256) = G_{129} + G_{385} + \dots + G_{1921}$

The sum is known, F(1, 256) + F(129, 256) = F(1, 128), and in calculation of $F(1, 256) \cdot F(129, 256)$ we come to the sum

$$G_1G_{129} + G_1G_{385} + \dots + G_1G_{897}$$

The numbers $\mu(k, 128)$, $1 \le k \le 128$, for this sum are between 0 and 5, and we denote $\mathcal{K}(m, 128)$, $1 \le m \le 5$, the set of numbers k for which applies $\mu(k, 128) = m$. We have here

 $\begin{aligned} \mathcal{K}(1,128) &= \{2,4,5,7,8,9,15,16,17,21,23,26,27,31,36,38,46,48,49,52,\\ 57,59,61,62,81,83,87,90,91,96,99,100,111,112,116,117,\\ 119,120,124,125,126\}, \end{aligned}$

$$\mathcal{K}(2, 128) = \{1, 34, 35, 37, 39, 41, 42, 43, 60, 64, 68, 71, 74, 75, 77, 80, 84, 88, 89, 95, 98, 102, 104, 105, 109, 110, 118, 122, 128\},\$$

 $\begin{aligned} \mathcal{K}(3, 128) &= \{11, 30, 101, 106\}, \\ \mathcal{K}(4, 128) &= \{66, 107, 115\}, \end{aligned}$

 $\mathcal{K}(5, 128) = \{58\}$

and for F(j, 256) and F(128 + j, 256), $1 \le j \le 128$, we obtain therefore

$$F(j,256) + F(128 + j,256) = F(j,128)$$

$$F(j,256) \cdot F(128 + j,256) = \sum_{m=1}^{5} m \left(\sum_{k \in \mathcal{K}(m,128)} F(\rho(k+j-1,128),128) \right)$$

The list of numbers j for which here applies F(j, 256) > F(128 + j, 256) is the following

1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 16, 20, 21, 24, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35, 41, 44, 47, 49, 53, 55, 56, 60, 61, 63, 65, 66, 67, 69, 71, 72, 73, 74, 76, 77, 78, 82, 83, 85, 91, 92, 93, 98, 100, 102, 104, 105, 107 108, 109, 110, 111, 113, 117, 120, 121, 124, 125, 126, 128

If any number j is not present in this list, we have F(j, 256) < F(128+j, 256). This information is sufficient to clearly calculate F(j, 256) and F(128+j, 256), $1 \le j \le 128$, with the help of the relevant quadratic equation.

Step 9. At first we consider the split of

$$F(1,256) = G_1 + G_{257} + G_{513} + \dots + G_{1537} + G_{1793}$$

into $F(1, 512) = G_1 + G_{513} + G_{1025} + G_{1537}$ and $F(257, 512) = G_{257} + G_{769} + G_{1281} + G_{1793}$

The sum is known, F(1, 512) + F(257, 512) = F(1, 256), and in calculation of $F(1, 512) \cdot F(257, 512)$ we come to the sum

 $G_1G_{257} + G_1G_{769}$

The numbers $\mu(k, 256)$, $1 \le k \le 256$, here are between 0 and 3. Analogous to the previous steps we denote here for $1 \le m \le 3$ the set $\mathcal{K}(m, 256)$ of numbers k for which applies $\mu(k, 256) = m$. We have here

$$\begin{aligned} \mathcal{K}(1,256) &= \{5,8,15,20,30,31,34,38,40,42,44,45,51,52,54,57,60,62, \\ &\quad 66,69,71,79,80,82,85,89,90,107,110,113,118,125,129,136, \\ &\quad 143,147,174,176,187,188,189,196,201,213,220,232,234, \\ &\quad 244,251,253,254\}, \end{aligned}$$

 $\mathcal{K}(2,256) = \{4,29,157,186,246\}, \\ \mathcal{K}(3,256) = \{83\}$

For F(j, 512) and $F(256 + j, 512), 1 \le j \le 256$, we get therefore

$$F(j,512) + F(256 + j,512) = F(j,256)$$

$$F(j,512) \cdot F(256 + j,512) = \sum_{m=1}^{3} m \left(\sum_{k \in \mathcal{K}(m,256)} F(\rho(k+j-1,256),256) \right)$$

and the list of the numbers j for which applies F(j, 512) > F(256 + j, 512)is the following

$$\begin{split} 1, 2, 3, 5, 6, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 30, 31, 32, 37, 38, \\ 39, 42, 44, 45, 46, 47, 48, 49, 52, 54, 55, 58, 59, 62, 63, 65, 66, 76, 77, 78, 79, \\ 82, 84, 87, 89, 90, 91, 93, 94, 96, 97, 98, 102, 103, 107, 110, 115, 117, 118, 119, \\ 123, 127, 133, 134, 136, 139, 144, 145, 147, 148, 149, 151, 152, 155, 156, 157, \\ 160, 161, 162, 166, 168, 170, 171, 180, 182, 185, 186, 187, 188, 189, 191, 194, \\ 195, 197, 200, 203, 206, 207, 209, 210, 213, 215, 217, 220, 221, 222, 223, 225, \\ 230, 232, 234, 235, 236, 237, 238, 240, 241, 242, 244, 245, 254, 255, 256 \end{split}$$

This information is sufficient to clearly calculate F(j, 512) and F(256+j, 512), $1 \le j \le 256$, with the help of the relevant quadratic equation.

Step 10. We consider at first the split of

$$F(1,512) = G_1 + G_{513} + G_{1025} + G_{1537}$$

into $F(1, 1024) = G_1 + G_{1025}$ and $F(513, 1024) = G_{513} + G_{1537}$.

The sum is known, F(1, 1024) + F(513, 1024) = F(1, 512), and in calculation of $F(1, 1024) \cdot F(513, 1024)$ we come to the product G_1G_{513} . The numbers $\mu(k, 512)$, $1 \le k \le 512$, for this product are between 0 and 2, and we denote similar to the previous for $1 \le m \le 2$ the set $\mathcal{K}(m, 512)$ of the numbers k, for which $\mu(k, 512) = m$. We have

$$\begin{aligned} \mathcal{K}(1,512) &= & \{41,49,81,92,106,109,114,211,226,233,269,275,278,\\ && 281,303,349,379,390,431,465\} \\ \mathcal{K}(2,512) &= & \{68,86,88,135,175,451\} \end{aligned}$$

and we get therefore for F(j, 1024) and $F(512 + j, 1024), 1 \le j \le 512$,

$$F(j, 1024) + F(152 + j, 1024) = F(j, 512)$$

$$F(j, 1024) \cdot F(512 + j, 1024) = \sum_{m=1}^{2} m \left(\sum_{k \in \mathcal{K}(m, 512)} F(\rho(k + j - 1, 512), 512) \right)$$

In step 11 we have seen that only 213 values F(j, 1024) are unconditionally required and therefore we have to split 181 values F(j, 512). The list of numbers j for which we have to split F(j, 512) into F(j, 1024) and F(512+j, 1024) is the following

$$\begin{split} 1, 2, 6, 14, 15, 18, 19, 20, 22, 23, 24, 25, 28, 32, 36, 37, 38, 43, 58, 62, 63, 64, \\ 68, 71, 73, 81, 82, 87, 88, 89, 92, 93, 94, 98, 101, 106, 111, 112, 114, 115, 116, \\ 117, 119, 123, 124, 125, 128, 129, 130, 131, 138, 144, 145, 150, 154, 155, 156, \\ 160, 163, 165, 168, 173, 174, 175, 176, 180, 181, 182, 184, 185, 186, 193, 203, \\ 206, 207, 208, 209, 211, 216, 217, 218, 221, 222, 223, 225, 236, 237, 238, 242, \\ 245, 247, 248, 249, 250, 252, 255, 260, 265, 266, 267, 268, 269, 272, 276, 277, \\ 278, 285, 290, 295, 299, 300, 303, 304, 308, 309, 310, 314, 315, 328, 329, 330, \\ 334, 339, 341, 342, 343, 346, 347, 350, 351, 352, 356, 357, 358, 359, 360, 361, \\ 364, 369, 371, 377, 382, 387, 391, 396, 401, 402, 406, 415, 420, 421, 422, 426, \\ 429, 433, 434, 435, 438, 439, 440, 443, 444, 445, 447, 448, 450, 452, 453, 456, \\ 458, 463, 474, 478, 479, 482, 483, 488, 493, 507, 509, 512 \end{split}$$

In the following list we present the part of these 181 numbers j for which we have F(j, 1024) > F(512 + j, 1024)

 $1, 2, 6, 18, 22, 24, 25, 37, 62, 68, 73, 93, 94, 98, 101, 106, 112, 116, 124, 125, \\131, 138, 144, 150, 154, 155, 156, 163, 165, 168, 175, 176, 180, 182, 184, 185, \\186, 206, 209, 211, 216, 218, 221, 225, 236, 238, 242, 260, 265, 268, 269, 272, \\276, 277, 295, 299, 300, 304, 309, 310, 314, 315, 328, 330, 334, 342, 350, 352, \\356, 357, 359, 360, 369, 371, 377, 382, 387, 396, 406, 415, 426, 429, 433, 438, \\440, 444, 447, 448, 452, 463, 474, 479, 482, 483, 512$

This information is sufficient to clearly calculate the absolutely required values F(j, 1024) and F(512+j, 1024). For these 181 splits of F(j, 512) we need both numbers F(j, 1024) and F(512+j, 1024) only for 32 numbers j. These 32 numbers j we have seen in step 11, (47).

The calculations in step 10 do not indicate that the calculations in step 9 can be substantially reduced. This means that we have to do all splits in the steps 1-9. That ends the case n = 65537.

11 Final remarks

In conclusion we want to make some remarks. At first we consider the choice of the factor for the determination of the invariant sets. In all steps it was not explicitly necessary that this factor was 3. Important was the shift property for the product of invariant sets and it is clear that this feature can be available, if we use an other proper factor. Crucial is here the possibility to determine the invariant sets with the help of this factor. Due to calculations *modulo* n this factor should be between 1 and n - 1.

We want to show that these are the numbers in \hat{G}_{2k} , $1 \leq k \leq ng/2$. ng is here, just as above, the number of all invariant sets.

The proof of the Proposition 3 shows plainly that all invariant sets have been determined with factor 3 due to the fact that $3^{ng} \mod n$ belongs to \hat{G}_1 and $3^{ng/2} \mod n$ doesn't belong to \hat{G}_1 . For any arbitrary factor q all invariant sets will be determined iff $q^{ng} \mod n$ belongs to \hat{G}_1 and $q^{ng/2} \mod n$ doesn't belong to \hat{G}_1 .

A number q from the invariant set \hat{G}_{2k+1} , $0 \leq k < ng/2$, has the form $q = 3^{2k}2^j$ with $0 \leq j < 2^{\nu+1}$, where we calculate modulo n. It applies then

$$q^{ng/2} modulo n = ((3^{ng})^k \cdot 2^{j \cdot ng/2} modulo n) \in \hat{G}_1$$

Indeed, the number $q_1 = 3^{ng} \mod n$ belongs to \hat{G}_1 and is therefore equal to 2^{j_1} or $n - 2^{j_1}$ with $0 \leq j_1 < 2^{\nu}$. It follows obviously that $q_1^k \mod n$ also has the same form and therefore also belongs to \hat{G}_1 . At the following $j \cdot ng/2$ doublings the numbers remain still in \hat{G}_1 . This means that q from \hat{G}_{2k+1} is not an appropriate factor to determine the invariant sets.

A number q from \hat{G}_{2k} , $1 \le k \le ng/2$, has the form

$$q = 3^{2k-1} \cdot 2^j, \ 0 \le j < 2^{\nu+1},$$

calculated modulo n. For this number we obtain

$$q^{ng} modulo n = (3^{ng})^{2k-1} \cdot 2^{j \cdot ng} modulo n.$$

The number $q_1 = 3^{ng} \mod n$ belongs to \hat{G}_1 and it follows obviously that the number $q_2 = q_1^{2k-1} \mod n$ also belongs to \hat{G}_1 . At the following $j \cdot ng$ doublings we obtain always numbers in \hat{G}_1 .

In order to show that $q^{ng/2}$ does not belong to \hat{G}_1 we represent q as follows:

$$q = 3 \cdot 3^{2(k-1)} \cdot 2^j$$

For $q^{ng/2}$ we have then

$$q^{ng/2} modulo n = 3^{ng/2} \cdot (3^{ng})^{(k-1)} \cdot 2^{j \cdot ng/2} modulo n$$

The number $q_1 = 3^{ng} \mod n$ and $q_2 = q_1^{(k-1)} \mod n$ also belongs to \hat{G}_1 . With the help of the factor $3^{ng/2}$ we come then from q_2 to a number in the set $\hat{G}_{1+ng/2}$. At the following $j \cdot ng/2$ doublings the numbers remain in $\hat{G}_{1+ng/2}$, and $\hat{G}_{1+ng/2} \neq \hat{G}_1$.

It is interesting to notice that for an other appropriate factor q we will get the same invariant sets but with other numbers and therefore in a different order if $q \notin \hat{G}_1$. We will in fact come to the same parts $F(k, 2^m)$ but with a different order. If we then use the same rule for splittings we will see a certain stability in the method. But it is possible to get variance in the realization of the method without changing the factor q if we calculate, for example, some products in a different way. We could see it in the case n = 17.

To assign the parts of the splittings to the solutions of the corresponding quadratic equations correctly, we need always the information which of these parts is bigger. In the case n = 17 this is trivial, as we can simply see the positions of the relevant points. In the case n = 257 and especially in the case n = 65537 this geometric overview is not available, and it is necessary to estimate the necessary parts numerically. The required calculations were made in the case n = 65537 with the help of a quite simple C program and the numerical accuracy is enough to guarantee that the assignments are correct.

In the presented approach we use the values $\mu(k, 2^m)$, $1 \leq k \leq 2^m$, if we split the parts $F(k, 2^m)$, $1 \leq k \leq 2^m$, into $F(j, 2^{m+1})$, $1 \leq j \leq 2^{m+1}$. To calculate the values $\mu(k, 2^m)$ we need a lot of products G_1G_j of invariant sets. In the case n = 65537 we need, dependent on the calculation method, in total 128 or 256 of these products. For the calculation of G_1G_j we can use the number 1 of the starting pair in G_1 and all numbers in \bar{G}_j of the pairs in G_j and calculate the 32 numbers of pairs in G_1G_j . These calculations can be made manually or trivial with the help of Excel. Bud next we have to detect to which sets \bar{G}_k each of these 32 numbers belongs. This can be done manually (if we have a list of the sets \bar{G}_k and can use a find-function), but that is an unpleasant job. The author passed this job and the calculation of the required values $\mu(k, 2^m)$ to the C program.

We will show that it is possible to calculate the values $\mu(k, 2^m)$ in another way. We show more precisely one step of the corresponding calculations. The values $\mu(k, 2)$, $1 \le k \le 2$, are known and we start with $\mu(k, 4)$, $1 \le k \le 4$.

After the step 2 of the splittings we have obviously the values F(k, 4), $1 \le k \le 4$. We will show that we can then exactly calculate the values $\mu(k, 4)$, $1 \le k \le 4$. For technical reasons we denote here $x_k = \mu(k, 4)$, $1 \le k \le 4$. Due to (30) we have for the values $x_k = \mu(k, 4)$ the following system of linear equations

$$F(1,4)x_1 + F(2,4)x_2 + F(3,4)x_3 + F(4,4)x_4 = F(1,8) \cdot F(5,8)$$

$$F(2,4)x_1 + F(3,4)x_2 + F(4,4)x_3 + F(1,4)x_4 = F(2,8) \cdot F(6,8)$$

$$F(3,4)x_1 + F(4,4)x_2 + F(1,4)x_3 + F(2,4)x_4 = F(3,8) \cdot F(7,8)$$

$$F(4,4)x_1 + F(1,4)x_2 + F(2,4)x_3 + F(3,4)x_4 = F(4,8) \cdot F(8,8)$$

and we can try to determine $\mu(k, 4), 1 \le k \le 4$, with the help of this system.

In the practical calculations we have in fact instead of the exact coeffitients F(k, 4) in the system only the already good calculated in step 2 approximations. For the products in the right side we also can use only the corresponding approximations, calculated, for example, with the C program. This means that on the basis of this system of equations we will get in fact approximations x_k for the values $\mu(k, 4)$. But it is possible to solve this system of linear equations without inappropriate transformations and estimate the accuracy of the solution. If then we will additionally take into account that the values $\mu(k, 4)$ are integer numbers, we can determine these values exactly.

With the help of the exact values $\mu(k, 4)$ we can then (as in the step 3 of splittings) get the good approximations for the values F(k, 8), $1 \le k \le 8$, and determine analog the values $\mu(k, 8)$, $1 \le k \le 8$. We can continue this work again and again for the followign values $\mu(k, 2^m)$.

In this approach we need only the approximative values $F(j, 2^m)$. These values can be calculated, for example, with the C program. The calculations for $\mu(k, 2^m)$ itself can be made without the C program. We can simply use Excel.

But the rang 2^m of the linear system for $\mu(k, 2^m)$, $1 \le k \le 2^m$, grows rapidly and, in addition, the accuracy of the calculations will get worse. It is therefore appropriate to calculate in this manner a part of the values $\mu(k, 2^m)$. A smal part of the values $\mu(k, 2^m)$ with too big numbers 2^m can be calculated manually.

At the very end only the remark that the presented method of the construction of regular n-gons fits for n = 3 and n = 5 also. In case n = 3 we have only one pair p_1 , and (2) means that $p_1 = -1$. In the case n = 5 we have only one invariant set with 2 pairs p_1 and p_2 and it applies $p_1p_2 = p_1 + p_2 = -1$. If we split here $S = p_1 + p_2$ into p_1 and p_2 , we obtain for p_1 and p_2 the quadratic equation

 $x^2 + x - 1 = 0$

and have to consider that $p_1 > p_2$.

12 References

1. Gauss C. F. Werke, Bd. 1 Disquisitiones arithmeticae, § 365.. ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universität-Druckerei 1863.

2. C. F. Gauss. Disquisitiones Arithmeticae, English translation by Arthur A. Clarke, New Haven, CT: Yale University Press, (1966).

3. Carl Friedrich Gauß. Göttingische Gelehrte Anzeigen. Band 87, Nr. 203, 19. Dezember 1825, S. 2025–2027.

4. Magnus Georg Paucker. Geometrische Verzeichnung des regelmäßigen Siebzehn-Ecks und Zweyhundertsiebenundfunfzig-Ecks in den Kreis. Jahresverhandlungen der Kurländischen Gesellschaft für Literatur und Kunst. Band 2, 1822, S. 160–219.

5. Richelot, F. J. De resolutione algebraica aequationis $X^{257} = 1$, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata. J. reine angew. Math. 9, 1-26, 146-161, 209-230, and 337-358, 1832.

6. Richmond H. E. A Construction for a regular polygon of seventeen sides, Quarterly Journal of Pure and Applied Mathematics. Band 26, 1893, S. 206-207.

7. Klein F. Vorträge über ausgewählte Fragen der Elementargeometrie, Leipzig 1895.

8. Duane W. DeTemple. Carlyle circles and Lemoine simplicity of polygon constructions. In: The American Mathematical Monthly. 98. Jahrgang, Nr. 2, Februar 1991, S. 104–107.

9. DeTemple, D. W. Carlyle Circles and the Lemoine Simplicity of Polygonal Constructions. Amer. Math. Monthly 98, 97-108, 1991.

10. Trott, M. " $\cos(2pi/257)$ à la Gauss." Mathematica Educ. Res. 4, 31-36, 1995.

11. Christian Gottlieb. The Simple and Straightforward Construction of the Regular 257-gon. In: Mathematical Intelligencer. Vol. 21, No. 1, 1999, S. 31–37, doi:10.1007/BF03024829.

12. Goldstein C, Schappacher N. Schwermer J. The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae, Springer-Verlag 2007.

13. Edwards H.M. The construction of solvable polynomials, Bull. Amer. Math. Soc. 46 2009, 397-411.

14. Carslaw H. S. Gauss's Theorem on the Regular Polygons which can be constructed by Euclid's Method, Cambridge University Press 1910.

15. J. Hermes. Ueber die Teilung des Kreises in 65537 gleiche Teile. (PDF) Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen Mathematisch-physikalische Klasse. SUB, Göttinger Universität Göttinger Digitalisierungszentrum, S. 170–186, abgerufen am 29. Mai 2023.

16. Skopenkov A. Some More Proofs from the Book: Solvability and Insolvability of Equations in Radicals, https://arxiv.org/abs/0804.4357 2014.