Quantum Pascal's Triangle and Sierpinski's carpet

Tom Bannink* Harry Buhrman*‡

bannink@cwi.nl buhrman@cwi.nl

August 2017

Abstract

In this paper we consider a quantum version of Pascal's triangle. Pascal's triangle is a well-known triangular array of numbers and when these numbers are plotted modulo 2, a fractal known as the Sierpinski triangle appears. We first prove the appearance of more general fractals when Pascal's triangle is considered modulo prime powers. The numbers in Pascal's triangle can be obtained by scaling the probabilities of the simple symmetric random walk on the line. In this paper we consider a quantum version of Pascal's triangle by replacing the random walk by the quantum walk known as the Hadamard walk. We show that when the amplitudes of the Hadamard walk are scaled to become integers and plotted modulo three, a fractal known as the Sierpinski carpet emerges and we provide a proof of this using Lucas's theorem. We furthermore give a general class of quantum walks for which this phenomenon occurs.

1 Introduction

Pascals's triangle exhibits many interesting properties one of which is the appearance of a fractal when the numbers are considered modulo a prime p [3, 4]. This is shown in Figure 2, and for $p = 2$ the fractal is known as the Sierpinski triangle or Sierpinski gasket. One way of obtaining the numbers in Pascal's triangle is through a random walk on a line. This paper explores the results of replacing the 1-dimensional random walk by a quantum walk. This too yields the Sierpinski triangle when the numbers are considered modulo 2, but more interestingly one can find another fractal known as the Sierpinski carpet hidden in the amplitudes modulo 3 which is not present in Pascal's triangle. When these quantum walk numbers are plotted modulo p, more general fractals appear.

*QuSoft and CWI Amsterdam, Science Park 123, 1098 XG Amsterdam, The Netherlands

‡University of Amsterdam, Science Park 904, 1098 XH Amsterdam, The Netherlands

	Pascal's triangle	Hadamard walk	General quantum walk
mod 2	Triangle_2	Triangle_2	Triangle_2
mod 3	Triangle_3	Carpet	Carpet or Triangle_3
mod p	Triangle_p	See Figure 10	See Figure 10
mod p^k	Triangle_p level k	More complicated fractal	

Table 1: Summary of the fractals that result from considering various sets of numbers modulo a prime p or prime power. Triangle_p refers to the version of the Sierpinski triangle where $p(p+1)/2$ copies of the triangle are found in every recursion level. See Figure 2 for $p \in \{2, 3, 5, 7\}$. The level k triangle is discussed in Section 2.2. Carpet refers to the Sierpinski carpet as shown in Figure 7.

Table 1 provides a summarising overview of the different fractals that are obtained from these different sources. Whereas the quantum walk probabilities contain the Sierpinski carpet, the classical set of numbers only gives various versions of the Sierpinski triangle and the carpet is never found. We therefore suggest that the carpet might be a signature of the quantum properties which the classical random walk does not possess.

There are other possible notions of a quantum version of Pascal's triangle that can be found in the literature. For instance, one can consider a triangle consisting of the so-called q-deformed binomial coefficients. This can be thought of as representing a Galton board but where the particles are subject to a magnetic field [7]. This triangle is sometimes called the q-Pascal's triangle, studied for example in [8] and [9]. However, these approaches are different from ours and give rise to different sets of numbers.

Section 2 provides background information on how Pascal's triangle is related to the Sierpinski triangle when the numbers are taken modulo a prime. In Section 2.2 we provide a proof of the appearance of a more general version of the Sierpinski triangle when instead we take prime *powers*. Then, in Section 3, quantum walks are introduced with an emphasis on a walk that is commonly known as the Hadamard walk. We derive an expression for the probabilities of these walks and then the appearance of both the Sierpinski triangle and Sierpinski carpet is shown as well as some other properties. In Section 4 we argue that the appearance of the carpet can be a sign of the quantum nature of the probability distribution.

2 Pascal's triangle

Pascal's triangle is an array of integers arranged in a triangle, where the k'th value in the n'th row (both n and k start at zero) is the binomial coefficient $\binom{n}{k}$. As shown in Figure 1, it can be thought of as probabilities of a symmetric random walk on $\mathbb{Z}$ scaled by a factor 2^n in the n'th row.

(a)

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

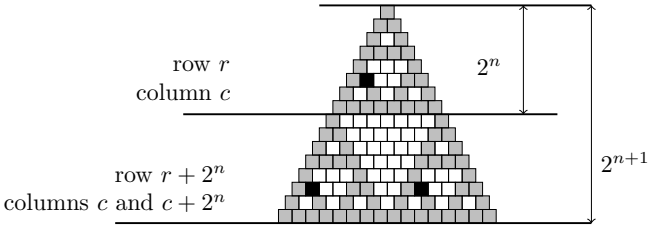
(b)

$$\begin{array}{ccccccccc} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 & \frac{2}{4} & 0 & \frac{1}{4} & 0 & 0 \\ 0 & \frac{1}{8} & 0 & \frac{3}{8} & 0 & \frac{3}{8} & 0 & \frac{1}{8} & 0 \\ \frac{1}{16} & 0 & \frac{4}{16} & 0 & \frac{6}{16} & 0 & \frac{4}{16} & 0 & \frac{1}{16} \end{array}$$

Figure 1: The top five rows of Pascal's triangle (a) and the probabilities of the first 5 steps of a random walk (b). The probabilities equal to zero in (b) are in light-grey for clarity.

2.1 Pascal's triangle modulo a prime

One of the interesting features of Pascal's triangle comes from considering all numbers modulo a prime p [3] as shown in Figure 2. The appearing figure approaches the fractal known as the Sierpinski triangle (or the Sierpinski gasket). This can be proven by showing that for all n, the shape given by the first p^{n+1} rows contains exactly $p(p+1)/2$ copies of the first p^n rows, and nothing more than those copies, i.e. with 'white' in-between.



If we index Pascal's triangle by row r and column c then we need to show that

$$(\text{"copies"})\ \forall\ 0 \le q \le l < p,\ 0 \le c \le r < p^n \qquad \binom{r}{c} \equiv \binom{r + l \cdot p^n}{c + q \cdot p^n} \mod p, \quad (1)$$

$$(\text{"empty"})\ \forall\ 0 \le q < l < p,\ 0 \le r < c < p^n \qquad 0 \equiv \binom{r + l \cdot p^n}{c + q \cdot p^n} \mod p. \quad (2)$$

The values of (l, q) index the $p(p+1)/2$ copies. These equations follow easily from Lucas's theorem. We represent a number by it's base-p digits as

$$n = [n_m n_{m-1} \cdots n_0]_p = \sum_{j=0}^{m} n_j\ p^j \qquad \text{with } 0 \le n_i < p \text{ for each } i.$$

Theorem (Luc1878)**.** *Let p be prime and n, k non-negative integers. Let $n = [n_m \cdots n_0]_p$ and $k = [k_m \cdots k_0]_p$. Define $\binom{a}{b} = 0$ for $a < b$. Then*

$$\binom{n}{k} \equiv \binom{n_m}{k_m}\binom{n_{m-1}}{k_{m-1}} \cdots \binom{n_0}{k_0} \mod p.$$

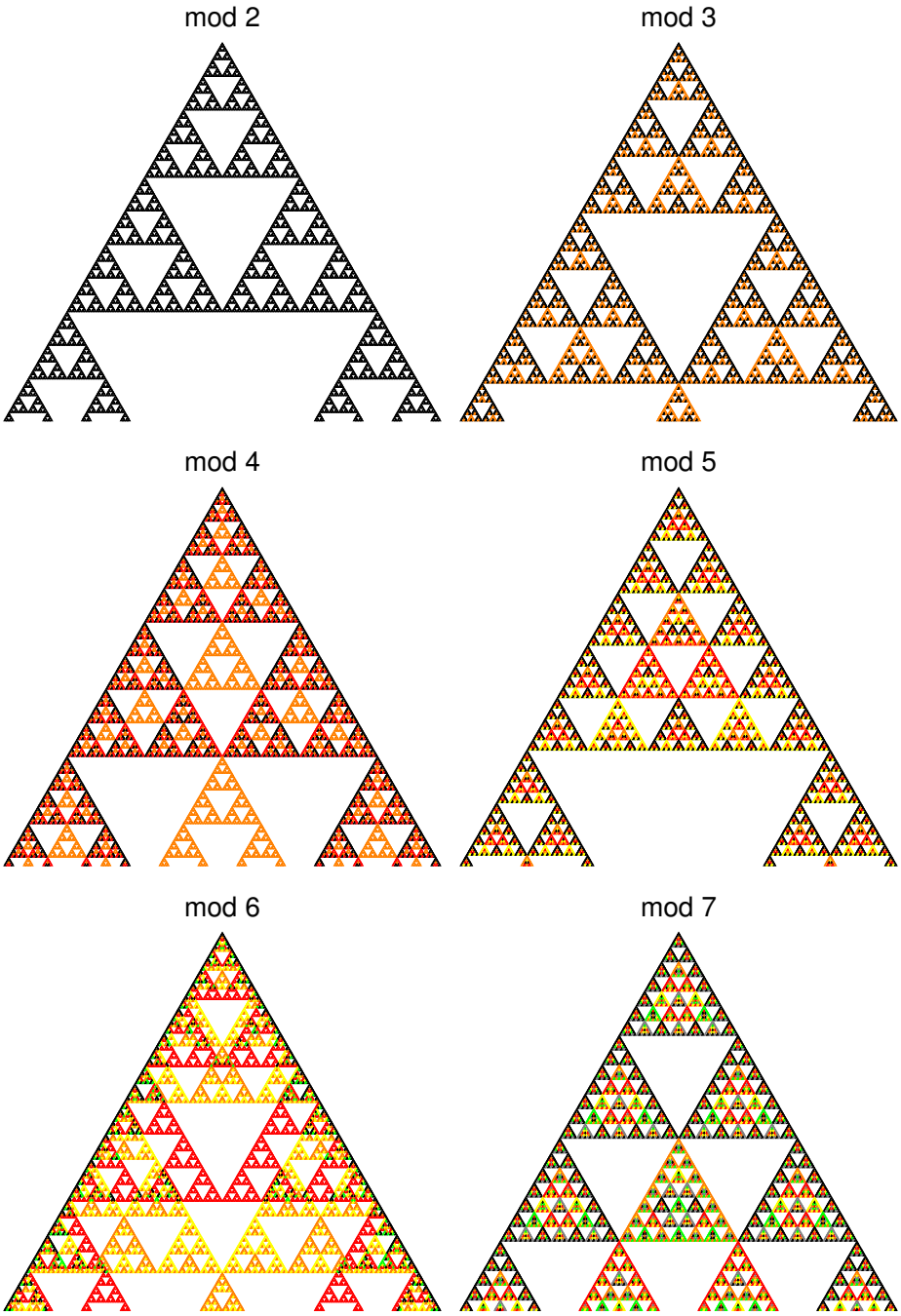


Figure 2: The first 180 of rows of Pascal's triangle shown modulo n where $n \in \{2, 3, 4, 5, 6, 7\}$. If a value was zero modulo n it is coloured white, otherwise it is given a different colour.

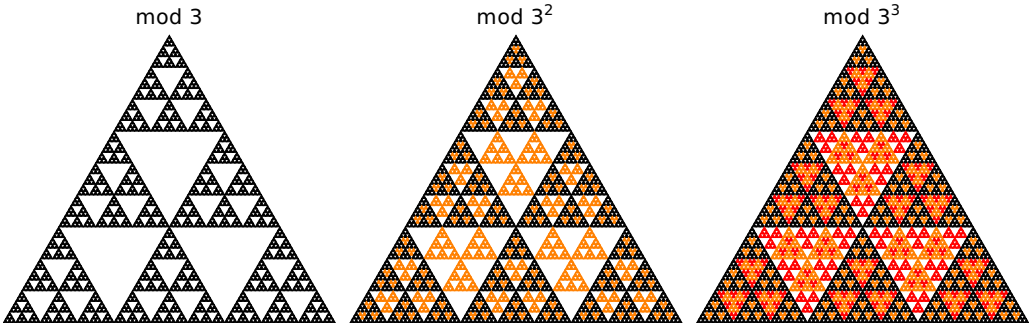


Figure 3: Pascal's triangle plotted modulo powers of 3. The colours give the 3-adic valuation $\nu_3(\binom{r}{c})$, where black is 0, orange is 1 and red is 2.

This famous theorem knows many extensions and generalisations, see for example [11]. A moments thought shows the following corollaries.

Corollary 1 (Anton's Lemma)**.** *If $n, k < p^m$ and then for all $l, q \geq 0$,*

$$\binom{l \cdot p^m + n}{q \cdot p^m + k} \equiv \binom{l}{q}\binom{n}{k} \mod p.$$

Corollary 2. *For any prime p,*

$$\binom{n}{k} \equiv 0 \mod p \quad \iff \quad \exists i \ : \ k_i > n_i$$

Corollary 1 adds the extra digits l to n and q to k and by induction it implies Lucas's theorem. Equation (1) follows from Corollary 1 and (2) follow from 2 by noting that for $r < c$ there is an i such that $c_i > r_i$.

2.2 Pascals triangle modulo general integers

One can plot Pascal's triangle modulo general n, shown in Figure 2 for $n \in \{2, 3, 4, 5, 6, 7\}$. Primes were discussed in the previous section. When $n = p_1^{k_1} \cdots p_m^{k_m}$ then the shape is the union of the ones for the prime powers $p_i^{k_i}$ albeit with different colours. For example, at $n = 6$, shown in Figure 2, one can see the union of the shapes of $p = 2$ and $p = 3$. This is simply because $x \equiv 0 \mod n$ if and only if for all i we have $x \equiv 0 \mod p_i^{k_i}$.

When $n = p^k$ is a prime power then the pattern becomes more involved. Figure 3 shows what happens for powers of 3 from which we can see the general pattern which we capture in the following definition.

Definition. For prime p and $k \geq 1$, define the level-k Sierpinski-p triangle as follows. For $k = 1$ it is defined as the normal Sierpinski triangle with $p(p+1)/2$ copies at each recursion step. The level $k+1$ triangle is obtained from the level k triangle by adding $p(p-1)/2$ copies of the level-1 triangle in every empty region of the level-k triangle.

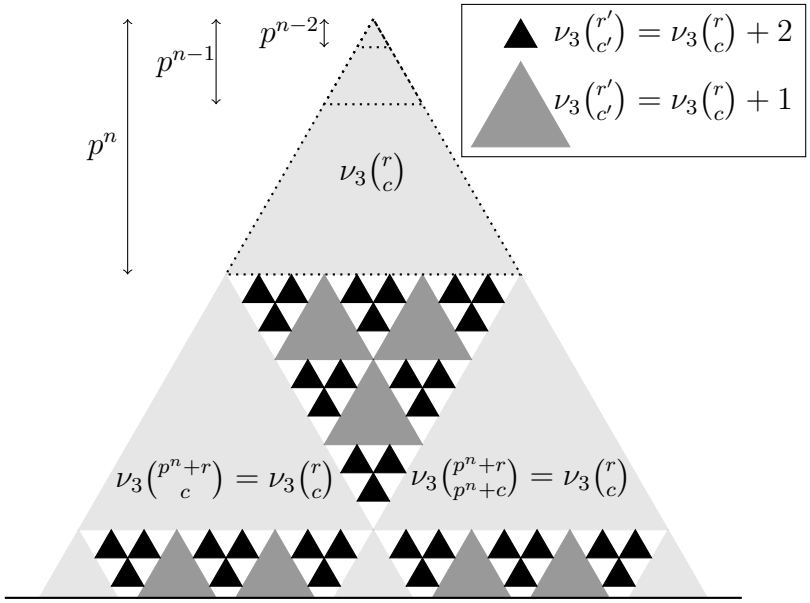


Figure 4: Schematic overview of the statements of Lemma 1, here shown for $p = 3$. We show that for a number $\binom{r}{c}$, the p-adic valuation in the other size-p^n triangles, i.e. $\binom{l\cdot p^n+r}{q\cdot p^n+c}$, is the same and for the smaller triangles of size p^{n-k}, the p-adic valuation is k higher.

Lemma 1. *For prime p and $k \geq 1$, the values of Pascal's triangle modulo p^k converge to the level-k Sierpinski-p triangle.*

To prove this we require the following definition.

Definition. The p-adic valuation $\nu_p(n)$ of n is the largest power of p that divides n.

When colouring the triangle we only care whether or not a number is zero modulo p^k. Since $n \equiv 0 \mod p^k$ if and only if $\nu_p(n) \geq k$ we have

Observation. *If $\nu_p(n) = \nu_p(m)$ then for any k: $n \equiv 0 \mod p^k \iff m \equiv 0 \mod p^k$.*

This reduces the problem to showing that the p-adic evaluation of certain binomial coefficients are equal. The statements that we want to prove are most easily explained with a picture, shown in Figure 4. We will show that at each recursion level of the triangle, the p-adic valuation of the numbers $\binom{r'}{c'}$ in a copy is the same as that of the corresponding number $\binom{r}{c}$ in the original region. Furthermore, we show that the smaller triangles of size p^{n-k} inside the regions that were empty in the 'mod p triangle' have p-adic valuations that are k higher than their original.

Repeating what we did before for the mod p triangle, we can see that at recursion level n, the "copies" and "empty regions" correspond to the following binomial coefficients:

$$\binom{l \cdot p^n + r}{q \cdot p^n + c} \qquad \begin{array}{ll} \text{"copies"} \rightarrow & 0 \leq q \leq l < p\ ,\ 0 \leq c \leq r < p^n \\ \text{"empty"} \rightarrow & 0 \leq q < l < p\ ,\ 0 \leq r < c < p^n \end{array} .$$

Here (l, q) index the different copies or empty regions whereas r and c index points within those regions. The proof for the copies is done below in Claim 1. The proof for the empty regions is done in Claim 2 and Claim 3.

We first require Kummer's theorem.

Theorem (Kum1852)**.** *Let p be prime and n, k non-negative integers, $n \geq k$. Then the p-adic valuation $\nu_p(\binom{n}{k})$ of $\binom{n}{k}$ is equal to the number of "carries" when k and $n-k$ are added in base-p arithmetic.*

To find the number of carries that occur when k is added to $n-k$ in base-p, consider the base-p digits of n and k, and define

$$c_{-1}^{n,k} = 0, \qquad c_i^{n,k} = \begin{cases} 1 & n_i < k_i \\ 0 & n_i > k_i \\ c_{i-1}^{n,k} & n_i = k_i \end{cases}.$$

The number of carries is equal to $\sum_{i \geq 0} c_i^{n,k}$. Kummer's theorem states $\nu_p(\binom{n}{k}) = \sum_{i \geq 0} c_i^{n,k}$.

Claim 1. *Let p be prime and n, k, q, l, m non-negative integers with $0 \leq k \leq n < p^m$ and $0 \leq q \leq l < p$. Then*

$$\nu_p(\binom{l \cdot p^m + n}{q \cdot p^m + k}) = \nu_p(\binom{n}{k})$$

Proof. Define $n' = l \cdot p^m + n$ and $k' = q \cdot p^m + k$, which differ only from n, k in the m-th digit in base p. Therefore $c_i^{n,k} = c_i^{n',k'}$ for $i < m$, and

$$c_m^{n',k'} = \begin{cases} 1 & l < q \\ 0 & l > q \\ c_{m-1}^{n,k} & l = q \end{cases}.$$

By Kummer's theorem it remains to show that $c_m^{n',k'} = 0$. By assumption we know $q \leq l$ so the only non-trivial case is $l = q$ where $c_m^{n',k'} = c_{m-1}^{n,k}$. If $n = k$ then all the $c_i^{n,k}$ are zero so we are done. If $n \neq k$ then the consider the most significant digit where n and k differ, i.e. take the highest i for which $n_i \neq k_i$ and call it i^*. Since $k < n$ by assumption, it must be true that $k_{i^*} < n_{i^*}$ and therefore $c_{i^*}^{n,k} = 0$. For all $i > i_*$ we have $n_i = k_i$ so $c_{m-1}^{n,k} = c_{i^*}^{n,k}$. □

Claim 2. *Let r', c' be the row and column of a point in a size-p^{n-k} triangle that lies in the empty region of the base triangle, see the darker shaded triangles in Figure 4. Then $\nu_p(\binom{r'}{c'}) = \nu_p(\binom{r}{c}) + k$ where r, c are the row and column in the original smaller triangle.*

Proof. The smaller triangles of size p^{n-k} can be indexed as follows. Let $0 \leq c \leq r < p^{n-k}$ represent a point in this triangle. The location of the copy at r', c' somewhere in the

empty region of the larger triangle can be written as $r' = [r'_n \cdots r'_{n-k} r_{n-k-1} \cdots r_0]_p$ and $c' = [c'_n \cdots c'_{n-k} c_{n-k-1} \cdots c_0]_p$ with the following constraints on the newly added digits. Similar to the proof of Claim 1 we consider the carries $c_i^{r',c'}$.

$$\begin{aligned}
0 \le c'_n < r'_n < p \qquad & c_n^{r',c'} = 0 \\
0 \le r'_{n-1} \le c'_{n-1} < p \qquad & c_{n-1}^{r',c'} = 1 \text{ or } c_{n-1}^{r',c'} = c_{n-2}^{r',c'} \\
\vdots \qquad & \vdots \\
0 \le r'_{n-k+1} \le c'_{n-k+1} < p \qquad & c_{n-k+1}^{r',c'} = 1 \text{ or } c_{n-k+1}^{r',c'} = c_{n-k}^{r',c'} \\
0 \le r'_{n-k} < c'_{n-k} < p \qquad & c_{n-k}^{r',c'} = 1 \\
0 \le c \le r < p^{n-k} \qquad & \nu_3 \binom{r}{c}.
\end{aligned}$$

The extra carries sum to k, so by Kummer's theorem this completes the proof. □

We still have to show that the empty regions in the 'mod p^k triangle' are indeed empty.

Claim 3. *Let r', c' be the row and column in the empty region of the 'mod p^k triangle'. Then $\nu_p(\binom{r'}{c'}) \ge k+1$.*

Proof. These values of r', c' have the same constraints on the digits as in the proof of Claim 2 except for $0 \le r'_{n-k} \le c'_{n-k} < p$ and $0 \le r < c < p^{n-k}$. We can apply the same idea as in the proof of Claim 1 by noting that the first digit where r and c differ will satisfy $r_{i^*} < c_{i^*}$ and hence all the carries $c_i^{r',c'}$ are 1 for $i \ge i^*$. This gives $\nu_3\binom{r'}{c'} \ge k+1$. □

3 Hadamard Walk

Quantum walks are simple models for a quantum particle moving through some system. This paper is only concerned with the probability distributions that emerge from them, and therefore the physical aspects are left out. We refer the reader to [10] for a complete introduction to the field of quantum information. The state of a particle is described by a unit vector in a complex Hilbert space, and quantum mechanics dictates that time evolution is limited to applying unitary operators to this vector. We use the 'bra-ket' notation, writing $|\psi\rangle$ for a vector as opposed to $\vec{\psi}$. We can write $|\psi\rangle$ in an orthonormal basis, $|\psi\rangle = \sum_i \alpha_i |x_i\rangle$ where $\alpha_i \in \mathbb{C}$ and $\sum_i |\alpha_i|^2 = 1$. The $|x_i\rangle$ form a basis of the Hilbert space and the coefficients α_i are known as *amplitudes*. One of the axioms of quantum mechanics states that one can observe (measure) the state $|\psi\rangle$ in a chosen basis and the result is $|x_i\rangle$ with probability $|\alpha_i|^2$.

A simple example of a quantum walk on a one-dimensional line is the Hadamard walk [6] on the Hilbert space $\mathcal{H} = \text{span}\{|n, c\rangle \mid n \in \mathbb{Z}, c \in \{\uparrow, \downarrow\}\}$. The particle has an internal degree of freedom other than its position, often called the *coin state* of the particle. The

most general state of the particle is $|\psi\rangle = \sum_{n\in\mathbb{Z}} (\alpha_{n,\uparrow}|n,\uparrow\rangle + \alpha_{n,\downarrow}|n,\downarrow\rangle)$, with normalization $\sum_{n\in\mathbb{Z}} (|\alpha_{n,\uparrow}|^2 + |\alpha_{n,\downarrow}|^2) = 1$. The dynamics of the particle are given by repeated application of a unitary operator U that consists of two steps. The first step is a 'coin flip', a unitary matrix H known as the Hadamard matrix that is only applied to the internal state

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ where } |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The second step updates the position conditioned on the outcome of the coin,

$$S|n,\uparrow\rangle = |n+1,\uparrow\rangle, \qquad S|n,\downarrow\rangle = |n-1,\downarrow\rangle.$$

The time evolution operator U is then given by $U = S \cdot (\mathrm{Id}_{\text{position}} \otimes H)$, so a full step of the Hadamard walk, acting on the basis state $|n,\downarrow\rangle$ for example, is given by

$$U|n,\downarrow\rangle \overset{\text{coin}}{=} S\left(\frac{1}{\sqrt{2}}|n,\uparrow\rangle - \frac{1}{\sqrt{2}}|n,\downarrow\rangle\right) \overset{\text{shift}}{=} \frac{1}{\sqrt{2}}|n+1,\uparrow\rangle - \frac{1}{\sqrt{2}}|n-1,\downarrow\rangle.$$

If we now were to measure the system, the result would be either $|n+1,\uparrow\rangle$ or $|n-1,\downarrow\rangle$, both with probability $|\pm 1/\sqrt{2}|^2 = 1/2$. In this paper we will always use $|0,\uparrow\rangle$ as the starting state. The amplitudes of the first five steps of the resulting walk are shown in Figure 6.

3.1 Expressions for amplitudes

Meyer [5] gave explicit expressions for the amplitudes of the Hadamard walk. We will give a slightly shorter proof of this for a general coin operator, i.e. replace H by some general matrix C. This proof also allows us to make an additional observation stated in the lemma below. Let C be any unitary 2x2 matrix. Any such matrix can be written as follows

$$C = \begin{pmatrix} c_r & c_u \\ c_d & c_l \end{pmatrix} = \begin{pmatrix} \sqrt{p}\, e^{i\alpha} & \sqrt{1-p}\, e^{i\beta} \\ -\sqrt{1-p}\, e^{i\gamma} & \sqrt{p}\, e^{i(\gamma+\beta-\alpha)} \end{pmatrix} \quad , \quad \text{with } 0 \le p \le 1.$$

Lemma. *Let $\psi_\uparrow(n,t)$ and $\psi_\downarrow(n,t)$ be the up and down amplitudes at position n at time t for the quantum walk with coin operator C starting in the state $|0,\uparrow\rangle$. When $t+n$ is odd or when $|n| > t$ we have $\psi_\uparrow(n,t) = \psi_\downarrow(n,t) = 0$. Otherwise the amplitudes are given by*

$$\psi_\uparrow(n,t) = \begin{cases} e^{i\alpha n}\sqrt{p^t} & n = t \\ e^{i(\alpha n + (\gamma+\beta)(t-n)/2)}\sqrt{p^t}\sum_{k\ge 1}\binom{(t+n)/2}{k}\binom{(t-n)/2-1}{k-1}\left(-\frac{1-p}{p}\right)^k & n < t \end{cases}$$

$$\psi_\downarrow(n,t) = -e^{i(\alpha n + (\gamma+\beta)(t-n)/2 - \beta)} \times \sqrt{(1-p)p^{t-1}}\sum_{k\ge 0}\binom{\frac{t+n}{2}}{k}\binom{\frac{t-n}{2}-1}{k}\left(-\frac{1-p}{p}\right)^k$$

The probabilities $|\psi_\uparrow(n,t)|^2$ and $|\psi_\downarrow(n,t)|^2$ associated to these amplitudes are independent of the complex phases α, β, γ of the coin operator.

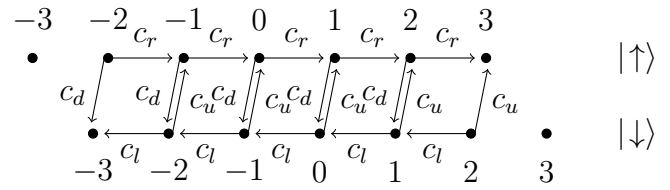


Figure 5: Schematic representation of one step U of the walk with generic coin.

Note that for a more general starting state, not equal to $|0,\uparrow\rangle$, the probabilities *do* depend on the complex phases present in the coin operator.

Proof. We sum over all possible paths on the directed graph shown in Figure 5, starting at $|0,\uparrow\rangle$ and ending at the desired state, where each path gets a complex amplitude.

Up component. If $n = t$ there is exactly one path from $|0,\uparrow\rangle$ to $|n,\uparrow\rangle$ and it has amplitude $(c_r)^t$. Now assume $-t < n < t$ and let r, l, u, d be the number of times a path uses the right, left, up and down arrows respectively. To end at $|n,\uparrow\rangle$ we require

$$\begin{aligned} r + l + u + d &= t && \text{total number of steps,} \\ r - l &= n && \text{ending column,} \\ u &= d && \text{start up and end up.} \end{aligned}$$

Let $k = u = d$, then we have $r = \frac{t+n}{2} - k$ and $l = \frac{t-n}{2} - k$. We have $k \geq 1$ (we need to go down and up at least once) and $k \leq \frac{t-n}{2}, \frac{t+n}{2}$. For fixed r, l, u, d, the particle is in the $|\uparrow\rangle$ state (top layer) $k + r = \frac{t+n}{2}$ times, out of which r times it goes right and k times it goes down. This can be done in $\binom{(t+n)/2}{k}$ possible ways. Likewise, the particle is in the $|\downarrow\rangle$ state (bottom layer) $l + k = \frac{t-n}{2}$ times and has to choose between left and up. The *last* of these choices should always be up, so this gives $\binom{(t-n)/2-1}{k-1}$ possibilities. These choices uniquely determine the path, and the amplitude of such a path is $(c_r)^r (c_l)^l (c_u)^u (c_d)^d$, therefore

$$\psi_\uparrow(n,t) = \begin{cases} (c_r)^t & n = t \\ \sum_{k\geq 1} \binom{(t+n)/2}{k} \binom{(t-n)/2-1}{k-1} c_r^{(t+n)/2-k} c_l^{(t-n)/2-k} c_u^k c_d^k & n < t \end{cases}.$$

The sum above in terms of p and α, β, γ is equal to

$$e^{i(\alpha n + (\gamma+\beta)(t-n)/2)} \sqrt{p^t} \sum_{k\geq 1} \binom{(t+n)/2}{k} \binom{(t-n)/2-1}{k-1} \left(-\frac{1-p}{p}\right)^k,$$

as claimed. Note that $-\frac{1-p}{p}$ is always a real (negative) number, regardless of the complex phases present in the entries of the coin matrix. The probability $|\psi_\uparrow(n,t)|^2$ of being at $|n,\uparrow\rangle$

after t steps when starting in $|0,\uparrow\rangle$ is independent of α,β,γ since the only dependence on these variables is in the prefactor $e^{i(\alpha n+(\gamma+\beta)(t-n)/2)}$ which always has norm 1.

Down component. For the down component, the equations are similar:

$$\begin{aligned} r+l+u+d &= t && \text{total number of steps,}\\ r-l &= n+1 && \text{ending column (tilted),}\\ u+1 &= d && \text{start up and end down.} \end{aligned}$$

The argument is the same as before, but now the last choice in the top layer has to be 'down' with no restrictions on the last choice in the bottom layer, which yields

$$\psi_{\downarrow}(n,t)=\sum_{k\geq 0}\binom{(t+n)/2}{k}\binom{(t-n)/2-1}{k}c_u^k c_d^{k+1}c_l^{(t-n)/2-k-1}c_r^{(t+n)/2-k}.$$

Rewriting this in terms of p,α,β,γ gives the expression given in the claim. □

3.2 Hadamard triangle

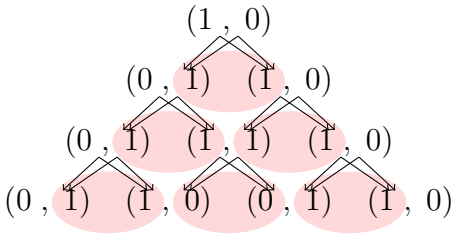
When we scale the amplitudes or probabilities of the Hadamard walk by a factor of $\sqrt{2^n}$ they become integer and we obtain a quantum analogue of Pascal's triangle. Note that we could either use the *amplitudes* or the *probabilities* which are simply their squares. However, since we are primarily interested in whether or not they are divisible by some prime p, squaring the amplitudes does not make a difference. We therefore continue with the (unsquared) amplitudes. Figure 6 shows the start of the Hadamard triangle.

3.3 Hadamard walk modulo 2 - Sierpinski triangle

When the amplitudes of the (scaled) Hadamard walk are plotted modulo two, the Sierpinski triangle appears in a similar fashion to Pascal's triangle. To see why, note that the amplitudes modulo two at time t can be found by considering a process where *every* time-step is done modulo two. The scaled Hadamard operator becomes

$$\sqrt{2}H \equiv \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \mod 2,$$

and we can immediately see that the amplitude sent to the right is the same as the amplitude sent to the left, resulting in the following triangle.



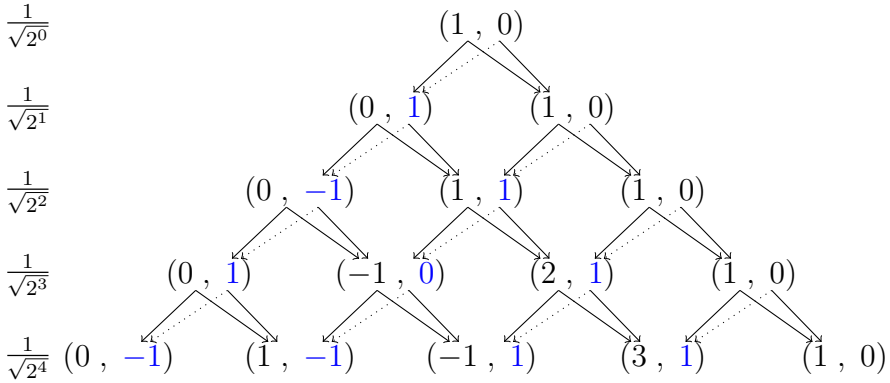


Figure 6: The up- and down-amplitudes of the first steps of the Hadamard walk, starting in $|0,\uparrow\rangle$, where every row is one time-step. The normalisation of a row is shown at the left side. At even timesteps, only the even positions are shown and at odd time-steps only the odd positions are shown, similar to Figure 1. The arrows represent the time-step of the Hadamard walk. A dotted arrow means the incoming amplitude is multiplied by -1 before being added to the other incoming amplitude. The blue colouring denotes the set amplitudes that is used in Section 3.3 and 3.4.

An ellipse is drawn around the pairs of amplitudes of states $|n-1,\downarrow\rangle$ and $|n+1,\uparrow\rangle$ which are always equal modulo two, and are the sum of the values in the two neighbouring ellipses above it. This is the same rule with which Pascal's triangle can be constructed. Indeed, taking one value out of every ellipse gives the Sierpinski triangle.

3.4 Hadamard walk modulo 3 - Sierpinski carpet

We will now show that the $|\downarrow\rangle$ components of the scaled walk (the *blue* values in Figure 6), modulo three, give rise to the Sierpinski carpet. We colour a square white if and only if the amplitude is divisible by 3. Figure 7 shows the start of the resulting fractal. The top of the carpet is at $t = 1$ and $n = -1$ so row r and column c correspond to $t = r + 1$ and $n = 2c - r - 1$. For the structure of the Sierpinski carpet, however, it is more convenient to consider coordinates x, y that are aligned with the square structure of the carpet. The choice of these directions is indicated in Figure 7 and we define $\Phi(x, y)$ as the amplitude at these coordinates

$$\Phi(x,y) = (-1)^y \sum_{k=0}^{\min(x,y)} \binom{x}{k}\binom{y}{k}(-1)^k.$$

A pixel at coordinates x, y is now coloured white if $\Phi(x, y) \equiv 0 \mod 3$ and a different colour otherwise.

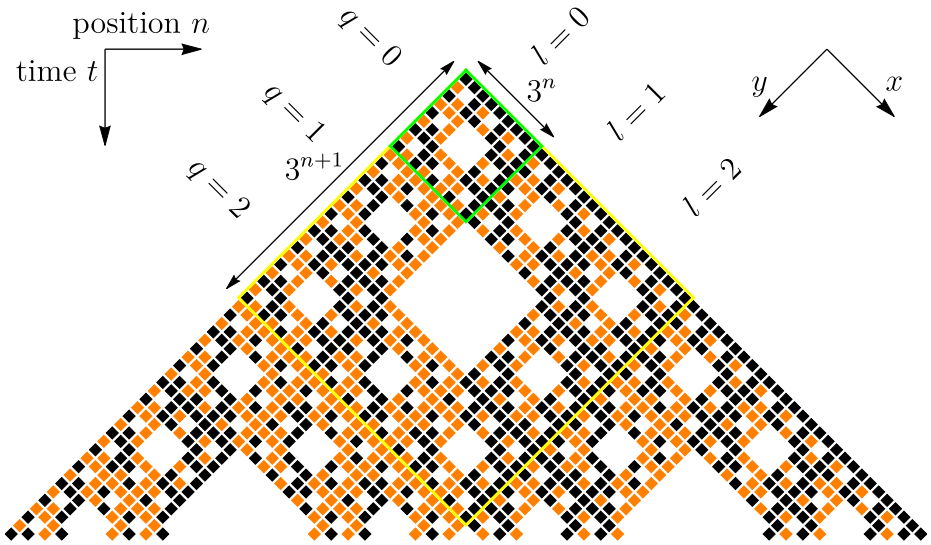


Figure 7: The start of the Sierpinski carpet resulting from colouring the scaled Hadamard walk amplitudes modulo 3. The horizontal direction is position and the vertical direction is time. The shape drawn at each point is a diamond, i.e. a rotated square instead of a square, because this gives a better visualisation of the x, y coordinates.

Lemma 2. *The down components of the Hadamard walk modulo 3, i.e.* $\Phi(x,y) \mod 3$*, give rise to the Sierpsinski carpet.*

To show this we will first prove some other claims.

Definition 1. For any $m \in \mathbb{Z}$ define $f_m : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ as

$$f_m(x,y) = \sum_{k=0}^{\min(x,y)} \binom{x}{k}\binom{y}{k}(-m)^k$$

This function is a special case of the so-called hypergeometric function ${}_2F_1(a,b;c;z)$, namely $f_m(x,y) = {}_2F_1(-x,-y,1,-m)$. The following claim could be seen as something similar to Corollary 1 but for f_m:

Claim 4. *Let p be a prime and let $0 \le l, q \le p-1$. Then we have for all $m \in \mathbb{Z}$ and for all $0 \le x, y \le p^n - 1$*

$$f_m(l \cdot p^n + x\ ,\ q \cdot p^n + y) \equiv f_m(l,q) \cdot f_m(x,y) \mod p.$$

Proof. Note that any sum can be split in the following way:

$$\sum_{k=0}^{p^{n+1}-1} g(k) = \sum_{s=0}^{p-1}\sum_{k=0}^{p^n-1} g(s \cdot p^n + k),$$

where s takes the role of the most significant digit and k takes the role of the other digits. We apply this idea to the sum in $f_m(x,y)$ where we note that $\min(lp^n+x, qp^n+y) \leq p^{n+1}-1$ but we can let the sum range all the way to $p^{n+1}-1$ because the summand is zero in this extra range. Therefore we have

$$\begin{aligned} f_m(l\cdot p^n + x\ ,\ q\cdot p^n + y) &= \sum_{k=0}^{p^{n+1}-1} \binom{l\cdot p^n + x}{k}\binom{q\cdot p^n + y}{k}(-m)^k \\ &= \sum_{s=0}^{p-1}\sum_{k=0}^{p^n-1} \binom{l\cdot p^n + x}{s\cdot p^n + k}\binom{q\cdot p^n + y}{s\cdot p^n + k}(-m)^{s\cdot p^n+k} \end{aligned}$$

Note that by Fermat's little theorem we have $m^p \equiv m \mod p$ so $m^{s\cdot p^n} \equiv m^s \mod p$. Now we apply Corollary 1 to the binomial coefficients to obtain

$$\begin{aligned} f_m(l\cdot p^n + x\ ,\ q\cdot p^n + y) &\equiv \sum_{s=0}^{p-1}\sum_{k=0}^{p^n-1} \binom{l}{s}\binom{q}{s}\binom{x}{k}\binom{y}{k}(-m)^{s+k} \\ &\equiv \left(\sum_{s=0}^{p-1}\binom{l}{s}\binom{q}{s}(-m)^s\right) f_m(x,y) \\ &\equiv f_m(l,q)\cdot f_m(x,y) \mod p, \end{aligned}$$

as required. □

Note that l, q take the role of the most significant digits and x, y are the other digits. Just as Corollary 1 implies Lucas's theorem, we can apply this claim inductively on the number of digits to arrive at a result very similar to Lucas's theorem but now for the function f_m:

Corollary 3 (Lucas'-like theorem for f_m)**.** *Let p be prime and x, y non-negative integers. Let $x = [x_n x_{n-1}\cdots x_0]_p$ and $y = [y_n y_{n-1}\cdots y_0]_p$. Then for all $m \in \mathbb{Z}$ we have*

$$f_m(x,y) \equiv f_m(x_n, y_n)\ f_m(x_{n-1}, y_{n-1})\cdots f_m(x_0, y_0) \mod p.$$

We can now prove Lemma 2.

Proof. We have to show that for all $n \geq 1$ and $0 \leq l, q \leq 2$ with $(l,q) \neq (1,1)$,

$$\Phi(x,y) \equiv \pm\Phi(l\cdot 3^n + x, q\cdot 3^n + y) \mod 3 \qquad \text{for all } 0 \leq x, y \leq 3^n - 1 \tag{3}$$

where this means that for every x, y, l, q the equivalence should hold with either a plus or minus sign. For $(l,q) = (1,1)$ we require

$$\Phi(3^n + x, 3^n + y) \equiv 0 \mod 3 \qquad \text{for all } 0 \leq x, y \leq 3^n - 1 \tag{4}$$

Figure 7 shows this graphically. The values $(l,q) = (1,1)$ corresponds to the empty square in the middle, and all other values of (l,q) should be copies of the square at $(l,q) = (0,0)$, up to exchanging the non-white colours. These equations simply follow from Claim 4 by noting that $\Phi(x,y) = (-1)^y f_1(x,y)$ so

$$\Phi(l \cdot 3^n + x, q \cdot 3^n + y) \equiv (-1)^{q \cdot 3^n} f_1(l,q)\Phi(x,y) \equiv \Phi(l,q)\Phi(x,y) \mod 3.$$

where we used that $(-1)^{q \cdot 3^n} = (-1)^q$. Note that $\Phi(1,1) = 0$ which proves (4) and $\Phi(l,q) \equiv \pm 1 \mod 3$ for the other values of l, q which proves (3). □

3.5 Results for a more general quantum walk

In this section we generalise the results of the previous section. We can consider the same triangle modulo any prime p, but more generally, the Hadamard operator H could be replaced by any matrix $C \in U(2)$,

$$C = \begin{pmatrix} c_r & c_u \\ c_d & c_l \end{pmatrix} = \begin{pmatrix} \sqrt{p}\, e^{i\alpha} & \sqrt{1-p}\, e^{i\beta} \\ -\sqrt{1-p}\, e^{i\gamma} & \sqrt{p}\, e^{i(\gamma+\beta-\alpha)} \end{pmatrix} \quad , \quad \text{with } 0 \le p \le 1.$$

In Lemma 3.1 we gave expressions for the amplitudes, and in x, y coordinates they read:

$$\Phi_C(x,y) = c_d c_r^x c_l^y \sum_{k \ge 0} \binom{x}{k} \binom{y}{k} \left(-\frac{1-p}{p}\right)^k = c_d c_r^x c_l^y \; f_m(x,y).$$

where $m = (1-p)/p \ge 0$ and where we extend the definition of f_m for non-integer m. As these *amplitudes* can become complex, we now consider the *probabilities*

$$|\Phi_C(x,y)|^2 = |c_d c_r^x c_l^y|^2 \left(f_m(x,y)\right)^2,$$

a distinction that was irrelevant for the Hadamard walk. For $|\Phi_C(x,y)|^2$ to be integer, we assume that the coin matrix is such that $m = (1-p)/p$ is integer, i.e. $p = \frac{1}{1+m}$ with $m \in \mathbb{N}$. This can not be achieved by scaling the entire matrix because m is invariant under such scalings. The complex phases α, β, γ do not influence $|\Phi_C(x,y)|^2$, hence the most general form of the matrix we can consider to obtain integer probabilities is the unitary matrix

$$C_m = \begin{pmatrix} \sqrt{1/(1+m)} & \sqrt{m/(1+m)} \\ \sqrt{m/(1+m)} & -\sqrt{1/(1+m)} \end{pmatrix} \quad \text{for } m \in \mathbb{Z},\ m \ge 0,$$

where have set $\alpha = \beta = 0$ and $\gamma = \pi$ such that $C_1 = H$, but any other setting of phases would be equally valid. If we want to scale the matrix by a factor λ such that $|c_d c_r^x c_l^y|^2$ is integer, then this requires $\lambda = \sqrt{n(1+m)}$ for any integer $n \ge 1$. This gives a scaled matrix

$$\sqrt{n(1+m)} C_m = \sqrt{n} \begin{pmatrix} 1 & \sqrt{m} \\ \sqrt{m} & -1 \end{pmatrix}, \tag{5}$$

and for this scaled matrix, $|c_d c_r^x c_l^y|^2 = mn^{x+y+1}$. By Claim 4 we have for this scaled coin matrix that

$$\begin{aligned}|\Phi_C(l \cdot p^n + x, q \cdot p^n + y)|^2 &\equiv \frac{n^{(l+q)(p^n-1)-1}}{m} |\Phi_C(l,q)|^2 |\Phi_C(x,y)|^2 \mod p \\ &\equiv \frac{1}{mn} |\Phi_C(l,q)|^2 |\Phi_C(x,y)|^2 \mod p,\end{aligned}$$

where we used Fermat's little theorem in the second step. For $m = 1$ and $n = 1$ we recover the exact same rules as for the Hadamard matrix. When n or m is divisible by p, there are no fractals generated by the distinction $|\Phi(x,y)|^2 \equiv 0 \mod p$. When both n, m are non-zero modulo p then we have $|\Phi(x,y)|^2 \equiv 0 \mod p$ if and only if $f_m(x,y) \equiv 0 \mod p$, independent of n. Now we can apply the quantum version of Lucas' theorem. By Corollary 3, $f_m(x,y) \equiv 0 \mod p$ if and only if there is an i such that $f_m(x_i, y_i) \equiv 0 \mod p$, where x_i, y_i are the base-p digits of x, y.

In general, to find the fractal generated by a quantum walk with the general coin from Equation (5) for some n, m that are non-zero modulo p, we simply have to compute $f_m(x,y) \mod p$ for only $0 \leq x, y < p$ to find what we call the *base image*. Figure 8 shows these base images for several values of m and p. From this the fractal can be constructed in a simple recursive way, shown in Figure 9, resulting in the fractals shown in Figure 10. This recursive method is valid because each recursion step corresponds to adding another digit to x and y, and as mentioned above, a pixel will be white if and only if there are digits (i.e. a recursion step) in which the region corresponding to those digits is white.

3.6 Other properties of the Hadamard triangle

One can add the probabilities in each row of the triangle and this sum will always be equal to one (or 2^t after rescaling) since they are probabilities. When summing the *amplitudes* in a row one finds the sums $1, 2, 2, 4, 4, 8, 8, \ldots$. To see why, define the column vector $\Psi(t) = (\Psi_\uparrow(t) \;\; \Psi_\downarrow(t))^T$ where $\Psi_\uparrow(t)$ is the sum of the up amplitudes at time t, i.e. $\Psi_\uparrow(t) = \sum_{n=-t}^{t} \psi_\uparrow(n,t)$, and similar for $\Psi_\downarrow(t)$. Looking at the definition of the Hadamard walk, a moments thought shows that $\Psi(t+1) = H\Psi(t)$. Since $H^2 = \mathrm{Id}$, the sum over all amplitudes only depends on the parity of t. After rescaling (i.e. $H' = \sqrt{2}H$), starting in $|0, \uparrow\rangle$ gives

$$\Psi'_\uparrow(t) + \Psi'_\downarrow(t) = \begin{cases} 2^{t/2} & t \text{ even}, \\ 2^{(t+1)/2} & t \text{ odd}. \end{cases}$$

Pascal's triangle has the property that summing over the so-called *shallow diagonals* yields the Fibonacci sequence. The n'th shallow diagonal d_n ($n \geq 0$) corresponds to the sum $d_n = \sum_{c=0}^{\lfloor n/2 \rfloor} \binom{n-c}{c}$, and by $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ it follows that $d_n = d_{n-1} + d_{n-2}$, i.e. the Fibonacci sequence. We can consider the same diagonals in our Hadamard triangle. In particular we will consider the same numbers that gave rise to the Sierpinski triangle,

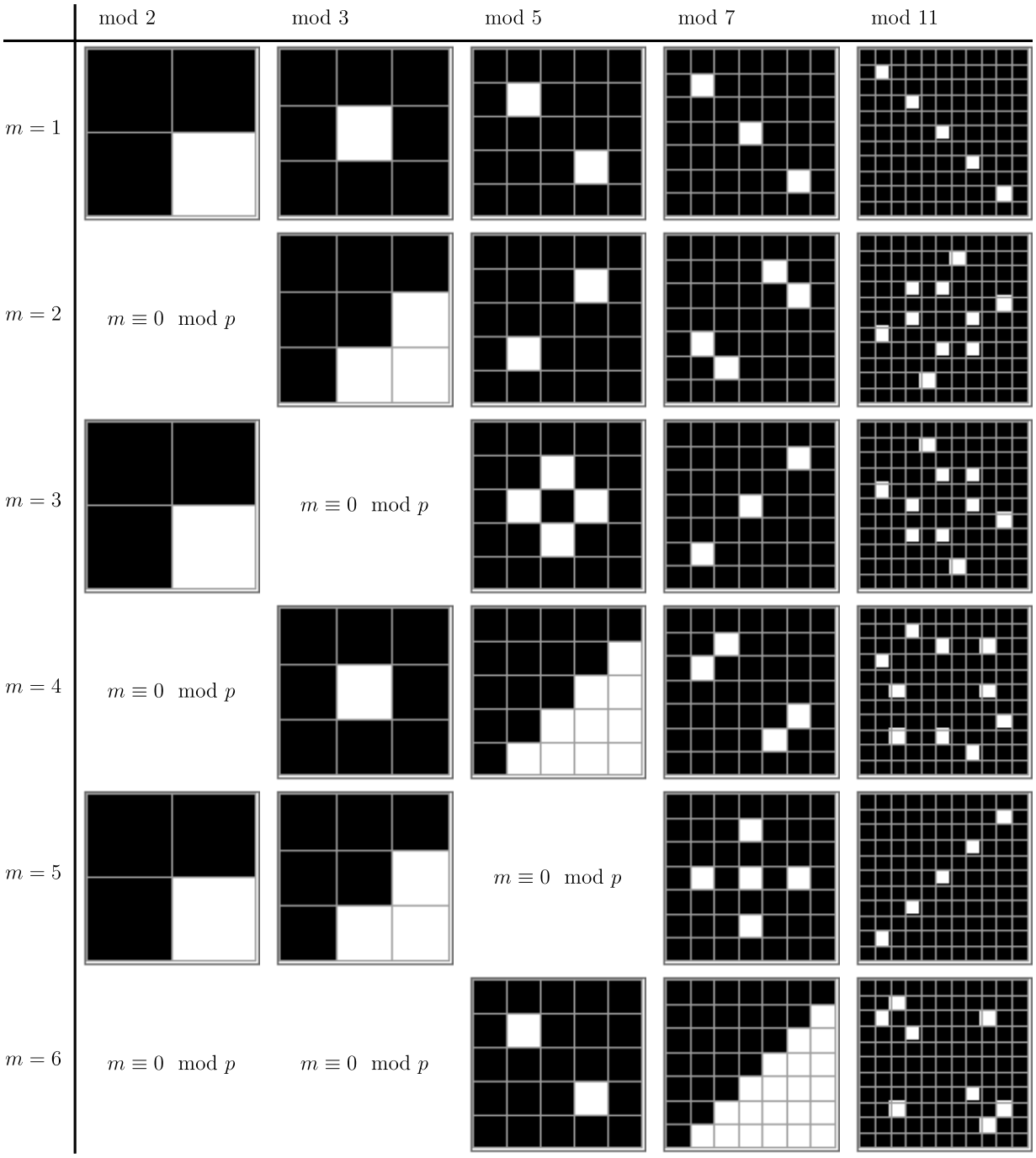


Figure 8: Base images: plots of $f_m(x, y) \mod p$ for $0 \leq x, y < p$ for different values of m and p. Figure 9 explains how to construct the fractals from these base images and Figure 10 shows the resulting fractals.

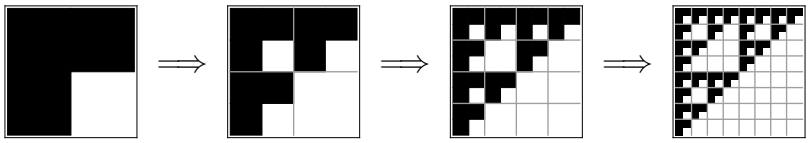


Figure 9: Construction of the fractal from the *base image*. The leftmost picture shows one of the base images from Figure 8. At each step, every black pixel is replaced by a copy of the base image. Infinite recursion steps yield the fractal. Some of these fractals are shown in Figure 10 (for finite recursion steps).

namely down components indicated by the blue numbers in Figure 6. The number at row R and column C is given by

$$T(R,C) = (-1)^{R-C} \sum_{k=0}^{\min(C,R-C)} \binom{C}{k}\binom{R-C}{k}(-1)^k.$$

Unlike the case of Pascal's triangle, the direction of the diagonal matters. We denote the $\diagup$ sums by A_n and the $\diagdown$ sums by B_n, defined as

$$A_n = \textstyle\sum_{c\geq 0} T(n-c,c) \quad \text{and} \quad B_n = \textstyle\sum_{c\geq 0} T(n-c,n-2c).$$

Using the same property of binomial coefficients, we find

$$A_n = -A_{n-1} + A_{n-2} + 2A_{n-3} \quad \text{and} \quad B_n = B_{n-1} - B_{n-2} + 2B_{n-3}.$$

4 Quantum signature

We have seen that different versions of the Sierpinski triangle can appear when the scaled classical random walk probabilities are plotted modulo a prime. The quantum walk, however, can also give rise to the carpet.

Let us argue that a more general classical walk will only give the Sierpinski triangle and not the carpet. A random walk with probabilities $p, 1-p$ of moving right and left can be scaled to integer probabilities precisely when $p \in \mathbb{Q}$. Therefore assume $p = u/(v+w)$ with $u, v, w \in \mathbb{N}$, then scaling all values by $(v+w)^n$ will yield a triangle with the integer $\binom{r}{c}v^c w^{r-c}$ at row r and column c. When v or w is divisible by p, then all these values are zero modulo p and hence there is no fractal. On the other hand, when both v, w are non-zero modulo p then $\binom{r}{c}v^c w^{r-c}$ is zero modulo p if and only if $\binom{r}{c}$ is zero modulo p. The fractal will therefore always be the Sierpinski triangle and never the Sierpinski carpet. It can be argued that a more fair comparison would allow the classical walk to take place on the directed graph shown in Figure 5, since that is the underlying graph of the quantum walk. Doing so is easily seen to be equivalent to changing the coin matrix to one that is stochastic as opposed to unitary, and one then finds the function f_m (Definition 1) but now

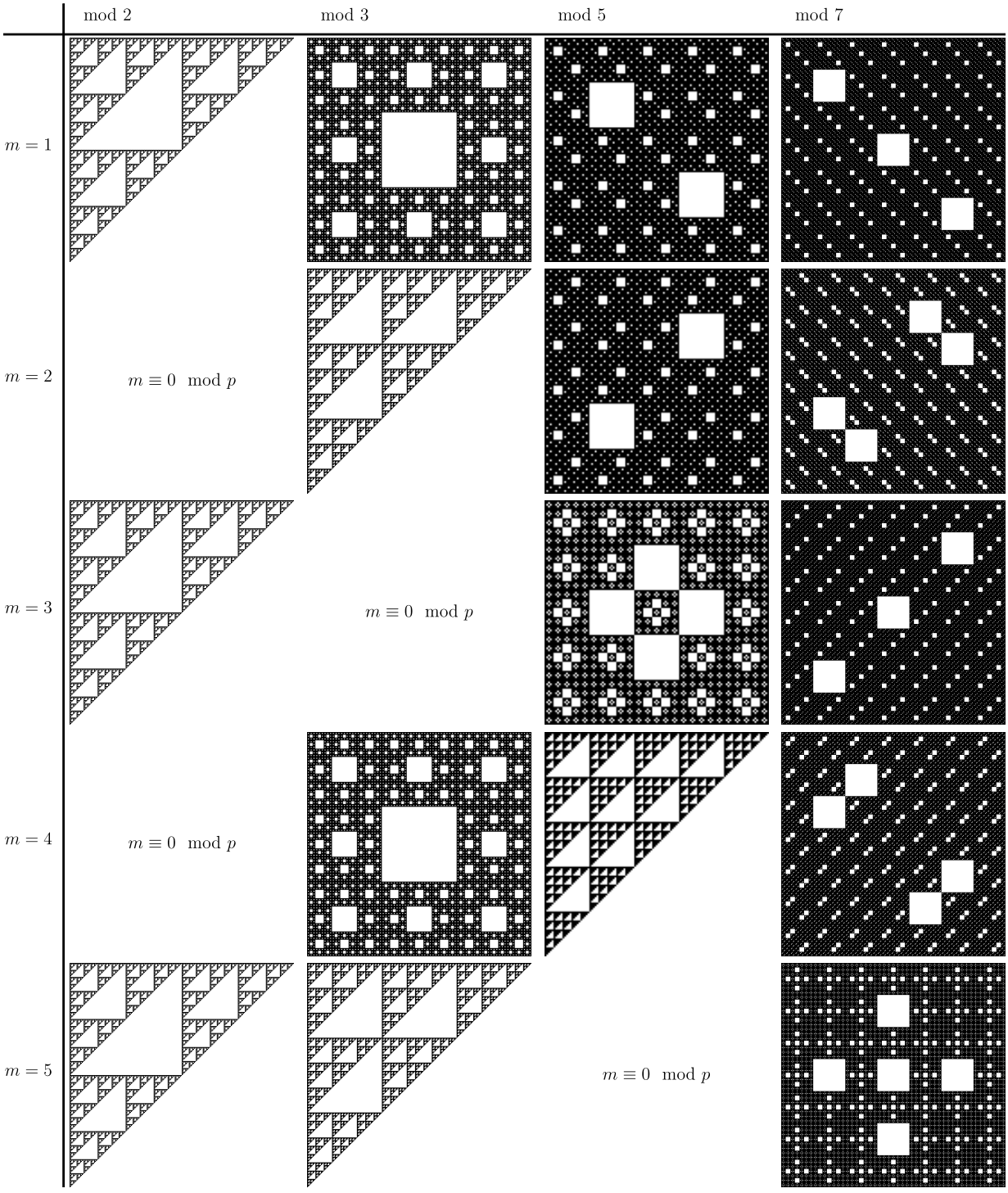


Figure 10: Fractals obtained from general 1-dimensional quantum walks plotted modulo a prime. The number m on the left represents the coin class, where $m = 1$ includes the Hadamard coin.

for $m < 0$ and with some additional prefactors. An exhaustive search through all valid stochastic matrices, however, reveals that the carpet can not be found in the probabilities modulo 3. When the classical numbers are taken modulo higher primes, one does obtain fractals different from the Sierpinski triangle, but the carpet is not seen.

The appearance of the Sierpinski carpet can therefore be considered a sign of the quantum nature of the probability distribution.

5 Acknowledgements

The authors would like to thank Florian Speelman, Jeroen Zuiddam and Māriz Ozols for useful discussions and Frank den Hollander for feedback. The work in this paper is supported by the Netherlands Organisation for Scientific Research (NWO) through Gravitation-grant NETWORKS-024.002.003.

References

[1] E.E. Kummer. "Über die Ergänzungssätze zuden allgemeinen Reciprocitätsgesetzen". In: *J. Reine Angew. Math.* 44 (1852), pp. 93–146.

[2] E. Lucas. "Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier". In: *Bull. Soc. Math. France* 6 (1878), pp. 49–54.

[3] Stephen Wolfram. "Geometry of Binomial Coefficients". In: *The American Mathematical Monthly* 91.9 (1984), pp. 566–571. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2323743.

[4] Ian Stewart. "Four encounters with sierpińriski's gasket". In: *The Mathematical Intelligencer* 17.1 (1995), pp. 52–64. ISSN: 0343-6993. DOI: 10.1007/BF03024718. URL: http://dx.doi.org/10.1007/BF03024718.

[5] David A. Meyer. "From quantum cellular automata to quantum lattice gases". In: *Journal of Statistical Physics* 85 (Dec. 1996), pp. 551–574. DOI: 10.1007/BF02199356. arXiv: quant-ph/9604003 [quant-ph].

[6] Andris Ambainis et al. "One-dimensional Quantum Walks". In: *Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing*. STOC '01. Hersonissos, Greece: ACM, 2001, pp. 37–49. ISBN: 1-58113-349-9. DOI: 10.1145/380752.380757. URL: http://doi.acm.org/10.1145/380752.380757.

[7] John Baez. *This Week's Finds in Mathematical Physics (Week 188)*. 2002. URL: http://math.ucr.edu/home/baez/week188.html (visited on 03/07/2019).

[8] Pedro G. S. Cardoso et al. "Some properties of deformed q-numbers". In: *Braz J Phys* 39 (Aug. 2009), pp. 402–407. ISSN: 0103-9733. DOI: 10.1590/S0103-97332009000400009. URL: https://doi.org/10.1590/S0103-97332009000400009.

[9] Alexander Gnedin and Grigori Olshanski. "A q-Analogue of de Finetti's Theorem". In: *Electr. J. Comb.* 16.1 (2009). URL: http://www.combinatorics.org/Volume%5C_16/Abstracts/v16i1r78.html.

[10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 10th. New York, NY, USA: Cambridge University Press, 2011. ISBN: 9781107002173.

[11] R. Meštrović. "Lucas' theorem: its generalizations, extensions and applications (1878–2014)". In: *ArXiv e-prints* (Sept. 2014). arXiv: 1409.3820 [math.NT].