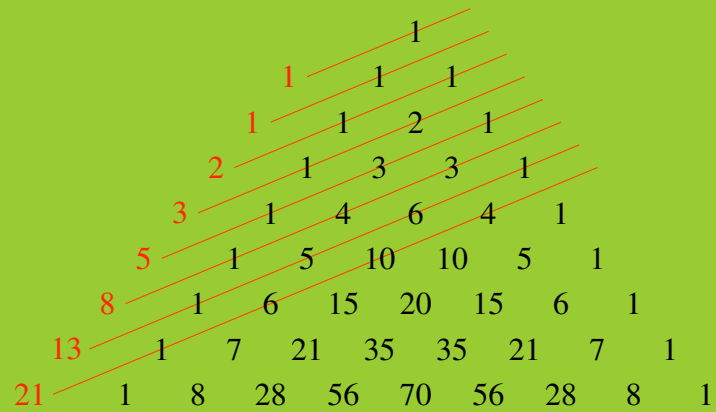


Cellular Automaton and Binomials



Hans Montanus
Ron Westdijk

Cellular Automaton and Binomials

Hans Montanus

Ron Westdijk

Preface

Cellular automation is a discrete model of computation. It computes the evolution of a pattern of states in a grid of discrete cells where each cell is in one of the states. Some cellular automata simulate or mimic patterns found in biology, chemistry and physics. Although the grid can be of any dimension the present book is restricted to two dimensions and mainly to one dimension. Even in one dimension the dynamics of cellular automata can be very rich. A simple but important one dimensional cellular automaton leads to the Pascal triangle with binomial coefficients or to triangular patterns visualising the divisibility of binomial coefficients by a prime number. Since binomial coefficients and their divisibility properties are a large area of research it has been given much attention and space.

The present book is intended to be a simple and informal introduction to cellular automation and binomial coefficients. With simple is meant that a high school level of mathematics (together with the willingness to study) suffices to understand the contents. With informal is meant that the book is not organised as an enumeration of theorems and proofs. Instead it rather is a random walk through famous dynamical systems. In general, proofs are omitted, formal language is avoided and citations are restricted to a few occasions.

The present book has just been written for educational purposes. It is intended for high school students with talent for mathematics and for readers with (a little more than) a high school level mathematical background.

november 2022, Hans Montanus, Ron Westdijk

Contents

1 Cellular automata step by step	5
1.1 Introduction	5
1.2 Rules	7
1.3 Configuration width	10
1.4 Fractals	10
1.5 States	12
1.6 Dimension	13
1.7 Summary	16
2 Elementary cellular automata	17
2.1 Elementary cellular automata	17
2.2 Transition equation	19
2.3 Uniqueness	20
2.4 Generating functions	21
2.5 Cycles	22
2.6 Unreachables	25
3 Modular CA	29
3.1 Modular addition in one dimension	29
3.2 Tabulation of periods	30
3.3 Preperiodic points	37
3.4 Modular addition in two dimensions	39
3.5 Game of Life	40
4 Pascal triangle	43
4.1 Binomial coefficients	43
4.2 Sierpinski triangle	44
4.3 Discrete Sierpinski triangle	46
4.4 Pascal triangle modulo q	48
4.5 Skewed triangles	53

4.6	Gould's sequence	56
4.7	Skewed Pascal triangle modulo q	57
4.8	Kummer's method	62
5	Properties of Binomials	65
5.1	Series in Pascal's triangle	65
5.2	Stern series	67
5.3	Divisors of products of binomials	68
5.4	A multiplicity conjecture	69
5.5	Binomials and π	70
6	Divisibility aspects of binomials	75
6.1	Introduction	75
6.2	Algorithm for SW-pairs	77
6.3	Number of SW-pairs	81
6.4	Confining to prime divisors of n	86
6.5	Algorithm for covering sets of prime divisors of n	90
6.6	Primorials	91
6.7	Distributions	92
A	Proof of Kummer's theorem	95
B	P-adic numbers	99
B.1	Infinite repetitions	99
B.2	10-adic zero divisors	101
B.3	p-adic numbers	102
C	Two binomial identities	105
	Bibliography	108

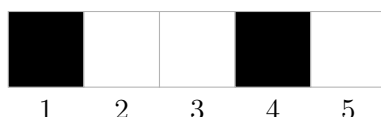
Chapter 1

Cellular automata step by step

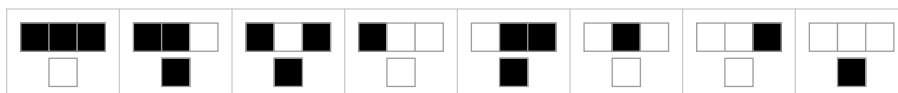
1.1 Introduction

A cellular automaton (CA) is a configuration of *cells*. Each cell is in a *state*. For a two state CA the states can be represented by **0** and **1** or **white** and **black** or \ominus and \otimes or whatever two different symbols. The iterative development of states is determined by a *rule*. An example of a rule for two state cells is: a cell flips to another state if and only if the nearest neighbour cells are all in the same state. The consequences of a rule also depends on the *dimension* of the configuration.

As an example we consider a 1-dimensional configuration of 5 adjacent square cells, say



The nearest neighbours of cell 2 is cell 1 and cell 3. The nearest neighbours of cell 3 is cell 2 and cell 4. The nearest neighbours of cell 4 is cell 3 and cell 5. The sequence of cells is thought to be periodic: cell 5 is thought to be a neighbour of cell 1. Suppose we take the example rule mentioned before: a cell flips to another state if and only if the nearest neighbour cells are all in the same state. For the eight combinations for a triple of cells consisting of a cell with its two nearest neighbours the rule is visualized in the following pictogram:



If we apply this rule to the initial configuration, then cell 1 turns into white, cell 2 stays white, cell 3 stays white, cell 4 turns into white and cell 5 turns into black. Shortly, only cell 1, cell

4 and cell 5 flip their state. As a consequence the initial configuration is evolved into the following configuration:



If the rule is applied repeatedly the cell states after each step become



The result after six steps is identical to the initial configuration. That is, we obtained a period 6 cycle. There are four more period 6 cycles. There also is a period 2 cycle:



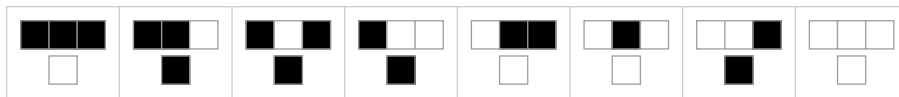
The five period 6 cycles actually are ‘copies’ of each other. To be specific, if the cell states in each configuration are shifted (periodically) by one cell (for instance, cell 1 to cell 2, cell 2 to cell 3, cell 3 to cell 4, cell 4 to cell 5 and cell 5 to cell 1) a cycle turns into one of the other cycles. One more shift leads to another cycle, and so on. For configurations of five cells one can make five shifts and therefore there are five period 6 cycles. If the 5 cells are all black or all white, a shift does not lead to another cycle. Therefore there is a single period 2 cycle. For 5 cells there are $2^5 = 32$ different states of which 30 occur in the five period 6 cycles and two occur in the period 2 cycle. For the present rule applied to a one dimensional (1D) configuration of 5 cells the evolution is depicted in the following directed *graph*:



Finally we mention that a *cell* is also called a *site*, a *state* is also called a *color* and a *configuration* is also called a *grid*. In case of numbers a *configuration* is also called a *tuple*.

1.2 Rules

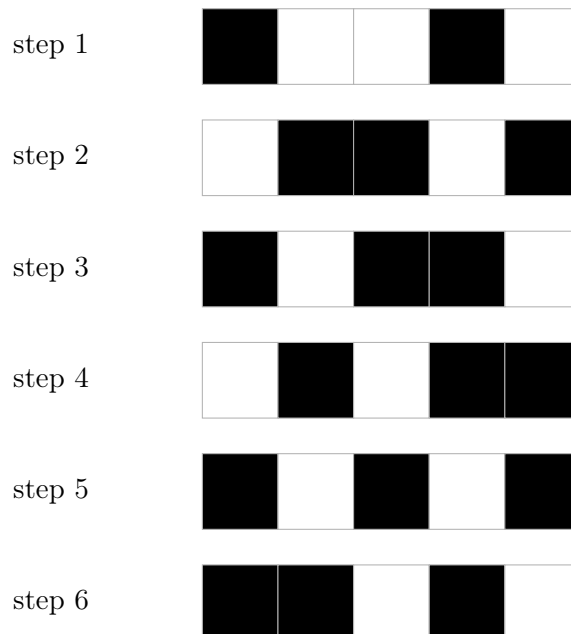
Other rules may lead to other graphs. For instance, if we apply the rule



to the initial sequence

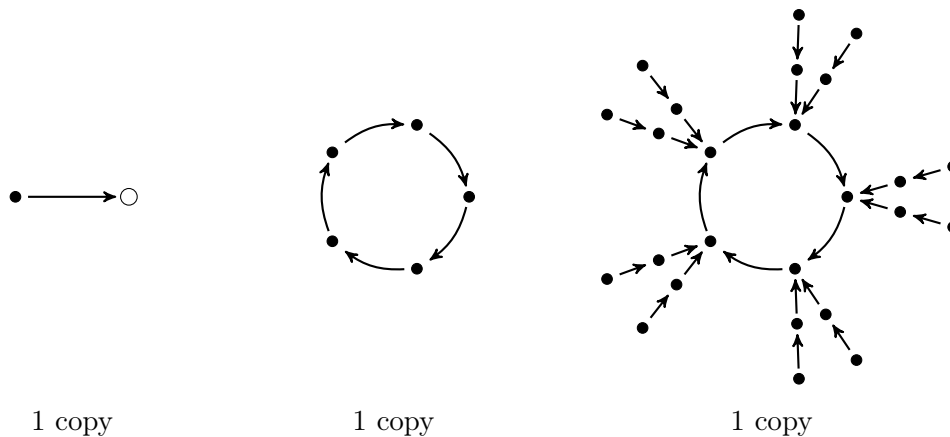


we successively obtain

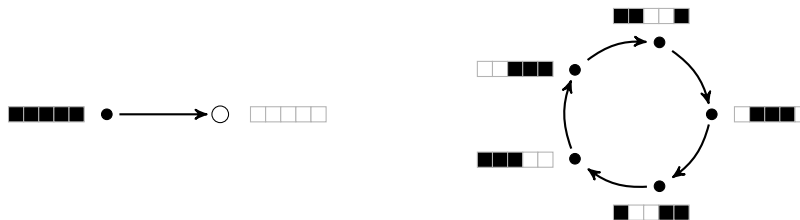




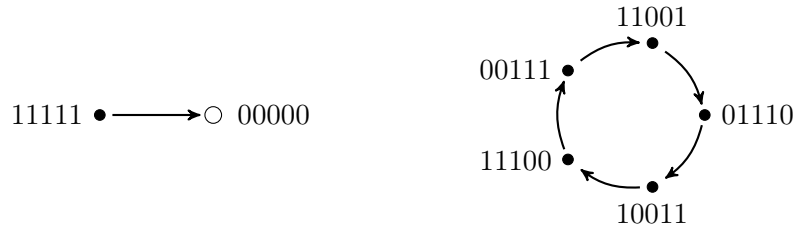
We see the configuration after step 7 is identical to the configuration after step 2. That is, after two preperiodic configurations a period 5 cycle occurs. In fact, the configuration after step 3 is just the configuration after step 2 shifted (periodically) one cell to the right. Similarly, the configuration after step 4 is the configuration after step 3 shifted one cell, and so on. As a consequence, the configuration after step 7 is the configuration after step 2. Therefore, the graph will contain a period 5 cycle with preperiodic configurations. Application of the present rule to all the 32 different configurations of 5 cells leads to the following graph:



The latter rule maps the configuration of 5 black cells to a configuration of 5 white cells, while it maps the configuration of 5 white cells on itself, see left part of the graph. The 5 white cells form a period 1 cycle; a fixed point. Fixed points will be drawn as open dots. From the other 30 configurations 5 are in a bare period 5 cycle and 25 are in a period 5 cycle with 20 preperiodic configurations. Periodic cycles are attractors. In the latter figure only the structure of the graph is shown, not the configurations. With configurations the period 1 cycle and the bare period 5 cycle of the latter figure are as shown below.



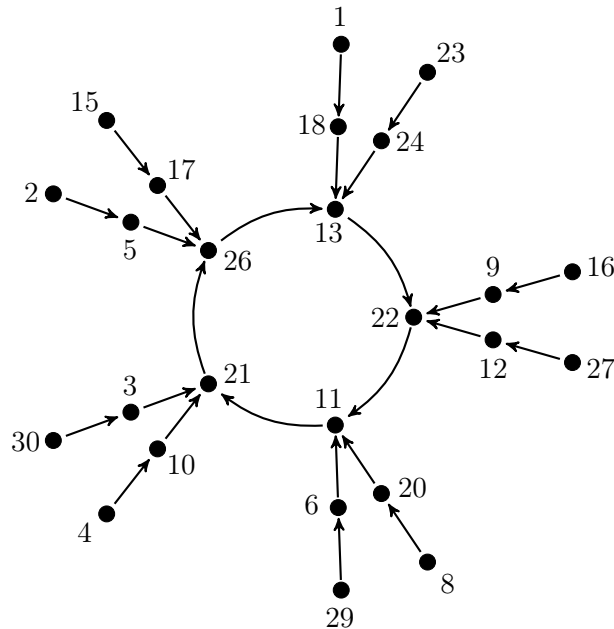
Another way to represent the configurations is by denoting a black cell as a 1 and a white cell as a zero. Then the period 1 cycle and the bare period 5 cycle of the latter figure are as follows.



An abbreviation can be achieved by interpreting the numbers in the latter figure as binary numbers. The configurations can also be represented by the decimal value of the binary numbers. Thus 0 for 00000, 1 for 00001, 2 for 00010, 3 for 00011, 4 for 00100 through 31 for 11111. Then the period 1 cycle and the bare period 5 cycle of the latter figure will be as follows.



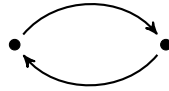
The other numbers are in the period 5 cycle with the 20 preperiodic configurations:



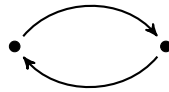
Usually one is only interested in the structure of the graphs and not in the individual configurations. So, hereafter we will confine to graphs without configuration representations.

1.3 Configuration width

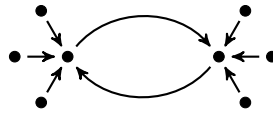
The configuration in the previous section has a width of 5 cells. Other configuration widths may lead to other graphs. Application of the rule of the first section to configuration widths of 1 cell, 2 cells, 3 cells, 4 cells and 6 cells lead to the graphs



1 copy



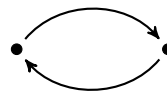
2 copies



1 copy

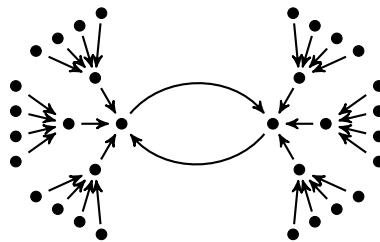


4 copies



6 copies

and

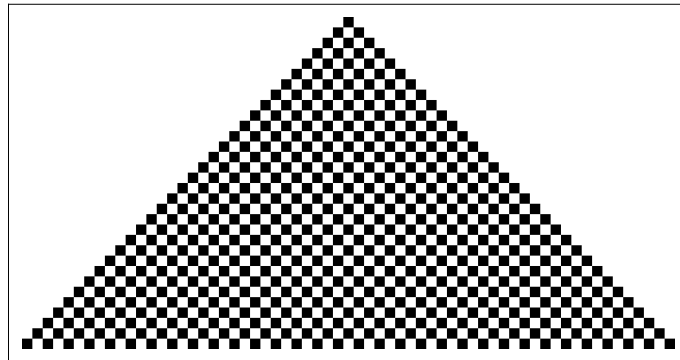


2 copies

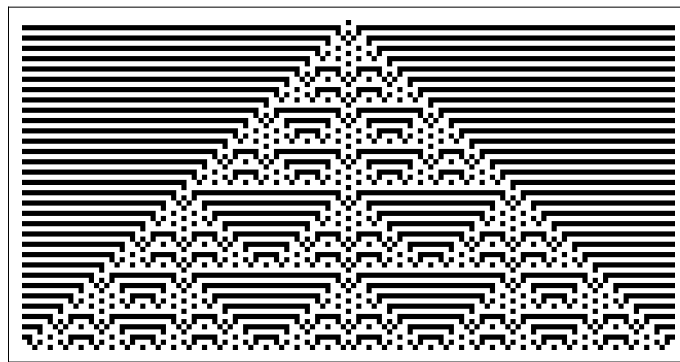
respectively. Clearly, the graphs depend on the configuration width.

1.4 Fractals

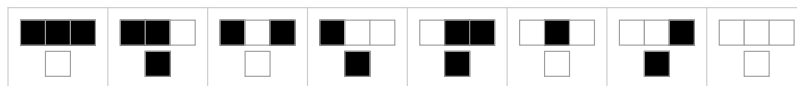
Often a relatively large number of zeros (white cells) with a single 1 (black cell) is taken as the initial configuration. For instance, the evolution of a single black cell under the rule of the second section leads to a checkerboard pattern, see the next figure.



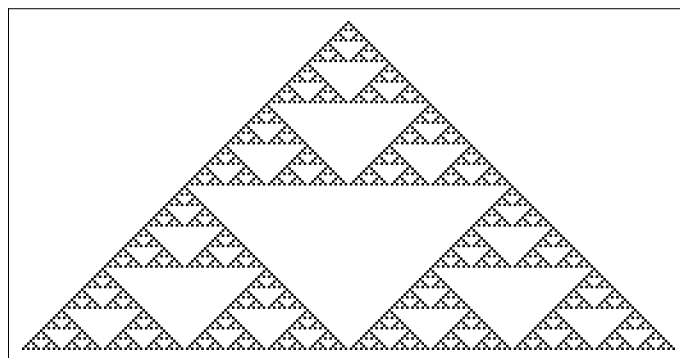
The evolution of a single black cell under the rule of the first section is as follows:



The latter pattern contains self similarity on smaller scales. That is, it has fractal properties. Application of the rule



leads to a fractal which is known as the Sierpinski triangle:



1.5 States

If for a one dimensional n state CA a new state of a cell is determined by the old state of the cell and the state of its nearest neighbours, the rule has to cover n^3 possibilities. For a one dimensional two state CA a rule covers $2^3 = 8$ possibilities as we saw in the previous sections. For a one dimensional three state CA a rule covers $3^3 = 27$ possibilities. In the next figure we see an example of a three state rule.



In the latter example a state is depicted by a colour: either white, orange or purple. If we apply it to the following configuration of 5 cells



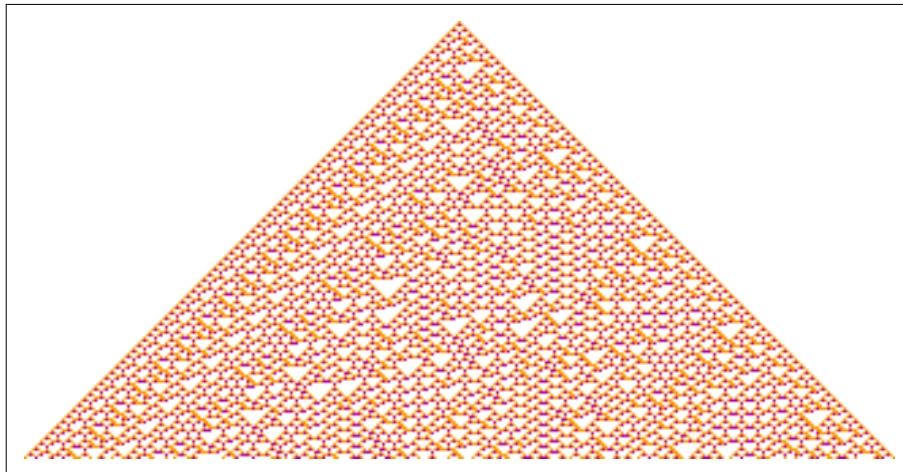
we successively obtain



⋮ ⋮

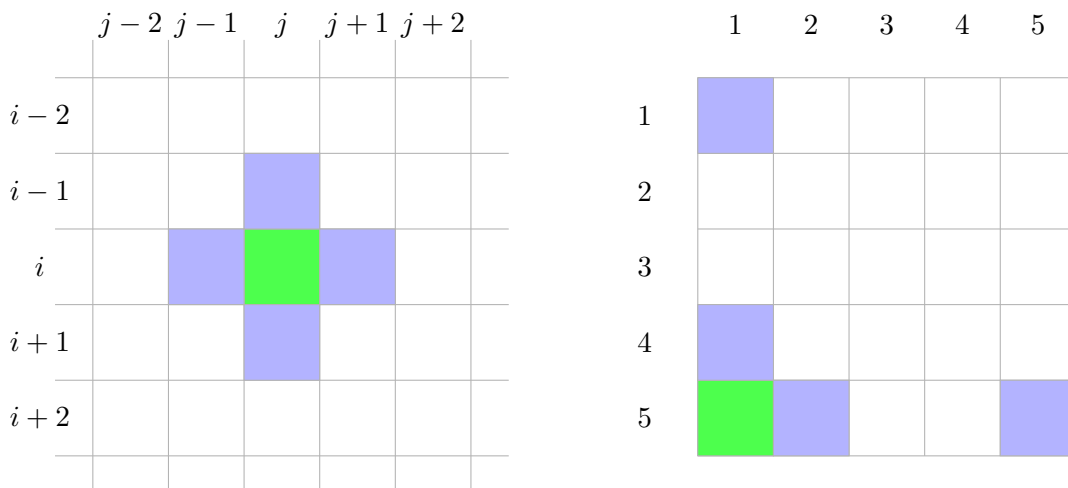


That is, after 25 steps we arrive at the initial configuration; a period 25 cycle. For large configurations the evolution of a single orange cell leads to the following the pattern:

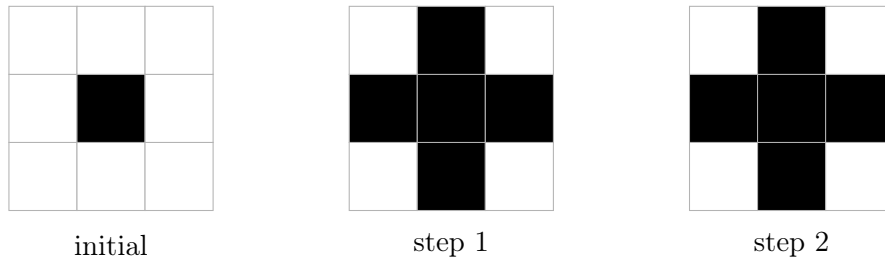


1.6 Dimension

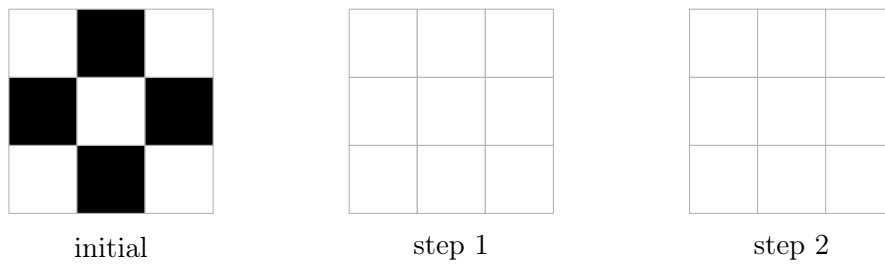
In the previous sections we confined to one dimensional configurations. However, a CA can also live in more than one dimension. An example is a two dimensional (2D) grid of square cells. The nearest neighbours of cell $c_{i,j}$ are $c_{i-1,j}$, $c_{i,j-1}$, $c_{i+1,j}$ and $c_{i,j+1}$. Also here the configurations are periodic. In the next figure the four blue cells are the nearest neighbours of the green cell. The right panel illustrates the consequences of a grid with periodic boundaries.



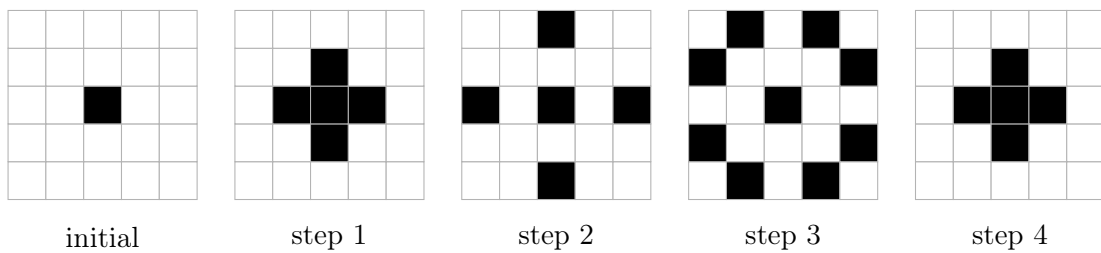
Suppose a rule for the 2D square grid with two states is: a cell flips its state if it has an odd number of black nearest neighbours. For a 3×3 periodic grid it leads to the following evolution of a single black cell:



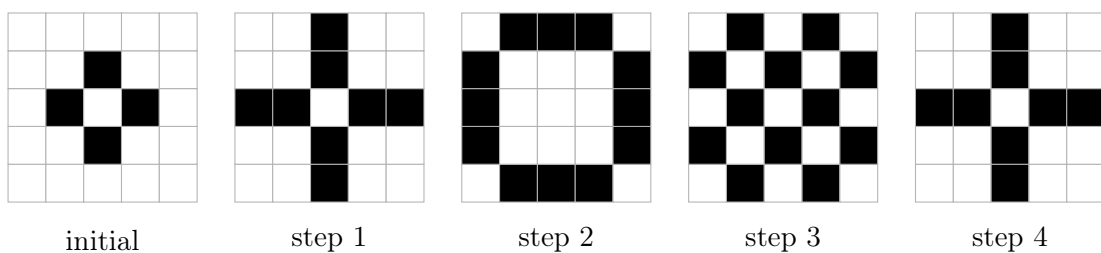
The final configuration is a fixed point. This is also the case in the example:



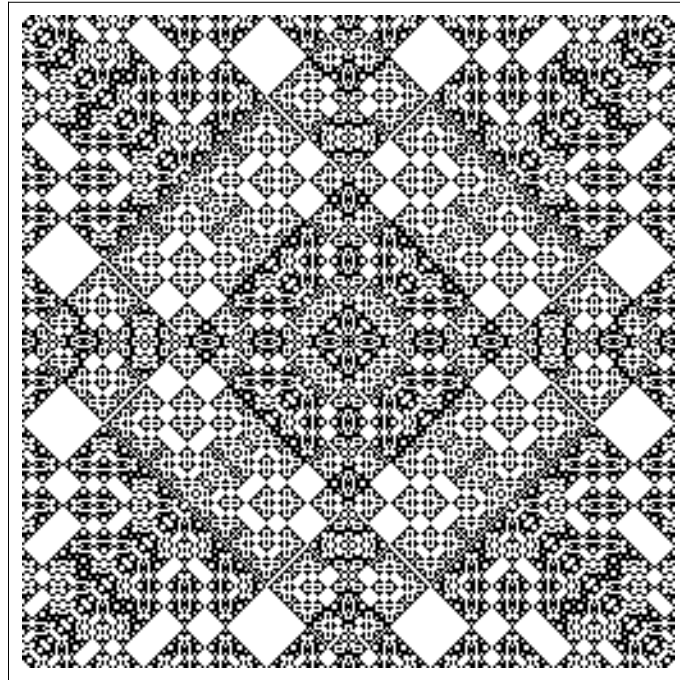
If we consider the foregoing two initial configurations in a 5×5 periodic grid, the present rule leads to



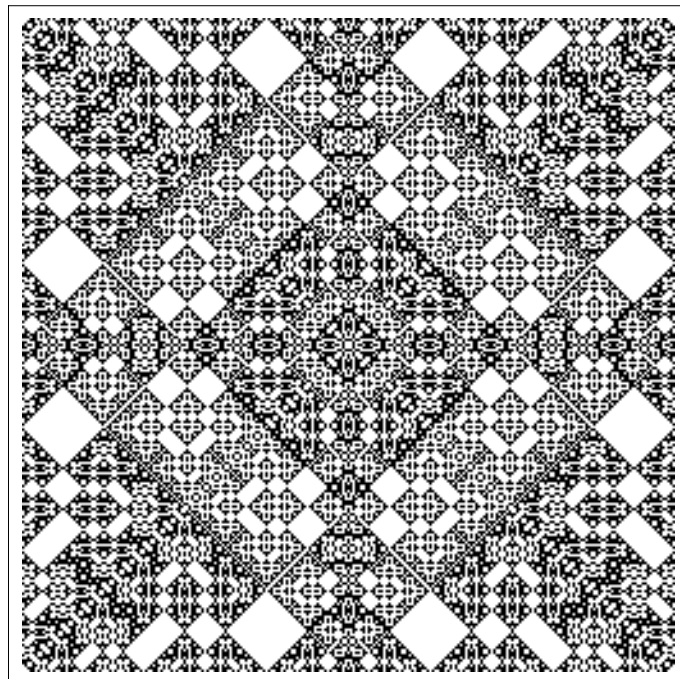
and





respectively. In both cases we arrive at a period 3 cycle. For larger grids the evolution patterns become more refined and aesthetic. The evolution of two initial configurations considered in a 255×255 periodic grid leads after 255 steps for the single black cell to



and for the other initial configuration after 255 steps to



For both case holds: if we take one step further, thus after step 256, the result is identical to the result after the first step. So, the cycle has a period of 255 steps. The previous two figures are almost identical. They differ only in the 3×3 grid at the center:  and  respectively.

1.7 Summary

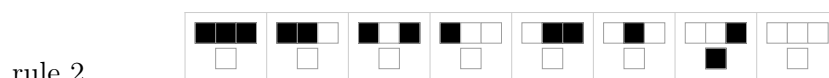
This chapter was a small tour through the world of CA. We saw how a CA is determined by the dimension of the grid, the size of the grid, the number of different states a cell can possibly have, the initial configuration and the rules of evolution. We also saw how periodic cycles can come into existence. For convenience we confined so far to CA with grids of square cells. However, grids do not have to consist of square cells. A regular grid of triangles or hexagons or even less regular grids may serve as well. In addition, rules do not have to be restricted to nearest neighbours. For sequences it may depend on next to nearest neighbours as well, or even further away. Also for a square cell $c_{i,j}$ one does not have to restrict to neighbour cells with $i \pm 1$ and $j \pm 1$. In stead one can also consider neighbour cells with $i \pm 2$ and $j \pm 2$ or even further away. In the chapters to come we will confine to one dimensional CA's and investigate some properties.

Chapter 2

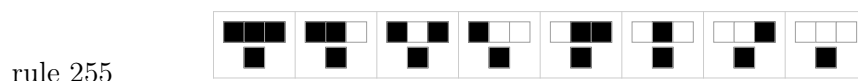
Elementary cellular automata

2.1 Elementary cellular automata

A one dimensional cellular automaton is called *elementary* if there are two possible states for a cell and if the evolution of a cell depends on the states of the cell itself and its two nearest neighbours. The very first rule of chapter 1 is an elementary cellular automaton. For each elementary cellular automaton there are 8 different possibilities for the triple of states of a cell and its two nearest neighbours. For each triple there are 2 possible new states for the cell in the middle. Therefore there are $2^8 = 256$ elementary cellular automata. The elementary cellular automata were introduced by Stephen Wolfram [1, 2]. The rules are



through



If we represent the two states by a 0 and a 1 instead of white and black, then the rule are as follows

rule 0	111	110	101	100	011	010	001	000
	0	0	0	0	0	0	0	0

rule 1	111	110	101	100	011	010	001	000
	0	0	0	0	0	0	0	1

rule 2	111	110	101	100	011	010	001	000
	0	0	0	0	0	0	1	0

rule 3	111	110	101	100	011	010	001	000
	0	0	0	0	0	0	1	1

and so on through

rule 255	111	110	101	100	011	010	001	000
	1	1	1	1	1	1	1	1

For a rule

rule d	111	110	101	100	011	010	001	000
	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0

with $a_k \in \{0, 1\}$, the decimal rule number is given by

$$d = \sum_{k=0}^7 a_k 2^k. \quad (2.1)$$

With the use of the latter equation it follows that the rule in section 1.1 has decimal number 105. The rule in section 1.2 has decimal number 114. The rule which resulted in the Sierpinski triangle in section 1.3 has decimal number 90. These three examples are usually denoted as rule 105, rule 114 and rule 90.

2.2 Transition equation

In the binary system, where a state is 0 or 1, a rule d of an elementary cellular automaton can be summarised as

$$\text{rule } d \quad \begin{array}{|c|} \hline LCR \\ \hline N \\ \hline \end{array}$$

It represents the transition of the state (C) of a cell, the state (L) of its left neighbour and the state (R) of its right neighbour to a new state N of the cell for each of the 8 possible configurations of the LCR triples. Each rule d can be casted in a single equation:

$$N = (b_0 + b_1R + b_2C + b_3C * R + b_4L + b_5L * R + b_6L * C + b_7L * C * R) \bmod 2, \quad (2.2)$$

where the coefficients $b_k \in \{0, 1\}$. The coefficients b_i depend on the coefficients a_i :

$$\begin{aligned} b_0 &\cong a_0 \bmod 2, & b_1 &\cong (a_1 - a_0) \bmod 2, & b_2 &\cong (a_2 - a_0) \bmod 2 \\ b_3 &\cong (a_3 - a_2 - a_1 + a_0) \bmod 2, & b_4 &\cong (a_4 - a_0) \bmod 2 \\ b_5 &\cong (a_5 - a_4 - a_1 + a_0) \bmod 2, & b_6 &\cong (a_6 - a_4 - a_2 + a_0) \bmod 2 \\ b_7 &\cong (a_7 - a_6 - a_5 + a_4 - a_3 + a_2 + a_1 - a_0) \bmod 2. \end{aligned} \quad (2.3)$$

A transition equation is obtained by substituting the values a_i in the latter system of 8 equations. As an example we explicitly calculate the b_k for rule 105. Rule 105 reads

rule 105	1 1 1	1 1 0	1 0 1	1 0 0	0 1 1	0 1 0	0 0 1	0 0 0
	0	1	1	0	1	0	0	1

That is, for rule 105 $(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0) = (0, 1, 1, 0, 1, 0, 0, 1)$. Substitution of these a_i in the 8 equations of equation 2.3 leads to $b_0 = b_1 = b_2 = b_4 = 1$ and $b_3 = b_5 = b_6 = b_7 = 0$. Hence, the transition equation for rule 105 is

$$N_{105} = (1 + R + C + L) \bmod 2 \quad (2.4)$$

In a similar way one finds, for example, for rule 114 and rule 90 the transition equations

$$N_{114} = (R + C * R + L + L * R) \bmod 2, \quad N_{90} = (R + L) \bmod 2. \quad (2.5)$$

In equation 2.1 the coefficient a_i for rule $255 - d$ is 0 if the coefficient a_i for rule d is 1, and the coefficient a_i for rule $255 - d$ is 1 if the coefficient a_i for rule d is 0. As a consequence, $a_i - a_j$ for rule $255 - d$ does not differ from $a_i - a_j$ for rule d . The b_1 through b_7 for rule $255 - d$ therefore does not differ from the b_1 through b_7 for rule d . Only the b_0 for rule $255 - d$ is 0 (1) if the b_0 for rule d is 1 (0).

2.3 Uniqueness

Among the 256 rules for the elementary cellular automata there are rules which are trivially equivalent to each other. For instance a change of roles of L and R only leads to a mirror situation. A mirror rule number occurs if both the coefficients a_1 and a_3 in equation (2.1) for a rule number are exchanged with coefficient a_4 and a_6 respectively. A trivial equivalency also occurs if the roles of 0 and 1 are exchanged. That is, if the complement situation is considered. The latter occurs if L , C and R in the triple and the a_k flip their state. In effect this means that the new coefficients follow from a given one via $a_k = 1 - a_{7-k}$ for $k = 0$ through 7. Finally, a trivial equivalence also occurs if the complement of a mirror rule is taken. As an example we consider rule 30:

rule 30	1 1 1	1 1 0	1 0 1	1 0 0	0 1 1	0 1 0	0 0 1	0 0 0
	0	0	0	1	1	1	1	0

If we exchange a_1 with a_4 and a_3 with a_6 we obtain as mirror rule 86:

rule 86	1 1 1	1 1 0	1 0 1	1 0 0	0 1 1	0 1 0	0 0 1	0 0 0
	0	1	0	1	0	1	1	0

If we exchange a_k with $1 - a_{7-k}$ for $k = 0$ through 7, we obtain as complement rule 135:

rule 135	1 1 1	1 1 0	1 0 1	1 0 0	0 1 1	0 1 0	0 0 1	0 0 0
	1	0	0	0	0	1	1	1

The complement of the mirror rule is rule 149:

rule 149	1 1 1	1 1 0	1 0 1	1 0 0	0 1 1	0 1 0	0 0 1	0 0 0
	1	0	0	1	0	1	0	1

Among the 256 rules there are 88 unique rules in the sense that they are inequivalent under mirror and complement transformations.

Starting with the smallest decimal rule numbers and discarding equivalent rules with larger decimal numbers, the 88 unique rules are: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 18, 19, 22, 23, 24, 25, 26, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 40, 41, 42, 43, 44, 45, 46, 50, 51, 54, 56, 57, 58, 60, 62, 72, 73, 74, 76, 77, 78, 90, 94, 104, 105, 106, 108, 110, 122, 126, 128, 130, 132, 134, 136, 138, 140, 142, 146, 150, 152, 154, 156, 160, 162, 164, 168, 170, 172, 178, 184, 200, 204, 232.

2.4 Generating functions

As an example we consider the evolution of a single 1 among zero's under rule 50:

```

0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,0,1,0,1,0,0,0,0,0,0
0,0,0,0,0,0,0,0,1,0,1,0,1,0,0,0,0,0
0,0,0,0,0,0,1,0,1,0,1,0,1,0,0,0,0,0
0,0,0,0,0,1,0,1,0,1,0,1,0,1,0,0,0,0
0,0,0,0,1,0,1,0,1,0,1,0,1,0,1,0,0,0
0,0,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,0
0,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0
0,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0
    
```

For the binary number interpretation the blue line indicates the border between negative and non negative powers of 2. The first number left from the blue line is the coefficient of 2^0 , one more to the left is the coefficient of 2^1 , etc. If we interpret each row as a binary number this way, then the decimal values of the generated sequence are 1, 5, 21, 85, 341, 1365, 5461, 21845, ... Each new number is 4 times the previous number plus 1. The difference equation for such a sequence is $u_n = 4u_{n-1} + 1$ with $u_0 = 1$. A direct equation is

$$u(n) = \frac{4 \cdot 4^n - 1}{3}. \tag{2.6}$$

A Taylor expansion of the function $\frac{1}{(1-x)(1-4x)}$ yields

$$\frac{1}{(1-x)(1-4x)} \approx 1 + 5x + 21x^2 + 85x^3 + 341x^4 + 1365x^5 + 5461x^6 + 21845x^7 + \dots \tag{2.7}$$

Because of the analogy between the coefficients of the powers of x and the generated sequence, the function $\frac{1}{(1-x)(1-4x)}$ is a *generating function* for rule 50.

As another example we consider the evolution of a single 1 under rule 6:

```

0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
    
```

With respect to the blue line the decimal values of the generated sequence are 1, 6, 16, 96, 256, 1536, 4096, 24576, Once you have a sequence for a rule you can look for its direct equation and generating function at the OEIS site [3]. The sequence 1, 6, 16, 96, 256, 1536, 4096, 24576, ... for rule 6, for instance, is known as sequence A266180. It has $4^{n-1} (5 - (-1)^n)$ as direct equation and $\frac{1 + 6x}{(1 - 4x)(1 + 4x)}$ as the generating function.

A rule for which the input 000 leads to $a_0 = 1$ will have an odd rule number. As a consequence, a odd rule applied to the first row ...000001000000..., will cause the cells at the right of the blue diagonal in the second row to be filled with a 1. Then one can not interpret the second row as a binary number. Therefore the generating functions are restricted to rules with an even rule number.

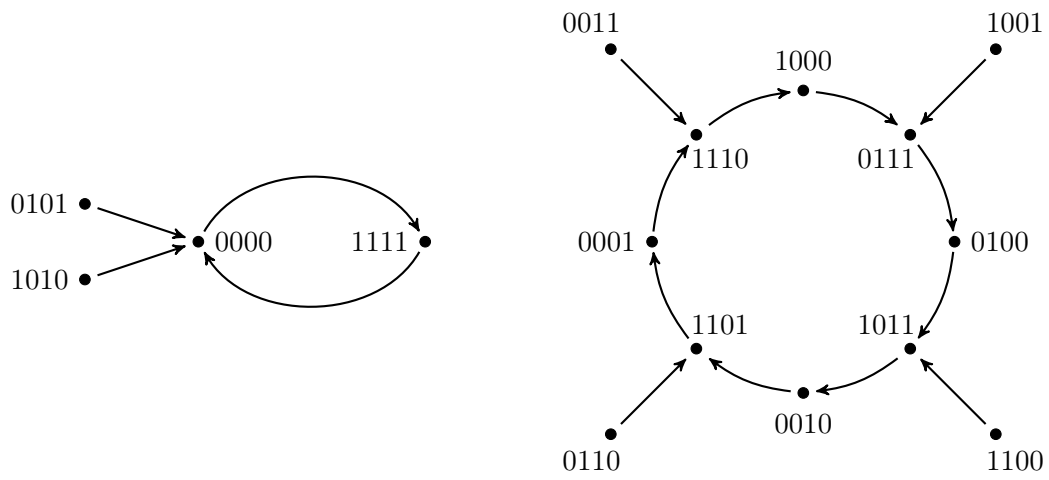
2.5 Cycles

In this section we will apply elementary cellular automata to periodic tuples of finite width. If the width of a tuple is n binary digits, then there are 2^n possible tuples to start with. Let us consider, for instance, rule 27

rule 27

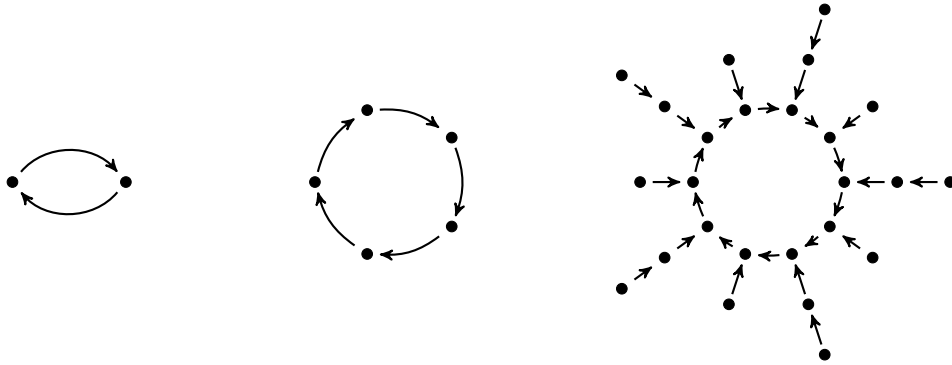
1 1 1	1 1 0	1 0 1	1 0 0	0 1 1	0 1 0	0 0 1	0 0 0
0	0	0	1	1	0	1	1

Application of rule $d = 27$ to the 16 different tuples with width 4 leads to the following graph:



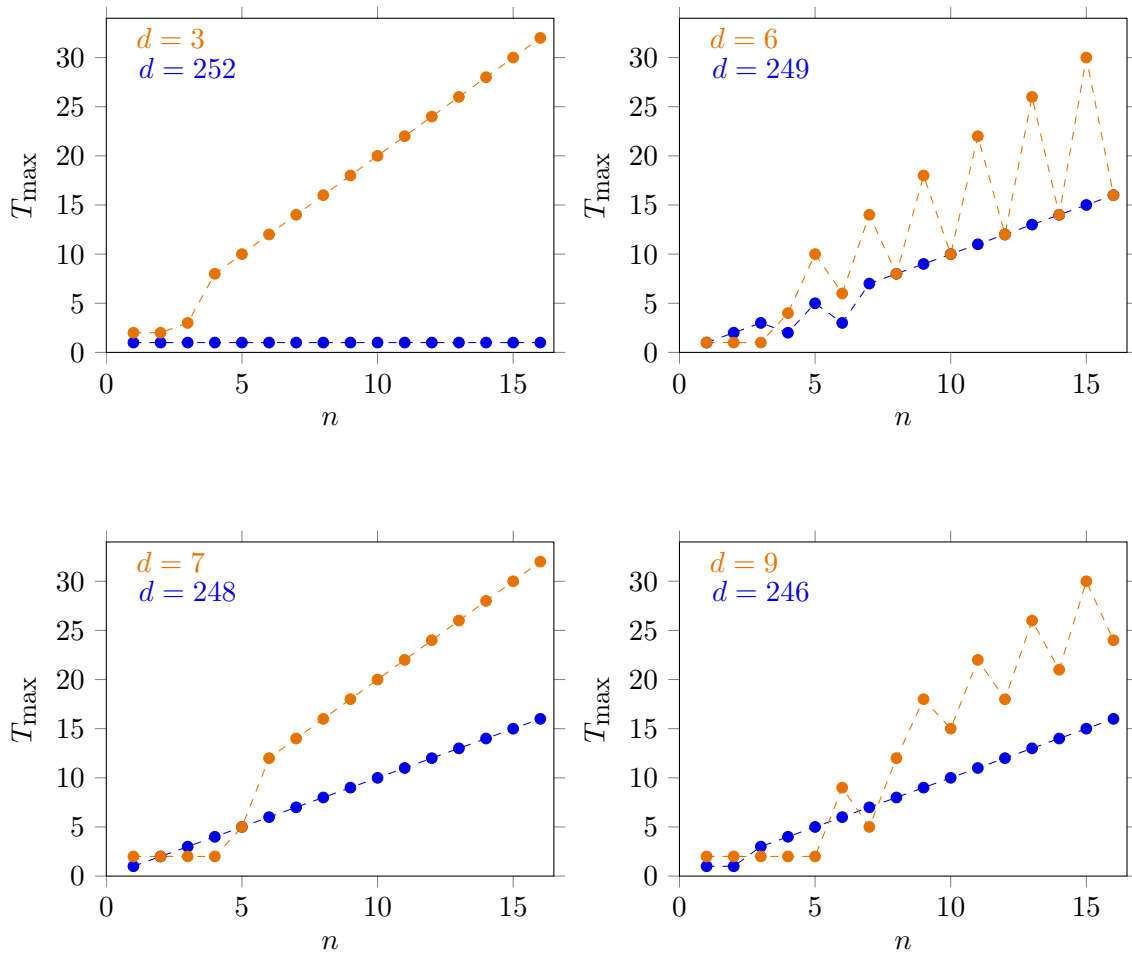
There is a period 2 cycle and a period 8 cycle. In total, 6 out of the 16 possible tuples have no predecessor. They are called ‘unreachables’ or ‘gardens of eden’. A fixed point is ‘reachable’: it is reached from itself.

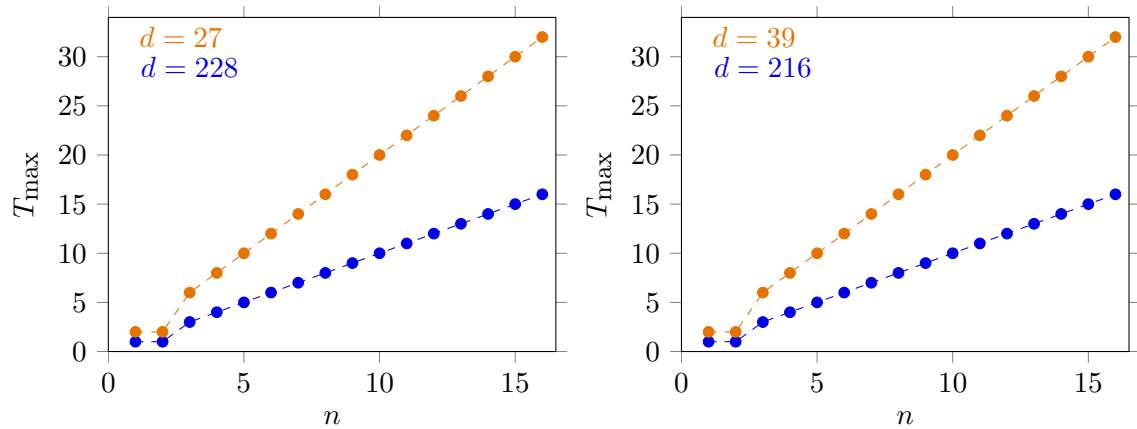
Application of rule $d = 27$ to the 32 different tuples with width 5 leads to the next graph.



That is, application of rule $d = 27$ to tuples with width 5 leads to a period 2 cycle, a period 5 cycle and a period 10 cycle, and 10 out of the 32 possible tuples are unreachable.

Let T_{\max} be the maximum period occurring for a given rule d and a given width n . In the next figures T_{\max} is plotted against the width n for several rules.

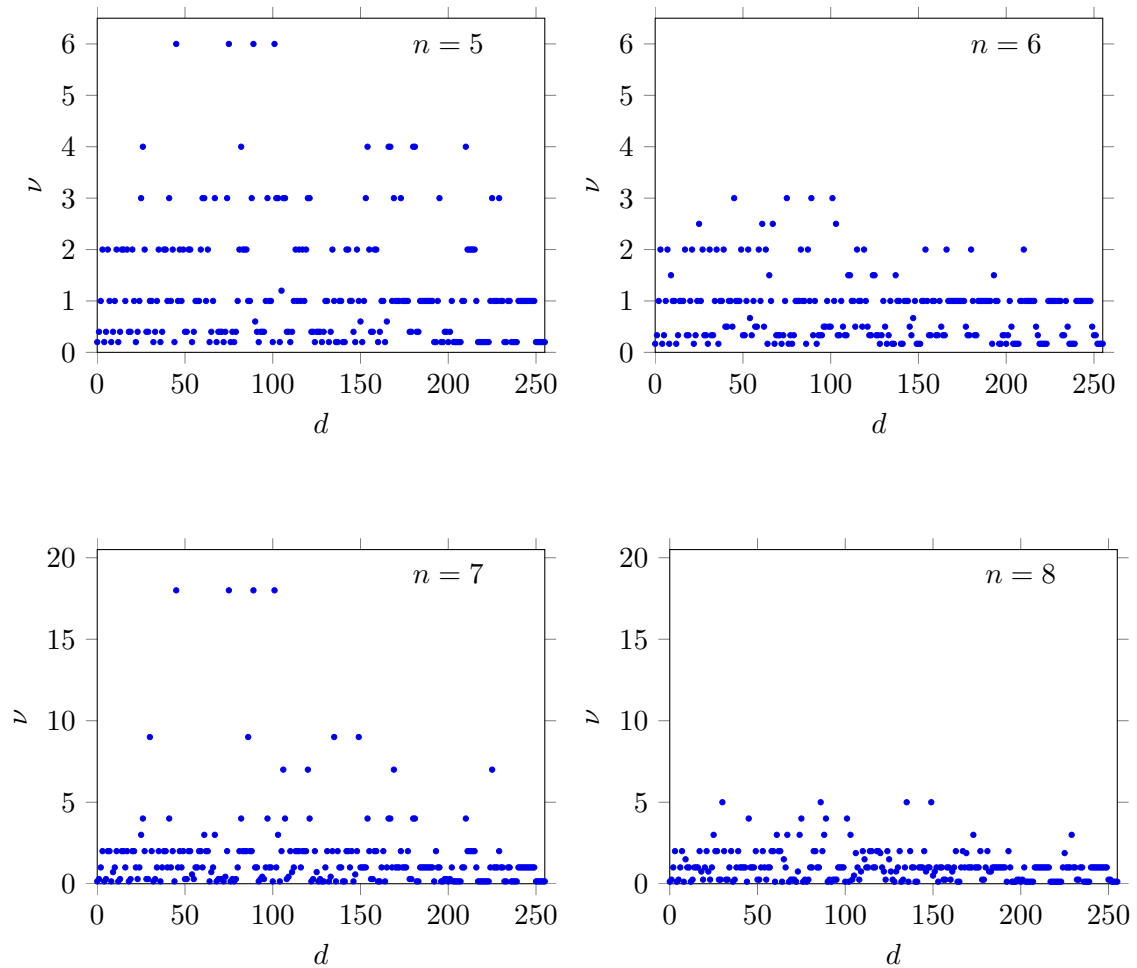


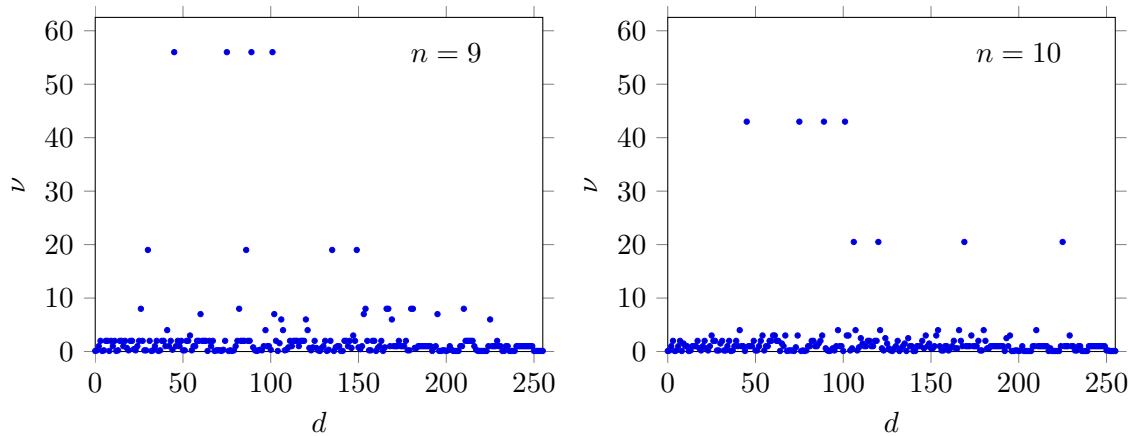


The figures above suggest the maximum period often is 1, 2, $n/2$, n , $3n/2$ or $2n$.

Let ν be the ratio of the largest period and the tuple width. Thus $\nu = T_{\max}/n$.

In the next figures ν is plotted against rule number d for widths $n = 5, 6, 7, 8, 9$ and 10 .





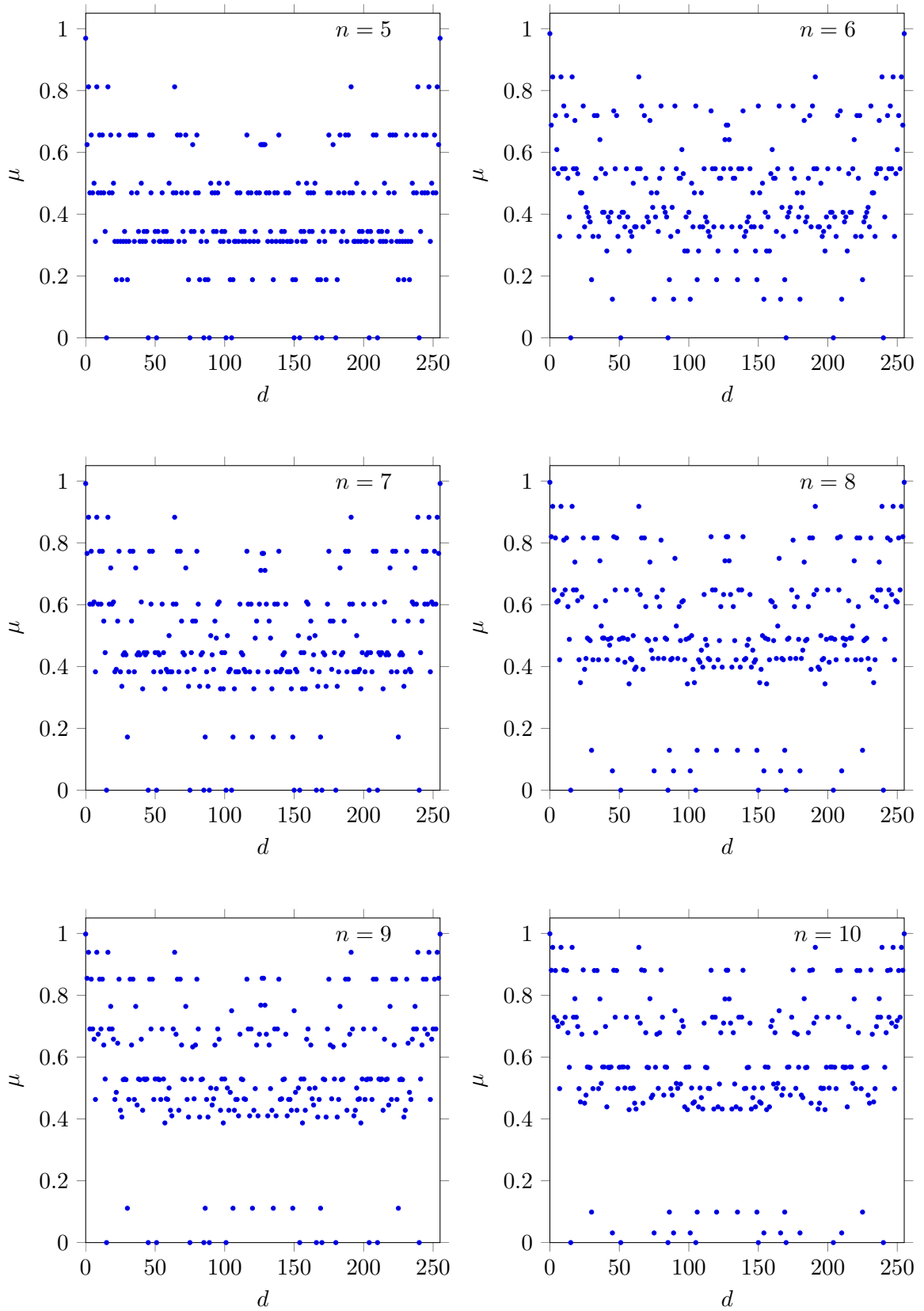
The largest value of ν often occurs for the four rules 45, 75, 89 and 101. Large values for ν also occur for the four rules 30, 86, 135 and 149, the four rules 106, 120, 169 and 225, the four rules 154, 166, 180, and 210, and the four rules 26, 82, 167 and 181. For each of these sets of four rules the first rule is unique, the other three rules are its mirror, its complement and its mirrored complement. For the periods of the sets it suffices to consider only the rules 26, 30, 45, 106 and 154. For these rules the maximum period is shown for widths up to 16 is shown in the next table.

$d \backslash n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
26	1	1	6	1	20	6	28	16	72	20	88	24	104	56	120	32
30	1	1	1	8	5	1	63	40	171	15	154	102	832	1428	1455	6016
45	2	2	3	2	30	18	126	32	504	430	979	240	1105	2198	6820	2816
106	1	2	3	4	15	6	49	15	54	205	176	168	416	448	1095	2688
154	1	1	6	4	20	12	28	8	72	40	88	24	104	56	120	16

Table 2.1: T_{max} for tuple widths $1 \leq n \leq 16$ and rules $d = 26, 30, 45, 106$ and 154 .

2.6 Unreachables

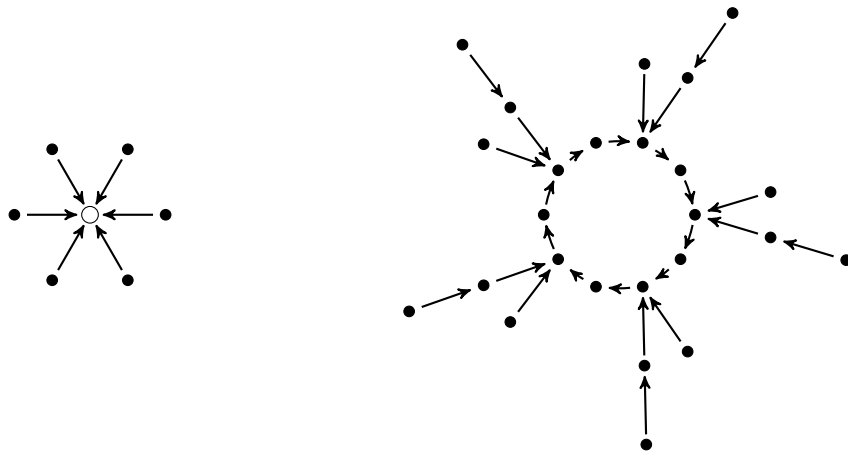
Let μ be the fraction unreachables. In the next six figures μ is plotted against rule number d for tuple width of 5, 6, 7, 8, 9 and 10 numbers.



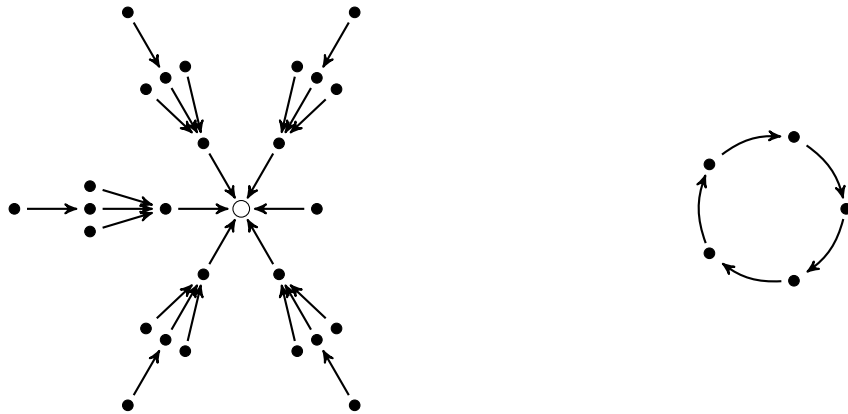
We see that the rule numbers 0, 2, 8, 16, 64, 191, 239, 247, 253 and 255 have the largest number of unreachables for all tuple widths. We see that the rule numbers 15, 45, 51, 75, 85, 89, 101, 154, 166, 170, 180, 204, 210, 240 have a number of unreachables equal to 0 or close to 0. Furthermore the plots are symmetric with respect to the $d = 127.5$ axis. They illustrate the symmetry law that μ for rule d is identical to μ for rule $255 - d$. Formally

$$\mu(d, n) = \mu(255 - d, n). \tag{2.8}$$

The symmetry is remarkable since the graphs of a rule d and its opposite rule $255 - d$ can be completely different. As an illustration, the graph for $d = 20$ and $n = 5$ is



while the graph for $d = 235$ and $n = 5$ is



Although completely different both graphs contain 16 unreachables out of 32 tuples.

The reason for the similarity can be explained by looking at the rules d and $255 - d$. Let us take the two rules in the example above: $d = 20$ and $d = 235$. The two opposite rules are shown below.

rule 20	111	110	101	100	011	010	001	000
	0	0	0	1	0	1	0	0

rule 235	111	110	101	100	011	010	001	000
	1	1	1	0	1	0	1	1

As we see, if $a_k = 1$ for rule 20 then $a_k = 0$ for rule 235 and if $a_k = 0$ for rule 20 then $a_k = 1$ for rule 235. Each a_k of rule 20 is the opposite of the a_k of rule 235 and therefore rule 235 will be called the opposite rule of rule 20. The application of rule 20 and rule 235 to tuple 10010, for instance, leads to 11010 and 00101 respectively. The latter two tuples are each others opposite. Alternatively, if 11010 has 10010 as a predecessor under rule 20, then 00101 has 10010 as a predecessor under rule 235. The property holds for other tuples: if a tuple $(s_1, s_2, s_3, s_4, s_5)$ has tuple $(t_1, t_2, t_3, t_4, t_5)$ as its predecessor under rule 20, then $(1 - s_1, 1 - s_2, 1 - s_3, 1 - s_4, 1 - s_5)$ has tuple $(t_1, t_2, t_3, t_4, t_5)$ as its predecessor under rule 235. As a consequence, each tuple $(s_1, s_2, s_3, s_4, s_5)$ has as many predecessors under rule 20 as tuple $(1 - s_1, 1 - s_2, 1 - s_3, 1 - s_4, 1 - s_5)$ has under rule 235. Indeed, in both the above graphs for rule 20 and rule 235, and $n = 5$, there are 1 tuple with 6 predecessors, 5 tuples with 3 predecessors, 10 tuples with 1 predecessor and 16 tuples with 0 predecessors. The 16 tuples with 0 predecessors are 16 unreachables. We see there are as many unreachables under rule 20 as under rule 235.

Of course, the argument can be generalised to other rules and other tuple widths: if a tuple (s_1, s_2, \dots, s_n) has tuple (t_1, t_2, \dots, t_n) as its predecessor under rule d , then $(1 - s_1, 1 - s_2, \dots, 1 - s_n)$ has tuple (t_1, t_2, \dots, t_n) as its predecessor under rule $255 - d$. As a consequence, each tuple (s_1, s_2, \dots, s_n) has as many predecessors under rule d as tuple $(1 - s_1, 1 - s_2, \dots, 1 - s_n)$ has under rule $255 - d$. In particular, if a tuple (s_1, s_2, \dots, s_n) has no predecessors under rule d then tuple $(1 - s_1, 1 - s_2, \dots, 1 - s_n)$ has no predecessors under rule $255 - d$. Therefore, there are as many unreachables under rule d as under rule $255 - d$.

Chapter 3

Modular CA

3.1 Modular addition in one dimension

In this section we will consider tuples where each number in a tuple is an element of a field $F_k = \{0, 1, 2, 3, \dots, k - 1\}$ with $k > 1$ an integer.

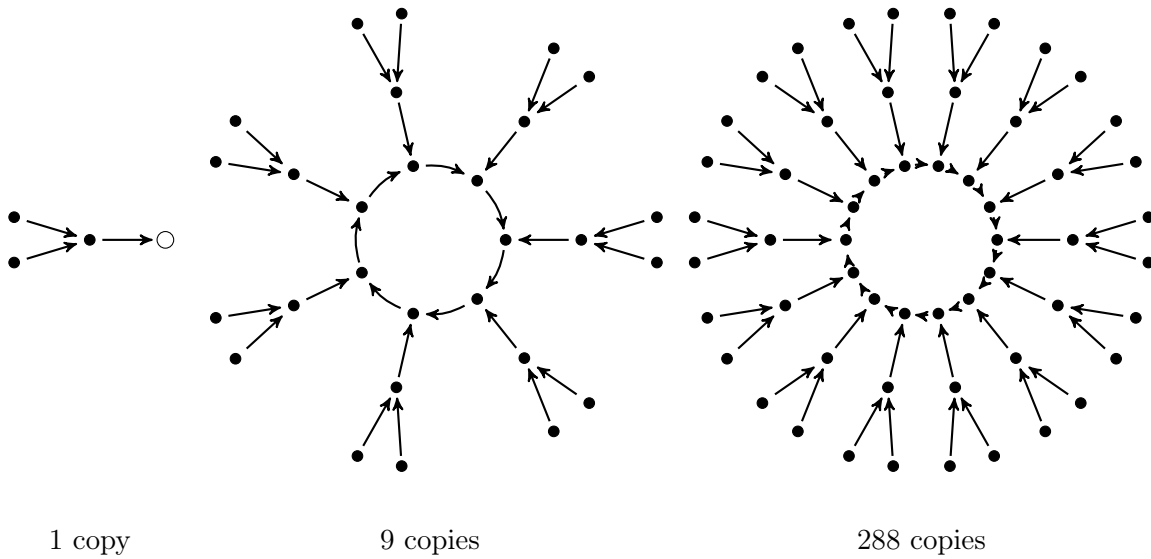
We consider a tuple with width 7 with numbers in $F_4 = \{0, 1, 2, 3\}$, for example,

$$(1, 3, 2, 0, 0, 1, 2) .$$

Suppose a rule is as follows: each number in a tuple is the addition, in F_4 , of the number itself and its left neighbour number. Starting with $(1, 3, 2, 0, 0, 1, 2)$ the repetitive application of this rule leads to the following evolution:

step 1	$(3, 0, 1, 2, 0, 1, 3)$
step 2	$(2, 3, 1, 3, 2, 1, 0)$
step 3	$(2, 1, 0, 0, 1, 3, 1)$
\vdots	\vdots
step 15	$(1, 2, 3, 0, 2, 3, 1)$
step 16	$(2, 3, 1, 3, 2, 1, 0)$

The tuple after step 16 is identical to the tuple after step 2. So, the period is 14 steps. It turns out there are 288 period 14 cycles and 9 period 7 cycles. The tuples $(1, 1, 1, 1, 1, 1, 1)$ and $(3, 3, 3, 3, 3, 3, 3)$ are mapped on the tuple $(2, 2, 2, 2, 2, 2, 2)$ which in turn is mapped on the fixed point $(0, 0, 0, 0, 0, 0, 0)$. The complete graph is shown below.



We see the tuples are attracted to either a fixed point, or to one of the 9 period 7 cycles or to one of the 288 period 14 cycles. In the present graph there are everywhere 3 preperiodic points which arrive (in one or two steps) at a cyclic point. So, in the present graph there are four times as many points as there are cyclic points. For a tuple of 7 numbers in F_4 there are $4^7 = 16384$ different tuples. Since $4 \times (1 \times 1 + 9 \times 7 + 288 \times 14) = 16384$ the book keeping is in order. For the graph a fraction $1/2$ of the tuples is unreachable.

3.2 Tabulation of periods

A left neighbour will be denoted as L and a right neighbour as R . A number itself is denoted as C . There are seven types of rules based on nearest neighbours in one dimensional tuples: L , C , R , $L + C$, $C + R$, $L + R$ and $L + C + R$. The rule L means that each new number inside a tuple just obtains the value of its left neighbour. This is just a shift of states to the left. Under rule C nothing changes. The rule R leads to a shift of states to the right. In F_k the rule $L + C$ means that each number in a tuple is the result of the addition modulo k of the number itself and its left neighbour. Rule $C + R$ means the addition modulo k of a number itself and its right neighbour. Rule $L + R$ means the addition modulo k of the left neighbour and the right neighbour. Rule $L + C + R$ means the addition modulo k of a number itself, its left neighbour and its right neighbour. Rules L , C and R are trivial. Rules $C + R$ is just the mirror of rule $L + C$. Therefore only the three rules $L + C$, $L + R$ and $L + C + R$ will be investigated. For each rule we will investigate tuples of width n in F_k . For each (n, k) pair we will keep track of the different periods of the occurring cycles and the fraction of unreachable tuples. The results are shown in the next three tables for $L + C$, $L + R$ and $L + C + R$ respectively. Each table takes two pages.

$n \backslash k$	1	2	3	4	5	6	7
1	1 0	$1 \frac{1}{2}$	1,2 0	$1 \frac{1}{2}$	1,4 0	$1,2 \frac{1}{2}$	1,3 0
2	1 0	$1 \frac{1}{2}$	$1,2 \frac{2}{3}$	$1 \frac{3}{4}$	$1,4 \frac{4}{5}$	$1,2 \frac{5}{6}$	$1,3 \frac{6}{7}$
3	1 0	$1,3 \frac{1}{2}$	1,2,6 0	$1,3,6 \frac{1}{2}$	1,4,6,12 0	$1,2,3,6 \frac{1}{2}$	1,3,6 0
4	1 0	$1 \frac{1}{2}$	$1,2,8 \frac{2}{3}$	$1 \frac{3}{4}$	$1,2,4 \frac{4}{5}$	$1,2,8 \frac{5}{6}$	$1,3,24 \frac{6}{7}$
5	1 0	$1,15 \frac{1}{2}$	1,2,40 0	$1,15,30 \frac{1}{2}$	1,4,20 0	1,2,15,30, 40,120 $\frac{1}{2}$	1,3,80, 240 0
6	1 0	$1,3,6 \frac{1}{2}$	$1,2,6 \frac{2}{3}$	$1,3,6,12 \frac{3}{4}$	$1,4,6,12,24 \frac{4}{5}$	$1,2,3,6 \frac{5}{6}$	$1,2,3,6 \frac{6}{7}$
7	1 0	$1,7 \frac{1}{2}$	1,2,91,182 0	$1,7,14 \frac{1}{2}$	1,4,217,868 0	1,2,7,14,91, 182 $\frac{1}{2}$	1,3,21 0
8	1 0	$1 \frac{1}{2}$	$1,2,4,8 \frac{2}{3}$	$1 \frac{3}{4}$	$1,2,4,12,24 \frac{4}{5}$	$1,2,4,8 \frac{5}{6}$	$1,3,16,24,48 \frac{6}{7}$
9	1 0	$1,3,63 \frac{1}{2}$	1,2,6,18 0	1,3,6,63, 126 $\frac{1}{2}$	1,4,6,12,558, 1116 0	1,2,3,6,18, 63,126 $\frac{1}{2}$	1,3,6,342 0
10	1 0	1,15,30 $\frac{1}{2}$	1,2,40,80 $\frac{2}{3}$	1,15,30,60 $\frac{3}{4}$	1,4,20 $\frac{4}{5}$	1,2,15,30,40, 80,120,240 $\frac{5}{6}$	1,3,80,240, 480 $\frac{6}{7}$
11	1 0	$1,341 \frac{1}{2}$	1,242 0	1,341,682 $\frac{1}{2}$	1,4,142,284, 1562,3124 0	1,2,242,341, 682,7502 $\frac{1}{2}$	1,3,61622, 184866 0
12	1 0	$1,3,6,12 \frac{1}{2}$	1,2,6,8,24 $\frac{2}{3}$	1,3,6,12,24 $\frac{3}{4}$	1,2,4,6,8,12, 24 $\frac{4}{5}$	1,2,3,6,8,12, 24 $\frac{5}{6}$	1,2,3,6,24,48 $\frac{6}{7}$
13	1 0	$1,819 \frac{1}{2}$	1,2,13,26 0	1,819,1638 $\frac{1}{2}$	1,4,156,312 0	1,2,13,26,819, 1638 $\frac{1}{2}$	1,3,169936, 509808 0
14	1 0	$1,7,14 \frac{1}{2}$	1,2,91,182, 364 $\frac{2}{3}$	$1,7,14,28 \frac{3}{4}$	1,4,217,868, 1736 $\frac{4}{5}$	1,2,7,14,91, 182,364 $\frac{5}{6}$	$1,3,21 \frac{6}{7}$
15	1 0	1,3,5,15 $\frac{1}{2}$	1,2,6,40, 120 0	1,3,5,6,10, 15,30 $\frac{1}{2}$	1,4,6,12,20, 30,60 0	1,2,3,5,6,10, 15,30,40,120 $\frac{1}{2}$	1,3,6,80,240, 1200 0
16	1 0	$1 \frac{1}{2}$	1,2,4,8,40, 80 $\frac{2}{3}$	$1 \frac{3}{4}$	1,2,4,12,24, 312,624 $\frac{4}{5}$	1,2,4,8,40,80 $\frac{5}{6}$	1,3,8,16,24,48 $\frac{6}{7}$

$n \backslash k$	8	9	10	11	12
1	$1 \frac{1}{2}$	1,2,6 0	$1,4 \frac{1}{2}$	1,10 0	$1,2 \frac{1}{2}$
2	$1 \frac{7}{8}$	$1,2,6 \frac{8}{9}$	$1,4 \frac{9}{10}$	$1,10 \frac{10}{11}$	$1,2 \frac{11}{12}$
3	$1,3,6 \frac{1}{2}$	1,2,6,18 0	$1,3,4,6,12 \frac{1}{2}$	1,6,10,30 0	$1,2,3,6 \frac{1}{2}$
4	$1 \frac{7}{8}$	$1,2,6,8,24 \frac{8}{9}$	$1,2,4 \frac{9}{10}$	$1,10,40 \frac{10}{11}$	$1,2,8 \frac{11}{12}$
5	$1,15,30,60 \frac{1}{2}$	1,2,6,40,120 0	$1,4,15,20,60 \frac{1}{2}$	1,2,5,10 0	$1,2,15,30,40,120 \frac{1}{2}$
6	$1,3,6,12,24 \frac{7}{8}$	$1,2,6,18 \frac{8}{9}$	$1,3,4,6,12,24 \frac{9}{10}$	$1,6,10,30,60 \frac{10}{11}$	$1,2,3,6,12 \frac{11}{12}$
7	$1,7,14,28 \frac{1}{2}$	1,2,6,91,182, 273,546 0	$1,4,7,28,217,$ $868 \frac{1}{2}$	1,10,19,133,190, 1330 0	$1,2,7,14,91,182 \frac{1}{2}$
8	$1 \frac{7}{8}$	$1,2,4,6,8,12,24 \frac{8}{9}$	$1,2,4,12,24 \frac{9}{10}$	$1,10,30,40,120 \frac{10}{11}$	$1,2,4,8 \frac{11}{12}$
9	$1,3,6,63,126,$ $252 \frac{1}{2}$	1,2,6,18,54 0	$1,3,4,6,12,63,126,$ $252,558,1116,$ $3906,7812 \frac{1}{2}$	$1,6,10,30,2394,$ 11970 0	$1,2,3,6,18,63,$ $126 \frac{1}{2}$
10	$1,15,30,60,$ $120 \frac{7}{8}$	$1,2,6,40,80,120,$ $240 \frac{8}{9}$	$1,4,15,20,30,60 \frac{9}{10}$	$1,2,5,10 \frac{10}{11}$	$1,2,15,30,40,60,$ $80,120,240 \frac{11}{12}$
11	$1,341,682,$ $1364 \frac{1}{2}$	1,2,6,242,726 0	$1,4,142,284,341,$ $1364,1562,3124,$ $48422,96844 \frac{1}{2}$	1,10,110 0	$1,2,242,341,682,$ $7502 \frac{1}{2}$
12	$1,3,6,12,24,$ $48 \frac{7}{8}$	$1,2,6,8,18,24,72 \frac{8}{9}$	$1,2,3,4,6,8,12,24 \frac{9}{10}$	$1,6,10,30,40,60,$ $120 \frac{10}{11}$	$1,2,3,6,8,12,24 \frac{11}{12}$
13	$1,819,1638,$ $3276 \frac{1}{2}$	1,2,6,13,26,39, 78 0	$1,4,156,312,819,$ $3276,6552 \frac{1}{2}$	1,10,1535352, 7676760 0	$1,2,13,26,819,$ $1638 \frac{1}{2}$
14	$1,7,14,28,56 \frac{7}{8}$	$1,2,6,91,182,273,$ $364,546, 1092 \frac{8}{9}$	$1,4,7,14,28,217,$ $434,868,1736 \frac{9}{10}$	$1,10,19,95,133,$ $190,665,1330 \frac{10}{11}$	$1,2,7,14,28,91,$ $182,364 \frac{11}{12}$
15	$1,3,5,6,10,15,$ $20,30,60 \frac{1}{2}$	$1,2,6,18,40,120,$ 360 0	$1,3,4,5,6,12,15,$ $20,30,60 \frac{1}{2}$	$1,2,5,6,8,10,24,$ $30,40,120 0$	$1,2,3,5,6,10,15,$ $30,40,120 \frac{1}{2}$
16	$1 \frac{7}{8}$	$1,2,4,6,8,12,24,$ $40,80,120,240 \frac{8}{9}$	$1,2,4,12,24,312,$ $624 \frac{9}{10}$	$1,10,30,40,120,$ $3660,7320,14640 \frac{10}{11}$	$1,2,4,8,40,80 \frac{11}{12}$

Table 3.1: Cycle periods (separated by a comma) and (separated by a blanc) the fraction of unreachable tuples for tuples with width n under the modular addition rule $L + C$ modulo k , see text.

$n \backslash k$	1	2	3	4	5	6	7
1	1 0	$1 \frac{1}{2}$	1,2 0	$1 \frac{1}{2}$	1,4 0	$1,2 \frac{1}{2}$	1,3 0
2	1 0	$1 \frac{3}{4}$	1,2 0	$1 \frac{3}{4}$	1,4 0	$1,2 \frac{3}{4}$	1,3,6 0
3	1 0	$1 \frac{1}{2}$	1,2,6 0	$1,2 \frac{1}{2}$	1,2,4 0	$1,2,6 \frac{1}{2}$	1,2,3,6 0
4	1 0	$1 \frac{3}{4}$	$1,2 \frac{8}{9}$	$1 \frac{15}{16}$	$1,4 \frac{24}{25}$	$1,2 \frac{35}{36}$	$1,3,6 \frac{48}{49}$
5	1 0	$1,3 \frac{1}{2}$	1,2,8 0	$1,3,6 \frac{1}{2}$	1,4,20 0	$1,2,3,6,8,24 \frac{1}{2}$	1,3,16,48 0
6	1 0	$1,2 \frac{3}{4}$	1,2,3,6 0	$1,2 \frac{3}{4}$	1,2,4 0	$1,2,3,6 \frac{3}{4}$	1,2,3,6 0
7	1 0	$1,7 \frac{1}{2}$	1,2,13,26 0	$1,7,14 \frac{1}{2}$	1,4,31,124 0	1,2,7,13,14,26, $91,182 \frac{1}{2}$	1,3,21 0
8	1 0	$1 \frac{3}{4}$	$1,2,4 \frac{8}{9}$	$1 \frac{15}{16}$	$1,4,8 \frac{24}{25}$	$1,2,4 \frac{35}{36}$	$1,3,6 \frac{48}{49}$
9	1 0	$1,7 \frac{1}{2}$	1,2,6,18 0	$1,2,7,14 \frac{1}{2}$	1,2,4,62, 124 0	1,2,6,7,14,18, $42,126 \frac{1}{2}$	1,2,3,6,114 0
10	1 0	$1,3,6 \frac{3}{4}$	1,2,8 0	$1,3,6 \frac{3}{4}$	1,4,20 0	$1,2,3,6,8,24 \frac{3}{4}$	1,3,6,16,48 0
11	1 0	$1,31 \frac{1}{2}$	1,2,242 0	$1,31,62 \frac{1}{2}$	1,4,1562, 3124 0	1,2,31,62,242, $7502 \frac{1}{2}$	1,3,5602,16806 0
12	1 0	$1,2,4 \frac{3}{4}$	$1,2,3,6 \frac{8}{9}$	$1,2,4 \frac{15}{16}$	$1,2,4,8 \frac{24}{25}$	$1,2,3,4,6,124 \frac{35}{36}$	$1,2,3,6,12 \frac{48}{49}$
13	1 0	$1,63 \frac{1}{2}$	1,2,13,26 0	$1,63,126 \frac{1}{2}$	1,4,12,24 0	1,2,13,26,63, $126,819,1638 \frac{1}{2}$	1,3,13072, 39216 0
14	1 0	$1,7,14 \frac{3}{4}$	1,2,13,26 0	$1,7,14 \frac{3}{4}$	1,4,31,62, 124 0	1,2,7,13,14,26, $91,182 \frac{3}{4}$	1,3,6,21,42 0
15	1 0	$1,3,15 \frac{1}{2}$	1,2,6,8,24 0	1,2,3,6,15, $30 \frac{1}{2}$	1,2,4,10,20 0	1,2,3,6,8,15, $24,30,120 \frac{1}{2}$	1,2,3,6,16,48, 400,1200 0
16	1 0	$1 \frac{3}{4}$	$1,2,4,16 \frac{8}{9}$	$1 \frac{15}{16}$	$1,4,8,48 \frac{24}{25}$	$1,2,4,16 \frac{35}{36}$	$1,3,4,6,12 \frac{48}{49}$

$n \backslash k$	8	9	10	11	12
1	$1 \frac{1}{2}$	1,2,6 0	$1,4 \frac{1}{2}$	1,10 0	$1,2 \frac{1}{2}$
2	$1 \frac{3}{4}$	1,2,3,6 0	$1,4 \frac{3}{4}$	1,5,10 0	$1,2 \frac{3}{4}$
3	$1,2 \frac{1}{2}$	1,2,6,18 0	$1,2,4 \frac{1}{2}$	1,2,10 0	$1,2,6 \frac{1}{2}$
4	$1 \frac{63}{64}$	1,2,3,6 $\frac{80}{81}$	$1,4 \frac{99}{100}$	1,5,10 $\frac{120}{121}$	$1,2 \frac{143}{144}$
5	$1,3,6,12 \frac{1}{2}$	1,2,6,8,24 0	$1,3,4,12,20,60 \frac{1}{2}$	1,5,10 0	$1,2,3,6,8,24 \frac{1}{2}$
6	$1,2 \frac{3}{4}$	1,2,3,6,9,18 0	$1,2,4 \frac{3}{4}$	1,2,5,10 0	$1,2,3,6 \frac{3}{4}$
7	$1,7,14,28 \frac{1}{2}$	1,2,6,13,26,39,78 0	$1,4,7,28,31,124,217,868 \frac{1}{2}$	1,10,133,1330 0	$1,2,7,13,14,26,91,182 \frac{1}{2}$
8	$1 \frac{63}{64}$	1,2,3,4,6,12 $\frac{80}{81}$	$1,4,8 \frac{99}{100}$	1,5,10,20 $\frac{120}{121}$	$1,2,4 \frac{143}{144}$
9	$1,2,7,14,28 \frac{1}{2}$	1,2,6,18,54 0	$1,2,4,7,14,28,62,124,434,868 \frac{1}{2}$	1,2,10,266,1330 0	$1,2,6,7,14,18,42,126 \frac{1}{2}$
10	$1,3,6,12 \frac{3}{4}$	1,2,3,6,8,24 0	$1,3,4,6,12,20,60 \frac{3}{4}$	1,5,10 0	$1,2,3,6,8,24 \frac{3}{4}$
11	$1,31,62,124 \frac{1}{2}$	1,2,6,242,726 0	$1,4,31,124,1562,3124,48422,96844 \frac{1}{2}$	1,10,110 0	$1,2,31,62,242,7502 \frac{1}{2}$
12	$1,2,4,8 \frac{63}{64}$	1,2,3,6,9,18 $\frac{80}{81}$	$1,2,4,8 \frac{99}{100}$	1,2,5,10 $\frac{120}{121}$	$1,2,3,4,6,12 \frac{143}{144}$
13	$1,63,126,252 \frac{1}{2}$	1,2,6,13,26,39,78 0	$1,4,12,24,63,252,504 \frac{1}{2}$	1,10,118104,590520 0	$1,2,13,26,63,126,819,1638 \frac{1}{2}$
14	$1,7,14,28 \frac{3}{4}$	1,2,3,6,13,26,39,78 0	$1,4,7,14,28,31,62,124,217,434,868 \frac{3}{4}$	1,5,10,133,266,665,1330 0	$1,2,7,13,14,26,91,182 \frac{3}{4}$
15	$1,2,3,6,12,15,30,60 \frac{1}{2}$	1,2,6,8,18,24,72 0	$1,2,3,4,6,10,12,15,20,30,60 \frac{1}{2}$	1,2,5,10,120 0	$1,2,3,6,8,15,24,30,120 \frac{1}{2}$
16	$1 \frac{63}{64}$	1,2,3,4,6,12,16,48 $\frac{80}{81}$	$1,4,8,48 \frac{99}{100}$	1,5,10,20,240 $\frac{120}{121}$	$1,2,4,16 \frac{143}{144}$

Table 3.2: Cycle periods (separated by a comma) and (separated by a blanc) the fraction of unreachable tuples for tuples with width n under the modular addition rule $L + R$ modulo k , see text.

$n \backslash k$	1	2	3	4	5	6	7
1	1 0	1 0	$1 \frac{2}{3}$	1,2 0	1,4 0	$1 \frac{2}{3}$	1,6 0
2	1 0	1 0	$1,2 \frac{2}{3}$	1,2 0	1,2,4 0	$1,2 \frac{2}{3}$	1,2,6 0
3	1 0	$1 \frac{3}{4}$	$1 \frac{8}{9}$	$1,2 \frac{15}{16}$	$1,4 \frac{24}{25}$	$1 \frac{35}{36}$	$1,6 \frac{48}{49}$
4	1 0	1,2 0	$1,2 \frac{2}{3}$	1,2,4 0	1,2,4 0	$1,2 \frac{2}{3}$	1,2,6 0
5	1 0	1,3 0	$1,8 \frac{2}{3}$	1,2,3,6 0	1,4,20 0	$1,3,8,24 \frac{2}{3}$	1,6,16,48 0
6	1 0	$1 \frac{3}{4}$	$1,2,6 \frac{8}{9}$	$1,2 \frac{15}{16}$	$1,2,4 \frac{24}{25}$	$1,2,6 \frac{35}{36}$	$1,2,3,6 \frac{48}{49}$
7	1 0	1,7 0	$1,26 \frac{2}{3}$	1,2,7,14 0	1,4,62,124 0	$1,7,26,182 \frac{2}{3}$	1,6,42 0
8	1 0	1,2,4 0	$1,2,8 \frac{2}{3}$	1,2,4,8 0	1,2,4,12 0	$1,2,4,8 \frac{2}{3}$	1,2,3,6 0
9	1 0	$1,7 \frac{3}{4}$	$1 \frac{8}{9}$	1,2,7,14 $\frac{15}{16}$	$1,4,124 \frac{24}{25}$	$1,7 \frac{35}{36}$	$1,6,171,342 \frac{48}{49}$
10	1 0	1,3,6 0	$1,2,4,8 \frac{2}{3}$	1,2,3,6,12 0	1,2,4,10,20 0	1,2,3,4,6,8, $12,24 \frac{2}{3}$	1,2,6,8,16, 24,48 0
11	1 0	1,31 0	$1,121 \frac{2}{3}$	1,2,31,62 0	1,4,781, 3124 0	$1,31,121,3751 \frac{2}{3}$	1,6,2801,16806 0
12	1 0	$1,2 \frac{3}{4}$	$1,2,3,6 \frac{8}{9}$	$1,2,4 \frac{15}{16}$	$1,2,4,24 \frac{24}{25}$	$1,2,3,6 \frac{35}{36}$	$1,2,3,6,48 \frac{48}{49}$
13	1 0	1,21 0	$1,13 \frac{2}{3}$	1,2,21,42 0	1,3,4,8,12, 24 0	$1,13,21,273 \frac{2}{3}$	1,6,817,4902 0
14	1 0	1,7,14 0	$1,2,26 \frac{2}{3}$	1,2,7,14,28 0	1,2,4,62, 124 0	$1,2,7,14,26,182 \frac{2}{3}$	1,2,6,14,42 0
15	1 0	1,3,5,15 $\frac{3}{4}$	$1,8,24 \frac{8}{9}$	1,2,3,5,6, 10,15,30 $\frac{15}{16}$	$1,4,20 \frac{24}{25}$	1,3,5,8,15,24, $40,120 \frac{35}{36}$	1,6,16,48,600, 1200 0
16	1 0	1,2,4,8 0	$1,2,8,80 \frac{2}{3}$	1,2,4,8,16 0	1,2,4,12, 312 0	$1,2,4,8,80 \frac{2}{3}$	1,2,3,6,24,48 0

$n \backslash k$	8	9	10	11	12
1	1,2 0	$1 \frac{2}{3}$	1,4 0	1,5 0	$1,2 \frac{2}{3}$
2	1,2,4 0	$1,2 \frac{2}{3}$	1,2,4 0	1,2,5,10 0	$1,2 \frac{2}{3}$
3	$1,2 \frac{63}{64}$	$1 \frac{80}{81}$	$1,4 \frac{99}{100}$	$1,5 \frac{120}{121}$	$1,2 \frac{143}{144}$
4	1,2,4,8 0	$1,2 \frac{2}{3}$	1,2,4 0	1,2,5,10 0	$1,2,4 \frac{2}{3}$
5	1,2,3,6,12 0	$1,8,24 \frac{2}{3}$	1,3,4,12,20,60 0	1,5,10 0	$1,2,3,6,8,24 \frac{2}{3}$
6	$1,2,4 \frac{63}{64}$	$1,2,6,18 \frac{80}{81}$	$1,2,4 \frac{99}{100}$	$1,2,5,10 \frac{120}{121}$	$1,2,6 \frac{143}{144}$
7	1,2,7,14,28 0	$1,26,78 \frac{2}{3}$	1,4,7,28,62,124, 434,868 0	1,5,266,1330 0	$1,2,7,14,26,182 \frac{2}{3}$
8	1,2,4,8,16 0	$1,2,8,24 \frac{2}{3}$	1,2,4,12 0	1,2,5,10,24,120 0	$1,2,4,8 \frac{2}{3}$
9	1,2,7,14,28 $\frac{63}{64}$	$1 \frac{80}{81}$	1,4,7,28,124, 868 $\frac{99}{100}$	1,5,1330 $\frac{120}{121}$	$1 \frac{143}{144}$
10	1,2,3,4,6,12, 24 0	$1,2,4,8,12,24 \frac{2}{3}$	1,2,3,4,6,10,12, 20,30,60 0	1,2,5,10 0	$1,2,3,4,6,8,12,24 \frac{2}{3}$
11	1,2,31,62,124 0	$1,121,363 \frac{2}{3}$	1,4,31,124,781, 3124,24211, 96844 0	1,5,55 0	$1,2,31,62,121, 242,3751,7502 \frac{2}{3}$
12	$1,2,4,8 \frac{63}{64}$	$1,2,3,6,9,18 \frac{80}{81}$	$1,2,4,24 \frac{99}{100}$	$1,2,5,10 \frac{120}{121}$	$1,2,3,4,6,12 \frac{143}{144}$
13	1,2,21,42,84 0	$1,13,39 \frac{2}{3}$	1,3,4,8,12,21,24, 84,168 0	1,5,4921,24605 0	$1,2,13,21,26,42, 273,546 \frac{2}{3}$
14	1,2,4,7,14,28, 56 0	$1,2,26,78 \frac{2}{3}$	1,2,4,7,14,28,62, 124,434,868 0	1,2,5,10,266, 1330 0	$1,2,7,14,26,28, 182,364 \frac{2}{3}$
15	1,2,3,5,6,10, 12,15,20,30, $60 \frac{63}{64}$	$1,8,24,72 \frac{80}{81}$	1,3,4,5,12,15,20, $60 \frac{99}{100}$	1,5,10,40,60,120 $\frac{120}{121}$	$1,2,3,5,6,8,10, 15,24,30,40,120 \frac{143}{144}$
16	1,2,4,8,16,32 0	$1,2,8,24,80,240 \frac{2}{3}$	1,2,4,8,12,24,312 0	1,2,5,10,24,120, 2928,14640 0	$1,2,4,8,16,80 \frac{2}{3}$

Table 3.3: Cycle periods (separated by a comma) and (separated by a blanc) the fraction of unreachable tuples for tuples with width n under the modular addition rule $L + C + R$ modulo k , see text.

The fraction of unreachables will be denoted by μ . In each table a pattern can be recognized for the fractions of unreachables.

For the $L + C$ rule:

$$\mu = \begin{cases} 0 & \text{if } n \text{ is odd and } k \text{ is odd;} \\ \frac{1}{2} & \text{if } n \text{ is odd and } k \text{ is even;} \\ \frac{k-1}{k} & \text{if } n \text{ is even.} \end{cases} \quad (3.1)$$

For the $L + R$ rule:

$$\mu = \begin{cases} 0 & \text{if } n \not\equiv 0 \pmod{4} \text{ and } k \text{ is odd;} \\ \frac{3}{4} & \text{if } n \equiv 2 \pmod{4} \text{ and } k \text{ is even;} \\ \frac{1}{2} & \text{if } n \text{ is odd and } k \text{ is even;} \\ \frac{k^2-1}{k^2} & \text{if } n \equiv 0 \pmod{4}. \end{cases} \quad (3.2)$$

For the $L + C + R$ rule:

$$\mu = \begin{cases} 0 & \text{if } n \not\equiv 0 \pmod{3} \text{ and } k \not\equiv 0 \pmod{3}; \\ \frac{2}{3} & \text{if } n \not\equiv 0 \pmod{3} \text{ and } k \equiv 0 \pmod{3}; \\ \frac{k^2-1}{k^2} & \text{if } n \equiv 0 \pmod{3}. \end{cases} \quad (3.3)$$

3.3 Preperiodic points

If we start with tuple $(0, 0, 1)$ and follow the evolution under $L + C$ modulo 4, we successively obtain $(1, 0, 1)$, $(2, 1, 1)$, $(3, 3, 2)$, $(1, 2, 1)$, $(2, 3, 2)$, $(0, 1, 1)$, $(1, 1, 2)$, $(3, 2, 3)$, $(2, 1, 1)$. The first of these tuples which is part of a cycle is $(2, 1, 1)$. The two tuples $(0, 0, 1)$ and $(1, 0, 1)$ are preperiodic tuples. We will denote the number of preperiodic tuples as p . In general p depends on the width n and the field F_k : $p = p(n, k)$. For the given example $p(3, 4) = 2$. For $1 \leq n \leq 16$ and $1 \leq k \leq 8$ the $p(n, k)$ are shown in the table on the next page.

We denote the prime factorization of n as $n = 2^{\eta_2} \cdot 3^{\eta_3} \cdot 5^{\eta_5} \cdot \dots$ and of k as $k = 2^{\kappa_2} \cdot 3^{\kappa_3} \cdot 5^{\kappa_5} \cdot \dots$. The $p(n, k)$ can be expressed as a function of the powers η_j and κ_j .

If we consider the column for each k than the $p(n, k)$ seem to obey the following rules:

$$\begin{aligned} p(n, 1) &= 0, \\ p(n, 2) &= 2^{\eta_2}, \\ p(n, 3) &= \text{mod } [n + 1, 2] \cdot 3^{\eta_3}, \\ p(n, 4) &= \text{mod } [n, 2] \cdot 2 + \text{mod } [n + 1, 2] \cdot 3^{\eta_2-1}, \\ p(n, 5) &= \text{mod } [n + 1, 2] \cdot 5^{\eta_5}, \\ p(n, 6) &= \max(p(n, 2), p(n, 3)), \\ p(n, 7) &= \text{mod } [n + 1, 2] \cdot 7^{\eta_7}, \\ p(n, 8) &= \text{mod } [n, 2] + 2^{\eta_2+1}, \end{aligned}$$

where $\text{mod } [a, b]$ stands for $a \text{ mod } b$.

If we consider the row for each n than the $p(n, k)$ seem to obey the following rules:

$$p(1, k) = \kappa_2,$$

$$p(2, k) = \kappa_2 + 1,$$

$$p(3, k) = \kappa_2,$$

$$p(4, k) = 2\kappa_2 + 2 - \text{mod } [k, 2],$$

$$p(5, k) = \kappa_2,$$

$$p(6, k) = 1 + \max(\kappa_2, 2\kappa_3),$$

$$p(7, k) = \kappa_2,$$

$$p(8, k) = 4\kappa_2 + 4 - 3 \text{ mod } [k, 2],$$

$$p(9, k) = \kappa_2,$$








$$p(10, k) = 4\kappa_5 \text{ if } \text{mod } (k, 5) = 0 \text{ and } p(10, k) = \kappa_2 + 1 \text{ if } \text{mod } (k, 5)! = 0,$$



$$p(11, k) = \kappa_2, \text{ etc.}$$



It is not known to us if it is possible to cast $p(n, k)$ in a single general equation or in a limited set of simple rules.

$n \backslash k$	1	2	3	4	5	6	7	8
1	0	1	0	2	0	1	0	3
2	0	2	1	3	1	2	1	4
3	0	1	0	2	0	1	0	3
4	0	4	1	6	1	4	1	8
5	0	1	0	2	0	1	0	3
6	0	2	3	3	1	3	1	4
7	0	1	0	2	0	1	0	3
8	0	8	1	12	1	8	1	16
9	0	1	0	2	0	1	0	3
10	0	2	1	3	5	2	1	4
11	0	1	0	2	0	1	0	3
12	0	4	3	6	1	4	1	8
13	0	1	0	2	0	1	0	3
14	0	2	1	3	1	2	7	4
15	0	1	0	2	0	1	0	3
16	0	16	1	24	1	16	1	32

3.4 Modular addition in two dimensions

We return to the 2D circular grid with two states per cell (black and white say) and the rule that a cell flips its state if it has an odd number of black (or white) nearest neighbours as we already met in section 1.6. There we saw how a single black cell in a circular 3×3 grid  evolves to a cross  which on its turn evolves in itself. That is,  is a preperiodic point and  is a fixed point. We also saw how a single cell in a circular 5×5 grid evolves to the cross  which is part of a period 3 cycle. Further investigations deliver that the cross in a 4×4 grid is part of a period 2 cycle. In a 6×6 grid the cross is a preperiodic point which evolves in a period 2 cycle. In a 7×7 grid the cross is part of a period 7 cycle, and so on. Below some cycle lengths are tabulated for different $n \times n$ grids and for two different initial configurations,  and , with the evolution according to the aforementioned rule.

grid size	init. conf.	
		
3×3	1	1
5×5	3	3
7×7	7	7
9×9	7	7
11×11	31	31
13×13	63	63
15×15	15	15
17×17	15	15
19×19	511	511
21×21	63	63
23×23	2047	2047
25×25	1023	1023
27×27	511	511
29×29	16383	16383
31×31	31	31

grid size	init. conf.	
		
4×4	2	1
6×6	2	1
8×8	4	4
10×10	6	6
12×12	4	4
14×14	14	14
16×16	8	8
18×18	14	14
20×20	12	12
22×22	62	62
24×24	8	8
26×26	126	126
28×28	28	28
30×30	30	30
32×32	16	16

If a white state and a black state of a cell is represented with a 0 and a 1 respectively, then the rule under concern can also be written as:

$$c'_{i,j} = (c_{i,j} + c_{i-1,j} + c_{i+1,j} + c_{i,j-1} + c_{i,j+1}) \pmod{2},$$

where $c_{i,j}$ is the state of cell with index i and index j . Thus $c_{i,j}$ either is 0 or 1. This means that the foregoing investigation actually was about modular addition in two dimensions. Of course, the investigation can be extended to more complicated addition rules and to cells with more than two states. However, further investigations in this direction is beyond our scope.

3.5 Game of Life

In addition to the four nearest neighbours of a cell often the four next-nearest neighbours participate in the rules of evolution. That is, the eight blue cells in the next figure determine the evolution of the green cell at the center.





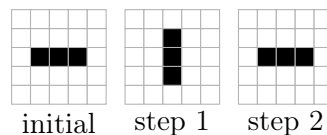
A cell can be black or white. For the situation with 8 neighbours a famous set of rules for the evolution of cell states is:

- 1 If 0 or 1 of the 8 neighbour cells are black, the center cell will stay white if it was white or become white if it was black.
- 2 If 2 of the 8 neighbour cells are black, the center cell will stay white if it was white or stay black if it was black.
- 3 If 3 of the 8 neighbour cells are black, the center cell will become black if it was white or stay black if it was black.
- 4 If more than 3 of the 8 neighbour cells are black, the center cell will stay white if it was white or become white if it was black.

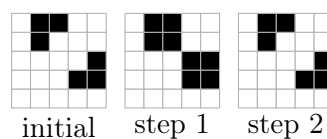
If 'black' stands for 'live' and 'white' for 'dead', then the four rules can be given a sort of biological interpretation:

- 1 A cell will not be viable if there are too less live neighbours to care for.
- 2 A cell stays as it is if it has 2 live neighbours.
- 3 A cell will come to live if it has 3 live neighbours.
- 4 A cell will extinct because of overpopulation if it has more than 3 live neighbours.

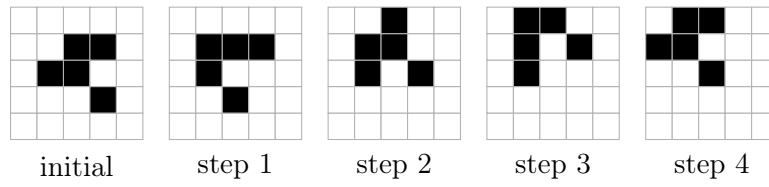
The cellular automaton which evolves according to these rules is known as Conway's *Game of Life*. For each initial configuration one follows the evolution of the pattern of live cells. For some initial patterns the live cells all extinct after one or more generations. For some initial patterns, such as  or , the pattern does not change. Such fixed points are called a 'still lifes'. Other patterns might become periodic, the 'oscillators'. Two examples of period 2 cycles are



and



It also happens that a cyclic pattern translates across the grid, the ‘spaceships’. One of the simplest spaceships is the ‘glider’, see next figure.



The glider pattern repeats after every four steps, except that it has translated across the grid in a diagonal direction.

Chapter 4

Pascal triangle

4.1 Binomial coefficients

The Pascal triangle is a triangular array of binomial coefficients. That is, of the coefficients $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{k}, \dots, \binom{n}{n}$ as they occur in the expansion of the polynomial $(x+y)^n$:

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \dots + \binom{n}{n}y^n = \sum_{k=0}^n \binom{n}{k}x^{n-k}y^k.$$

The first eleven rows of the Pascal triangle are shown below:

					1																																							
						1			1																																			
							1			2			1																															
								1		3			3			1																												
									1		4			6			4			1																								
										1		5			10			10			5			1																				
											1		6			15			20			15			6			1																
												1		7			21			35			35			21			7			1												
													1		8			28			56			70			56			28			8			1								
														1		9			36			84			126			126			84			36			9			1				
															1		10			45			120			210			252			210			120			45			10			1

The coefficients $\binom{n}{k}$ in the expansion $(x+y)^n = \sum_{k=0}^n \binom{n}{k}x^{n-k}y^k$ determine the coefficients

$\binom{n+1}{k}$ in the expansion $(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k}x^{n+1-k}y^k$. Since

$$\sum_{k=0}^{n+1} \binom{n+1}{k}x^{n+1-k}y^k = (x+y)^{n+1} = (x+y)(x+y)^n = (x+y) \sum_{k=0}^n \binom{n}{k}x^{n-k}y^k \quad (4.1)$$

it follows

$$\sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k = x^{n+1} + y^{n+1} + \sum_{k=1}^n \left(\binom{n}{k} + \binom{n}{k-1} \right) x^k. \quad (4.2)$$

As a consequence,

$$\begin{aligned} \binom{n+1}{0} &= \binom{n}{0}, & \binom{n+1}{1} &= \binom{n}{0} + \binom{n}{1}, & \binom{n+1}{2} &= \binom{n}{1} + \binom{n}{2}, & \dots \\ \dots &, & \binom{n+1}{n} &= \binom{n}{n-1} + \binom{n}{n}, & \binom{n+1}{n+1} &= \binom{n}{n} \end{aligned}$$

If we define $\binom{n}{k} = 0$ if $k < 0$ or $k > n$ we can summarise the foregoing rules by

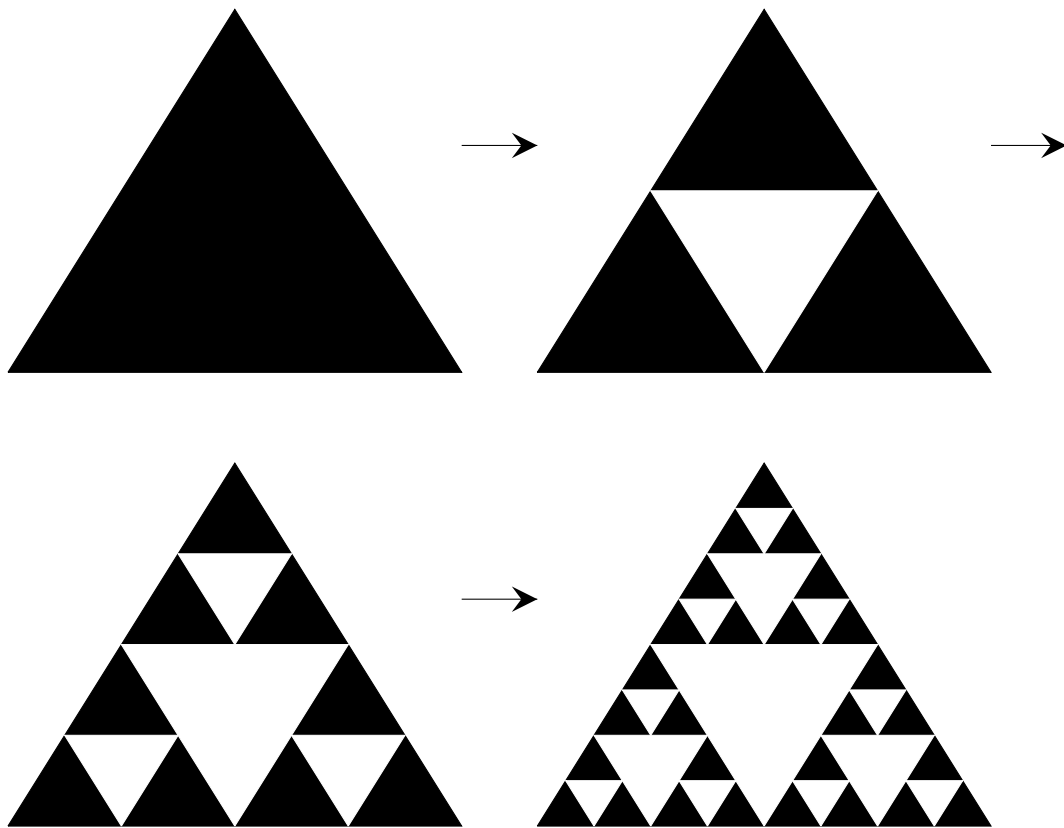
$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

In this way we obtain a scheme where for every row the coefficients can be obtained from the coefficients of the preceding row:

0	0	0	0	0	0	1	0	0	0	0	0
	0	0	0	0	1	1	0	0	0	0	0
0	0	0	0	1	2	1	0	0	0	0	0
	0	0	0	1	3	3	1	0	0	0	0
0	0	0	1	4	6	4	1	0	0	0	0
	0	0	1	5	10	10	5	1	0	0	0
0	0	1	6	15	20	15	6	1	0	0	0
	0	1	7	21	35	35	21	7	1	0	0
0	1	8	28	56	70	56	28	8	1	0	0
	1	9	36	84	126	126	84	36	9	1	0
1	10	45	120	210	252	210	120	45	10	1	0

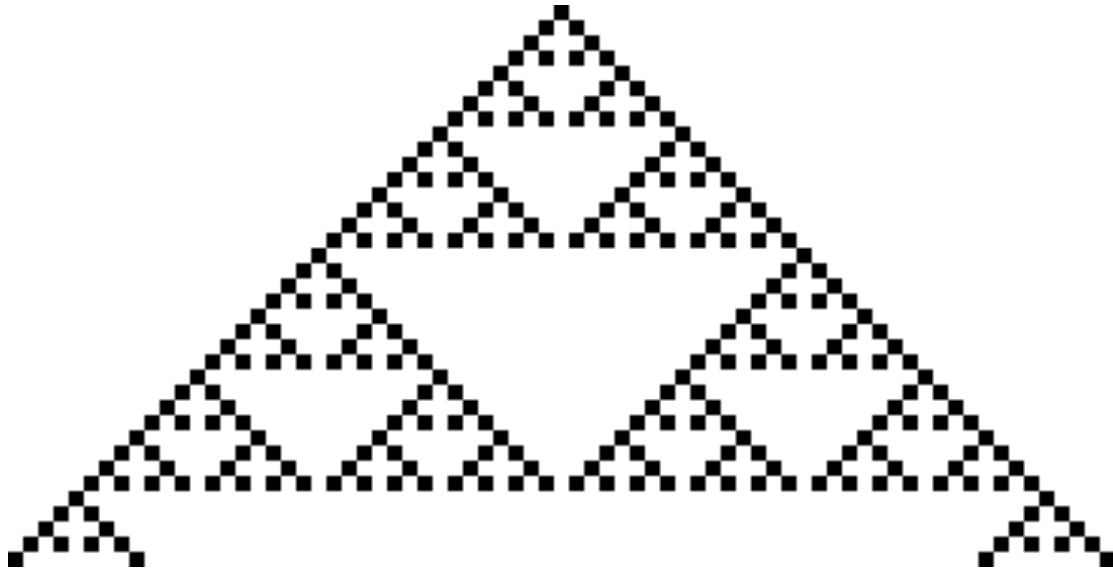
4.2 Sierpinski triangle

The Sierpinsky triangle, sometimes also called the Sierpinsky gasket or the Sierpinsky sieve, is created as follows. Start with a dark triangle and take out a triangle whose sizes are twice as small. Repeat the procedure with the remaining dark triangles. The construction is visualized in the figure below.

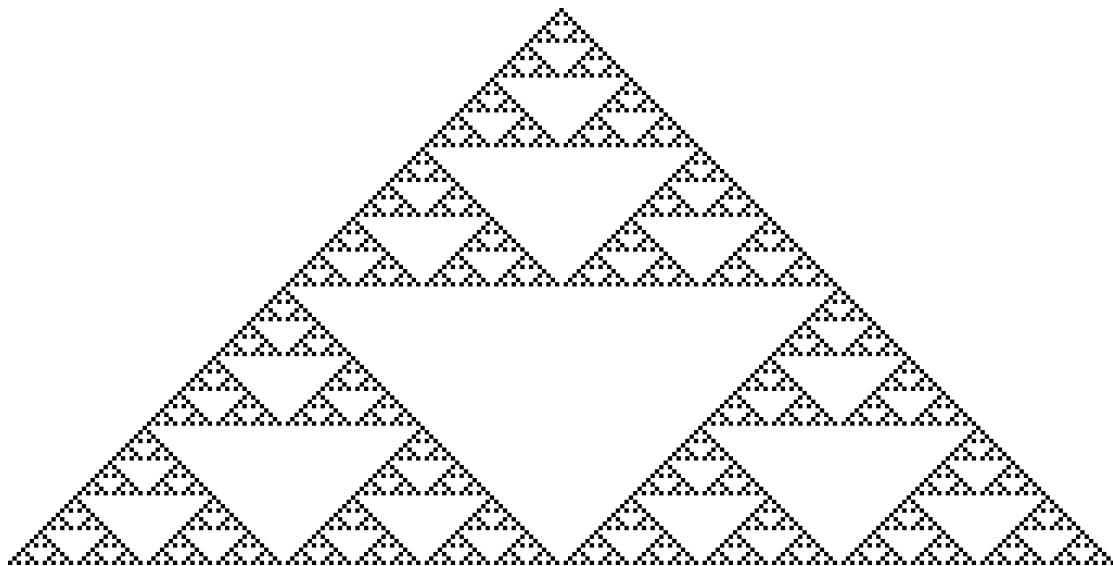


Repetition of the construction steps to infinity results in the Sierpinski triangle. There is a connection between the Sierpinski triangle and the scheme at the end of the previous section. To illustrate the connection we add a zero between every horizontal pair of numbers in that scheme. The additional zeros are coloured blue in the next scheme.

0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	0	2	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	3	0	3	0	1	0	0	0	0	0	0
0	0	0	0	0	0	1	0	4	0	6	0	4	0	1	0	0	0	0	0
0	0	0	0	0	1	0	5	0	10	0	10	0	5	0	1	0	0	0	0
0	0	0	0	1	0	6	0	15	0	20	0	15	0	6	0	1	0	0	0
0	0	0	1	0	7	0	21	0	35	0	35	0	21	0	7	0	1	0	0
0	0	1	0	8	0	28	0	56	0	70	0	56	0	28	0	8	0	1	0
0	1	0	9	0	36	0	84	0	126	0	126	0	84	0	36	0	9	0	1
1	0	10	0	45	0	120	0	210	0	252	0	210	0	120	0	45	0	10	0



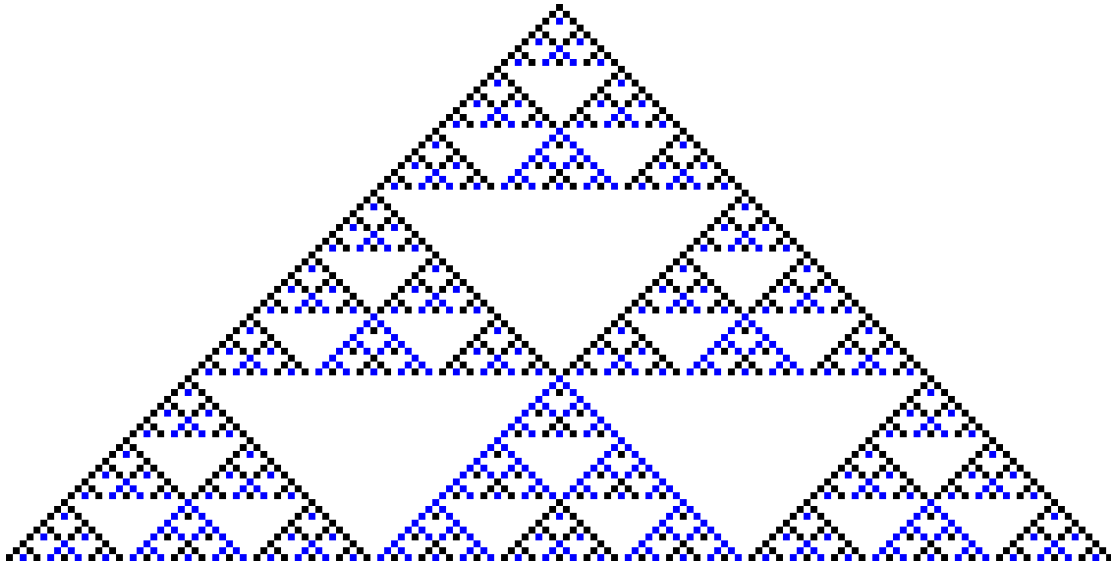
If we extend the number of rows to 128 the result is as shown below.



As for the Sierpinsky triangle there is self similarity present in the discrete Sierpinsky triangle. Extended to infinity both are a fractal.

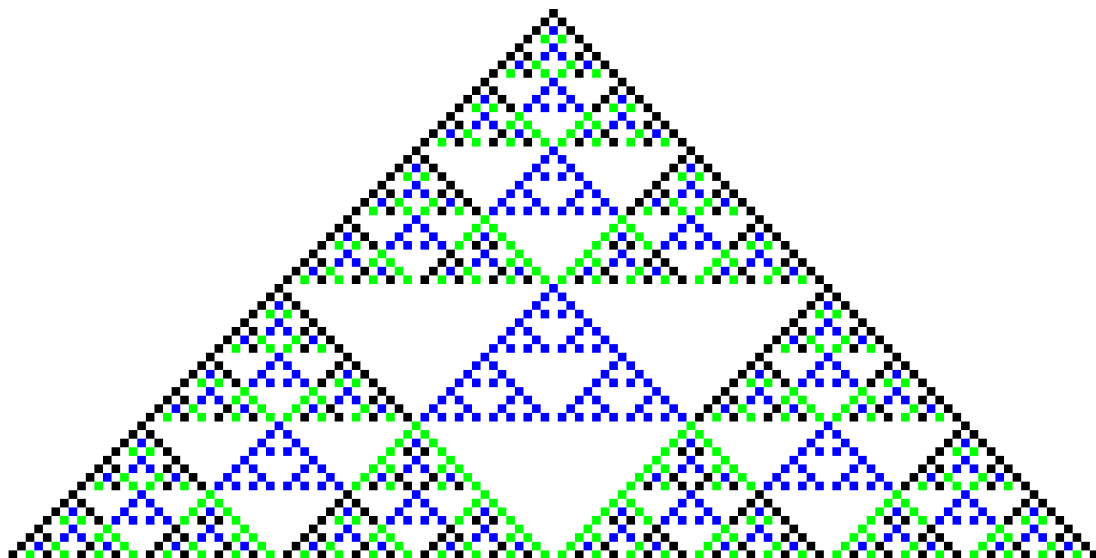
4.4 Pascal triangle modulo q

In this section we will take in the Pascal triangle the numbers modulo q , where q is an integer larger than 2. For $q = 3$ and 81 rows ($n \leq 80$) the result is

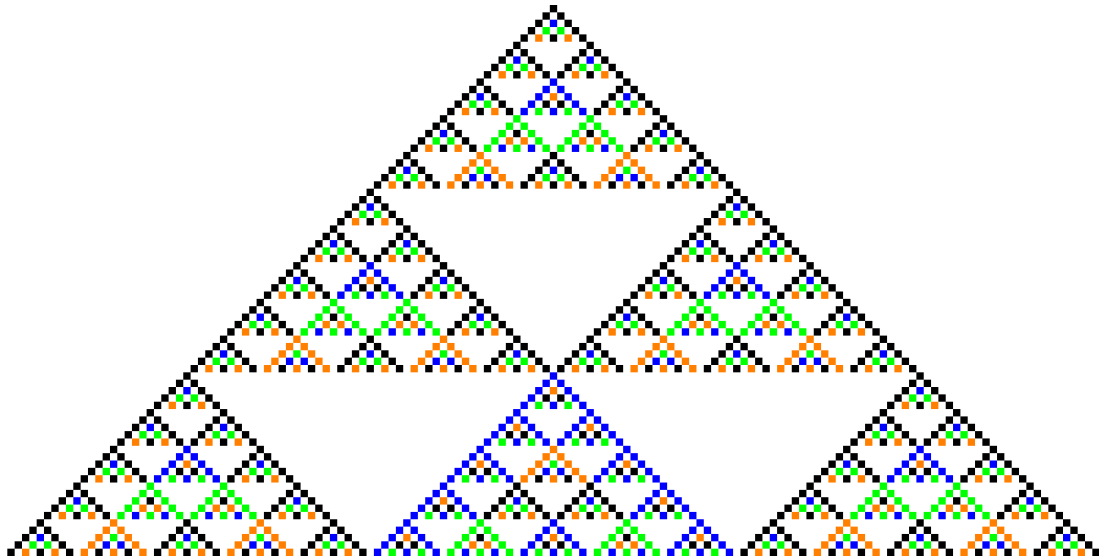


In the latter figure a black square is drawn if $q = 1 \pmod{3}$ and a blue square if $q = 2 \pmod{3}$.

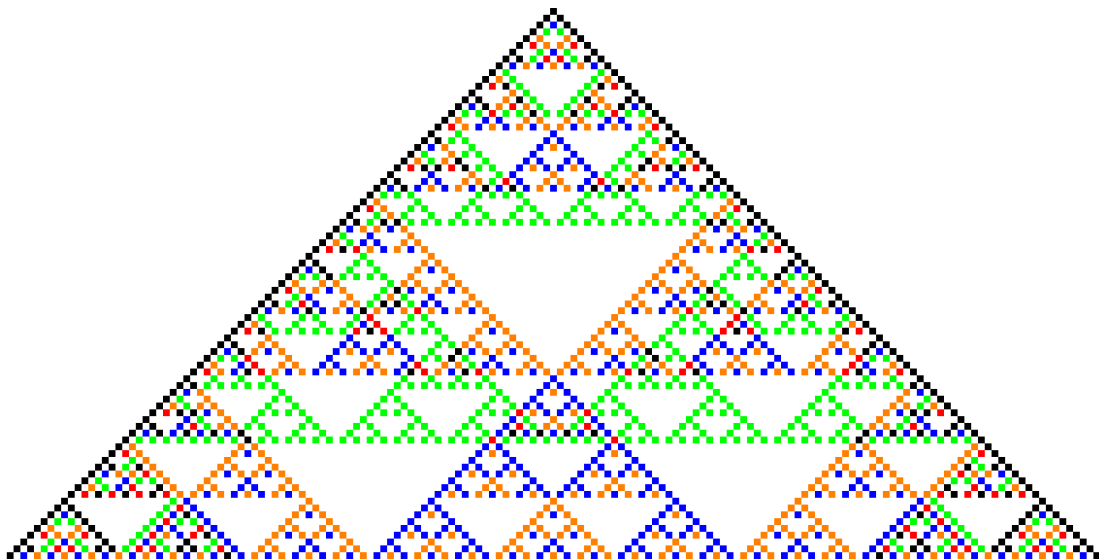
For $q = 4$ and $n \leq 63$ the result is



For $q = 5$ and $n \leq 74$ the result is

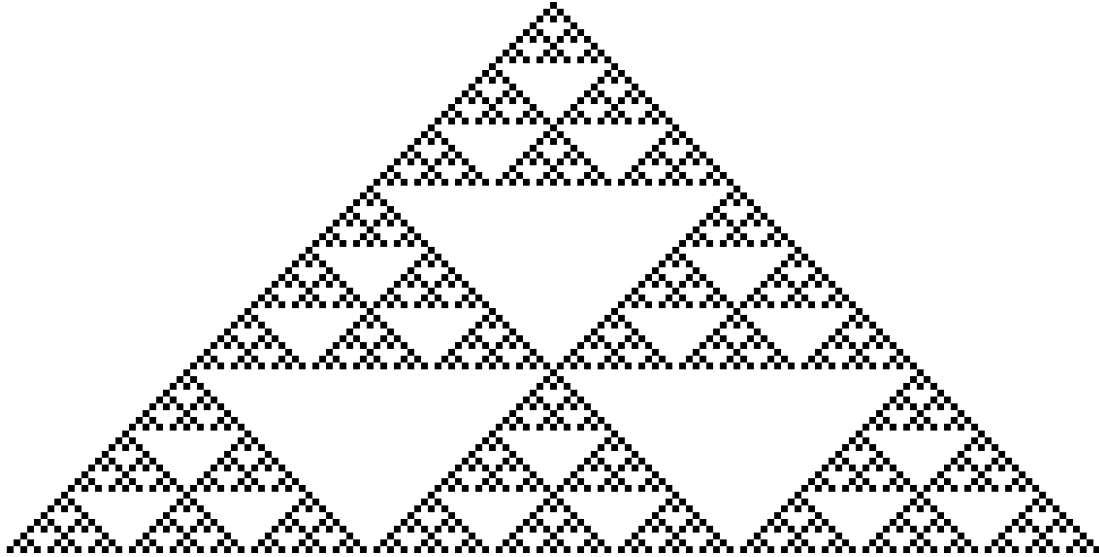


For $q = 6$ and $n \leq 80$ the result is

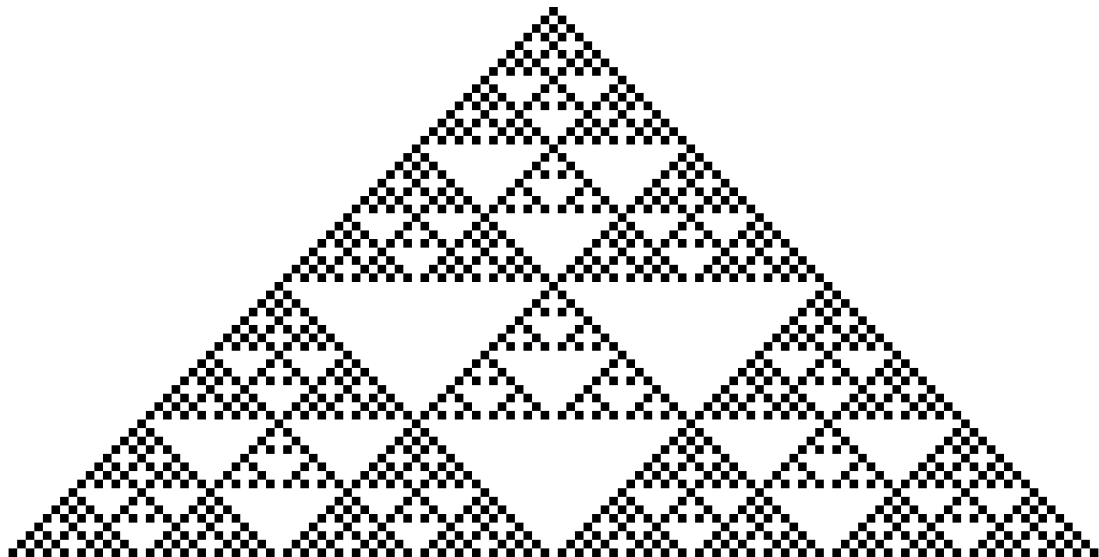


The triangles appear more regular if q is a prime. The regularity is even more apparent if we turn all the coloured squares into black squares. That is, a black square appears if a number is not divisible by q . For several q the resulting triangle is shown below.

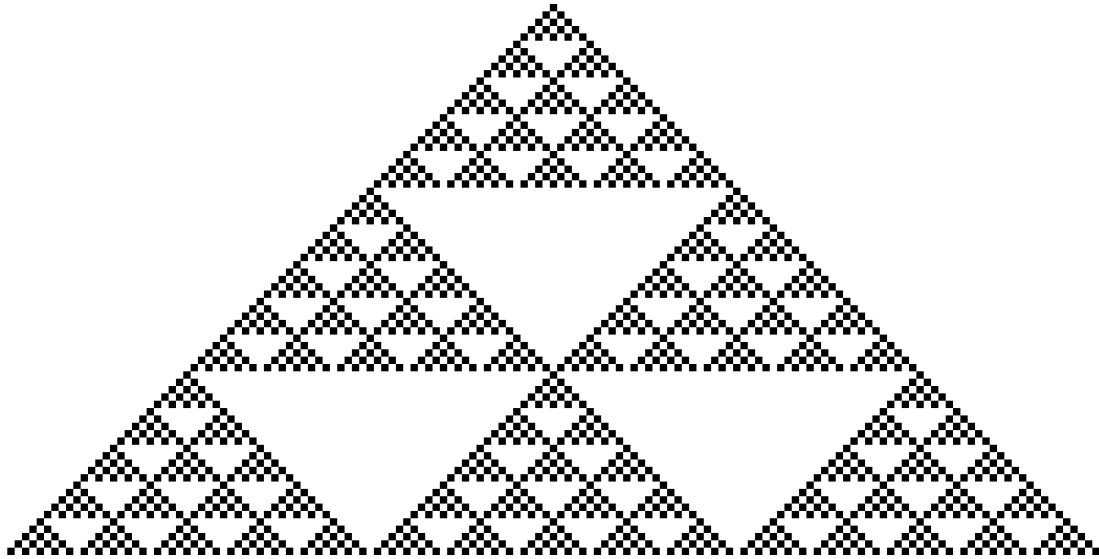
$$q = 3, n \leq 80$$



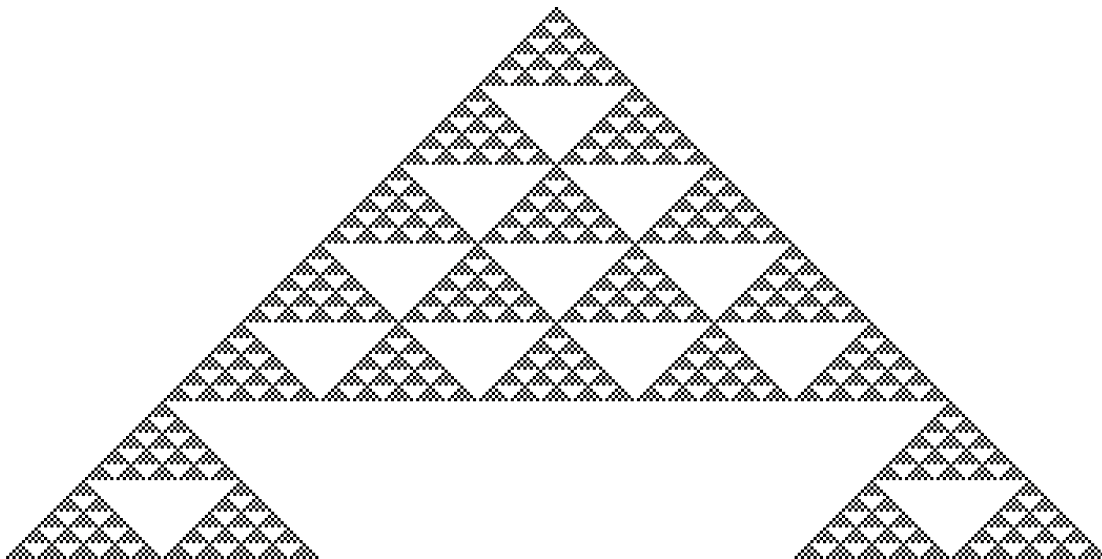
$$q = 4, n \leq 63$$



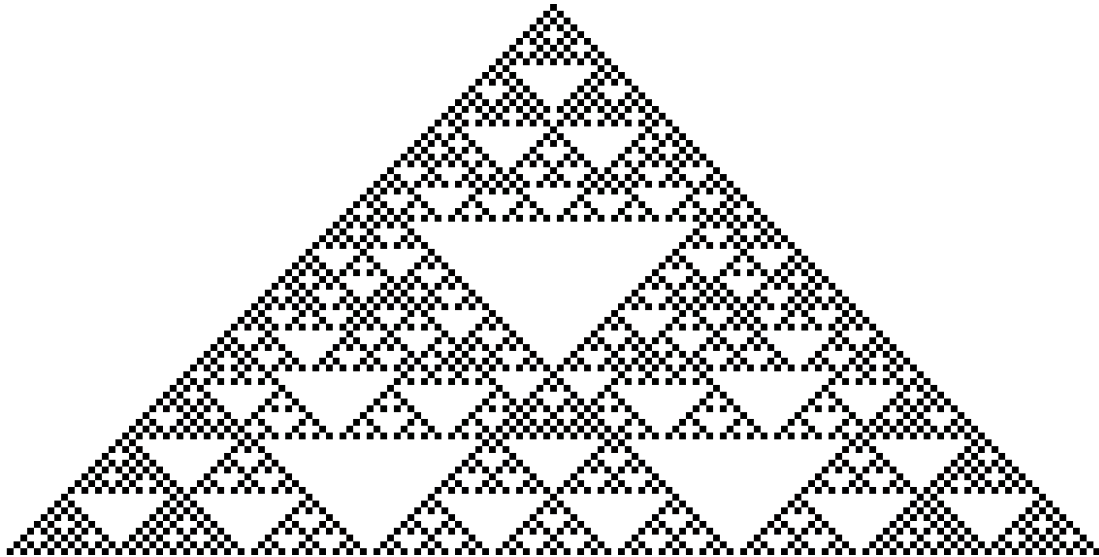
$$q = 5, n \leq 74$$



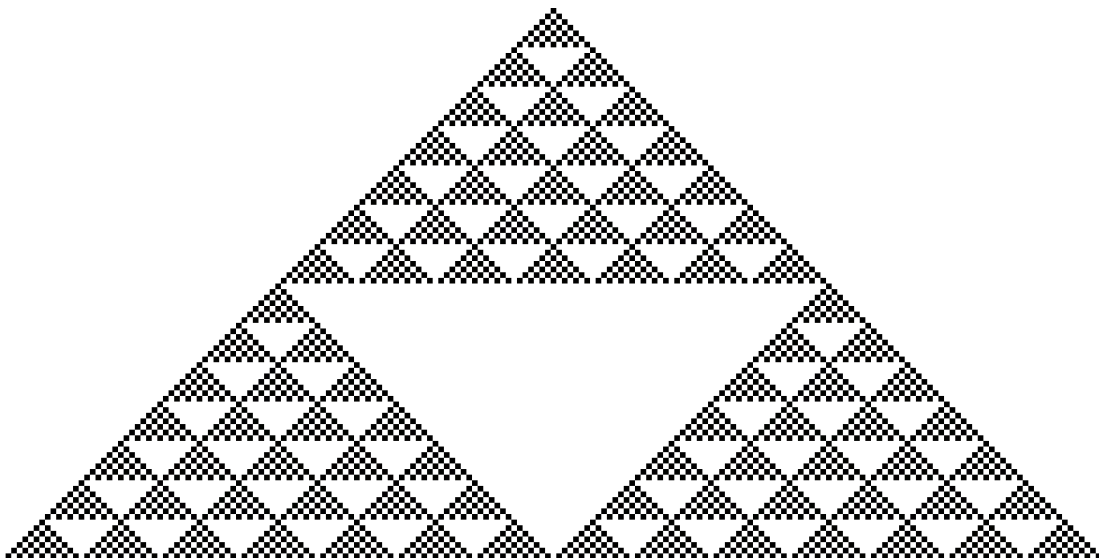
$$q = 5, n \leq 174$$



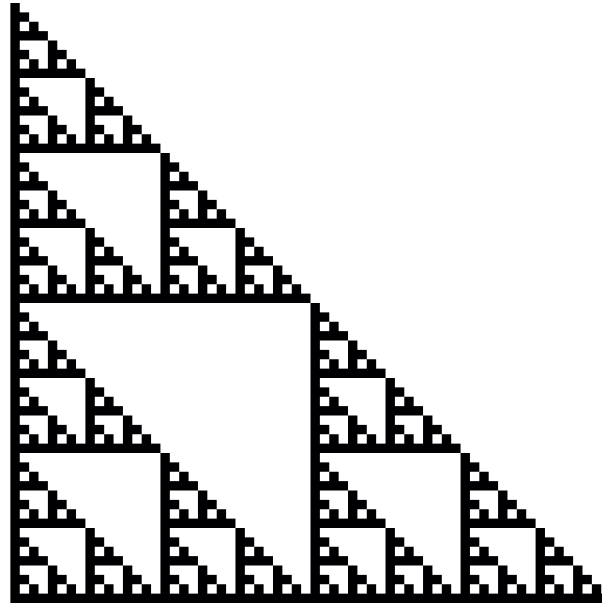
$$q = 6, n \leq 80$$



$$q = 7, n \leq 97$$



Obviously the patterns are more regular if q is a prime.



From the scheme with zeros and ones we see that a row whose row number n is a power of 2, $n = 2^m$, has only a 1 at the start, a 1 at the end and only zeros in between. This implies that $(1 + x)^{2^m} \cong 1 + x^{2^m} \pmod 2$.

Instead of modulo 2 we can take the coefficients modulo q . If q is a prime p then each row number n that is a power of p has a 1 at the left ($k = 0$), a 1 at the right ($k = n$), and only zeros in between, as can be seen in the previous table. As a consequence

$$(1 + x)^{p^m} \cong 1 + x^{p^m} \pmod p \tag{4.3}$$

if p is a prime. It can be proven by induction as follows.

For $m = 1$ we have

$$(1 + x)^p = \sum_{k=0}^p \binom{p}{k} x^k = \sum_{k=0}^p \frac{p!}{(p-k)!k!} x^k. \tag{4.4}$$

For $1 \leq k \leq p-1$ the divisors $(p-k)!$ and $k!$ do not divide a prime p . Hence, for $1 \leq k \leq p-1$ the binomial coefficients $\binom{p}{k}$ are a multiple of p . Only for $k = 0$ and $k = p$ the binomial coefficients are equal to 1. Therefore $(1 + x)^{p^m} \cong 1 + x^{p^m} \pmod p$ if p is a prime.

For $m + 1$ we have

$$(1 + x)^{p^{(m+1)}} = (1 + x)^{p^m \cdot p} = ((1 + x)^{p^m})^p. \tag{4.5}$$

Assuming the rule to be true for k it can be elaborated to

$$(1 + x)^{p^{(m+1)}} \cong (1 + x^{p^m})^p \cong (1 + x^p)^p \pmod p, \tag{4.6}$$

where $x' = x^{(p^m)}$. As for $(1+x)^p$ the coefficients of $(1+x')^p$ are 1 for x^0 and x^p , and a multiple of p otherwise. Therefore

$$(1+x')^p \cong 1+x'^p \pmod{p}. \quad (4.7)$$

Hence,

$$(1+x)^{(p^{(m+1)})} \cong 1+x'^p \cong 1+(x^{(p^m)})^p \cong 1+x^{(p^{(m+1)})} \pmod{p} \quad \square. \quad (4.8)$$

4.6 Gould's sequence

As we saw before the Sierpinski triangle and the skewed Sierpinski triangle are generated by rule 90 and rule 60 respectively. Both rules contain the transition

1 0 0
1

For this transition a periodicity in the successive configurations can not occur since the most right 1 in a configuration is shifted one cell to the right in the next configuration: ...100....
 \rightarrow ...X10..., where X is either a 0 or a 1. A cycle therefore is impossible.

In the first row, $n = 0$, of the discrete Sierpinski triangle there is a single black cell. On the second row, $n = 1$, there are 2 black cells. On the third row, $n = 2$, there are 2 black cells. On the fourth row, $n = 3$, there are 4 black cells. On the next row, $n = 4$, there are 2 black cells. In fact a triangle (width three cells and pointing downwards) of white cells starts at this row. Left and right from this white triangle there is a triangular configuration identical to the triangular configuration in the first four rows. Therefore the number of black cells in the rows $n = 4$ through $n = 7$ is twice the number of black cells in the rows $n = 0$ through $n = 3$ respectively. Similarly, the number of black cells in the rows $n = 8$ through $n = 15$ is twice the number of black cells in the rows $n = 0$ through $n = 7$ respectively. On the basis of the pattern one can generate a sequence with the number of black cells in each row. Starting with a 1 for the single black cell in row $n = 0$ and doubling it we obtain 2 for row $n = 1$. One step further, doubling the $\{1, 2\}$ we obtain $\{2, 4\}$ for the number of black cells in row 3 and 4. Hence for the first four rows we have $\{1, 2, 2, 4\}$. Doubling it we obtain $\{2, 4, 4, 8\}$ for the number of black cells in row $n = 4$ through row $n = 7$. Extending the sequence $\{1, 2, 2, 4, 2, 4, 4, 8\}$ for row $n = 0$ through row $n = 7$ with its double values, we obtain $\{1, 2, 2, 4, 2, 4, 4, 8, 2, 4, 4, 8, 4, 8, 8, 16\}$ for row $n = 0$ through row $n = 15$. In a scheme:

1
 1 2
 1,2 2,4
 1,2,2,4 2,4,4,8
 1,2,2,4,2,4,4,8 2,4,4,8,4,8,8,16
 and so on.

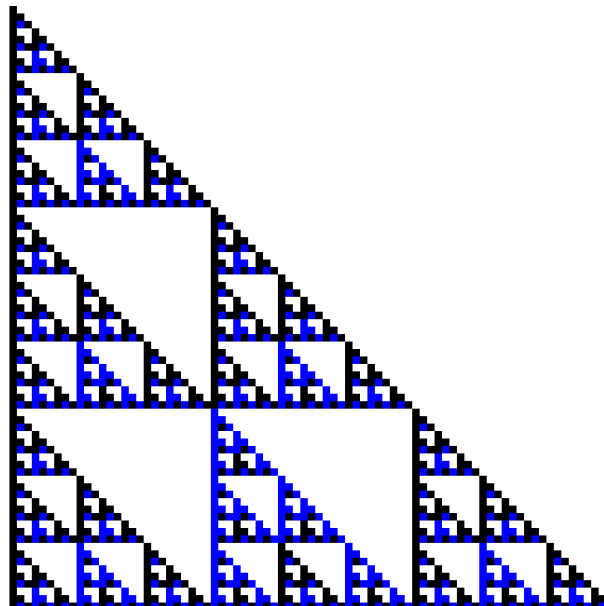
In the end it leads to the sequence 1, 2, 2, 4, 2, 4, 4, 8, 2, 4, 4, 8, 4, 8, 8, 16, 2, 4, 4, 8, 4, 8, 8, 16, 4, 8, 8, 16, 8, 16, 16, 32, ...

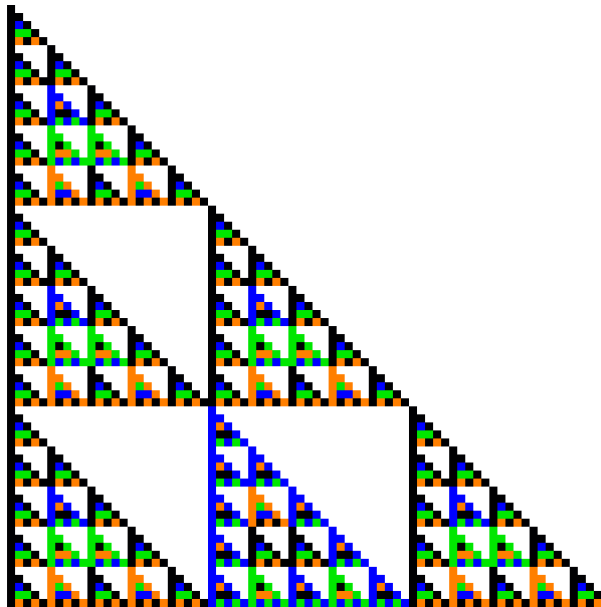
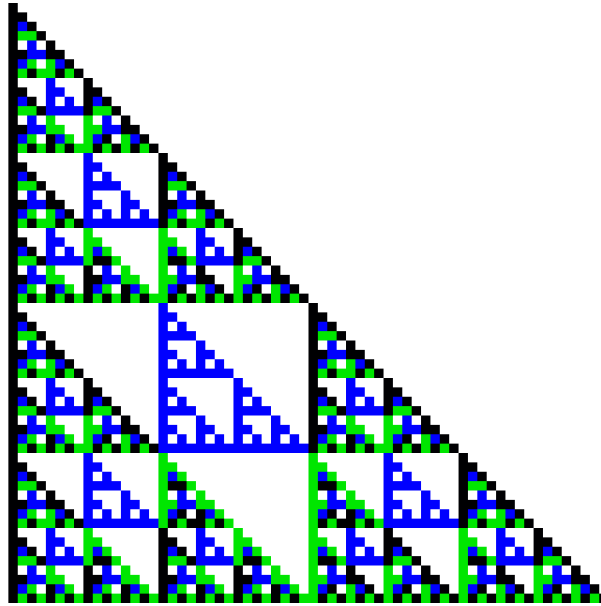
It is sequence A001316 in the OEIS [3]. The sequence is known as Gould's sequence.

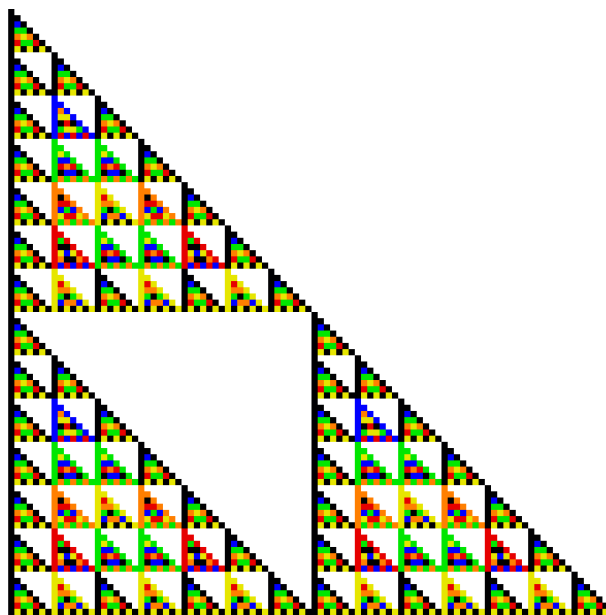
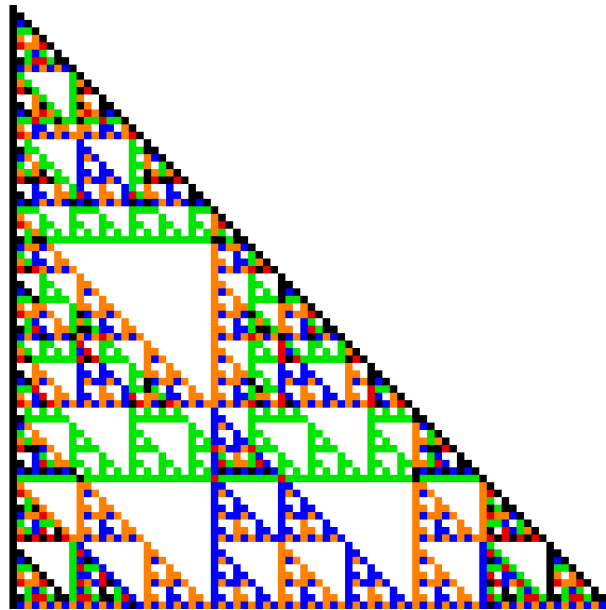
For a row n with $2^k \leq n < 2^{k+1}$ the number of black cells is twice the number of black cells in row $n - 2^k$, while the binary representation of n has one 1 more than the binary representation of $n - 2^k$. So, if $b(n)$ is the number of ones in the binary representation of n , then the number of black cells in row n is equal to $2^{b(n)}$.

4.7 Skewed Pascal triangle modulo q

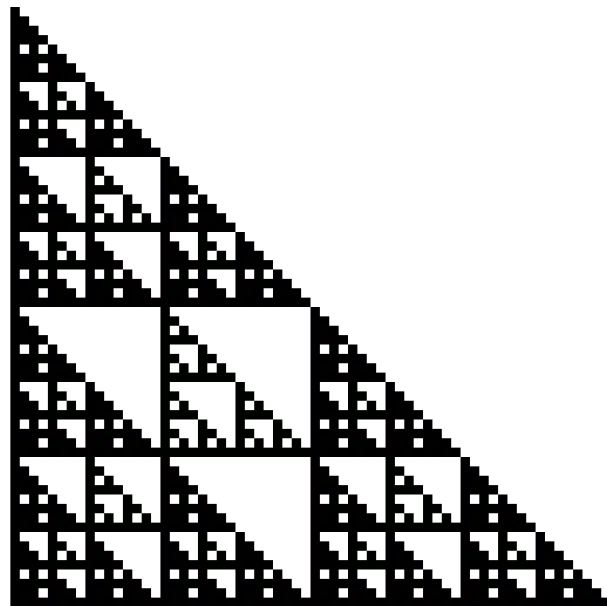
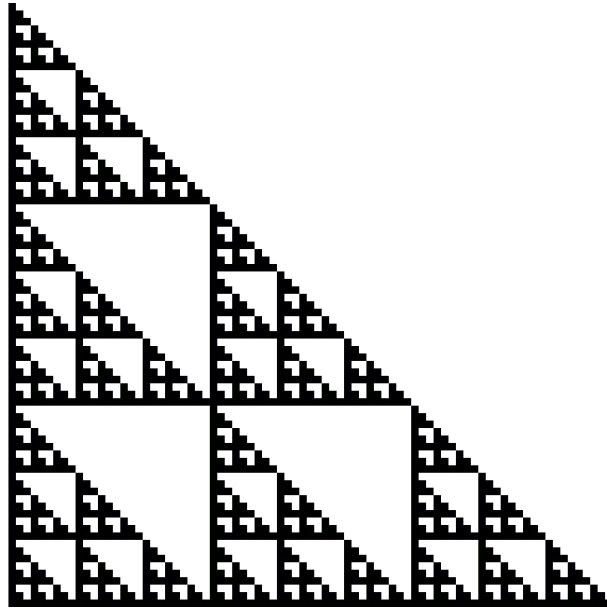
If we consider the binomial coefficients modulo 2, then a black square in a (skewed) Sierpinski triangle means the binomial coefficient is odd and a white square means the binomial coefficient is divisible by 2. If we take the binomial coefficients modulo q where $q=3, 4, 5, 6$ and 7, then we obtain the following figures:

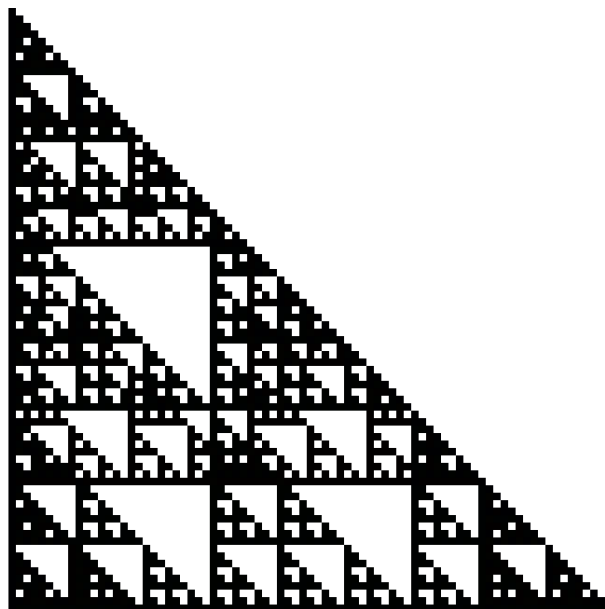
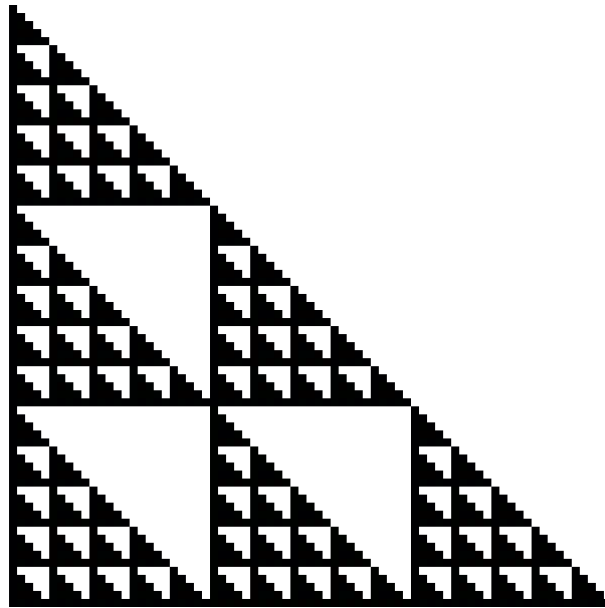


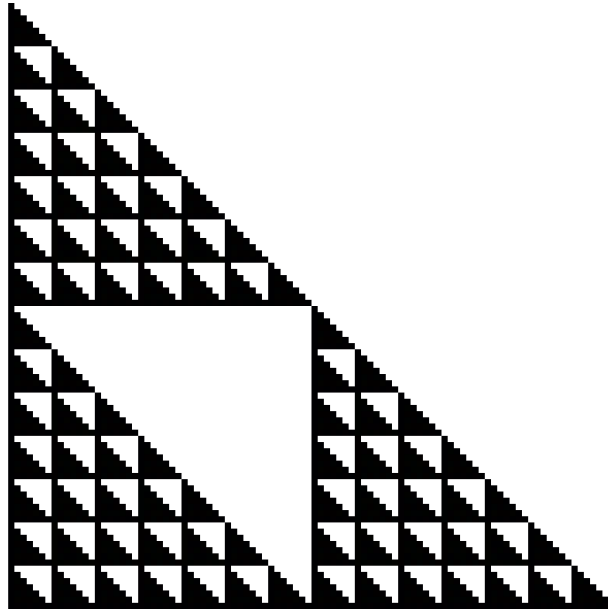




The patterns are quite regular. They are more regular if q is a prime. The latter becomes more emphatically visible if we colour a square white if the binomial coefficient is divisible by q and black otherwise. For $q = 2$ the figure will be the same. For $q = 3, 4, 5, 6$ and 7 the figures become as shown below.







We see the figures are most regular if q is a prime.

4.8 Kummer's method

The pictures of the previous section graphically represent the divisibility of a binomial by an integer q . If a square is black the binomial is not divisible by q , if the square is white it is divisible by q .

If the part of row n between k_1 and k_2 is white, then the part between $k_1 + 1$ and k_2 is white in row $n + 1$. That is, if the binomial coefficients $\binom{n}{k_1}$ through $\binom{n}{k_2}$ are divisible by a prime q , then the binomial coefficients $\binom{n+1}{k_1+1}$ through $\binom{n+1}{k_2}$ are also divisible by a prime q .

If q is composite it suffices to check for the divisibility by each prime divisor p of q . A binomial is divisible by q if it is divisible by all prime divisors of q . Checking binomials for divisibility by a prime sounds easy. However, for increasing n and k binomials $\binom{n}{k}$ soon become extremely large. Fortunately there is an alternative method to determine if a binomial is divisible by a prime number p . The method is based on Kummer's theorem [5]:

If p is a prime and r carries occur in the addition of $n - k$ and k in base p , then p^r does divide the binomial $\binom{n}{k}$ while p^{r+1} does not divide the binomial $\binom{n}{k}$.

A proof is given in appendix A. Here we confine to some examples.

Example 1: divisibility of $\binom{9}{4}$ by primes 2, 3, 5, ... or a power of them.

For the divisibility of $\binom{9}{4}$ by a power of 2 we write $9 - 4 = 5$ and 4 both in base 2 and count the carries in the addition:

$$\begin{array}{r} \text{carries} \quad 1 \ 0 \ 0 \\ 5 = \quad \quad 1 \ 0 \ 1_2 \\ 4 = \quad \quad 1 \ 0 \ 0_2 \\ \hline 1 \ 0 \ 0 \ 1_2 \end{array} +$$

Since there is one carry, $\binom{9}{4}$ is divisible by 2^1 but not by 2^2 .

For the divisibility of $\binom{9}{4}$ by a power of 3 we write $9 - 4 = 5$ and 4 both in base 3 and count the carries in the addition:

$$\begin{array}{r} \text{carries} \quad 1 \ 1 \\ 5 = \quad \quad 1 \ 2_3 \\ 4 = \quad \quad 1 \ 1_3 \\ \hline 1 \ 0 \ 0_3 \end{array} +$$

Since there are two carries, $\binom{9}{4}$ is divisible by 3^2 but not by 3^3 .

For the divisibility of $\binom{9}{4}$ by a power of 5 we write $9 - 4 = 5$ and 4 both in base 5 and count the carries in the addition:

$$\begin{array}{r} \text{carries} \quad 0 \ 0 \\ 5 = \quad \quad 1 \ 0_5 \\ 4 = \quad \quad 0 \ 4_5 \\ \hline 1 \ 4_5 \end{array} +$$

Since there are no carries, $\binom{9}{4}$ is not divisible by 5.

Now we know that $\binom{9}{4} = 126$ is divisible by 2 and by 3^2 . Since the product is smaller than 126 there must be another factor. There is no need to check the divisibility of $\binom{9}{4}$ by primes larger than 9 since it would not lead to carries. The only factor left is the prime 7 or a power of it. Indeed $2 \cdot 3^2 \cdot 7 = 126$. To show that the factor 7 also follows from the carries, we write $9 - 4 = 5$ and 4 both in base 7 and count the carries in the addition:
Since there is one carry, $\binom{9}{4}$ is divisible by 7^1 .

$$\begin{array}{r}
 \text{carries} \quad 1 \\
 5 = \quad 5_7 \\
 4 = \quad 4_7 \\
 \hline
 12_7 \quad +
 \end{array}$$

In summary, $\binom{9}{4}$ is only divisible by the primes 2, 3 and 7, by the prime power $3^2 = 9$ and by all combinations of them: $2 \cdot 3 = 6$, $2 \cdot 7 = 14$, $2 \cdot 3^2 = 18$, $3 \cdot 7 = 21$, $2 \cdot 3 \cdot 7 = 42$, $3^2 \cdot 7 = 63$, $2 \cdot 3^2 \cdot 7 = 126$.

Example 2: divisibility of $\binom{152}{19}$ by a power of 7.

To this end we write $152-19=133$ and 19 both in base 7 and count the carries in the addition:

$$\begin{array}{r}
 \text{carries} \quad 0 \ 1 \ 0 \\
 133 = \quad 2 \ 5 \ 0_7 \\
 19 = \quad 2 \ 5_7 \\
 \hline
 3 \ 0 \ 5_7 \quad +
 \end{array}$$

Since there is one carry, $\binom{152}{19}$ is divisible by 7^1 and not by 7^2 . We obtained the divisibility quite easily from small numbers 133 and 19 (written in base 7), while the binomial is large: $\binom{152}{19} = 724818552390382102384200$.

In summary, a binomial $\binom{n}{k}$ is divisible by a prime power $p_1^{m_1}$ if there are m_1 carries occur in the addition of $n - k$ and k in base p_1 . A binomial $\binom{n}{k}$ is divisible by a composite number $q = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3} \cdot \dots$ if it is divisible by $p_1^{m_1}$ and by $p_2^{m_2}$ and by $p_3^{m_3}$, etc., where each m_i is an integer larger than zero, and each p_i is a prime, $p_i \neq p_j$ if $i \neq j$. For the divisibility of a composite number one has to count carries in the successive bases p_1, p_2, p_3 , etc. As soon as it fails for a p_i one can conclude the binomial is not divisible by q .

In modern mathematics one often speaks of ' p -adic numbers' instead of 'numbers expanded in base p '. For the present purpose it does not matter. Nevertheless there is a subtle difference. A simple introduction to p -adic numbers is given in appendix B.

Chapter 5

Properties of Binomials

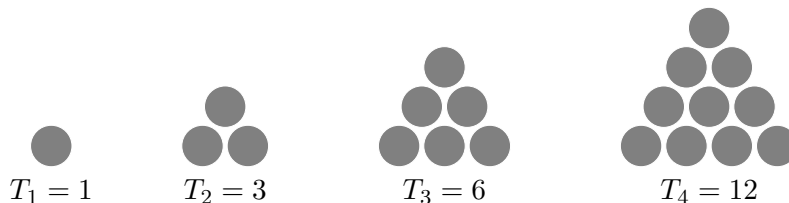
5.1 Series in Pascal's triangle

The diagonals of Pascal's triangle show a regular pattern. The edges contain only 1's: $\left\{\binom{n}{0} \mid n = 0, 1, 2, 3, \dots\right\} = \left\{\binom{n}{n} \mid n = 0, 1, 2, 3, \dots\right\} = \{1, 1, 1, 1, 1, \dots\}$. Moving inwards, the diagonals next to the edges contain the natural numbers: $\left\{\binom{n}{1} \mid n = 1, 2, 3, 4, \dots\right\} = \left\{\binom{n}{n-1} \mid n = 1, 2, 3, 4, \dots\right\} = \{1, 2, 3, 4, 5, \dots\}$. The next diagonals contain the triangular numbers: $\left\{\binom{n}{2} \mid n = 2, 3, 4, 5, \dots\right\} = \left\{\binom{n}{n-2} \mid n = 2, 3, 4, 5, \dots\right\} = \{1, 3, 6, 10, 15, \dots\}$. Next we have diagonals with tetrahedral numbers: $\left\{\binom{n}{3} \mid n = 3, 4, 5, 6, \dots\right\} = \left\{\binom{n}{n-3} \mid n = 3, 4, 5, 6, \dots\right\} = \{1, 4, 10, 20, 35, \dots\}$. next we have diagonals with pentatope numbers: $\left\{\binom{n}{4} \mid n = 4, 5, 6, 7, \dots\right\} = \left\{\binom{n}{n-4} \mid n = 4, 5, 6, 7, \dots\right\} = \{1, 5, 15, 35, 70, \dots\}$, and so on.

Explicit formulas for the triangular numbers are:

$$T_n = \sum_{k=1}^n k = 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} = \binom{n+1}{2}, \quad (5.1)$$

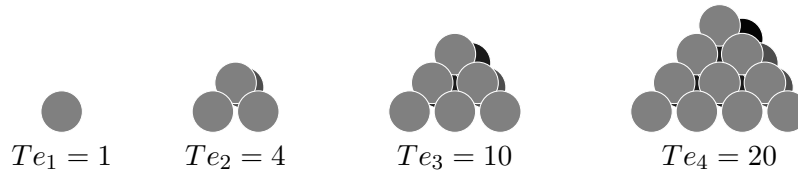
A triangular number T_n counts the number of elements arranged in an equilateral triangle with side n :



Explicit formulas for the tetrahedral numbers are:

$$Te_n = \sum_{k=1}^n T_k = \sum_{k=1}^n \frac{k(k+1)}{2} = \frac{n(n+1)(n+2)}{6}, \quad (5.2)$$

A tetrahedral number Te_n counts the number of elements arranged in an equilateral triangular pyramid with side n :



The bottom layer of the pyramid with side 4 is an equilateral triangle with side 4 and thus with $T_4 = 10$ elements. The next layer is an equilateral triangle with side 3 and thus with $T_3 = 6$ elements. The next layer is an equilateral triangle with side 2 and thus with $T_2 = 3$ elements. The top layer is just a single element, $T_1 = 1$. As a consequence the number of elements in the pyramid with side 4 is $Te_4 = T_1 + T_2 + T_3 + T_4 = 1 + 3 + 6 + 10 = 20$. In general, $Te_n = \sum_{k=1}^n T_k$.

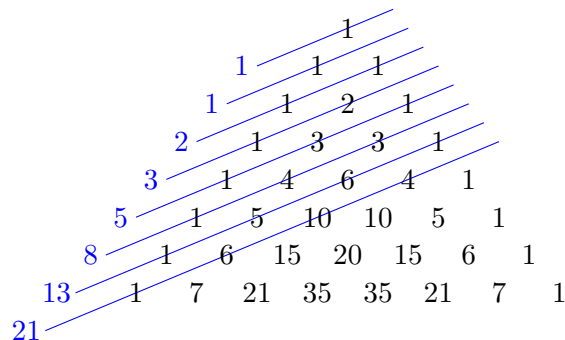
We saw that the sum of 1's results in natural numbers: $n = \sum_{k=1}^n 1$. That the sum of nat-

ural numbers results in triangular numbers: $T_n = \sum_{k=1}^n k$. That the sum of triangular numbers

results in tetrahedral numbers: $Te_n = \sum_{k=1}^n T_k$. One can continue the summations: the sum of

tetrahedral numbers results in pentatope numbers: $P_n = \sum_{k=1}^n Te_k$, and so on.

Instead of diagonals one can also consider 'shallow' diagonals, see blue lines in the figure below.



The k -th number of the Stern series will be denoted as $a(k)$: $a(1) = 1$, $a(2) = 1$, $a(3) = 2$, etc. The elements of the Stern series are given by:

$$a(1) = 1, \quad a(2k) = a(k), \quad a(2k + 1) = a(k) + a(k + 1). \quad (5.6)$$

In order to show some properties we consider sub-series $s(m)$ starting with $a(2^{m-1})$ and ending with $a(2^m)$:

$$s(1) = (a(1), a(2)) = (1, 1)$$

$$s(2) = (a(2), a(3), a(4)) = (1, 2, 1)$$

$$s(3) = (a(4), a(5), a(6), a(7), a(8)) = (1, 3, 2, 3, 1)$$

and so on.

To create, for instance, $s(4)$ from $s(3)$ is just a matter of stretching $s(3)$ by writing gaps between its elements, $(1, \ , 3, \ , 2, \ , 3, \ , 1)$, and filling each gap with the sum of its two adjacent neighbours: $(1, 4, 3, 5, 2, 5, 3, 4, 1)$. Each sub-series is a palindrome: $a(2^{m-1} + i) = a(2^m - i)$ for $i = 0, 1, 2, \dots, 2^{m-1}$. The sum of the element of sub-series $s(m)$ is equal to $3^{m-1} + 1$.

5.3 Divisors of products of binomials

In this section we will consider the set $B(n)$ of prime divisors of the product of binomials with n in the upper index

$$B(n) = \{p \mid p \text{ a prime and } p \mid \prod_{k=1}^{n-1} \binom{n}{k}\} \quad (5.7)$$

and the set C of primes smaller than or equal to n

$$C(n) = \{p \mid p \leq n \text{ and } p \text{ a prime}\}. \quad (5.8)$$

We give an example.

$$B(6) = \{p \mid p \text{ a prime and } p \mid \prod_{k=1}^5 \binom{6}{k}\} = \{2, 3, 5\}. \quad (5.9)$$

At the same time

$$C(6) = \{p \mid p \leq 6 \text{ and } p \text{ a prime}\} = \{2, 3, 5\}. \quad (5.10)$$

That is, the set $B(6)$ equals the set $C(6)$: $B(6) = C(6)$.

As another example

$$B(9) = \{p \mid p \text{ a prime and } p \mid \prod_{k=1}^8 \binom{9}{k}\} = \{2, 3, 7\}. \quad (5.11)$$

At the same time

$$C(9) = \{p \mid p \leq 9 \text{ and } p \text{ a prime}\} = \{2, 3, 5, 7\}. \quad (5.12)$$

That is, the set $B(9)$ equals the set $C(9)$ except for the number 5: $B(9) + \{5\} = C(9)$.

From inspection we find the following property for every n either $B(n) = C(n)$ or $B(n) + \{d(n+1)\} = C(n)$, where $d(n+1)$ is the largest prime divisor of $n+1$.

The numbers n for which $B(n) = C(n)$ are $\{1, 2, 4, 6, 10, 11, 12, 16, 18, 22, 23, 28, 29, 30, 35, 36, 39, 40, 42, 44, 46, 47, 52, 55, 58, 59, 60, 62, 66, 69, 70, 71, 72, 78, 79, 82, 83, 88, 89, 95, 96, 100, \dots\}$.

The series is known as A056077 in the the OEIS [3].

If we add 1 to the elements of this series, we get $\{2, 3, 5, 7, 11, 12, 13, 17, 19, 23, 24, 29, 30, 31, 36, 37, 40, 41, 43, 45, 47, 48, 53, 56, 59, 60, 61, 63, 67, 70, 71, 72, 73, 79, 80, 83, 84, 89, 90, 96, 97, 101, \dots\}$.

For the elements in the latter series holds that they are either a prime or they are mutinous. A number is mutinous if $n/p^k > p$, where p^k is the largest prime power dividing n . For example, 12 is mutinous since $12/4 > 2$, while 18 is not mutinous since $18/9 \not> 3$. The series with mutinous numbers is known as A027854 in the OEIS.

5.4 A multiplicity conjecture

In the Pascal triangle entries equal to 1 occur two times in a row and therefore infinitely many times in total. Entries larger than 1 occur just a finite number of times. We give some examples:

$$2 \text{ occurs just once: } \binom{2}{1} = 2,$$

$$3 \text{ occurs twice: } \binom{3}{1} = \binom{3}{2} = 3,$$

$$4 \text{ occurs twice: } \binom{4}{1} = \binom{4}{3} = 4,$$

$$5 \text{ occurs twice: } \binom{5}{1} = \binom{5}{4} = 5,$$

$$6 \text{ occurs three times: } \binom{6}{1} = \binom{6}{5} = \binom{4}{2} = 6,$$

$$7 \text{ occurs twice: } \binom{7}{1} = \binom{7}{6} = 7,$$

$$8 \text{ occurs twice: } \binom{8}{1} = \binom{8}{7} = 8,$$

$$9 \text{ occurs twice: } \binom{9}{1} = \binom{9}{8} = 9,$$

$$10 \text{ occurs four times: } \binom{10}{1} = \binom{10}{9} = \binom{5}{2} = \binom{5}{3} = 10.$$

For $n = 1, 2, 3, \dots$ the number of times n appears in Pascal's triangle, the multiplicity, is $\infty, 1, 2, 2, 2, 3, 2, 2, 2, 4, 2, 2, 2, 2, 4, 2, 2, 2, 2, 3, 4, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 4, 4, 2, 2, 2, 2, 2, 2, 2, 2, 4, 4, 2, 2, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 2, 2, 6, 2, 2, 2, 2, 2, 4, 2, 2, \dots$

It is sequence A003015 in the OEIS [3].

It turns out there are infinitely many entries with multiplicity 2. There are infinitely many entries with multiplicity 3. There are infinitely many entries with multiplicity 4. It is not known if there exist an entry with multiplicity 5. There are infinitely many entries with multiplicity 6. The smallest example is

$$120 = \binom{120}{1} = \binom{120}{119} = \binom{16}{2} = \binom{16}{14} = \binom{10}{3} = \binom{10}{7}.$$

It is not known if there exist an entry with multiplicity 7. There is one entry known with multiplicity 8:

$$3003 = \binom{3003}{1} = \binom{3003}{3002} = \binom{78}{2} = \binom{78}{76} = \binom{15}{5} = \binom{15}{10} = \binom{14}{6} = \binom{14}{8}.$$

It is not known if there is another entry with multiplicity 8 in Pascal's triangle. Despite advanced computer searches it is not known if there exists entries with multiplicity larger than 8. Singmaster, who proved there are infinitely many entries with multiplicity at least 6, has conjectured that 10 is an upperbound for the multiplicity of entries in Pascal's triangle [7].

5.5 Binomials and π

We consider a random walk in one dimension, the x -axis. The walk starts at $x = 0$. Each step is determined by coin tossing. For instance, **head**: one unit to the left, $\Delta x = -1$, and **tail**: one unit to the right, $\Delta x = 1$. The expectation of x after the first step is $E_1(x) = \frac{1}{2} \cdot -1 + \frac{1}{2} \cdot 1 = 0$. After two steps we are at $x = -2$ (1 way), at $x = 0$ (2 ways) or at $x = 2$ (1 way). The expectation of x after two steps is $E_2(x) = \frac{1}{4} \cdot -2 + \frac{2}{4} \cdot 0 + \frac{1}{4} \cdot 2 = 0$. After three steps we are at $x = -3$ (1 way), at $x = -1$ (3 ways), at $x = 1$ (3 ways) or at $x = 3$ (1 way). The expectation of x after three steps is $E_3(x) = \frac{1}{8} \cdot -3 + \frac{3}{8} \cdot -1 + \frac{3}{8} \cdot 1 + \frac{1}{8} \cdot 3 = 0$. After four steps it is $E_4(x) = 0$, etc. Since there are $\binom{n}{k}$ ways to arrive at $x = n - 2k$ and since there are 2^n ways to take n steps, the expectation of x after n steps is

$$E_n(x) = \sum_{k=0}^n \frac{1}{2^n} (n - 2k) \binom{n}{k} = \frac{n}{2^n} \sum_{k=0}^n \binom{n}{k} - \frac{2}{2^n} \sum_{k=0}^n k \binom{n}{k}. \quad (5.13)$$

The sum of all the ways to choose n times out of two possibilities must be equal to 2^n :

$$\sum_{k=0}^n \binom{n}{k} = 2^n. \quad (5.14)$$

Since

$$k \binom{n}{k} = \frac{n(n-1)!}{(n-1-k-1)!(k-1)!} = n \binom{n-1}{k-1}, \quad (5.15)$$

there holds

$$\sum_{k=0}^n k \binom{n}{k} = \sum_{k=1}^n n \binom{n-1}{k-1} = n \sum_{j=0}^{n-1} \binom{n-1}{j} = n2^{n-1}. \quad (5.16)$$

For the expectation of x after n steps we obtain

$$E_n(x) = \frac{n}{2^n} \sum_{k=0}^n \binom{n}{k} - \frac{2}{2^n} \sum_{k=0}^n k \binom{n}{k} = n - \frac{2}{2^n} n2^{n-1} = n - n = 0. \quad (5.17)$$

That is, the mean \bar{x} is zero.

The identity (5.16) is often derived at another way. Take the derivative of

$$\sum_{k=0}^n \binom{n}{k} y^k = (1+y)^n \quad (5.18)$$

with respect to y ,

$$\sum_{k=0}^n k \binom{n}{k} y^{k-1} = n(1+y)^{n-1}, \quad (5.19)$$

and substitute $y = 1$:

$$\sum_{k=0}^n k \binom{n}{k} = n2^{n-1}. \quad (5.20)$$

If we take once more the derivative with respect to y ,

$$\sum_{k=0}^n k(k-1) \binom{n}{k} y^{k-2} = n(n-1)(1+y)^{n-2}, \quad (5.21)$$

and substitute $y = 1$, we get

$$\sum_{k=0}^n k(k-1) \binom{n}{k} = n(n-1)2^{n-2}. \quad (5.22)$$

Therefore

$$\sum_{k=0}^n k^2 \binom{n}{k} = n(n-1)2^{n-2} + \sum_{k=0}^n k \binom{n}{k} = n(n-1)2^{n-2} + n2^{n-1} = n(n+1)2^{n-2}. \quad (5.23)$$

The latter allows to calculate the expectation of x^2 :

$$E_n(x^2) = \sum_{k=0}^n \frac{1}{2^n} (n-2k)^2 \binom{n}{k} = \frac{n^2}{2^n} \sum_{k=0}^n \binom{n}{k} - \frac{4n}{2^n} \sum_{k=0}^n k \binom{n}{k} + \frac{4}{2^n} \sum_{k=0}^n k^2 \binom{n}{k}. \quad (5.24)$$

Hence,

$$E_n(x^2) = n^2 - \frac{4n}{2^n} \cdot n2^{n-1} + \frac{4}{2^n} \cdot n(n+1)2^{n-2} = n^2 - 2n^2 + n^2 - n = n. \quad (5.25)$$

Since the mean is zero, the *variance* is equal to $E_n(x^2) = n$. The standard deviation σ is the square root of the variance: $\sigma = \sqrt{n}$.

Now we will investigate the expected value of the absolute distance $r = |x|$. After the first step we are at $x = -1$ or $x = 1$. The expectation of r after the first step is $E_1(r) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = 1$. After two steps we are at $x = -2$ (1 way), at $x = 0$ (2 ways) or at $x = 2$ (1 way). The expectation of r after two steps is $E_2(r) = \frac{1}{4} \cdot 2 + \frac{2}{4} \cdot 0 + \frac{1}{4} \cdot 2 = 1$. After three steps we are at $x = -3$ (1 way), at $x = -1$ (3 ways), at $x = 1$ (3 ways) or at $x = 3$ (1 way). The expectation of r after three steps is $E_3(r) = \frac{1}{8} \cdot 3 + \frac{3}{8} \cdot 1 + \frac{3}{8} \cdot 1 + \frac{1}{8} \cdot 3 = \frac{3}{2}$. After four steps it is $E_4(r) = \frac{3}{2}$. Continuing the calculus we obtain $E_5(r) = E_6(r) = \frac{15}{8}$, $E_7(r) = E_8(r) = \frac{35}{16}$, etc.

There are 2^n ways to take n steps and there are $\binom{n}{k}$ ways to arrive at $x = n - 2k$. The expectation of the distance r after n steps therefore is

$$E_n(r) = \sum_{k=0}^n \frac{|n - 2k|}{2^n} \binom{n}{k}. \quad (5.26)$$

For an even number of steps, $n = 2m$, this is

$$E_{2m}(r) = \frac{2}{2^{2m}} \sum_{k=0}^{m-1} (2m - 2k) \binom{2m}{k} \quad (5.27)$$

and for an odd number of steps, $n = 2m - 1$, this is

$$E_{2m-1}(r) = \frac{2}{2^{2m-1}} \sum_{k=0}^{m-1} (2m - 1 - 2k) \binom{2m-1}{k}. \quad (5.28)$$

In appendix C it is shown that

$$\sum_{k=0}^{m-1} (2m - 2k) \binom{2m}{k} = m \binom{2m}{m} \quad (5.29)$$

and that

$$\sum_{k=0}^{m-1} (2m - 1 - 2k) \binom{2m-1}{k} = \frac{m}{2} \binom{2m}{m}. \quad (5.30)$$

Hence

$$E_{2m}(r) = E_{2m-1}(r) = \frac{2m}{2^{2m}} \binom{2m}{m}. \quad (5.31)$$

According to the *central limit theorem* the *binomial distribution* tends towards a *normal distribution*. For $\bar{x} = 0$ and $\sigma = \sqrt{n}$ the normal distribution is given by

$$p(x) = \frac{1}{\sqrt{2\pi n}} e^{-\frac{x^2}{2n}}. \quad (5.32)$$

We approximate $E_n(r)$ by means of this normal distribution

$$E_n(r) \approx \int_{-\infty}^{\infty} |x| p(x) dx = \frac{2}{\sqrt{2\pi n}} \int_0^{\infty} x e^{-\frac{x^2}{2n}}. \quad (5.33)$$

Partial integration yields

$$E_n(r) \approx \frac{-2n}{\sqrt{2\pi n}} e^{\frac{-x^2}{2n}} \Big|_0^\infty = \frac{\sqrt{2}\sqrt{n}}{\sqrt{\pi}}. \quad (5.34)$$

In the limit where n goes to infinity the equality becomes exact

$$\lim_{n \rightarrow \infty} \frac{E_n(r)^2}{n} = \frac{2}{\pi}. \quad (5.35)$$

Both for $n = 2m$ and $n = 2m - 1$ we obtain the following relation between π and binomials

$$\pi = \lim_{m \rightarrow \infty} \frac{16^m}{m \binom{2m}{m}^2}. \quad (5.36)$$

The latter result also follows from Stirlings approximation:

$$n! \approx \sqrt{2\pi n} \frac{n^n}{e^n}. \quad (5.37)$$

Asymptotically there holds

$$\lim_{n \rightarrow \infty} \frac{\sqrt{2\pi n} n^n}{n! e^n} = 1. \quad (5.38)$$

The latter relation for $n = 2m$ divided by the square of the latter relation for $n = m$ gives

$$\lim_{n \rightarrow \infty} \frac{2\sqrt{\pi m} (2m)^{2m}}{(2m)! e^{2m}} \frac{m! m! e^{2m}}{2\pi m \cdot m^{2m}} = 1. \quad (5.39)$$

The latter is reduced to

$$\lim_{n \rightarrow \infty} \frac{4^m}{\sqrt{\pi m}} \frac{m! m!}{(2m)!} = 1. \quad (5.40)$$

That is

$$\lim_{n \rightarrow \infty} \frac{4^m}{\sqrt{m} \binom{2m}{m}} = \sqrt{\pi}. \quad (5.41)$$

The square of the latter indeed equals the identity (5.36).

For another relation for π notice that equation (5.31) implies

$$\frac{E_n(r)^2}{n} = \frac{n-1}{n} \frac{E_{n-1}(r)^2}{n-1} \quad (5.42)$$

and

$$\frac{E_n(r)^2}{n} = \frac{n}{n-1} \frac{E_{n-1}(r)^2}{n-1} \quad (5.43)$$

for n is even and n is odd respectively. Starting with $E_1(r)^2/1 = 1$ we obtain the following sequence

$$\lim_{n \rightarrow \infty} \frac{E_n(r)^2}{n} = 1 \cdot \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{3}{4} \cdot \frac{5}{4} \cdot \frac{5}{6} \cdot \frac{7}{6} \cdot \frac{7}{8} \cdot \frac{9}{8} \cdot \dots \quad (5.44)$$

The comparison with (5.35) then leads to the identity

$$\frac{\pi}{2} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdot \frac{8}{7} \cdot \frac{8}{9} \cdot \dots \quad (5.45)$$

or shortly

$$\frac{\pi}{2} = \prod_{k=1}^{\infty} \frac{4k^2}{4k^2 - 1}. \quad (5.46)$$

The latter is the *Wallis product*. The English mathematician John Wallis published it in 1656. It is curious because it is an infinite product while other approximations for π usually are infinite sums.

Chapter 6

Divisibility aspects of binomials

6.1 Introduction

For p a prime the binomials $\binom{p}{1}, \binom{p}{2} \dots \binom{p}{p-1}$ all have p as a divisor.

For p^α a prime power the binomials $\binom{p^\alpha}{1}, \binom{p^\alpha}{2} \dots \binom{p^\alpha}{p^\alpha-1}$ all have p as a divisor.

For n composite and not a prime power the binomials $\binom{n}{1}, \binom{n}{2} \dots \binom{n}{p-1}$ do not have a common prime divisor. Motivated by group theoretical considerations Sharsian and Woodroffe have formulated the following condition [8]:

Condition 1: There exist primes p and q such that if $1 \leq k \leq n-1$, the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p and q .

They ask if condition 1 holds for all positive integers n . Casacuberta discusses sufficient conditions under which an integer n satisfies condition 1 [9].

For example, if $1 \leq k \leq 5$ the binomials $\binom{6}{k}$ have the value 6, 15, 20, 15 and 6 respectively. Each of these binomials is divisible by 2 or 3 or both. Moreover, each of these binomials also is divisible by 2 or 5 or both, and each of these binomials also is divisible by 3 or 5 or both. So, there are three prime pairs $\{p, q\}$ that satisfy condition 1: $\{2, 3\}$, $\{2, 5\}$ and $\{3, 5\}$.

If $n = p + 1$ with p a prime, it is easy to see condition 1 is satisfied. Since $\binom{p}{k}$ is, for $1 \leq k \leq p-1$, divisible by p and since $\binom{p+1}{k} = \binom{p}{k-1} + \binom{p}{k}$ the binomials $\binom{p+1}{k}$ are divisible by p for $2 \leq k \leq p-1$. The two remaining binomials are $\binom{p+1}{1} = p+1$

and $\binom{p+1}{p} = p+1$ are divisible by 2. As a consequence, the prime pair $\{2, p\}$ does satisfy condition 1 if $n = p+1$.

As further examples we consider some n , neither a prime nor a prime power, with a larger gap to the largest prime or largest prime power smaller than n .

$n = 22$: The largest prime or prime power smaller than 22 is 19. For $1 \leq k \leq 11$ the binomials $\binom{22}{k}$ have the values 22, 231, 1540, 7315, 26334, 74613, 170544, 319770, 497420, 646646 and 705432 respectively. We do not have to consider $12 \leq k \leq 21$ for reasons of symmetry: $\binom{n}{n-k} = \binom{n}{k}$. The seven prime pairs $\{2, 7\}$, $\{2, 11\}$, $\{3, 11\}$, $\{7, 11\}$, $\{11, 13\}$, $\{11, 17\}$ and $\{11, 19\}$ do satisfy condition 1.

$n = 36$: The largest prime or prime power smaller than 36 is 32. For $1 \leq k \leq 18$ the binomials $\binom{36}{k}$ have the values 36, 630, 7140, 58905, etc. The eleven prime pairs $\{2, 3\}$, $\{2, 5\}$, $\{2, 7\}$, $\{2, 11\}$, $\{2, 17\}$, $\{3, 5\}$, $\{3, 7\}$, $\{3, 11\}$, $\{3, 17\}$, $\{3, 29\}$ and $\{3, 31\}$ do satisfy condition 1.

$n = 96$: The largest prime or prime power smaller than 96 is 89. The binomials $\binom{96}{k}$ have the value 96, 4560, 142880, etc. The nineteen prime pairs $\{2, 3\}$, $\{2, 5\}$, $\{2, 11\}$, $\{2, 13\}$, $\{2, 17\}$, $\{2, 19\}$, $\{2, 23\}$, $\{2, 37\}$, $\{2, 41\}$, $\{2, 43\}$, $\{2, 47\}$, $\{2, 67\}$, $\{2, 71\}$, $\{2, 73\}$, $\{2, 79\}$, $\{2, 83\}$, $\{2, 89\}$, $\{3, 19\}$ and $\{3, 47\}$ do satisfy condition 1.

According to Lucas' theorem the following congruence relation holds for non-negative numbers n and k and a prime p [10, 11]:

Let p be a prime and let

$$\begin{aligned} n &= n_r p^r + n_{r-1} p^{r-1} + \cdots + n_1 p + n_0 \\ k &= k_r p^r + k_{r-1} p^{r-1} + \cdots + k_1 p + k_0 \end{aligned}$$

be base p expansions of two positive integers, where $0 \leq n_i < p$ and $0 \leq k_i < p$ for all i , and $n_r \neq 0$. Then

$$\binom{n}{k} \equiv \prod_{i=0}^r \binom{n_i}{k_i} \pmod{p}.$$

A binomial coefficient $\binom{n_i}{k_i}$ is zero if $n_i < k_i$. In particular, $\binom{n_i}{k_i} = 0$ if $n_i = 0$ and $k_i > 0$. If a number n has a prime power p^α as a divisor, then the base p expansion of n ends with α zero's. As a consequence, $\binom{n}{k} = 0$ if the base p expansion of k ends with less than α zero's. That is, $\binom{n}{k}$ is divisible by p if k is not a multiple of p^α . In other words, if $n \equiv 0 \pmod{p^\alpha}$

then $\binom{n}{k} \equiv 0 \pmod{p^\alpha}$ if $k \not\equiv 0 \pmod{p^\alpha}$. If $n \equiv 0 \pmod{p^\alpha}$ and $k \equiv 0 \pmod{p^\alpha}$ then $\binom{n}{k} \pmod{p^\alpha}$ should be evaluated, for instance with Kummer's theorem.

It follows by means of Lucas' theorem that if and only if n is a prime power the binomial coefficient $\binom{n}{k}$ is divisible by that prime if $1 \leq k \leq n-1$. It also follows that if n is a product of two different prime powers the binomial coefficient $\binom{n}{k}$ is divisible by at least one of the two primes if $1 \leq k \leq n-1$. For these two cases condition 1 is satisfied. The situation is not trivial if n has more than two different prime divisors. It is an open question whether or not condition 1 is satisfied for all such n . A numerical inspection up to $n = 10^{10}$ delivered no counterexample. The algorithm used for the numerical inspection is briefly described in the next section.

6.2 Algorithm for SW-pairs

A numerical inspection learns that condition 1 of Shareshian and Woodroffe is satisfied for all positive integers up to 10 billion. Explicitly, for every positive integer n with $1 \leq n \leq 10^{10}$, there exist primes p and q such that, for all integers k with $1 \leq k \leq n-1$, the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p or q . Hereafter, a pair of primes satisfying the condition 1 of Shareshian and Woodroffe is denoted as SW-pair.

To find a SW-pair $\{p, q\}$ for all n up to 10 billion, we used a 7-step approach. Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ be the prime factorisation of n and let $p_\mu^{\alpha_\mu}$ be the maximum of $\{p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_m^{\alpha_m}\}$, then the 7-step algorithm for a given number n is as follows:

1. If n has one or two different prime factors (that is, if $m \leq 2$) then condition 1 is satisfied and the algorithm terminates, else it moves to step 2.
2. The algorithm takes p_μ as p and the largest prime smaller than n as q . If $p_\mu^{\alpha_\mu} > n - q$ then $\{p, q\}$ is a SW-pair and the algorithm terminates, else it moves to step 3.
3. For odd n the algorithm takes p_μ as p and the largest prime smaller than $n/2$ as q . If n is odd and $p_\mu^{\alpha_\mu} > n - 2q$ then $\{p, q\}$ is a SW-pair and the algorithm terminates, else it moves to step 4.
4. For even n the algorithm successively takes prime divisors p_i of n (running in descending order from the largest prime power $p_\mu^{\alpha_\mu}$ to smaller prime powers) as p and the largest prime smaller than $n/2$ as q . If n is even and $p_i^{\alpha_i} > n - 2q$ and $\binom{n}{n/2}$ is divisible by p_i then $\{p, q\}$ is a SW-pair and the algorithm terminates. If no SW-pair is found the algorithm moves to step 5. Of course, if $p_i = 2$ it is redundant to check if $\binom{n}{n/2}$ is

divisible by 2 since $\binom{n}{n/2}$ is always even for even n .

5. The algorithm creates a set L of pairs of different prime divisors of n . That is, $L = \{\{p_i, p_j\}\}$ with $1 \leq i < m$ and $i < j \leq m$. The algorithm successively takes a pair from L and investigates if the pair is such that, for all integers k with $2 \leq k \leq \lfloor n/2 \rfloor$, the binomial coefficient $\binom{n}{k}$ is divisible by at least one element of the pair. If such a pair $\{p_i, p_j\}$ exists, then $\{p_i, p_j\}$ is a SW-pair and the algorithm terminates. If no SW-pair is found the algorithm moves to step 6. Of course, for a pair $\{p_i, p_j\}$ the binomials the $\binom{n}{k}$ have only to be evaluated if k is a multiple of $p_i^{\alpha_i} p_j^{\alpha_j}$.
6. For each prime divisor p_i of n the algorithm takes p_i as p and it successively takes the largest prime smaller than n/j as q for $j = 3, 4, 5, \dots, \lfloor n/2 \rfloor$. As soon as a pair $\{p_i, q\}$ satisfies condition 1 the algorithm terminates. If no SW-pair is found the algorithm moves to step 7. Of course, for a pair $\{p_i, q\}$ the binomials the $\binom{n}{k}$ have only to be evaluated if k is a multiple of $p_i^{\alpha_i}$.
7. For each prime divisor p_i of n the algorithm takes p_i as p and it successively takes for a prime smaller than n as q . As soon as such a pair $\{p, q\}$ satisfies the condition 1 the algorithm terminates. Also here, for a pair $\{p_i, q\}$ the binomials the $\binom{n}{k}$ have only to be evaluated if k is a multiple of $p_i^{\alpha_i}$.

Step 1 is to sieve the trivial ones. Step 2, 3, 4 and 6 are to a large extent based on the work of Casacuberta [9]. Step 5 is based on the observation that for many numbers there exists SW-pairs $\{p, q\}$ such that both p and q are prime divisors of n . Step 6 is just for the few occasions where the algorithm has not terminated within 5 steps. Step 6 is based on the idea that for p_i a prime divisor of n and q_j the largest prime smaller than n/j , there is a large chance there exist a SW-pair among all the pairs $\{p_i, q_j\}$. Step 7 is in case even step 6 does not deliver a pair satisfying the condition 1. In step 7 the algorithm checks with a brute force approach if there exists a SW-pair $\{p_i, q\}$ with p_i a prime divisor of n and q a prime smaller than n . A number n passing step 7 would be a counterexample to the believe that the condition 1 of Shareshian and Woodroffe is satisfied for all numbers. However, for all the numbers we investigated, that is, for $n \leq 10^{10}$, there were even no numbers who passed step 6.

To illuminate the algorithm we give some examples.

Example 6.2.1. $n = 9$:

Since n is a prime power, $n = 3^2$, it is for sure that $\binom{9}{k}$ is divisible by 3 if $1 \leq k \leq 8$.

Therefore the algorithm terminates after step 1. For this situation $\{3, q\}$ is a SW-pair for any prime q .

Example 6.2.2. $n = 12$:

Since n is a product of two prime powers, $n = 2^2 \cdot 3$, it is for sure that $\binom{12}{k}$ is divisible by at least one element of $\{2, 3\}$ if $1 \leq k \leq 11$. For this situation $\{2, 3\}$ is a SW-pair. Therefore the algorithm terminates after step 1.

Example 6.2.3. $n = 220$:

That is, n is a product of more than two prime powers: $n = 2^2 \cdot 5 \cdot 11$. The largest prime power is 11^1 , so $p = 11$. As a consequence $\binom{220}{k}$ is divisible by 11 for $k < 11$ and $k > 209$. The largest prime smaller than 220 is 211, so the algorithm takes $q = 211$. As a consequence, $\binom{220}{k}$ is divisible by 211 for $9 < k < 211$. Hence, if $1 \leq k \leq 219$ the binomial $\binom{220}{k}$ is either divisible by 11 or by 211. In short, since $11^1 > 220 - 211$, the condition $p^\alpha > n - q$ is satisfied. Therefore the algorithm terminates after step 2.

Example 6.2.4. $n = 4199$:

That is, n is a product of more than two prime powers: $n = 13 \cdot 17 \cdot 19$. The largest prime power is 19^1 , so $p = 19$. As a consequence $\binom{4199}{k}$ is not divisible by 19 for $k = 19$. The largest prime smaller than 4199 is 4177, so in step 2 the algorithm takes $q = 4177$. As a result, $\binom{4199}{k}$ is divisible by 4177 for $22 < k < 4177$. The binomial $\binom{4199}{19}$ is neither divisible by 19 nor divisible by 4177. In short, since $19 \not> 4199 - 4177$, the requirement $p^\alpha > n - q$ is not satisfied and the algorithm jumps to step 3. In step 3 also $p = 19$. In step 3 the algorithm takes $q = 2099$ since 2099 is the largest prime smaller than $4199/2$. The binomial $\binom{4199}{k}$ is divisible by 2099 for $k = 2, 3, \dots, 2098$ and $k = 2101, 2102, \dots, 4197$. Since 19 is a divisor of n , 19 is not a divisor of $(n - 1)/2 = 2099$. Similarly, since 19 is a divisor of n , 19 is not a divisor of $(n + 1)/2 = 2100$. As a consequence, $\binom{4199}{2099}$ and $\binom{4199}{2100}$ are divisible by 19. So, $(19, 2099)$ is a SW pair. In short, since $19 > 4199 - 2 \cdot 2099$, the requirement $p^\alpha > n - 2q$ is satisfied. Therefore the algorithm terminates after step 3.

Example 6.2.5. $n = 126$:

That is, $n = 2 \cdot 3^2 \cdot 7$. The largest prime power is 3^2 , so $p = 3$ in step 2. The largest prime smaller than 126 is 113. So, in step 2 the algorithm takes $q = 113$. Since $9 \not> 126 - 113$, the requirement $p^\alpha > n - q$ is not satisfied and the algorithm jumps to step 3. In step 3 the algorithm jumps to step 4 since $n = 126$ is even. In step 4 the largest prime smaller than $n/2$ is 61, so $q = 61$. The algorithm first takes 3^2 for the prime power p^α . Since $\binom{126}{63}$ is divisible by 3 and $9 > 126 - 2 \cdot 61$, the pair $\{3, 61\}$ is a SW-pair. Therefore the algorithm terminates after step 4.

Example 6.2.6. $n = 210$:

That is, $n = 2 \cdot 3 \cdot 5 \cdot 7$. The largest prime power is 7^1 , so $p = 7$ in step 2. The largest prime smaller than 210 is 199. So, $q = 199$. Since $7 \not\geq 210 - 199$, the requirement $p^\alpha > n - q$ is not satisfied and the algorithm jumps to step 3. In step 3 the algorithm jumps to step 4 since $n = 210$ is even. In step 4 the largest prime smaller than $n/2$ is 103, so $q = 103$. The algorithm first takes 7^1 for the prime power p^α . Although $7 > 210 - 2 \cdot 103$, the binomial $\binom{210}{105}$ happens to be not divisible by 7. Next the algorithm takes 5^1 as p^α . Since $5 > 210 - 2 \cdot 103$ and $\binom{210}{105}$ is divisible by 5, $\{5, 103\}$ is a SW pair. Therefore the algorithm terminates after step 4.

Example 6.2.7. $n = 3432$:

That is, $n = 2^3 \cdot 3 \cdot 11 \cdot 13$. The largest prime power is 13^1 , so $p = 13$. The largest prime smaller than 3432 is 3413. So, in step 2 the algorithm takes $q = 3413$. Since $13 \not\geq 3432 - 3413$, the requirement $p^\alpha > n - q$ is not satisfied and the algorithm jumps to step 3. In step 3 the algorithm jumps to step 4 since $n = 3432$ is even. In step 4 the largest prime smaller than $n/2$ is 1709, so $q = 1709$. The algorithm first takes 13^1 for the prime power p^α . Since $13 \not\geq 3432 - 2 \cdot 1709$ the requirement $p^\alpha > n - 2q$ is not satisfied and the algorithm jumps to step 5. In step 5 the algorithm creates the list $L = \{\{2, 3\}, \{2, 11\}, \{2, 13\}, \{3, 11\}, \{3, 13\}, \{11, 13\}\}$ of which $\{2, 3\}$, $\{2, 13\}$, $\{3, 13\}$ and $\{11, 13\}$ are SW-pairs. Hence, the algorithm terminates after step 5.

Example 6.2.8. $n = 14280$:

That is, $n = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17$. The largest prime power is 17^1 , so $p = 17$. The largest prime smaller than 14280 is 14251. So, in step 2 the algorithm takes $q = 14251$. Since $17 \not\geq 14280 - 14251$, the requirement $p^\alpha > n - q$ is not satisfied and the algorithm jumps to step 3. In step 3 the algorithm jumps to step 4 since $n = 14280$ is even. In step 4 the largest prime smaller than $n/2$ is 7129, so $q = 7129$. The algorithm first takes 17^1 for the prime power p^α . Since $17 \not\geq 14280 - 2 \cdot 7129$ the requirement $p^\alpha > n - 2q$ is not satisfied and the algorithm jumps to step 5. In step 5 the algorithm creates the list $L = \{\{2, 3\}, \{2, 5\}, \{2, 7\}, \{2, 17\}, \{3, 5\}, \{3, 7\}, \{3, 17\}, \{5, 7\}, \{5, 17\}, \{7, 17\}\}$. Since non of these pairs are SW-pairs, the algorithm jumps to step 6. The largest prime smaller than $14280/3$ is 4759. Starting with the largest prime power 17 of 14280 the algorithm soon finds $\{17, 4759\}$ as a SW-pair. Therefore the algorithm terminates after step 6.

The smallest number which is sieved by step 1 is 2.

The smallest number which is sieved by step 2 is $30 = 2 \cdot 3 \cdot 5$.

The smallest number which is sieved by step 3 is $4199 = 13 \cdot 17 \cdot 19$.

The smallest number which is sieved by step 4 is $126 = 2 \cdot 3^2 \cdot 7$.

The smallest number which is sieved by step 5 is $3432 = 2^3 \cdot 3 \cdot 11 \cdot 13$.

The smallest number which is sieved by step 6 is $14280 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17$.

The following table shows, for consecutive intervals of n , the frequencies of numbers sieved by the step 1, step 2, step 3, step 4 and step 5.

n in billions	# step 1	# step 2	# step 3	# step 4	# step 5	# step 6
$0 < n \leq 1$	257 266 332	742 713 994	2973	13 291	2139	1271
$1 < n \leq 2$	242 891 175	757 100 138	1397	5882	760	648
$2 < n \leq 3$	238 070 712	761 922 660	1050	4534	569	475
$3 < n \leq 4$	235 055 035	764 939 230	951	3932	410	442
$4 < n \leq 5$	232 872 031	767 122 789	815	3536	432	397
$5 < n \leq 6$	231 157 511	768 837 909	724	3144	355	357
$6 < n \leq 7$	229 758 393	770 237 352	702	2915	329	309
$7 < n \leq 8$	228 575 421	771 420 740	619	2665	284	271
$8 < n \leq 9$	227 546 521	772 449 721	624	2578	271	285
$9 < n \leq 10$	226 639 716	773 356 772	554	2404	299	255

Table 6.1: Frequencies of numbers sieved by the step 1 through step 6 for consecutive intervals of n .

For some individual numbers the search for a SW-pair $\{p, q\}$ can be conducted in a more efficient way than the algorithm described above. For example, for the number $n = 126 = 2 \cdot 3^2 \cdot 7$ it is quickly seen that $n - 1 = 5^3$. One could therefore try $q = 5$ as one prime of a SW-pair. Since $\binom{126}{k}$ is divisible by 5 if k is in the interval $[2, 124]$, one needs a prime divisor of 126 as a second prime. Either 2, 3 or 7 suffices. Hence, the pairs $\{2, 5\}$, $\{3, 5\}$ and $\{5, 7\}$ are SW-pairs. However, for increasing n the relative density of prime powers with power larger than 1 decreases. The larger n the more inefficient the check for nearby prime powers. For this reason it is omitted in the algorithm.

6.3 Number of SW-pairs

First we consider the case where n has two prime divisors: $n = p^\alpha q^\beta$. Then $\{p, q\}$ is a SW-pair. Other SW-pairs may also occur. For instance, if $n = 6$, next to the obvious pair $\{2, 3\}$ also the pairs $\{2, 5\}$ and $\{3, 5\}$ are SW-pairs. The next number with two prime divisors is $n = 10$. Here 2, 3, 5 and 7 are the primes smaller than n of which 2 and 5 are divisors of n . Of the six possible pairs only $\{2, 3\}$, $\{2, 5\}$, $\{3, 5\}$ and $\{5, 7\}$ turn out to be SW-pairs. In the next figure the number of SW-pairs is plotted against n for the case n has two prime divisors.

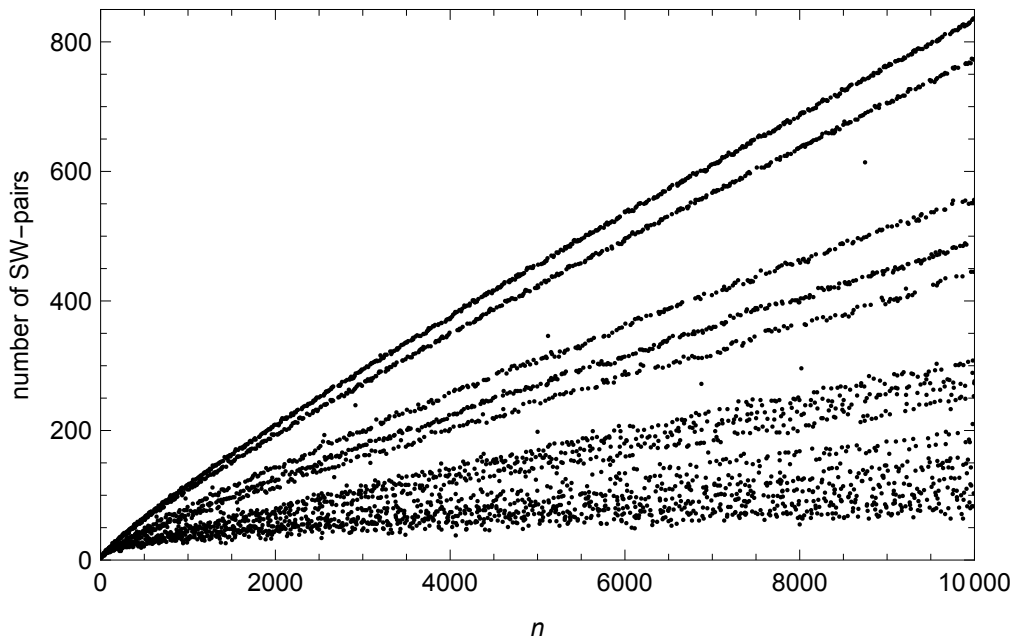


Figure 6.1: The number of SW-pairs for numbers n which have 2 prime divisors, plotted against n .

We recognise some curves for the numbers which have a relatively large number of SW-pairs. As an example we consider $n = 9998$. The number 9998 has 836 SW-pairs. The point $(9998, 836)$ is the most right dot on the upper curve. The value 9998 is two times a prime: $9998 = 2 \cdot 4999$. All 836 SW-pairs are of the type $\{q, 4999\}$ where the q runs over the 836 prime divisors of $\binom{9998}{4999}$. The largest prime below 9998 is 9973. Because of the gap between 9973 and 9998 there is no SW-pair of the type $\{2, p\}$ with p a prime smaller than 9998.

As a second example we consider $n = 9974$. The number 9974 has 834 SW-pairs. The point $(9974, 834)$ also is on the upper curve. Points on the upper curve are two times a prime or two times a prime power. The value 9974 is two times a prime: $9974 = 2 \cdot 4987^1$. There are 833 SW-pairs of the type $\{q, 4987\}$ where the q runs over the 833 prime divisors of $\binom{9974}{4987}$. There is an additional SW-pair, $\{2, 9973\}$, since 9973 is a prime just 1 smaller than 9974.

For numbers $n \leq 10000$ with two prime divisors the minimum number of SW-pairs is 3, which occurs for $n = 6$. The case of 4 SW-pairs occurs only for $n = 10$. The smallest number with 5 SW-pairs is $n = 12$. The smallest number with 6 SW-pairs is $n = 15$.

Next we consider the case where n has three prime divisors. The smallest number with three prime divisors is 30, which has 9 SW-pairs. The next number with three prime divisors is $n = 42$, which has 7 SW-pairs. For $n \leq 10000$ there is a local minimum for $n = 78$: 6 SW-pairs. In the next figure the number of SW-pairs is plotted against n for the case n has three prime divisors.

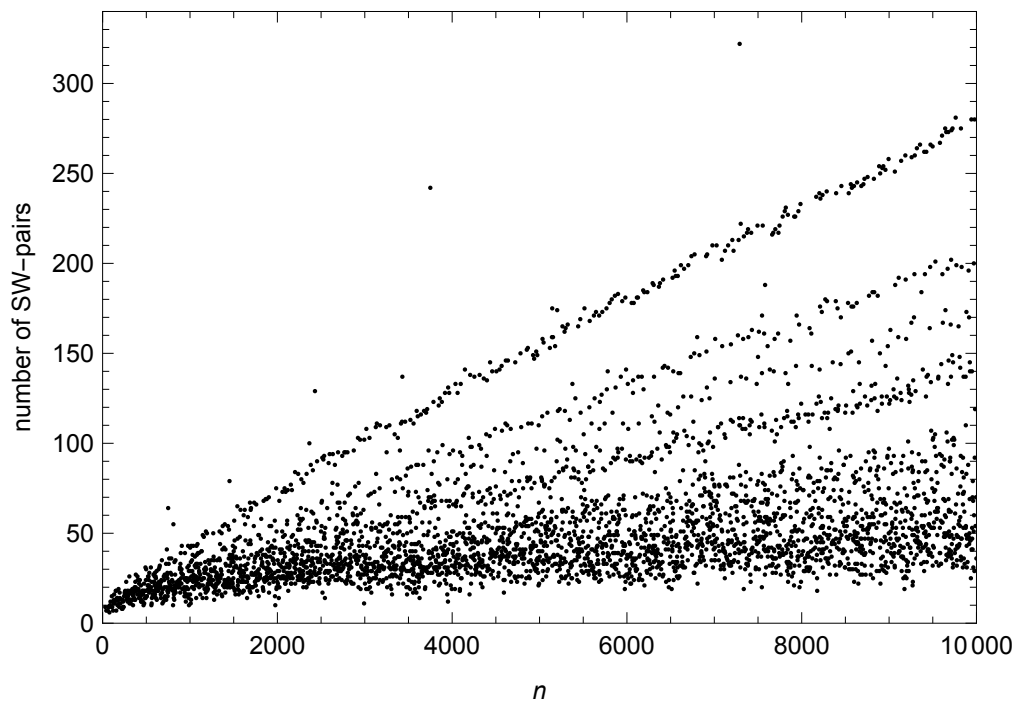


Figure 6.2: The number of SW-pairs for numbers n which have 3 prime divisors, plotted against n .

Local minima of small SW values slightly increase with n . For example, for the number 3952 there is a local minimum of 12 SW-pairs. As another example, for 9176 there is a local minimum of 19 SW-pairs. It seems as if the local minima increase with n .

Next we consider the case where n has four prime divisors. The smallest number with four prime divisors is 210, which has 9 SW-pairs. The next number with four prime divisors is $n = 330$, which has 12 SW-pairs. For $n \leq 10000$ there is a local minimum for $n = 3060$: 7 SW-pairs. In the next figure the number of SW-pairs is plotted against n for the case n has four prime divisors. For $n \leq 10000$ there are 5 numbers with 9 SW-pairs: 210, 2508, 3740, 3960, 5980.

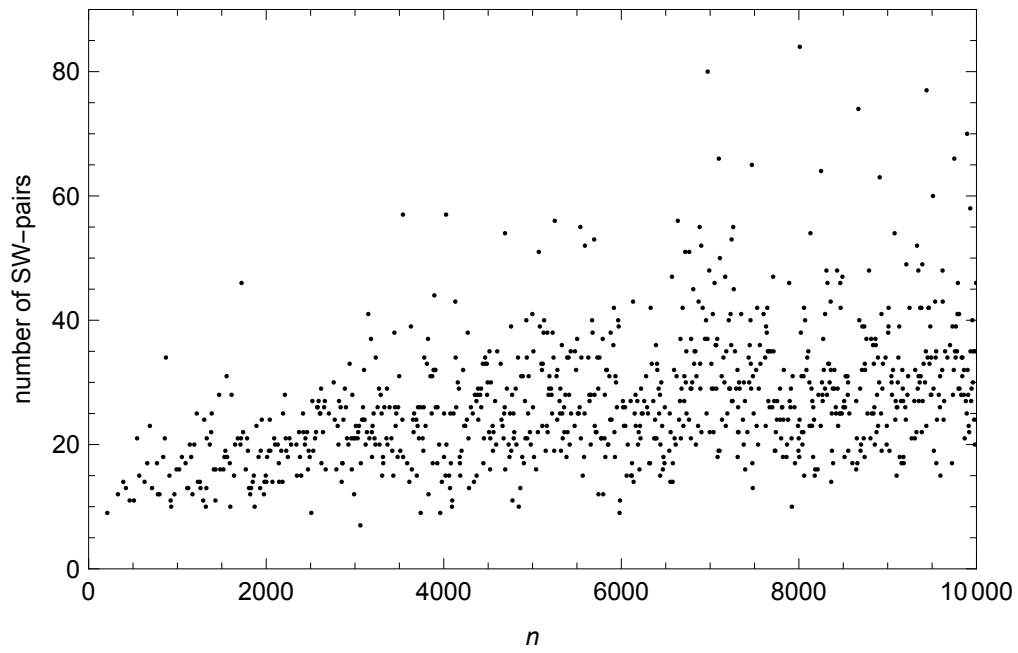


Figure 6.3: The number of SW-pairs for numbers n which have 4 prime divisors, plotted against n .

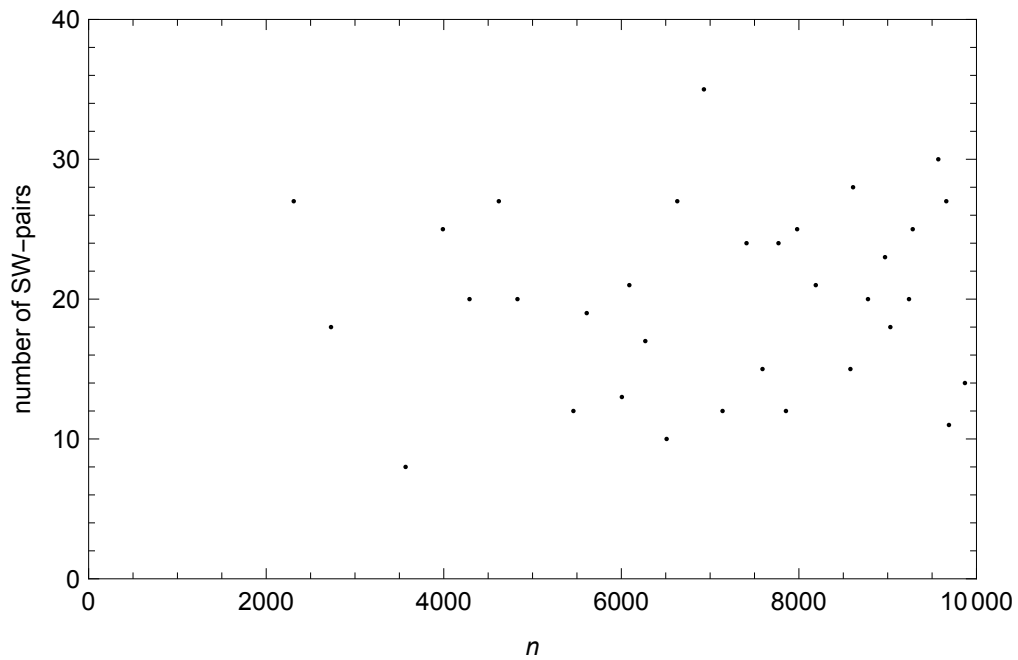
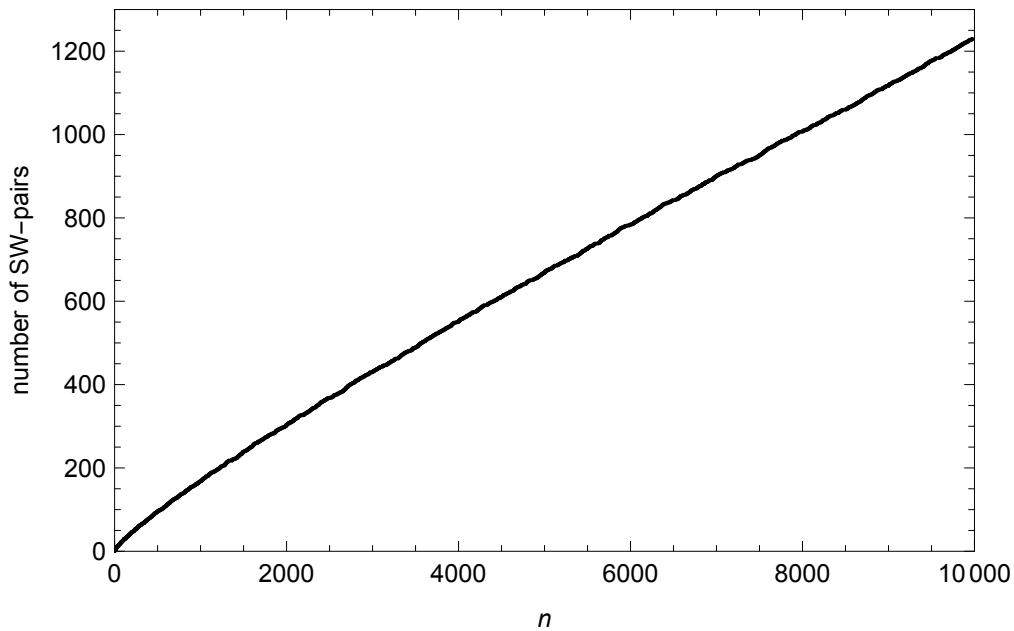


Figure 6.4: The number of SW-pairs for numbers n which have 5 prime divisors, plotted against n .

The situation where n has five prime divisors is shown in the previous figure. The smallest number with five prime divisors is 2310, which has 27 SW-pairs. The next number with five prime divisors is $n = 2730$, which has 18 SW-pairs. For $n \leq 10000$ there is a local minimum for $n = 3570$: 8 SW-pairs.

Finally, we consider the case where n is a prime p or a power of a prime p . Then any pair $\{p, q\}$ with q an arbitrary prime is a SW-pair. To avoid an infinity of SW-pairs we impose an additional condition: the members of SW-pairs should not to be larger than n . By its nature any divisor of the binomial $\binom{n}{k}$ is not larger than n . So, the additional condition has no consequences for SW-pairs of composite numbers, while it keeps the number of SW-pairs finite for primes and prime powers. To be specific, the element q of a SW-pair $\{p, q\}$ can be any prime not larger than n . If $n = 2$ there is only one SW-pair: $\{2, 2\}$. If $n = 3$ there are two SW-pairs: $\{3, 2\}$ and $\{3, 3\}$. If $n = 5$ there are three SW-pair: $\{5, 2\}$, $\{5, 3\}$ and $\{5, 5\}$, and so on. The number of SW-pairs therefore is given by the prime counting function $\pi(n)$ in case n is a prime p or a power of a prime p , see next figure.



For numbers $n \leq 10000$ we saw that for numbers with 1, 2, 3, 4 and 5 prime divisors the minimum number of SW-pairs is 1, 3, 6, 7 and 8 respectively. Although it may give the feeling that numbers with no SW-pairs are not very likely, it does prove nothing.

6.4 Confining to prime divisors of n

The identity $\binom{n}{1} = n$ implies that at least one of the primes of the SW-pair $\{p, q\}$ is a divisor of n . For many n a SW-pair $\{p, q\}$ exists such that both p and q are a prime divisor of n .

For $n \leq 1000$ there are 21 exceptions:

110, 220, 222, 231, 238, 240, 440, 444, 468, 476, 506, 561, 609, 615, 702, 720, 748, 814, 888, 966 and 988.

For $n \leq 10^4$ there are 314 exceptions. For $n \leq 10^5$ there are 5149 exceptions. For $n \leq 10^6$ there are 75 079 exceptions. For $n \leq 10^7$ there are 1 022 008 exceptions. For $n \leq 10^8$ there are 13 111 425 exceptions. The number of exceptions is plotted against n in the figure below. For comparison the function $f(n) = n$ is shown as a dashed line.

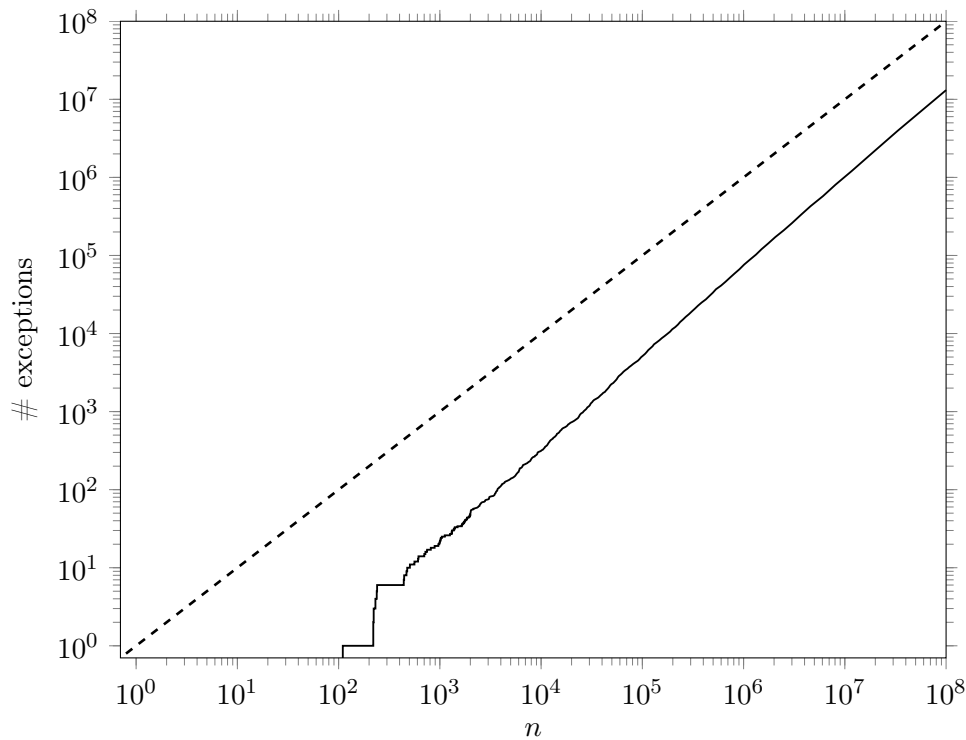


Figure 6.5: The number of integers $m \leq n$ for which no $\{p, q\}$ pair exists such that both p and q are a divisor of m , plotted against n . The dashed curve is the function $f(n) = n$.

For SW-pairs $\{p, q\}$ such that p and q are not both a divisor of n we change the problem to finding a set with three or more prime divisors of n such that if $1 \leq k \leq n - 1$ the binomial coefficient $\binom{n}{k}$ is divisible by at least one element of the set. We will call a set of prime divisors of n ‘covering’ if the set is such that if $1 \leq k \leq n - 1$ the binomial coefficient $\binom{n}{k}$ is divisible by at least one element of the set.

For instance, for each of the 21 exceptions given above for $n \leq 1000$ there exists a triple of primes $\{p, q, r\}$ all dividing n and such that if $1 \leq k \leq n - 1$ the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p, q and r . For $n \leq 100,000$ we find by inspection that a triple of prime divisors of n is not sufficient for $n = 47957$ and $n = 56826$. These two exceptions require a set of four prime divisors of n to do the covering. For much larger n it may occur that a set of five or more prime divisors of n is required to do the job.

For every integer $n > 1$ there exists a covering set. It is a consequence of Lucas' theorem. If $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ is the unique prime factorisation of n and if $1 \leq k \leq n - 1$, then $\binom{n}{k}$ is divisible by p_1 if $1 \leq k \leq p_1^{\alpha_1} - 1$, if $p_1^{\alpha_1} + 1 \leq k \leq 2p_1^{\alpha_1} - 1$, etc. The divisibility by p_1 is not certain if k is equal to $p_1^{\alpha_1}$ or a multiple of it. Similarly, the divisibility by p_2 is not certain if k is equal to $p_2^{\alpha_2}$ or a multiple of it. The situation where k is not divisible by both p_1 and p_2 can only occur if k is equal to $p_1^{\alpha_1} p_2^{\alpha_2}$. For $k = p_1^{\alpha_1} p_2^{\alpha_2}$ the binomial $\binom{n}{k}$ is divisible by p_3 except possibly when k is equal to $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$. Checking for all the prime divisors we find that the only exception can occur if k is equal to $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m} = n$, which is outside the range $1 \leq k \leq n - 1$. Therefore, the set of all prime divisors always is a covering. The minimal length of a covering set is smaller or equal to the number of divisors of n .

Let $u(n)$ be the number of prime divisors of n and let $v(n)$ be the smallest number of elements of the covering sets. For each n we have $v(n) \leq u(n)$. Furthermore, let $\sigma_{a,b}$ be the sequence of increasing n 's for which $u(n)$ and $v(n)$ have specified values a and b respectively:

$$\sigma_{a,b} = \{n \mid u(n) = a, v(n) = b\}. \quad (6.1)$$

Below are shown the first sequences for $n \leq 10^8$.

$$\sigma_{0,0} = \{1\},$$

$$\begin{aligned} \sigma_{1,1} = \{ & 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59, 61, 64, 67, \\ & 71, 73, 79, 81, 83, 89, 97, 101, 103, 107, 109, 113, 121, 125, 127, 128, 131, 137, 139, 149, 151, \\ & 157, 163, 167, 169, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 243, \\ & 251, 256, 257, 263, 269, 271, 277, 281, 283, 289, 293, 307, 311, 313, 317, 331, \dots \}, \end{aligned}$$

$$\begin{aligned} \sigma_{2,2} = \{ & 6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 33, 34, 35, 36, 38, 39, 40, 44, 45, 46, 48, 50, 51, 52, \\ & 54, 55, 56, 57, 58, 62, 63, 65, 68, 69, 72, 74, 75, 76, 77, 80, 82, 85, 86, 87, 88, 91, 92, 93, 94, 95, \\ & 96, 98, 99, 100, 104, 106, 108, 111, 112, 115, 116, 117, 118, 119, 122, 123, 124, 129, 133, 134, \\ & 135, 136, 141, 142, 143, 144, 145, 146, 147, 148, 152, 153, 155, 158, 159, 160, 161, \dots \}, \end{aligned}$$

$$\sigma_{3,2} = \{30, 42, 60, 66, 70, 78, 84, 90, 102, 105, 114, 120, 126, 130, 132, 138, 140, 150, 154, 156, 165, 168, 170, 174, 180, 182, 186, 190, 195, 198, 204, 228, 230, 234, 246, 252, 255, 258, 260, 264, 266, 270, 273, 276, 280, 282, 285, 286, 290, 294, 300, 306, 308, 310, 312, 315, 318, 322, 336, 340, 342, 345, 348, 350, 354, 357, 360, 364, 366, 370, 372, 374, 378, 380, 385, \dots\},$$

$$\sigma_{3,3} = \{110, 220, 222, 231, 238, 240, 440, 444, 468, 476, 506, 561, 609, 615, 702, 720, 748, 814, 888, 988, 1001, 1012, 1022, 1045, 1118, 1258, 1309, 1310, 1370, 1394, 1404, 1495, 1644, 1653, 1683, 1720, 1742, 1767, 1786, 1833, 1855, 1972, 1976, 2006, 2013, 2016, 2022, 2024, 2044, 2254, 2345, 2387, 2409, 2465, 2482, 2516, 2553, 2570, 2620, 2740, 2788, \dots\},$$

$$\sigma_{4,2} = \{210, 330, 390, 420, 462, 510, 546, 570, 630, 660, 690, 714, 770, 780, 798, 840, 858, 870, 910, 924, 930, 990, 1020, 1050, 1092, 1110, 1122, 1140, 1155, 1170, 1190, 1218, 1230, 1254, 1260, 1290, 1302, 1326, 1330, 1365, 1380, 1386, 1410, 1428, 1430, 1470, 1482, 1518, 1530, 1540, 1554, 1560, 1590, 1596, 1610, 1638, 1650, 1680, 1710, 1716, 1722, 1740, 1770, \dots\},$$

$$\sigma_{4,3} = \{966, 1320, 1870, 1932, 1995, 2002, 2142, 2145, 2470, 2508, 2860, 2990, 3066, 3198, 3612, 3696, 3710, 3740, 3828, 4002, 4095, 4182, 4284, 4446, 4522, 4818, 4845, 4902, 5016, 5110, 5244, 5418, 5775, 5796, 5820, 6045, 6060, 6072, 6110, 6118, 6138, 6396, 6486, 6578, 6622, 6710, 6902, 7084, 7095, 7134, 7310, 7395, 7480, 7735, 7820, 7905, 7920, 7990, \dots\},$$

$$\sigma_{4,4} = \{47957, 582967, 701845, 887485, 961741, 1003767, 1070399, 1115615, 1171247, 1175783, 1385359, 1385423, 1394789, 1402789, 1447589, 1639877, 1816879, 1822331, 1846019, 2033383, 2116989, 2167711, 2328065, 2417979, 2505137, 2621065, 2632069, 2796547, 3113891, 3119845, 3154459, 3226769, 3238459, 3284407, 3307603, \dots\},$$

$$\sigma_{5,2} = \{2310, 2730, 3570, 3990, 4290, 4620, 4830, 5460, 5610, 6090, 6270, 6510, 6630, 6930, 7140, 7410, 7590, 7770, 7980, 8190, 8580, 8610, 8778, 8970, 9030, 9240, 9282, 9570, 9660, 9870, 10010, 10230, 10374, 10626, 10710, 11130, 11220, 11310, 11730, 12012, 12090, 12180, 12390, 12540, 12558, 12810, 12870, 13020, 13090, 13110, 13260, 13398, \dots\},$$

$$\sigma_{5,3} = \{6006, 7854, 9690, 10920, 11550, 11970, 12210, 13566, 14190, 14280, 14322, 15180, 15330, 15708, 15834, 15990, 17290, 18060, 18270, 18354, 18870, 22110, 23100, 23370, 23478, 23870, 23940, 23970, 24420, 24990, 25080, 25662, 25806, 25935, 26220, 27132, 27370, 27390, 28014, 28470, 28490, 28560, 28644, 29070, 29820, 30360, 30450, \dots\},$$

$$\sigma_{5,4} = \{56826, 383990, 1113177, 1357345, 2773113, 2832387, 3305913, 3318095, 3999709, 4165323, 4188006, 4218465, 4251003, 4421313, 4684305, 5175667, 6484225, 6836523, 7023445, 7245485, 7293531, 7406035, 7700446, 7711319, 7757491, 7796555, 8184939, \dots\},$$

9187165, 9367475, 9601685, 9607465, 9640345, 9764765, 9902857, 10483676, ...},

$$\sigma_{5,5} = \{\},$$

$$\sigma_{6,2} = \{30030, 43890, 46410, 53130, 60060, 62790, 66990, 67830, 72930, 78540, 79170, 81510, 82110, 84630, 85470, 87780, 90090, 91770, 92820, 98670, 99330, 101010, 103530, 103740, 106260, 108570, 110670, 111930, 115710, 117810, 120120, 123690, 124410, 125580, 125970, 128310, 129030, 131670, 132090, \dots\},$$

$$\sigma_{6,3} = \{39270, 51870, 71610, 94710, 102102, 106590, 114114, 117390, 122430, 132990, 139230, 140910, 152490, 163590, 170170, 175560, 176358, 182910, 183540, 186186, 189210, 190190, 192270, 196350, 207480, 207570, 211470, 213486, 214890, 217770, 222870, 226590, 227010, 227766, 228228, 230010, \dots\},$$

$$\sigma_{6,4} = \{11960234, 12732915, 13639815, 20924365, 23330424, 23947066, 24600570, 26918535, 27545973, 28696479, 30757870, 33322718, 33382356, 33480042, 33713771, 36555805, 37453065, 38183445, 38496185, 38787455, 50230986, 54127485, 54198108, 55950076, 56232033, 56349436, 56448645, \dots\},$$

$$\sigma_{6,5} = \{\}, \sigma_{6,6} = \{\},$$

$$\sigma_{7,2} = \{510510, 690690, 903210, 930930, 1067430, 1138830, 1193010, 1217370, 1231230, 1291290, 1345890, 1381380, 1385670, 1411410, 1438710, 1452990, 1492260, 1531530, 1540770, 1560090, 1591590, 1607970, 1610070, 1623930, 1647030, 1677390, 1688610, 1717170, 1741740, 1763580, 1771770, 1799490, \dots\},$$

$$\sigma_{7,3} = \{570570, 746130, 870870, 881790, 1009470, 1021020, 1111110, 1141140, 1272810, 1360590, 1504230, 1711710, 1820910, 1845690, 1939938, 1946490, 2012010, 2222220, 2238390, 2284590, 2326170, 2363790, 2395470, 2434740, 2451570, 2462460, 2526810, 2545620, 2574390, 2631090, 2649570, 2677290, \dots\},$$

$$\sigma_{7,4} = \{50227870, 61623555, 77942865\},$$

$$\sigma_{7,5} = \{\}, \sigma_{7,6} = \{\}, \sigma_{7,7} = \{\},$$

$$\sigma_{8,2} = \{11741730, 15825810, 17687670, 18888870, 19399380, 20030010, 21111090, 21637770, 23130030, 23393370, 23483460, 24534510, 25555530, 25571910, 26246220, 26996970, 27057030, 27335490, 27999510, 28318290, 29609580, 29699670, 30240210, 30591330, 31141110, 31293570, 32083590, \dots\},$$

$$\sigma_{8,3} = \{9699690, 13123110, 14804790, 16546530, 17160990, 20281170, 20930910, 21411390, \\ 21951930, 23993970, 26193090, 26816790, 27606810, 29099070, 29274630, 30120090, \\ 30955470, 31651620, 31870410, 32626230, 33090330, 33093060, 34321980, 34597290, \\ 35225190, 35375340, 36606570, 37350390, 37447410, 38228190, 39369330, \dots\},$$

$$\sigma_{8,4} = \{\}, \sigma_{8,5} = \{\}, \sigma_{8,6} = \{\}, \sigma_{8,7} = \{\}, \sigma_{8,8} = \{\}.$$

The notation $\sigma_{a,b} = \{\}$ just means there are no elements in $\sigma_{a,b}$ lower than or equal to 10^8 . Empty sets will be filled by considering numbers larger than 10^8 . For instance, the first element of $\sigma_{5,5}$ is 1 245 792 257.

Of course, $\sigma_{1,1}$ is just the sequence of numbers that are divisible by exactly 1 prime. It is identical to the sequence A246655 of the OEIS [3]. Similarly, $\sigma_{2,2}$ is just the sequence of numbers that are divisible by exactly 2 different primes (A007774, OEIS). The union of $\sigma_{3,2}$ and $\sigma_{3,3}$ is the sequence of numbers that are divisible by exactly 3 different primes (A033992, OEIS). The union of $\sigma_{4,2}$, $\sigma_{4,3}$ and $\sigma_{4,4}$ is the sequence of numbers that are divisible by exactly 4 different primes (A033993, OEIS). The union of $\sigma_{5,k}$, with $2 \leq k \leq 5$, is the sequence of numbers that are divisible by exactly 5 different primes (A051270, OEIS). In general, the union of $\sigma_{a,b}$, with $2 \leq b \leq a$, is the sequence of numbers that are divisible by exactly a different primes.

6.5 Algorithm for covering sets of prime divisors of n

If n has exactly one prime divisor then the prime divisor is covering and the minimal length of the covering set is 1. If n has exactly two prime divisors then the two prime divisor form a covering pair and the minimal length of the covering set is 2. If n has three or more prime divisors the minimal length is determined with an algorithm. Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m}$ be the prime factorisation of n . Starting with the pair of primes $\{p_i, p_j\}$ with the largest product $p_i^{\alpha_i} \cdot p_j^{\alpha_j}$, the algorithm runs over the pairs to see, by means of Kummer's method, if for each k a multiple of $p_i^{\alpha_i} \cdot p_j^{\alpha_j}$ the binomial $\binom{n}{k}$ is divisible by either p_i or p_j . If so, the minimal length is 2. If no pair is found the algorithm runs over the subsets with length 3, starting with the triple with largest product $p_i^{\alpha_i} \cdot p_j^{\alpha_j} \cdot p_l^{\alpha_l}$, to see if for each k a multiple of $p_i^{\alpha_i} \cdot p_j^{\alpha_j} \cdot p_l^{\alpha_l}$ the binomial $\binom{n}{k}$ is divisible by either p_i or p_j . If it is, the minimal length is 3. If no triple is found the algorithm runs over subsets with length 4 and so on. As soon as a covering subset with minimal length is found the algorithm terminates.

To illuminate the algorithm we give some examples.

Example 6.5.1. $n = 42$:

That is, n has three prime divisors: $n = 2 \cdot 3 \cdot 7$. The algorithm starts with the pair $\{3, 7\}$. Since the binomial $\binom{42}{21}$ is divisible by 3, it is concluded that $\{3, 7\}$ is a covering set. Hence, the minimal length is 2.

Example 6.5.2. $n = 60$:

That is, n has three prime divisors: $n = 2^2 \cdot 3 \cdot 5$. The algorithm starts with the pair $\{2, 5\}$. Since the binomial $\binom{60}{20}$ is divisible by 5, it is concluded that $\{2, 5\}$ is a covering set. Hence, the minimal length is 2.

Example 6.5.3. $n = 110$:

That is, n has three prime divisors: $n = 2 \cdot 5 \cdot 11$. The algorithm starts with the pair $\{5, 11\}$. Since the binomial $\binom{110}{55}$ is divisible by neither 5 nor 11, it is concluded that $\{5, 11\}$ is not a covering set. Next the algorithm takes the pair $\{2, 11\}$. Since the binomial $\binom{110}{44}$ is divisible by neither 2 nor 11, it is concluded that $\{2, 11\}$ is not a covering set. Next the algorithm takes the pair $\{2, 5\}$. Since the binomial $\binom{110}{10}$ is divisible by neither 2 nor 5, it is concluded that $\{2, 5\}$ is not a covering set. Since all possible pairs are inspected, the algorithm draws the conclusion that $\{2, 5, 11\}$ is the smallest covering set. Hence, the minimal length is 3.

From the foregoing examples we see that 42 and 60 belong to the $\sigma_{3,2}$ sequence and that 110 belongs to the $\sigma_{3,3}$ sequence.

6.6 Primorials

A primorial is a product of subsequent primes starting with the first prime $p_1 = 2$. If $p_m\#$ denotes the m -th primorial, then $p_1\# = p_1 = 2$, $p_2\# = p_1p_2 = 2 \cdot 3 = 6$, $p_3\# = p_1p_2p_3 = 2 \cdot 3 \cdot 5 = 30$, $p_4\# = p_1p_2p_3p_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, etc. By inspection we observe the following:

The first element of $\sigma_{1,1}$ is $p_1\# = 2$.

The first element of $\sigma_{2,2}$ is $p_2\# = 6$.

The first element of $\sigma_{3,2}$ is $p_3\# = 30$.

The first element of $\sigma_{4,2}$ is $p_4\# = 210$.

The first element of $\sigma_{5,2}$ is $p_5\# = 2310$.

The first element of $\sigma_{6,2}$ is $p_6\# = 30\,030$.

The first element of $\sigma_{7,2}$ is $p_7\# = 510\,510$.

The first element of $\sigma_{8,3}$ is $p_8\# = 9\,699\,690$.

The first element of $\sigma_{9,2}$ is $p_9\# = 223\,092\,870$.

The first element of $\sigma_{10,2}$ is $p_{10}\# = 6\,469\,693\,230$.

The first element of $\sigma_{11,2}$ is $p_{11}\# = 200\,560\,490\,130$.

The first element of $\sigma_{12,3}$ is $p_{12}\# = 7\,420\,738\,134\,810$.

The first element of $\sigma_{13,3}$ is $p_{13}\# = 304\,250\,263\,527\,210$.

The first element of $\sigma_{14,3}$ is $p_{14}\# = 13\,082\,761\,331\,670\,030$.

We see that for relatively small a the primorials p_a are the first element of $\sigma_{a,2}$, while for increasing a the primorials p_a more and more are the first elements of $\sigma_{a,3}$.

6.7 Distributions

Let $S_{a,b}(x)$ denote the number of elements of $\sigma_{a,b}$ lower than or equal to x . To get an impression of the distributions we have tabulated $S_{a,b}(x)$ for several decades of x , see table 6.2.

	10	100	1000	10 000	100 000	1 000 000	10 000 000	100 000 000
$S_{0,0}$	1	1	1	1	1	1	1	1
$S_{1,1}$	7	35	193	1280	9700	78734	665134	5762859
$S_{2,2}$	2	56	508	4097	33759	288726	2536838	22724609
$S_{3,2}$	0	8	255	3465	35873	345445	3253887	30535779
$S_{3,3}$	0	0	20	230	2971	34275	388879	4264583
$S_{4,2}$	0	0	22	813	13986	176249	1948483	20253779
$S_{4,3}$	0	0	1	81	1868	31780	440751	5531494
$S_{4,4}$	0	0	0	0	1	5	199	4307
$S_{5,2}$	0	0	0	30	1511	34034	520767	6594422
$S_{5,3}$	0	0	0	3	304	8456	170408	2755964
$S_{5,4}$	0	0	0	0	1	2	34	907
$S_{5,5}$	0	0	0	0	0	0	0	0
$S_{6,2}$	0	0	0	0	21	1728	51705	966800
$S_{6,3}$	0	0	0	0	4	557	21197	523598
$S_{6,4}$	0	0	0	0	0	0	0	60
$S_{6,5}$	0	0	0	0	0	0	0	0
$S_{6,6}$	0	0	0	0	0	0	0	0
$S_{7,2}$	0	0	0	0	0	4	1177	49893
$S_{7,3}$	0	0	0	0	0	4	539	30223
$S_{7,4}$	0	0	0	0	0	0	0	3
$S_{7,5}$	0	0	0	0	0	0	0	0
$S_{7,6}$	0	0	0	0	0	0	0	0
$S_{7,7}$	0	0	0	0	0	0	0	0
$S_{8,2}$	0	0	0	0	0	0	0	433
$S_{8,3}$	0	0	0	0	0	0	1	286
$S_{8,4}$	0	0	0	0	0	0	0	0
$S_{8,5}$	0	0	0	0	0	0	0	0
$S_{8,6}$	0	0	0	0	0	0	0	0
$S_{8,7}$	0	0	0	0	0	0	0	0
$S_{8,8}$	0	0	0	0	0	0	0	0

Table 6.2: $S_{a,b}(x)$ for several decades of x . For example, the entry in the sixth column and the fifth row tells us $S_{3,3}(100000) = 35873$. That is, 35873 elements of the sequence $\sigma_{3,3}$ are lower than or equal to 100 000.

From the contents of table 6.2 it can be inferred that for almost 87% of the numbers $n \leq 100\,000\,000$ there exist a pair of prime divisors of n such that if $1 \leq k \leq n - 1$ then the binomial coefficient $\binom{n}{k}$ is divisible by at least one prime of the pair.

A visual presentation of the number of elements of $\sigma_{1,1}, \sigma_{2,2}, \sigma_{3,2}, \sigma_{3,3}, \sigma_{4,2}, \sigma_{4,3}, \sigma_{4,4}, \sigma_{5,2}, \sigma_{5,3}, \sigma_{5,4}, \sigma_{6,2}, \sigma_{6,3}, \sigma_{6,4}, \sigma_{7,2}, \sigma_{7,3}, \sigma_{7,4}, \sigma_{8,2}$ and $\sigma_{8,3}$ lower than or equal to n is shown in the next figure.

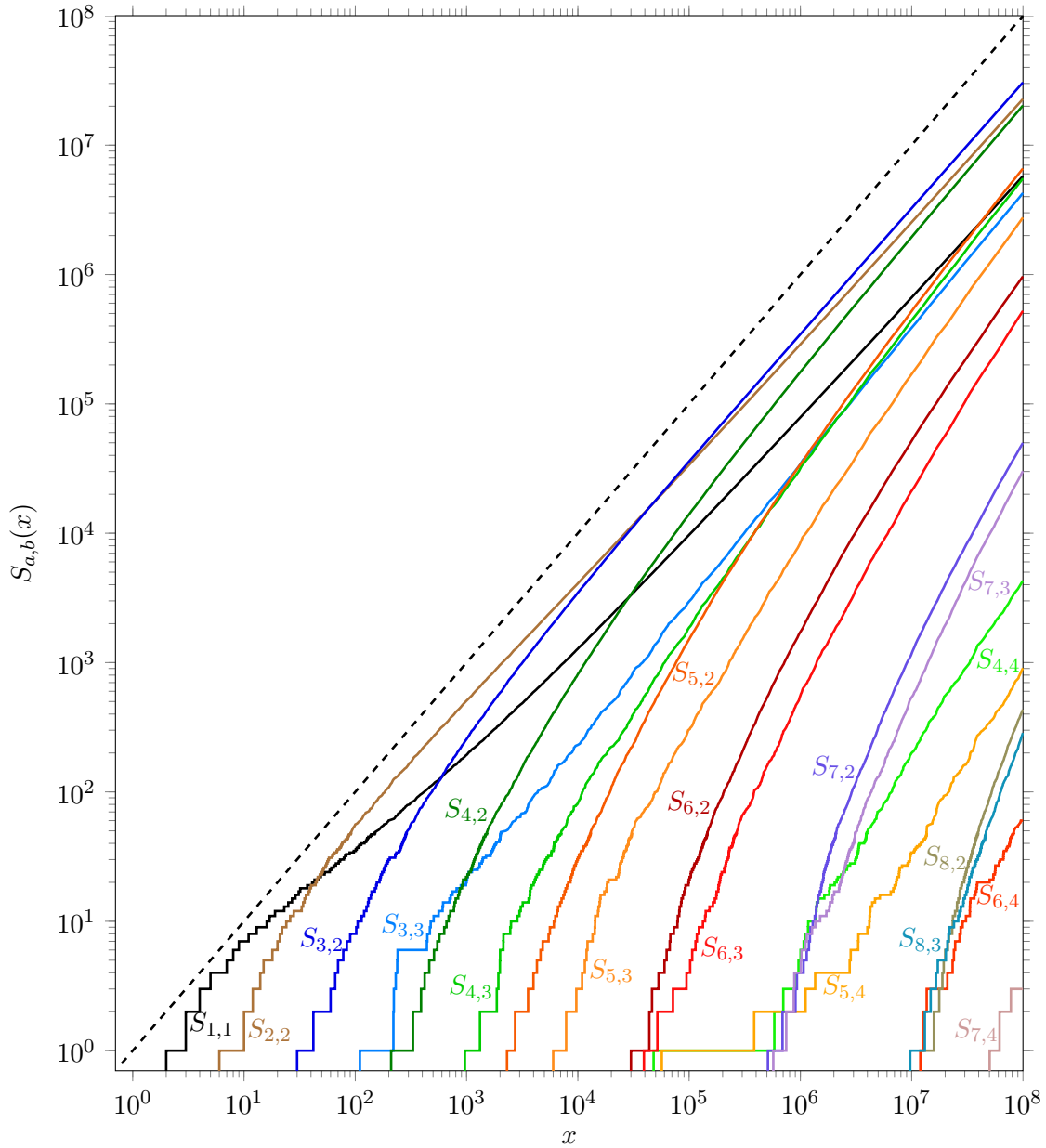


Figure 6.6: Various functions $S_{a,b}(x)$ plotted against x . The dashed curve is the function $f(n) = n$.

Appendix A

Proof of Kummer's theorem

Let μ be the largest integer exponent of the prime p such that p^μ divides $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$. That is, p^μ is a divisor of $n!$, while $p^{\mu+1}$ is not a divisor of $n!$. Since μ depends on n and p we will denote it as $\mu_p(n)$. For $\mu(n)$ holds the following identity:

$$\mu_p(n) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor. \quad (\text{A.1})$$

Here $\lfloor x \rfloor$ denotes the integer part of x ; the largest integer smaller than x . Thus $\lfloor 5.2 \rfloor = 5$, $\lfloor 6.7 \rfloor = 6$, $\lfloor 0.8 \rfloor = 0$, etc. The contribution of $\left\lfloor \frac{n}{p^i} \right\rfloor$ is zero as soon as $p^i > n$.

The identity can be explained as follows. The numbers $p, 2p, 3p, \dots, \left\lfloor \frac{n}{p^1} \right\rfloor p$ are divisible by p , so they contribute $\left\lfloor \frac{n}{p^1} \right\rfloor$ to $\mu_p(n)$. The numbers $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{n}{p^2} \right\rfloor p^2$ are divisible by p^2 . Together they contain $2 \cdot \left\lfloor \frac{n}{p^2} \right\rfloor$ times the factor p of which $\left\lfloor \frac{n}{p^2} \right\rfloor$ is already counted in $\left\lfloor \frac{n}{p^1} \right\rfloor$. The numbers $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{n}{p^2} \right\rfloor p^2$ therefore contribute $\left\lfloor \frac{n}{p^2} \right\rfloor$ to $\mu_p(n)$. The numbers $p^3, 2p^3, 3p^3, \dots, \left\lfloor \frac{n}{p^3} \right\rfloor p^3$ are divisible by p^3 . Together they contain $3 \cdot \left\lfloor \frac{n}{p^3} \right\rfloor$ times the factor p of which $\left\lfloor \frac{n}{p^3} \right\rfloor$ is already counted in $\left\lfloor \frac{n}{p^1} \right\rfloor$ and $\left\lfloor \frac{n}{p^3} \right\rfloor$ is already counted in $\left\lfloor \frac{n}{p^2} \right\rfloor$. The numbers $p^3, 2p^3, 3p^3, \dots, \left\lfloor \frac{n}{p^3} \right\rfloor p^3$ therefore contribute $\left\lfloor \frac{n}{p^3} \right\rfloor$ to $\mu_p(n)$. Continuing the line of reasoning we obtain the identity (A.1).

For example, if $n = 15$ and $p = 2$, then the $\left\lfloor \frac{15}{2^1} \right\rfloor = 7$ numbers 2,4,6,8,10,12 and 14 are divisible by 2. Together they contain 7 times the factor 2, so they contribute 7 to $\mu_2(15)$. The $\left\lfloor \frac{15}{2^2} \right\rfloor = 3$ numbers 4, 8 and 12 are divisible by 2^2 . Together they contain 6 times the factor 2 of which 3 times are already counted in $\left\lfloor \frac{15}{2^1} \right\rfloor$. The numbers 4,8 and 12 therefore contribute 3 to $\mu_2(15)$. The $\left\lfloor \frac{15}{2^3} \right\rfloor = 1$ number 8 is divisible by 2^3 . It contains 3 times the factor 2 of

which 2 times are already counted in $\left\lfloor \frac{15}{2^1} \right\rfloor$ and $\left\lfloor \frac{15}{2^2} \right\rfloor$. The number 8 therefore contributes 1 to $\mu_2(15)$. Altogether, $\mu_2(15) = 7 + 3 + 1 = 11$. That is, $15! = 1307674368000$ is divisible by 2^{11} but not by 2^{12} .

Example 2: $n = 19$ and $p = 3$. The $\left\lfloor \frac{19}{3^1} \right\rfloor = 6$ numbers 3,6,9,12,15 and 18 are divisible by 3. Together they contain 6 times the factor 3, so they contribute 6 to $\mu_3(19)$. The $\left\lfloor \frac{19}{3^2} \right\rfloor = 2$ numbers 9 and 18 are divisible by 3^2 . Together they contain 4 times the factor 3 of which 2 times are already counted in $\left\lfloor \frac{19}{3^1} \right\rfloor$. The numbers 9 and 18 therefore contribute 2 to $\mu_3(19)$. Hence, $\mu_3(19) = 6 + 2 = 8$. That is $19! = 121645100408832000$ is divisible by 3^8 but not by 3^9 .

By means of the identity (A.1) one can derive another identity. To this end we expand n , $n - k$ and k in base p :

$$n = \sum_{i=0}^{\infty} a_i p^i, \quad k = \sum_{i=0}^{\infty} b_i p^i, \quad n - k = \sum_{i=0}^{\infty} c_i p^i. \quad (\text{A.2})$$

If m such that $p^{m+1} > n$ while $p^m \leq n$, then $n = a_0 + a_1 p + a_2 p^2 + \dots + a_m p^m$. The integer parts of n divided by p^i expanded in base p then are $\left\lfloor \frac{n}{p^i} \right\rfloor = a_i + a_{i+1} p + \dots + a_m p^{m-i}$, where $i \leq m$. By means of the latter we can write $\mu_p(n)$ as

$$\begin{aligned} \mu_p(n) &= \sum_{i=1}^m \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^m (a_i + a_{i+1} p + a_{i+2} p^2 + \dots + a_m p^{m-i}) = \\ & (a_1 + a_2 p + a_3 p^2 + a_4 p^3 + \dots + a_m p^{m-1}) + \\ & (a_2 + a_3 p + a_4 p^2 + \dots + a_m p^{m-2}) + \\ & (a_3 + a_4 p + \dots + a_m p^{m-3}) + \\ & \vdots \\ & (a_{m-1} + a_m p) + \\ & a_m. \end{aligned} \quad (\text{A.3})$$

After a rearrangement of terms it can be written as

$$\mu_p(n) = \sum_{t=1}^m \sum_{j=0}^{t-1} a_t p^j. \quad (\text{A.4})$$

From the latter it follows

$$\begin{aligned} (p-1)\mu_p(n) &= \sum_{t=1}^m \sum_{j=1}^t a_t p^j - \sum_{t=1}^m \sum_{j=0}^{t-1} a_t p^j = \\ & \sum_{t=1}^m a_t p^t - \sum_{t=1}^m a_t = \sum_{t=0}^m a_t p^t - \sum_{t=0}^m a_t = n - \sigma_p(n), \end{aligned} \quad (\text{A.5})$$

where $\sigma_p(n)$ is the sum of all the digits in the base p expansion of n :

$$\sigma_p(n) = \sum_{t=0}^m a_t. \quad (\text{A.6})$$

Since $a_i = 0$ for $i > m$ the latter can also be written as

$$\sigma_p(n) = \sum_{t=0}^{\infty} a_t. \quad (\text{A.7})$$

In a similar way we obtain for $n - k$ and k :

$$\sigma_p(k) = \sum_{i=0}^{\infty} b_i, \quad \sigma_p(n - k) = \sum_{i=0}^{\infty} c_i. \quad (\text{A.8})$$

In (A.5) we have arrived at an identity which was already formulated by Legendre in 1808 [6]: If $\mu_p(n)$ is the largest integer exponent of the prime power $p^{\mu(n)}$ that divides $n!$, then

$$\mu_p(n) = \frac{n - \sigma_p(n)}{p - 1}. \quad (\text{A.9})$$

Let r be the largest integer exponent of p such that p^r divides $\binom{n}{k} = \frac{n!}{(n-k)!k!}$, then p^r is equal to $p^{\mu(n)} \cdot p^{-\mu(n-k)} \cdot p^{-\mu(k)}$. That is,

$$r = \mu_p(n) - \mu_p(n - k) - \mu_p(k). \quad (\text{A.10})$$

Substituting Legendre's identity we obtain

$$r = \frac{n - \sigma(n)}{p - 1} - \frac{n - k - \sigma(n - k)}{p - 1} - \frac{k - \sigma(k)}{p - 1} = \frac{\sigma(n - k) + \sigma(k) - \sigma(n)}{p - 1}. \quad (\text{A.11})$$

Substitution of (A.7) and (A.8) leads to

$$r = \frac{1}{p - 1} \left(\sum_{i=0}^{\infty} c_i + \sum_{i=0}^{\infty} b_i - \sum_{i=0}^{\infty} a_i \right). \quad (\text{A.12})$$

When we add k and $n - k$, the carries, which we will denote as δ_i , follow from $\delta_0 = \left\lfloor \frac{b_0 + c_0}{p} \right\rfloor$, $\delta_1 = \left\lfloor \frac{b_1 + c_1 + \delta_0}{p} \right\rfloor$, $\delta_2 = \left\lfloor \frac{b_2 + c_2 + \delta_1}{p} \right\rfloor$, $\delta_3 = \left\lfloor \frac{b_3 + c_3 + \delta_2}{p} \right\rfloor$, and so on. If we define $\delta_{-1} = 0$, then $\delta_i = \left\lfloor \frac{b_i + c_i + \delta_{i-1}}{p} \right\rfloor$ for $i = 0, 1, 2, 3, \dots$. Since the addition of $n - k$ and k results in n , we obtain

$$a_i = b_i + c_i + \delta_{i-1} - p\delta_i, \quad i = 0, 1, 2, 3, \dots \quad (\text{A.13})$$

Substitution of the latter into (A.12) leads to

$$r = \frac{1}{p-1} \left(\sum_{i=0}^{\infty} c_i + \sum_{i=0}^{\infty} b_i - \sum_{i=0}^{\infty} (b_i + c_i + \delta_{i-1} - p\delta_i) \right) = \frac{1}{p-1} \left(\sum_{i=0}^{\infty} (p\delta_i - \delta_{i-1}) \right). \quad (\text{A.14})$$

Since

$$\begin{aligned} \sum_{i=0}^{\infty} (p\delta_i - \delta_{i-1}) &= (p\delta_0 - \delta_{-1}) + (p\delta_1 - \delta_0) + (p\delta_2 - \delta_1) + (p\delta_3 - \delta_2) + \dots = \\ &= (p\delta_0 - 0) + (p\delta_1 - \delta_0) + (p\delta_2 - \delta_1) + (p\delta_3 - \delta_2) + \dots = \\ &= (p\delta_0 - \delta_0) + (p\delta_1 - \delta_1) + (p\delta_2 - \delta_2) + (p\delta_3 - \delta_3) + \dots = \\ &= \sum_{i=0}^{\infty} (p\delta_i - \delta_i) = (p-1) \sum_{i=0}^{\infty} \delta_i, \end{aligned} \quad (\text{A.15})$$

we finally obtain

$$r = \sum_{i=0}^{\infty} \delta_i. \quad (\text{A.16})$$

The latter is Kummer's theorem. In words:

if p is a prime and r carries occur in the addition of $n-k$ and k in base p , then r is the largest value of x for which p^x divides $\binom{n}{k}$.

Appendix B

P-adic numbers

B.1 Infinite repetitions

For normal numbers we are used to deal with endless repetitions of decimals. As an example, for the number $0.22222\dots$, also denoted as $0.\bar{2}$, we know it is equal to $2/9$. As another example, for the number $x = 3.2515151\dots = 3.2\bar{51}$ we can derive it is equal to $3\frac{83}{330}$. To see this, denote $0.0515151\dots$ as y . If you multiply y by 100 and subtract 5.1 from the result you obtain y : $100y - 5.1 = y$. The latter can be elaborated to $y = \frac{17}{330}$. Since $x = 3 + \frac{1}{5} + y$ we find $x = 3\frac{83}{330}$.

Instead of numbers with infinitely many digits to the right of the decimal point, we can consider numbers with infinitely many digits to the left of the decimal point. An example of such a number is $\dots999999\dots$, also denoted as $\bar{9}$. If we add 1 to this number the result is $\dots000000\dots$. Of course to the far left there is living a 1. However, it is infinitely far away from the decimal point. Ignoring the infinitely far away 1, we can think of $\dots000000\dots$ as being equal to zero. Then we can write $\dots999999\dots + 1 = \dots000000\dots$ as $\bar{9} + 1 = 0$. It implies $\bar{9} = -1$. To see if this makes sense a little we take the square of $\bar{9}$:

$$\begin{aligned}\bar{9}^2 &= \dots999999\dots \cdot \dots999999\dots = 9 \cdot \dots999999\dots + 90 \cdot \dots999999\dots + 900 \cdot \dots999999\dots + \dots = \\ &\dots9999991\dots + \dots9999910\dots + \dots999100\dots + \dots = \dots000001\dots = 1.\end{aligned}$$

Well, at least it is not against logic that we obtain $(-1)^2 = 1$.

The division of $\dots999999\dots$ by 9 leads to $\dots111111\dots$. That is, $\bar{1} = -\frac{1}{9}$. In a similar way $\bar{2} = -\frac{2}{9}$, $\bar{3} = -\frac{3}{9} = -\frac{1}{3}$, $\bar{4} = -\frac{4}{9}$, etc. If we add 1 to $\bar{3} = -\frac{1}{3}$, we obtain $\bar{3}4 = \frac{2}{3}$. Taking the square we get $\bar{5}6 = \frac{4}{9}$. Adding $\bar{4}$ results in $5\bar{6} + \bar{4} = 0$ as desired since $\frac{4}{9} - \frac{4}{9} = 0$.

The foregoing suggests the arithmetic is consistent for numbers with infinitely many digits to the left of the decimal point. However, without restrictions ambiguities can occur. For instance, if we add 1 to $\dots888888\dots = -\frac{8}{9}$ we get $\dots888889\dots = \frac{1}{9}$. If numbers with infinitely many digits to the right of the decimal point are not excluded then also $0.111111\dots = \frac{1}{9}$.

That is, we would have two different representations for the fraction $\frac{1}{9}$. To avoid the ambiguity in the representation of certain fractions, the numbers with infinitely many digits to the right of the decimal point are excluded. Numbers with infinitely many digits to the left of the decimal point and a finite number of digits to the right of the decimal point are called 10-adic numbers. Examples of 10-adic numbers are:

$$\frac{1}{2} = \dots 000000.6_{10},$$

$$-\frac{1}{3} = \dots 333333_{10} = \overline{3}_{10},$$

$$-\frac{2}{3} = \dots 666666_{10} = \overline{6}_{10},$$

$$\frac{1}{4} = \dots 000000.25_{10},$$

$$\frac{3}{4} = \dots 000000.75_{10},$$

$$\frac{1}{5} = \dots 000000.2_{10},$$

$$\frac{1}{6} = -\frac{1}{3} + \frac{1}{2} = \dots 333333_{10} + \dots 000000.5_{10} = \dots 333333.5_{10} = \overline{3.5}_{10},$$

$$-\frac{1}{6} = \frac{1}{3} - \frac{1}{2} = \dots 666667_{10} - \dots 000000.5_{10} = \dots 666666.5_{10} = \overline{6.5}_{10},$$

$$\frac{5}{6} = \frac{1}{3} + \frac{1}{2} = \dots 666667_{10} + \dots 000000.5_{10} = \dots 666667.5_{10} = \overline{67.5}_{10},$$

$$-\frac{1}{7} = \dots 142857142857_{10} = \overline{142857}_{10},$$

$$\frac{1}{7} = \dots 2857142857143_{10} = \overline{2857143}_{10},$$

$$3\frac{9}{14} = 3 + \frac{1}{7} + \frac{1}{2} = \dots 2857142857146.5_{10} = \overline{2857146.5}_{10},$$

$$3\frac{11}{28} = 3 + \frac{1}{7} + \frac{1}{4} = \dots 2857142857146.25_{10} = \overline{2857146.25}_{10},$$

$$\frac{1}{11} = \dots 090909091_{10} = \overline{091}_{10},$$

$$\frac{1}{13} = \dots 6923076923076923077_{10} = \overline{6923076923077}_{10},$$

$$\frac{1}{17} = \dots 294117647058823529411764705882353_{10} = \overline{29411764705882353}_{10},$$

$$\frac{1}{61} = \overline{0983606557377049180327868852459016393442622950819672131147541}_{10}.$$

The index 10 indicates the numbers are 10-adic.

The fraction $\frac{5}{6}$ can be obtained in different ways:

$$\frac{5}{6} = \frac{1}{3} + \frac{1}{2} = \overline{6}7.5_{10}$$

or

$$\frac{5}{6} = 1 - \frac{1}{6} = \overline{6}7.5_{10}$$

or

$$\frac{5}{6} = 5 \cdot \frac{1}{6} = \overline{6}7.5_{10}.$$

We see different routes lead to the same answer just as for addition, subtraction, multiplication and division of normal numbers. Formally, 10-adic numbers obey the following properties:

P1: associativity for (+): $a + (b + c) = (a + b) + c$.

P2: neutral element for (+): $a + 0 = 0 + a = a$.

P3: inverse for (+): $a + (-a) = (-a) + a = 0$.

P4: commutative (Abelian) for (+): $a + b = b + a$.

P5: associativity for (\cdot): $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

P6: distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$.

P7: neutral element for (\cdot): $a \cdot 1 = 1 \cdot a = a$.

P8: commutative (Abelian) for (\cdot): $a \cdot b = b \cdot a$.

Therefore 10-adic numbers form a CUR (commutative unitary ring). As we will see in the next section 10-adic numbers do not form an integral domain and therefore they do not form a field.

From the 10-adic number examples we see non-zero digits to the right of the decimal point if the denominator of the fractional part (in reduced form) is not coprime to 10. In general, for b -adic numbers non-zero digits to the right of the decimal point occur if the denominator of the fractional part (in irreducible form) is not coprime to b . As a consequence, for p -adic numbers, with p a prime, non-zero digits to the right of the decimal point occur only if the denominator of the fractional part (in irreducible form) is a multiple of p .

B.2 10-adic zero divisors

It turns out that 10-adic numbers have an awkward property: they have zero divisors. That is, there exists two numbers $a \neq 0$ and $b \neq 0$ such that $a \cdot b = 0$. Examples of such a pair are

$$a = \dots 63811000557423423230896109004106619977392256259918212890625,$$

$$b = \dots 63811000557423423230896109004106619977392256259918212890624$$

or

$$a' = \dots 36188999442576576769103890995893380022607743740081787109376,$$

$$b' = \dots 36188999442576576769103890995893380022607743740081787109375.$$

These numbers satisfy the equations $a^2 - a = 0$ and $b = a - 1$. Since $a^2 - a$ factors in $a \cdot (a - 1) = a \cdot b$ we have $a \cdot b = 0$. So, to find 10-adic numbers which satisfy $a \cdot b = 0$ is a matter of finding 10-adic numbers which satisfy $a^2 = a$. Next to the trivial solutions 0 and 1, such numbers must have a 5 or a 6 as the first digit to the left of the decimal point. Otherwise it will not equal the first digit to the left of the decimal point of the square.

A procedure to find a number with 5 as the first digit to the left of the decimal point is as follows [4]. First take the square of 5. Since 625 is the square of 25 the next digit must be 2. Since 390625 is the square of 625 the next digit is 6. Since 8212890625 is the square of 90625 the next two digits must be 90. If a zero digit occurs we take two digits at a time, if two adjacent zero digits occurs we take three digits a time, etc. Since 793212890625 is the square of 890625 the next digit must be 8. Since 8355712890625 is the square of 2890625 the next digit must be 2, and so on. Continuing the procedure leads to the first of the two aforementioned pairs.

The procedure for a number with 6 as the first digit to the left of the decimal point is a little more tedious. Since $36^2 = 1296$ the next digit can not be 3. However, $76^2 = 5776$ suggests to take 7 as the second digit. Since $376^2 = 141376$ we take 3 as the next digit. Since $9376^2 = 87909376$ the next digit must be 9. Since $109376^2 = 11963109376$ the next two digits are 10. Since $7109376^2 = 50543227109376$ the next digit is 7, and so on. Continuing the procedure leads to the second of the two aforementioned pairs.

The pairs are not unrelated: $a' = 1 - a$. Not a big surprise because the square of $1 - a$ equals $1 - a$. That is, $(a')^2 = (1 - a)^2 = 1 - 2a + a^2 = 1 - a = a'$. We could therefore have obtained the second pair directly from the first pair.

The reason for 10-adic zero divisors is that 10 is a composite number. As a consequence 10-adic numbers do not form a field. Zero divisors do not occur in p -adic numbers if p is a prime. As a consequence p -adic numbers form a field. The field of p -adic numbers is denoted as \mathbb{Z}_p . p -adic number for which non-zero digits do not occur to the right of the decimal point are p -adic integers. The field of p -adic integers is denoted as \mathbb{Q}_p . As we will see below, p -adic integers with finite digits to the left of the decimal point are just integers expanded in base p , while p -adic integers with a repetitive cycle of digits represent fractions.

B.3 p -adic numbers

The p -adic calculus will be illustrated for $p = 7$. Afterwards the reader can apply it to other primes. Some examples of 7-adic numbers are: $1 = 1_7$, $2 = 2_7$, $10 = 13_7$, $20 = 26_7$, $100 = 202_7$, $200 = 404_7$, $\frac{1}{7} = 0.1_7$, $\frac{1}{49} = 0.01_7$, $-1 = \dots 666666_7 = \bar{6}_7$, $-2 = \dots 666665_7 = \bar{6}5_7$,

$-8 = \dots 666656_7 = \overline{6}56_7$, $-\frac{1}{6} = \dots 111111_7 = \overline{1}_7$, $-\frac{1}{3} = \dots 222222_7 = \overline{2}_7$, $-\frac{1}{2} = \dots 333333_7 = \overline{3}_7$,
 $-\frac{2}{3} = \dots 444444_7 = \overline{4}_7$, $-\frac{5}{6} = \dots 555555_7 = \overline{5}_7$, $\frac{1}{6} = \dots 555556_7 = \overline{5}6_7$, $\frac{1}{3} = \dots 444445_7 = \overline{4}5_7$,
 and so on.

For instance, to find the 7-adic representation of $\frac{3}{5}$ one considers the expansion in base 7:

$$\frac{3}{5} = \sum_{i=0}^{\infty} a_i 7^i. \tag{B.1}$$

Multiplication by 5 gives

$$3 = \sum_{i=0}^{\infty} 5a_i 7^i. \tag{B.2}$$

Since $3 = 3_7$ there holds $5a_0 = 3 \pmod{7}$. The solution is $a_0 = 2$. Since $5 \cdot 2 = 10 = 13_7$ it gives 1 as a carry. Therefore, $5a_1 + 1 = 0 \pmod{7} \rightarrow a_1 = 4$. Since $5 \cdot 4 + 1 = 21 = 30_7$ it gives 3 as a carry. Therefore, $5a_2 + 3 = 0 \pmod{7} \rightarrow a_2 = 5$. Since $5 \cdot 5 + 3 = 28 = 40_7$ it gives 4 as a carry. Therefore, $5a_3 + 4 = 0 \pmod{7} \rightarrow a_3 = 2$. Since $5 \cdot 2 + 4 = 14 = 20_7$ it gives 2 as a carry. Therefore, $5a_4 + 2 = 0 \pmod{7} \rightarrow a_4 = 1$. Since $5 \cdot 1 + 2 = 7 = 10_7$ it gives 1 as a carry. Therefore, $5a_5 + 1 = 0 \pmod{7} \rightarrow a_5 = 4$. Since $a_i = 4$ leads to $a_{i+4} = 4$ the pattern repeats to infinity. Hence,

$$\frac{3}{5} = \dots 125412542_7 = \overline{12542}_7. \tag{B.3}$$

A fraction whose 7-adic representation has a repetition of k digits will have $7^k - 1$ in the denominator or a divisor of it if the numerator and denominator share a common divisor. For $k = 1$ the fraction has $6 = 2 \cdot 3$ in the denominator or a divisor of it. For $k = 2$ the fraction has $48 = 2^4 \cdot 3$ in the denominator or a divisor of it. For $k = 3$ the fraction has $342 = 2 \cdot 3^2 \cdot 19$ in the denominator or a divisor of it. For $k = 4$ the fraction has $2400 = 2^5 \cdot 3 \cdot 5^2$ in the denominator or a divisor of it. In the next table some numbers $7^k - 1$ are factorised.

To obtain a prime factor $p \neq 7$ in the denominator it suffices to consider $k = p - 1$. For instance, 4 is the smallest k for which 5 appears as a fraction of $7^k - 1$ and 10 is the smallest k for which 11 appears as a fraction of $7^k - 1$. It often happens that a prime factor appears for $k < p - 1$. For instance, 3 is the smallest k for which 19 appears as a fraction of $7^k - 1$ and 5 is the smallest k for which 2801 appears as a fraction of $7^k - 1$. If a prime factor p appears for $k < p - 1$ then the smallest k is a divisor of $p - 1$.

k	$7^k - 1$	factors
1	6	$2^1 3^1$
2	48	$2^4 3^1$
3	342	$2^1 3^2 19^1$
4	2400	$2^5 3^1 5^2$
5	16806	$2^1 3^1 2801^1$
6	117648	$2^4 3^2 19^1 43^1$
7	823542	$2^1 3^1 29^1 4733^1$
8	5764800	$2^6 3^1 5^2 1201^1$
9	40353606	$2^1 3^3 19^1 37^1 1063^1$
10	282475248	$2^4 3^1 11^1 191^1 2801^1$
11	1977326742	$2^1 3^1 1123^1 293459^1$
12	13841287200	$2^5 3^2 5^2 13^1 19^1 43^1 181^1$
13	96889010406	$2^1 3^1 16148168401^1$
14	678223072848	$2^4 3^1 29^1 113^1 911^1 4733^1$
15	4747561509942	$2^1 3^2 19^1 31^1 2801^1 159871^1$
16	33232930569600	$2^7 3^1 5^2 17^1 1201^1 169553^1$
17	232630513987206	$2^1 3^1 14009^1 2767631689^1$
18	1628413597910448	$2^4 3^3 19^1 37^1 43^1 1063^1 117307^1$
19	11398895185373142	$2^1 3^1 419^1 4534166740403^1$
20	79792266297612000	$2^5 3^1 5^3 11^1 191^1 281^1 2801^1 4021^1$
21	558545864083284006	$2^1 3^2 19^1 29^1 4733^1 11898664849^1$
22	3909821048582988048	$2^4 3^1 23^1 1123^1 293459^1 10746341^1$
23	27368747340080916342	$2^1 3^1 47^1 3083^1 31479823396757^1$
24	191581231380566414400	$2^6 3^2 5^2 13^1 19^1 43^1 73^1 181^1 193^1 409^1 1201^1$
25	1341068619663964900806	$2^1 3^1 2551^1 2801^1 31280679788951^1$
26	9387480337647754305648	$2^4 3^1 53^1 228511817^1 16148168401^1$
27	65712362363534280139542	$2^1 3^4 19^1 37^1 109^1 811^1 1063^1 2377^1 2583253^1$
28	459986536544739960976800	$2^5 3^1 5^2 29^1 113^1 911^1 4733^1 13564461457^1$
29	3219905755813179726837606	$2^1 3^1 59^1 127540261^1 71316922984999^1$
30	22539340290692258087863248	$2^4 3^2 11^1 19^1 31^1 43^1 191^1 2801^1 159871^1 6568801^1$

Appendix C

Two binomial identities

Here we will prove two identities for binomials. The first one is

$$\sum_{k=0}^{m-1} (2m - 2k) \binom{2m}{k} = m \binom{2m}{m}. \quad (\text{C.1})$$

We start splitting the sum in two sums:

$$\sum_{k=0}^{m-1} (2m - 2k) \binom{2m}{k} = \sum_{k=0}^{m-1} 2m \binom{2m}{k} - \sum_{k=1}^{m-1} 2k \binom{2m}{k}. \quad (\text{C.2})$$

It can also be written as

$$\sum_{k=0}^{m-1} (2m - 2k) \binom{2m}{k} = 2m \binom{2m}{m} + 2m \sum_{k=0}^{m-1} \binom{2m}{k} - 2 \sum_{k=1}^m k \binom{2m}{k}. \quad (\text{C.3})$$

Using

$$k \binom{2m}{k} = \frac{2m!k}{(2m-k)!k!} = \frac{(2m-1)!2m}{(2m-k)!(k-1)!} = 2m \binom{2m-1}{k-1} \quad (\text{C.4})$$

we get

$$\sum_{k=0}^{m-1} (2m - 2k) \binom{2m}{k} = 2m \binom{2m}{m} + 2m \sum_{k=0}^{m-1} \binom{2m}{k} - 2 \sum_{k=1}^m 2m \binom{2m-1}{k-1}. \quad (\text{C.5})$$

Changing variables in the most right sum we obtain

$$\sum_{k=0}^{m-1} (2m - 2k) \binom{2m}{k} = 2m \binom{2m}{m} + 2m \sum_{k=0}^{m-1} \binom{2m}{k} - 2 \sum_{j=0}^{m-1} 2m \binom{2m-1}{j}. \quad (\text{C.6})$$

Since $\sum_{j=0}^{m-1} 2m \binom{2m-1}{j}$ is identical to $\sum_{k=0}^{m-1} 2m \binom{2m-1}{k}$ and since

$$2m \binom{2m-1}{k} = 2m \binom{2m-1}{2m-k-1} = (2m-k) \binom{2m}{2m-k} = (2m-k) \binom{2m}{k}, \quad (\text{C.7})$$

there holds

$$\sum_{k=0}^{m-1} (2m-2k) \binom{2m}{k} = 2m \binom{2m}{m} + 2m \sum_{k=0}^{m-1} \binom{2m}{k} - 2 \sum_{k=0}^{m-1} (2m-k) \binom{2m}{k}. \quad (\text{C.8})$$

The latter implies,

$$\sum_{k=0}^{m-1} (2m-2k) \binom{2m}{k} = 2m \binom{2m}{m} - 2 \sum_{k=0}^{m-1} (m-k) \binom{2m}{k}. \quad (\text{C.9})$$

Hence

$$2 \sum_{k=0}^{m-1} (2m-2k) \binom{2m}{k} = 2m \binom{2m}{m} \quad \square \quad (\text{C.10})$$

The second binomial identity we will prove here is

$$\sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = \frac{m}{2} \binom{2m}{m}. \quad (\text{C.11})$$

We start splitting the sum in two sums:

$$\sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = \sum_{k=0}^{m-1} (2m-1) \binom{2m-1}{k} - 2 \sum_{k=1}^{m-1} k \binom{2m-1}{k}. \quad (\text{C.12})$$

It can also be written as

$$\sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = m \binom{2m}{m} + (2m-1) \sum_{k=0}^{m-1} \binom{2m-1}{k} - 2 \sum_{k=1}^m k \binom{2m-1}{k}. \quad (\text{C.13})$$

Using

$$k \binom{2m-1}{k} = \frac{(2m-1)!k}{(2m-1-k)!k!} = \frac{(2m-2)!(2m-1)}{(2m-1-k)!(k-1)!} = (2m-1) \binom{2m-2}{k-1} \quad (\text{C.14})$$

we get

$$\sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = m \binom{2m}{m} + (2m-1) \sum_{k=0}^{m-1} \binom{2m-1}{k} - 2 \sum_{k=1}^m (2m-1) \binom{2m-2}{k-1}. \quad (\text{C.15})$$

Changing variables in the most right sum we obtain

$$\sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = m \binom{2m}{m} + (2m-1) \sum_{k=0}^{m-1} \binom{2m-1}{k} - 2 \sum_{j=0}^{m-1} (2m-1) \binom{2m-2}{j}. \quad (\text{C.16})$$

Since $\sum_{j=0}^{m-1} (2m-1) \binom{2m-2}{j}$ is identical to $\sum_{k=0}^{m-1} (2m-1) \binom{2m-2}{k}$ and since

$$(2m-1) \binom{2m-2}{k} = (2m-1-k) \binom{2m-1}{2m-1-k} = (2m-1-k) \binom{2m-1}{k}, \quad (\text{C.17})$$

there holds

$$\sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = m \binom{2m}{m} + (2m-1) \sum_{k=0}^{m-1} \binom{2m-1}{k} - \sum_{k=0}^{m-1} (4m-2-2k) \binom{2m-1}{k}. \quad (\text{C.18})$$

The latter implies,

$$\sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = m \binom{2m}{m} - \sum_{k=0}^{m-1} (2m-1-2k) \binom{2m}{k}. \quad (\text{C.19})$$

Hence

$$2 \sum_{k=0}^{m-1} (2m-1-2k) \binom{2m-1}{k} = m \binom{2m}{m} \quad \square \quad (\text{C.20})$$

Bibliography

- [1] S. Wolfram, Statistical Mechanics of Cellular Automata, *Rev. Mod. Phys.* , **55**, 601-644 (1983)
- [2] S. Wolfram, *A New Kind of Science*, Wolfram Media, Champaign IL., (2002)
- [3] N.J.A. Sloane, *The Online Encyclopedia of Integer Sequences*, <https://oeis.org>
- [4] D. Richeson, *A 10-adic number that is a zero divisor*, <https://divisbyzero.com/2008/12/29/a-10-adic-number-that-is-a-zero-divisor/>
- [5] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. *J. reine u. angew. Math.*, **44**, 93-146 (1852)
- [6] A.M. Legendre, *Théorie des Nombres*, **Vol.II**, 3rd ed., Firmin Didot Freres, Paris (1930)
- [7] D. Singmaster, Repeated binomial coefficients and Fibonacci numbers, *Fibonacci Quart.* **13**, 295-298 (1975)
- [8] J. Sharesian and R. Woodroffe, Divisibility of binomial coefficients and generation of alternating groups, arXiv:1505.05143v3 (2017)
- [9] S. Casacuberta, On the divisibility of binomial coefficients, arXiv:1906.07652v1 (2019)
- [10] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.*, **1**, 184-240 (1878).
- [11] N. J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly*, **54**, 589-592 (1947).