Hans Walser, [20100612a]

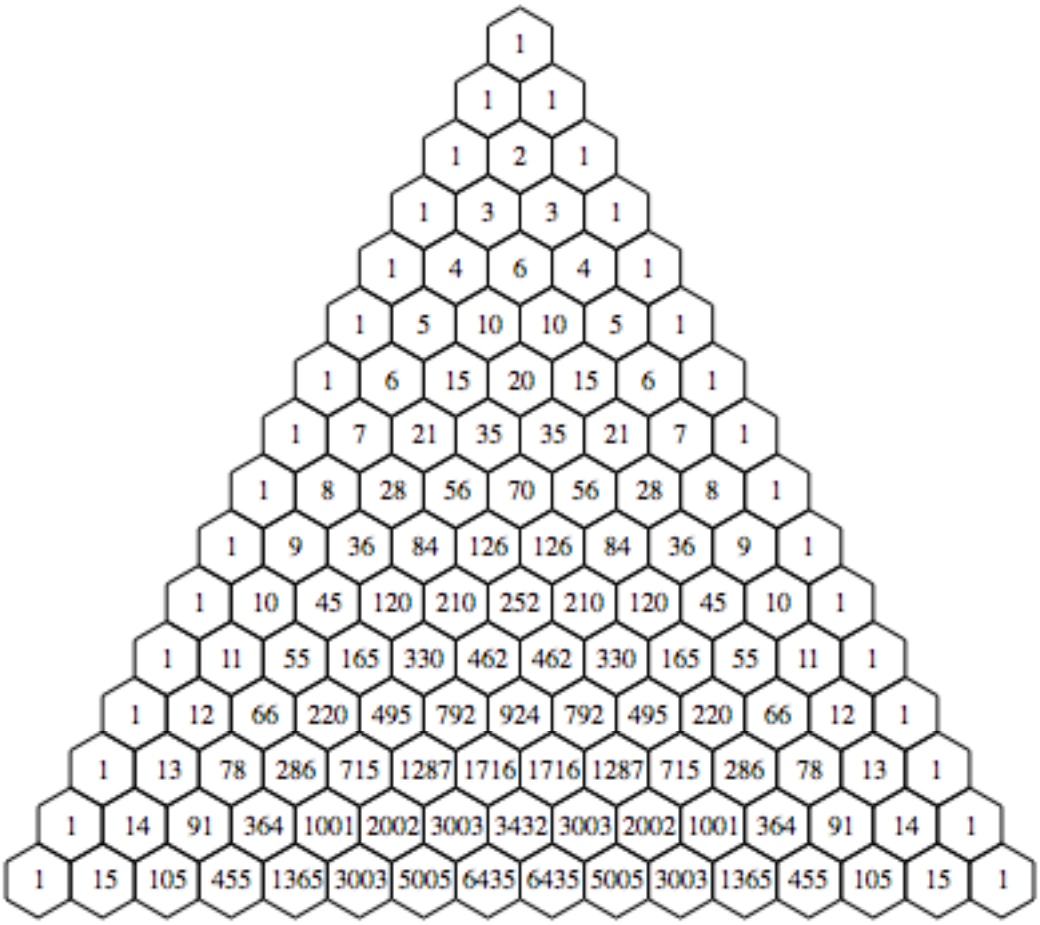
Binomialkoeffizienten modulo eine Zahl

1 Worum geht es?

Die Binomialkoeffizienten $\binom{n}{k}$ werden einerseits wie üblich mit einer festen Zahl moduliert, andererseits aber auch mit den variablen Zahlen n und k. Entsprechend wird eingefärbt. Die Resultate hängen mit dem kleinen Satz von Fermat zusammen.

2 Binomialkoeffizienten

Diese werden in einem Hexagonalraster dargestellt.

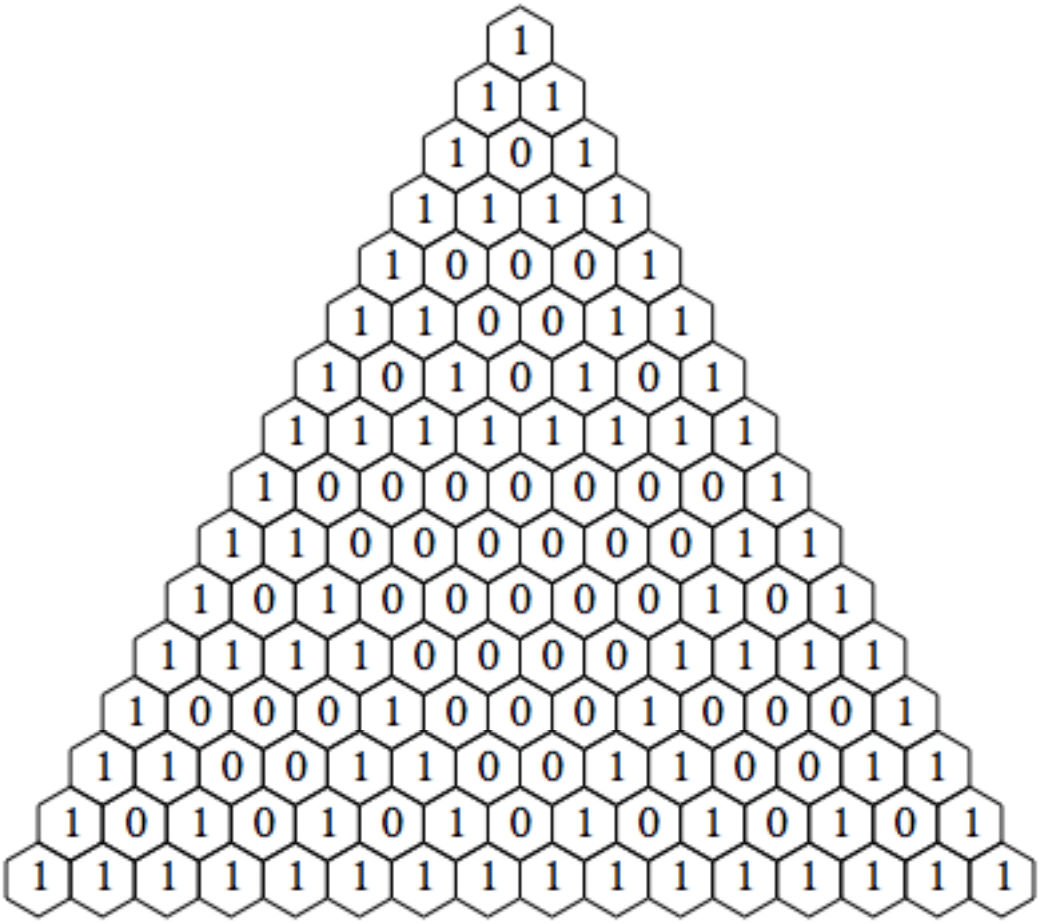


Binomialkoeffizienten

3 Binomialkoeffizienten modulo *m*

3.1 Modulo 2

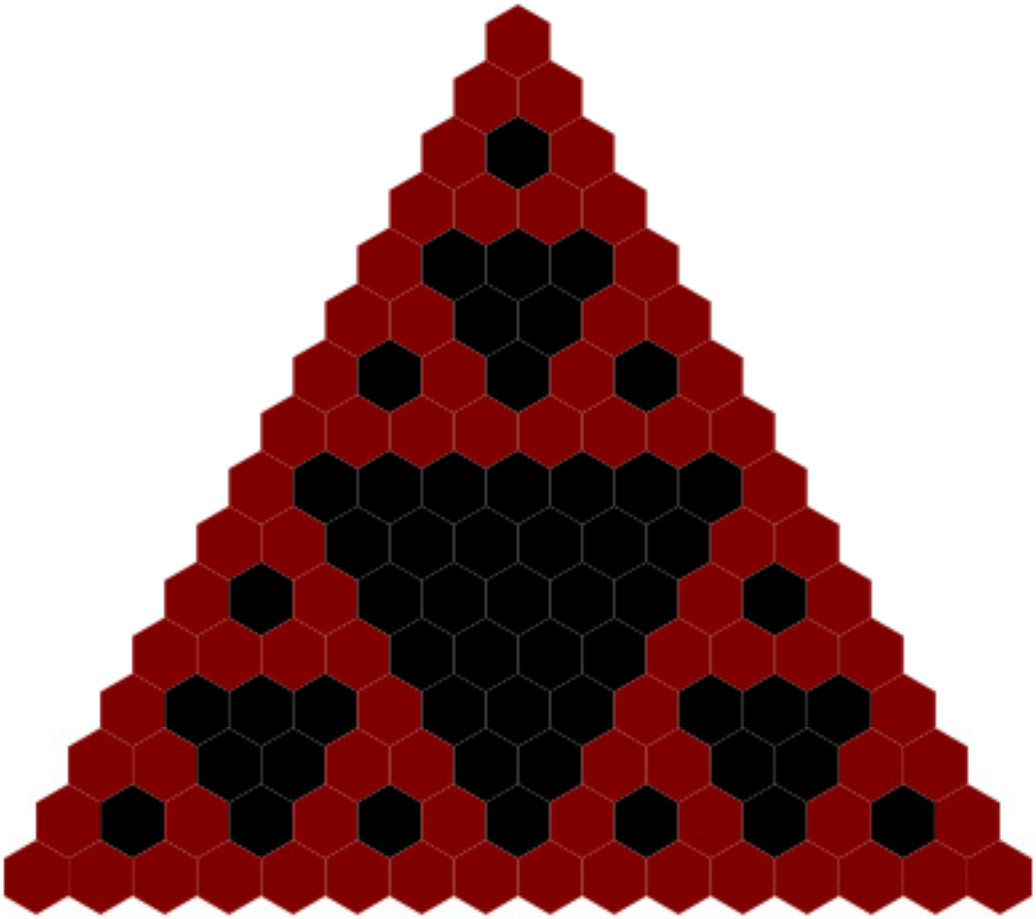
Wir tragen jeweils $\operatorname{mod}\left(\binom{n}{k},2\right)$ ein. Wir unterscheiden also die Binomialkoeffizienten nur bezüglich gerade und ungerade.



Binomialkoeffizienten modulo 2

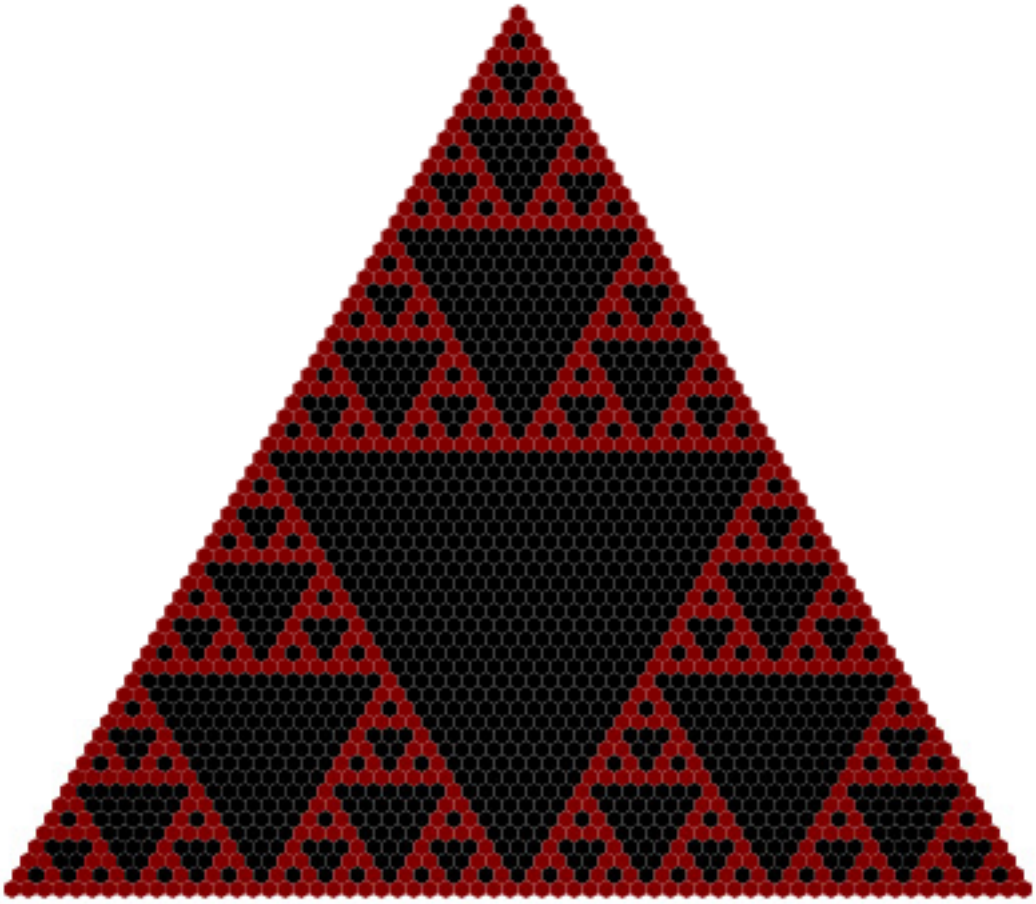
3.2 Zwei Farben

Wir färben nun die Sechsecke mit zwei Farben ein. Wir erkennen die Struktur des Sierpinski-Dreieckes.



Bicolor

Dazu noch ein größerer Ausschnitt.



Größerer Ausschnitt

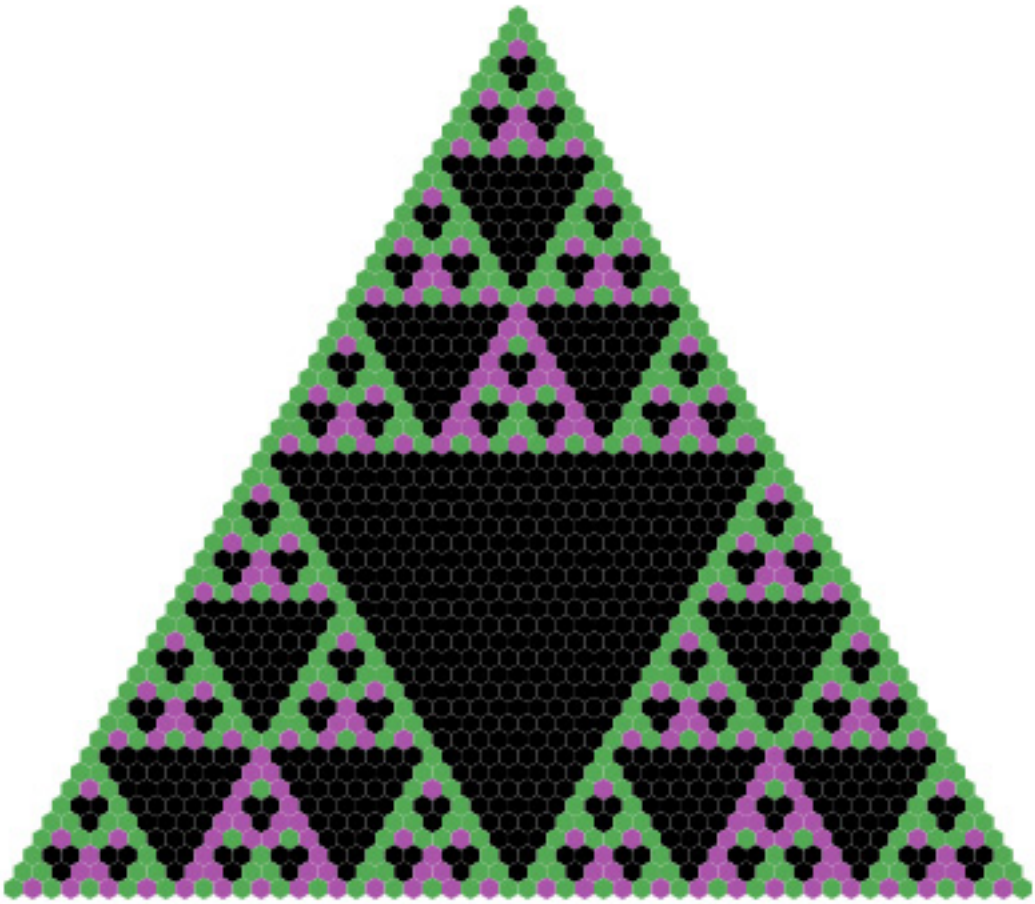
Wir haben ein schönes schwarzes Dreieck in der Mitte.

3.3 Drei Farben

Wir tragen $\operatorname{mod}\left(\binom{n}{k},3\right)$ ein und färben entsprechend mit drei Farben.

Der Farbcode variiert mit der Anzahl der Farben. Die Einsen auf dem Dach haben daher eine andere Farbe. Die Zahl Null wird aber immer schwarz eingefärbt.

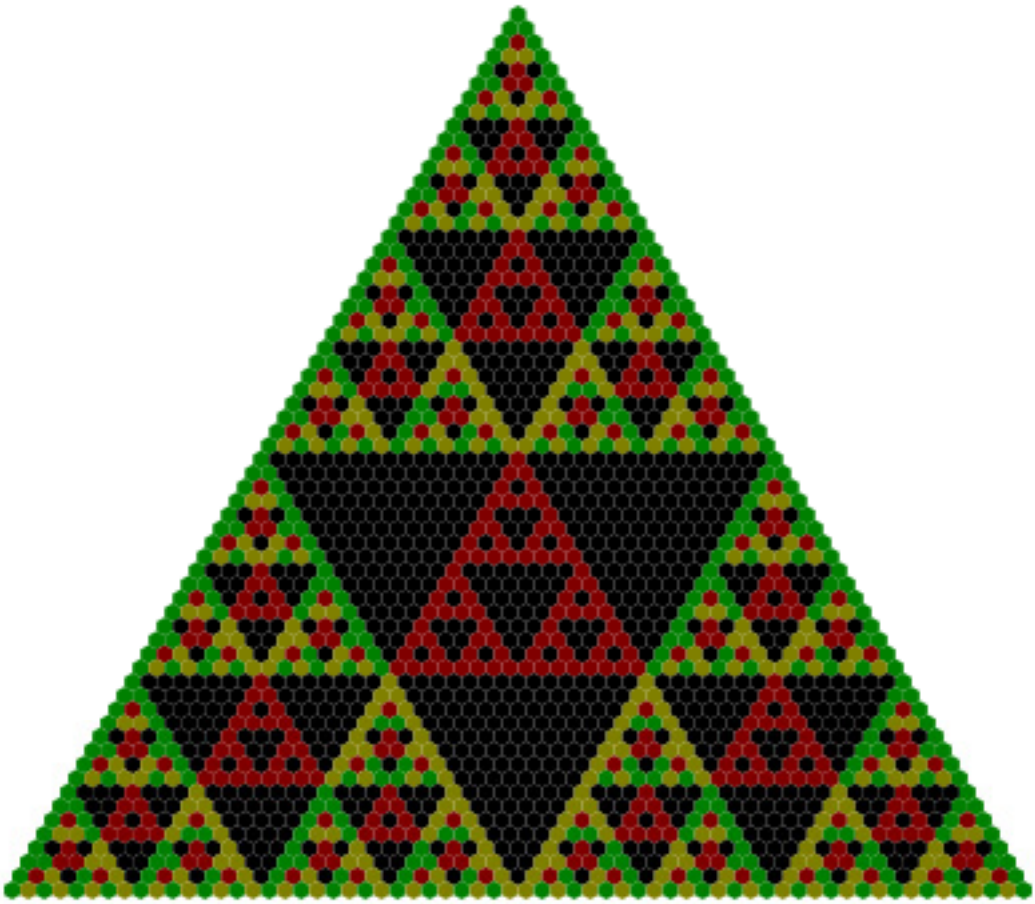
Den Ausschnitt wählen wir passend, sodass eine schöne Figur entsteht.



Modulo 3

Wir haben ein schwarzes Dreieck in der Mitte.

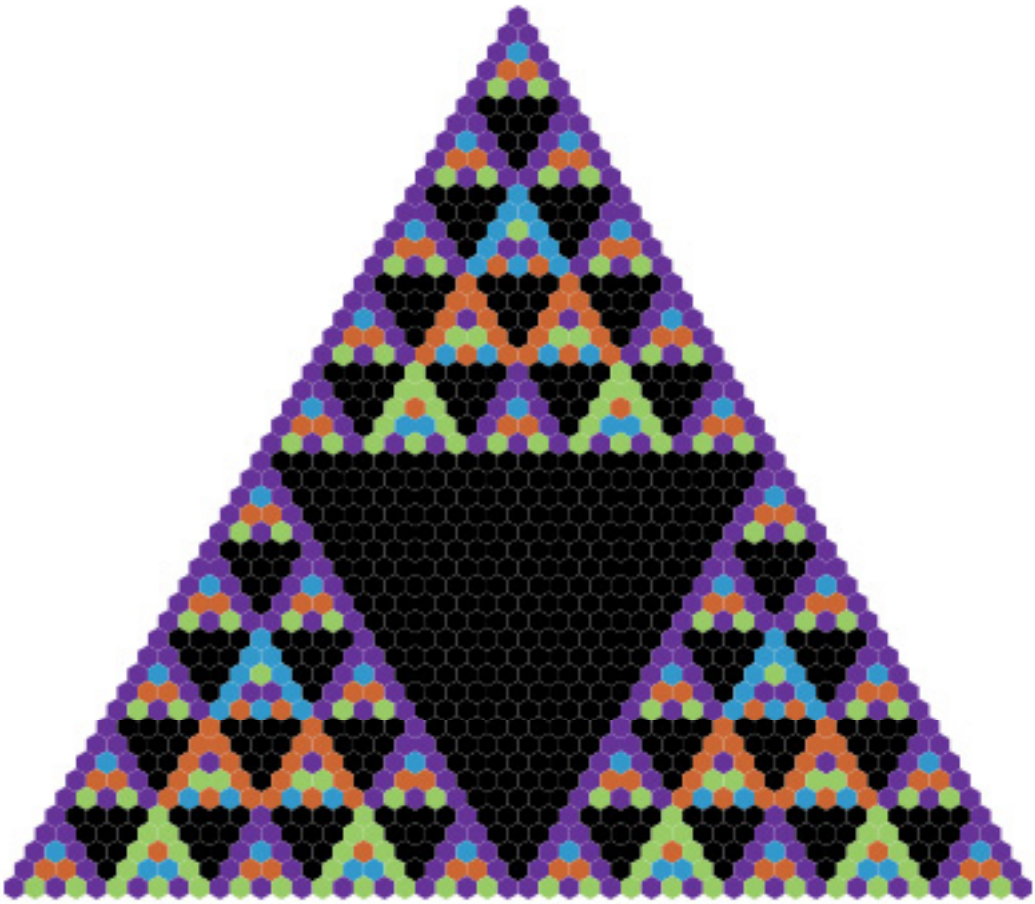
3.4 Vier Farben



Modulo 4

Das schwarze Dreieck in der Mitte ist nicht vollständig schwarz.

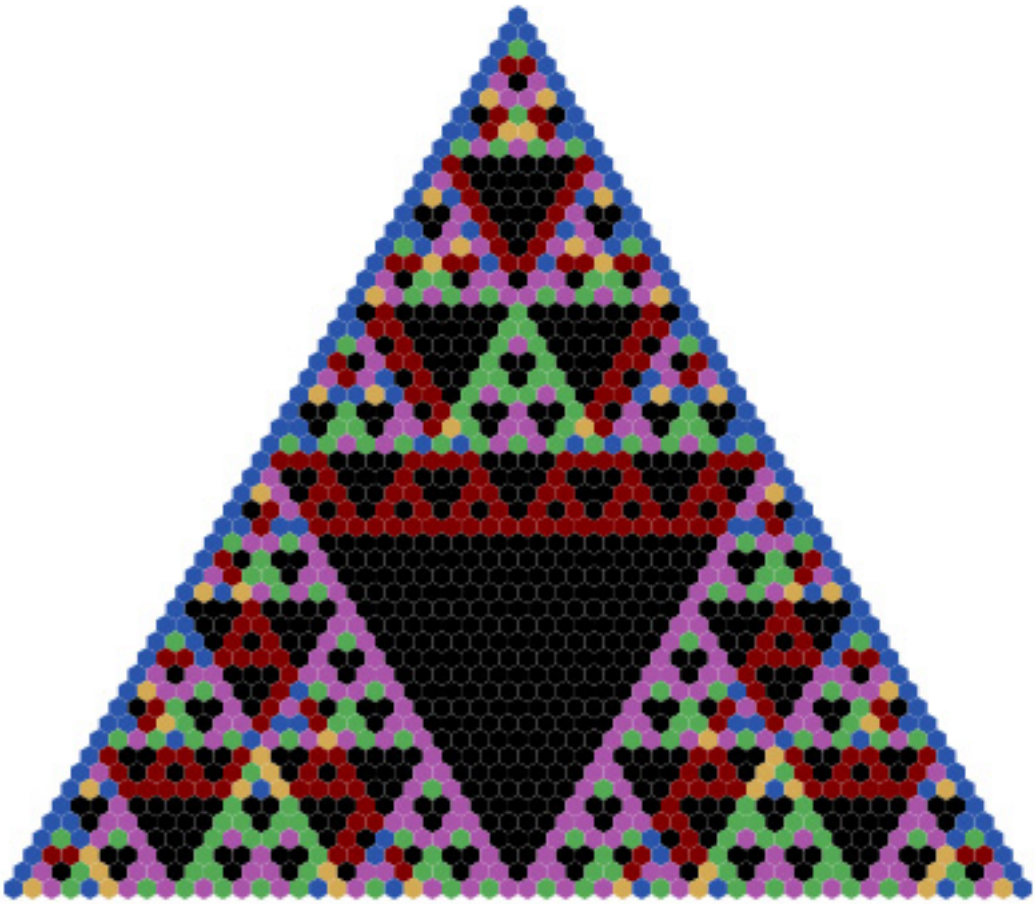
3.5 Fünf Farben



Modulo 5

In der Mitte ist ein vollständig schwarzes Dreieck.

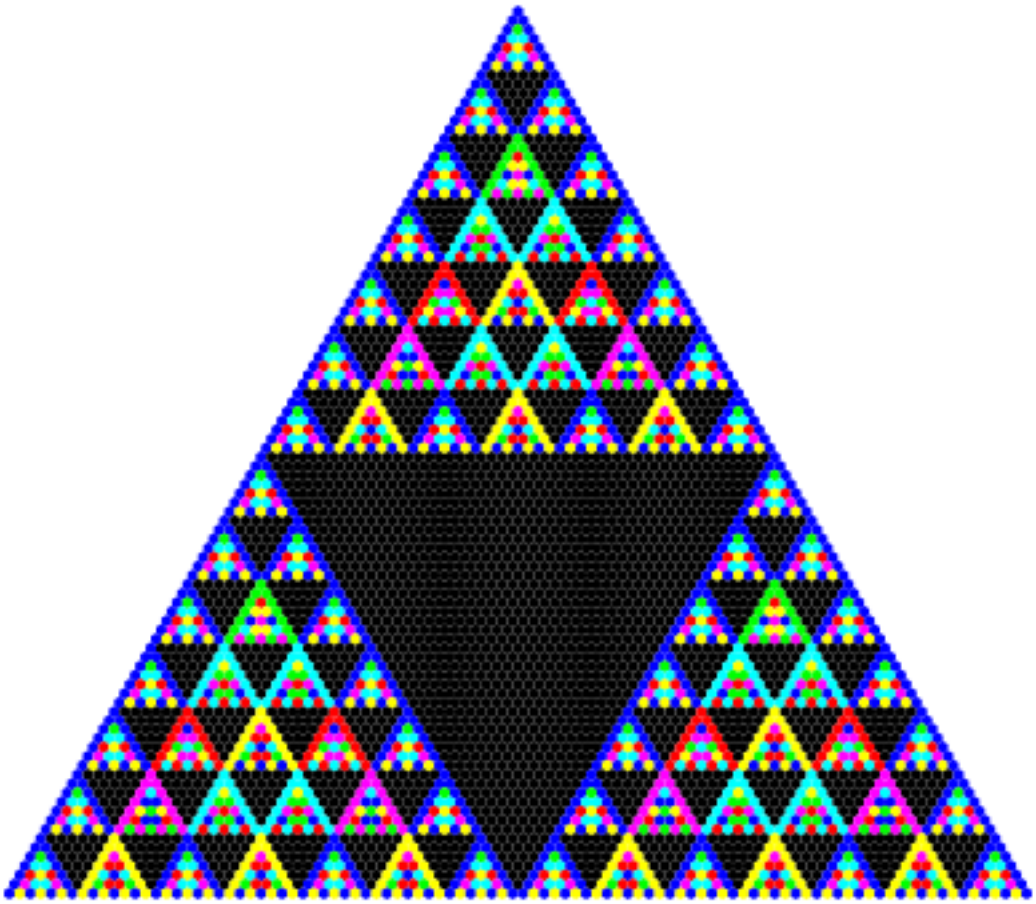
3.6 Sechs Farben



Modulo 6

Die Figur ist etwas eigenartig.

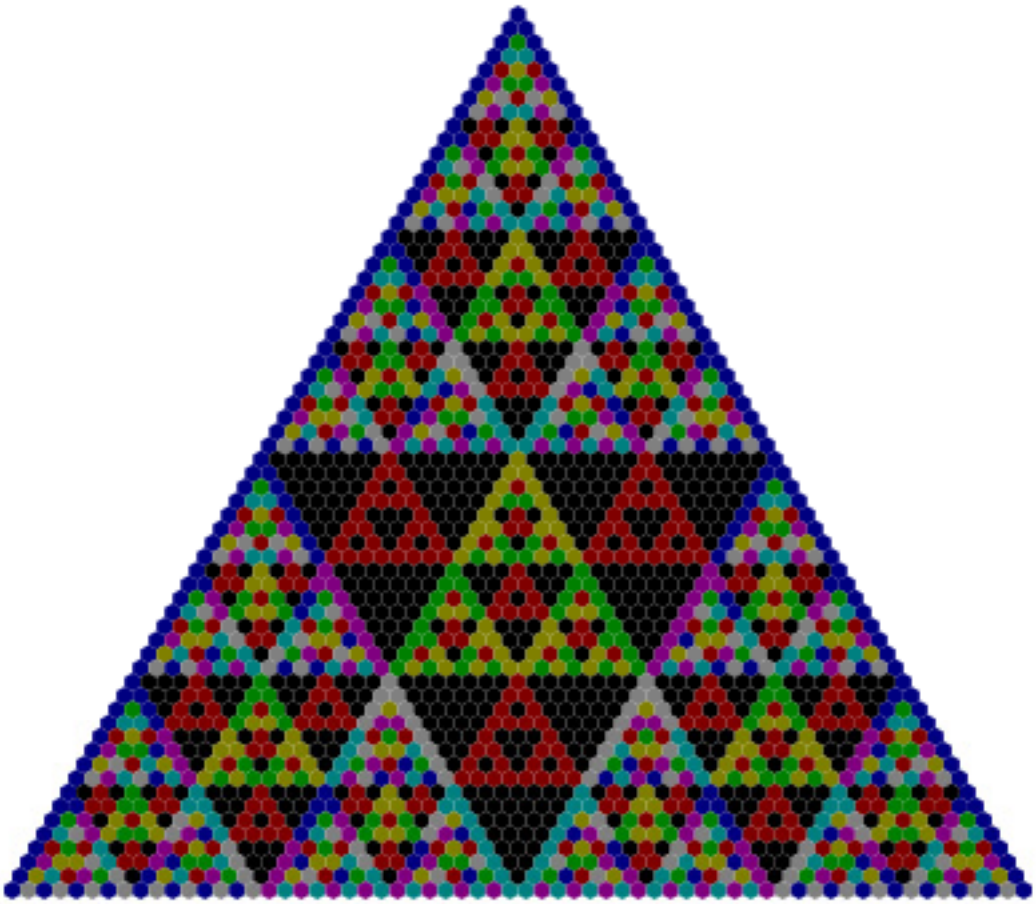
3.7 Sieben Farben



Modulo 7

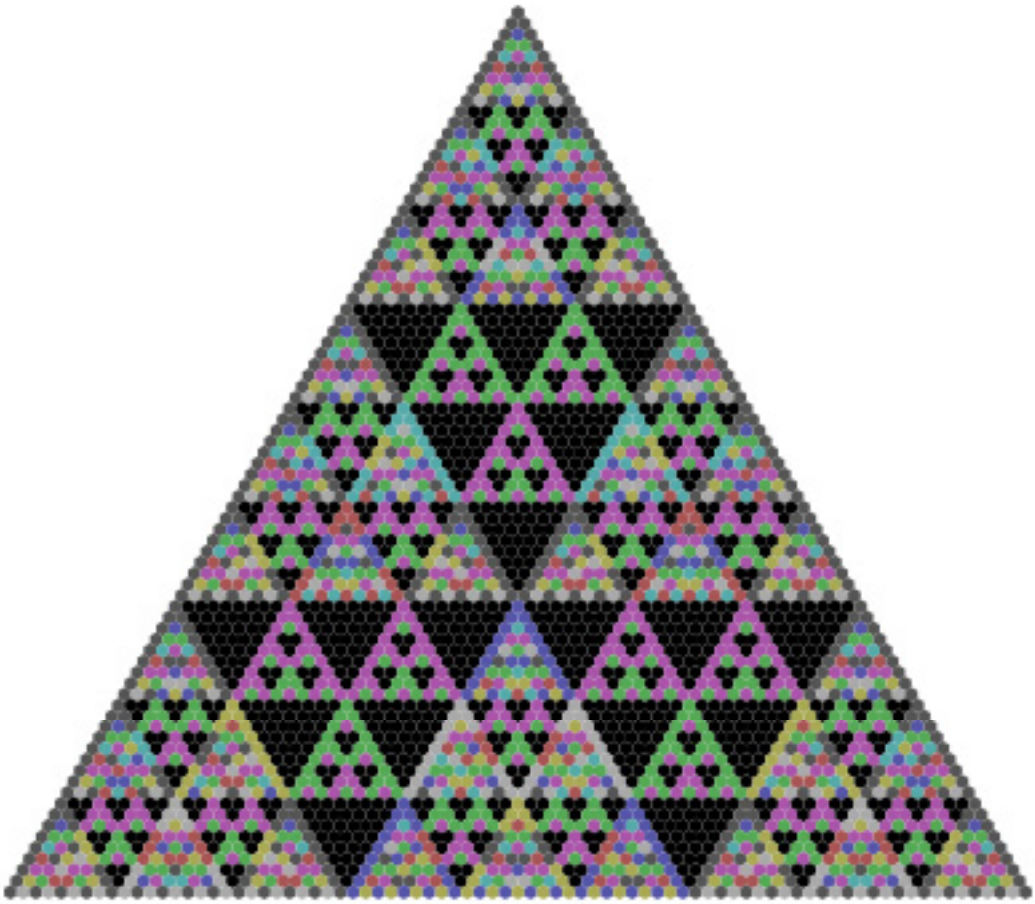
Nun wieder ein vollständig schwarzes Dreieck in der Mitte.

3.8 Acht Farben



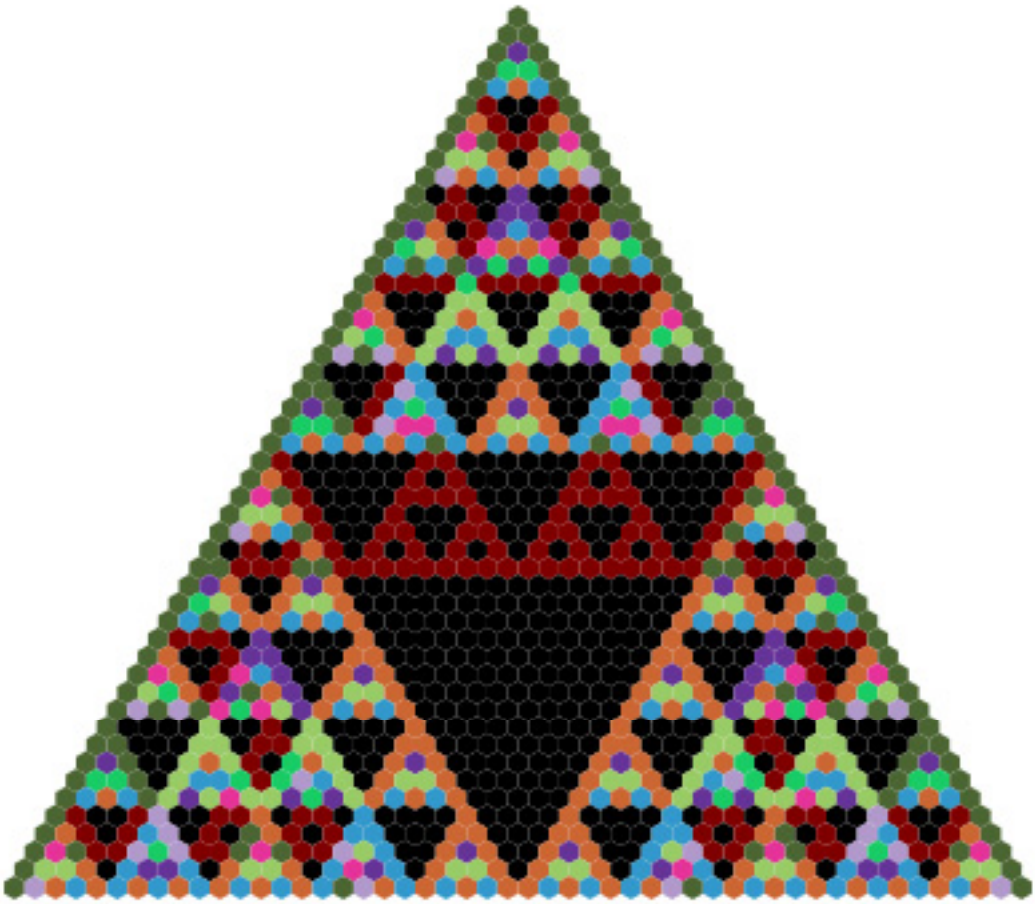
Modulo 8

3.9 Neun Farben



Modulo 9

3.10 Zehn Farben



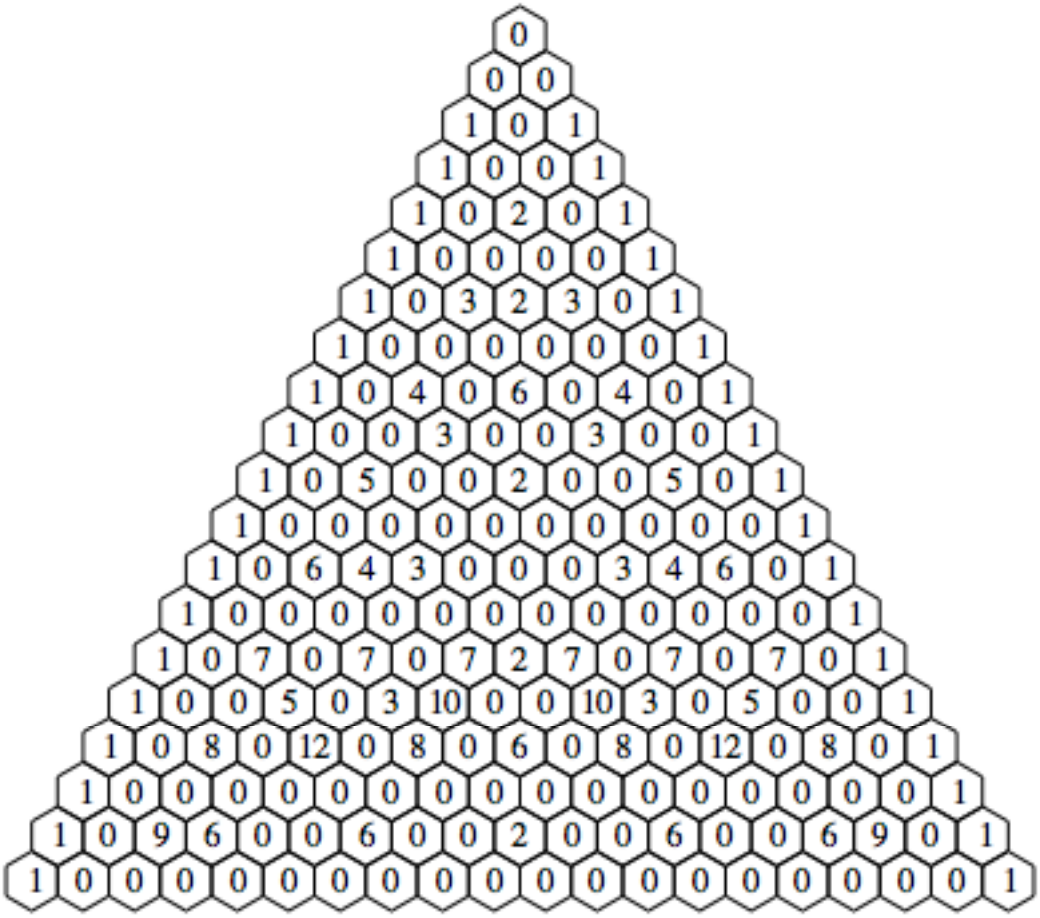
Modulo 10

3.11 Primzahlen

Es fällt auf, dass wir bei den Primzahlen jeweils Zeilen haben, die mit Ausnahme der beiden Enden vollständig schwarz sind, also der Zahl null entsprechen (in allen verwendeten Farbcodierungen entspricht die schwarze Farbe der Zahl null). Diese schwarzen Zeilen sind dann die Oberkante eines hängenden vollständig schwarzen gleichseitigen Dreieckes. Dies ergibt sich aus der Rekursion der Binomialkoeffizienten. Zur Primzahl p sind diese schwarzen Zeilen — soweit übersehbar — auf den Niveaus $p, p^2, p^3, \ldots$. Beweis folgt.

4 Binomialkoeffizienten modulo n

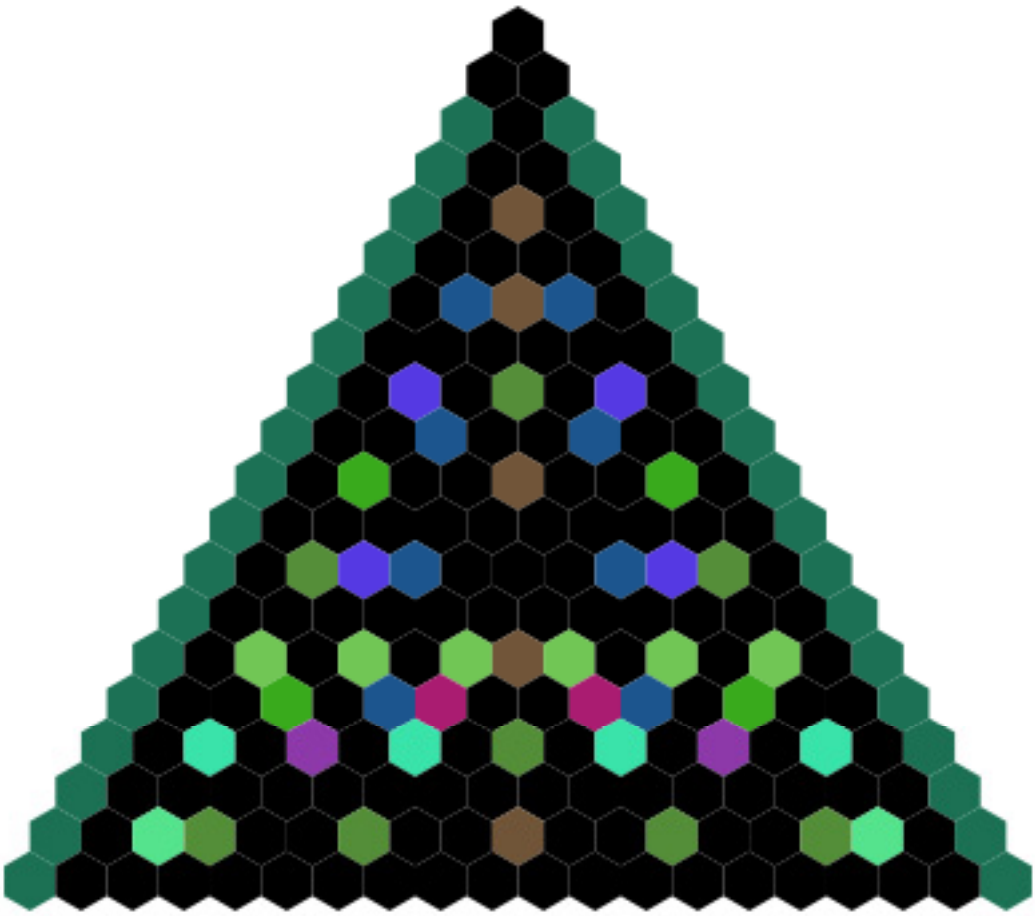
Wir tragen nun $\operatorname{mod}\left(\binom{n}{k}, n\right)$ ein. Die Modulzahl nimmt also pro Zeile um eins zu.



Modulo *n*

Bei den Zeilen mit Primzahlniveau haben wir mit Ausnahme der Enden ausschließlich Nullen.

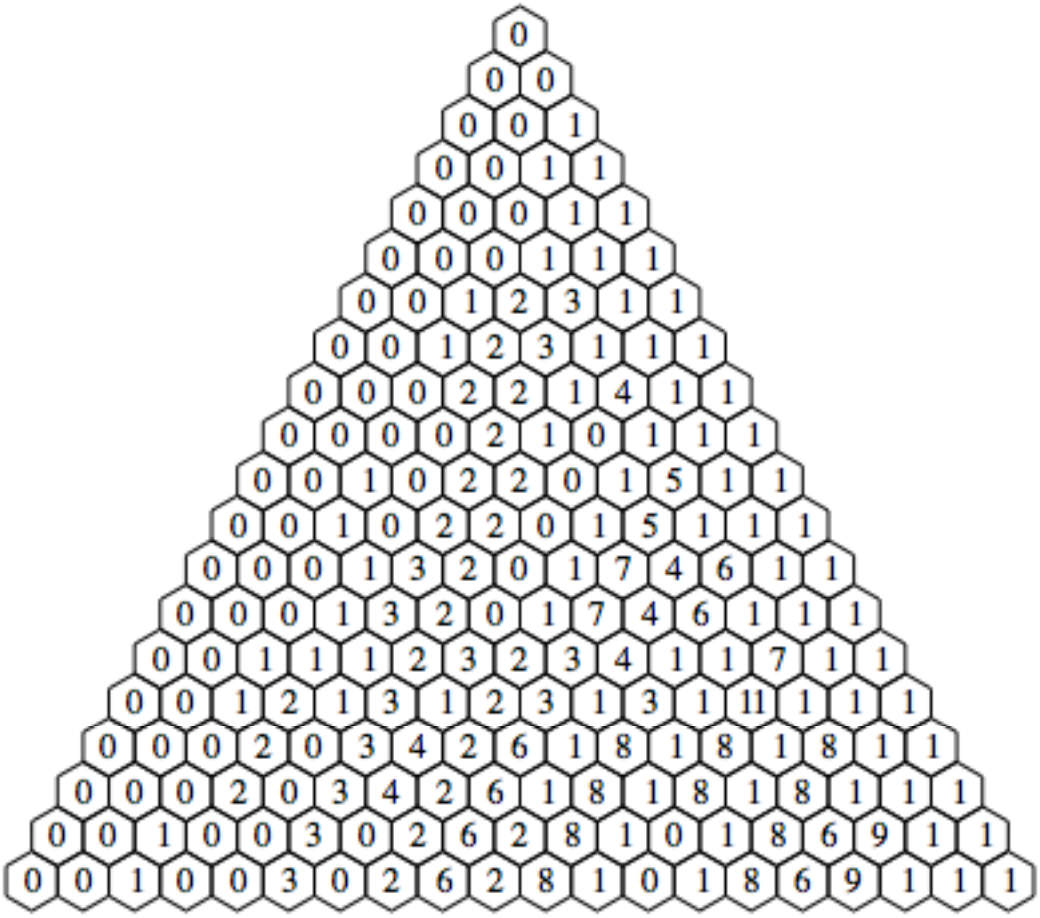
Nun färben wir entsprechend. Das gibt schwarze Zeilen bei den Primzahlniveaus.



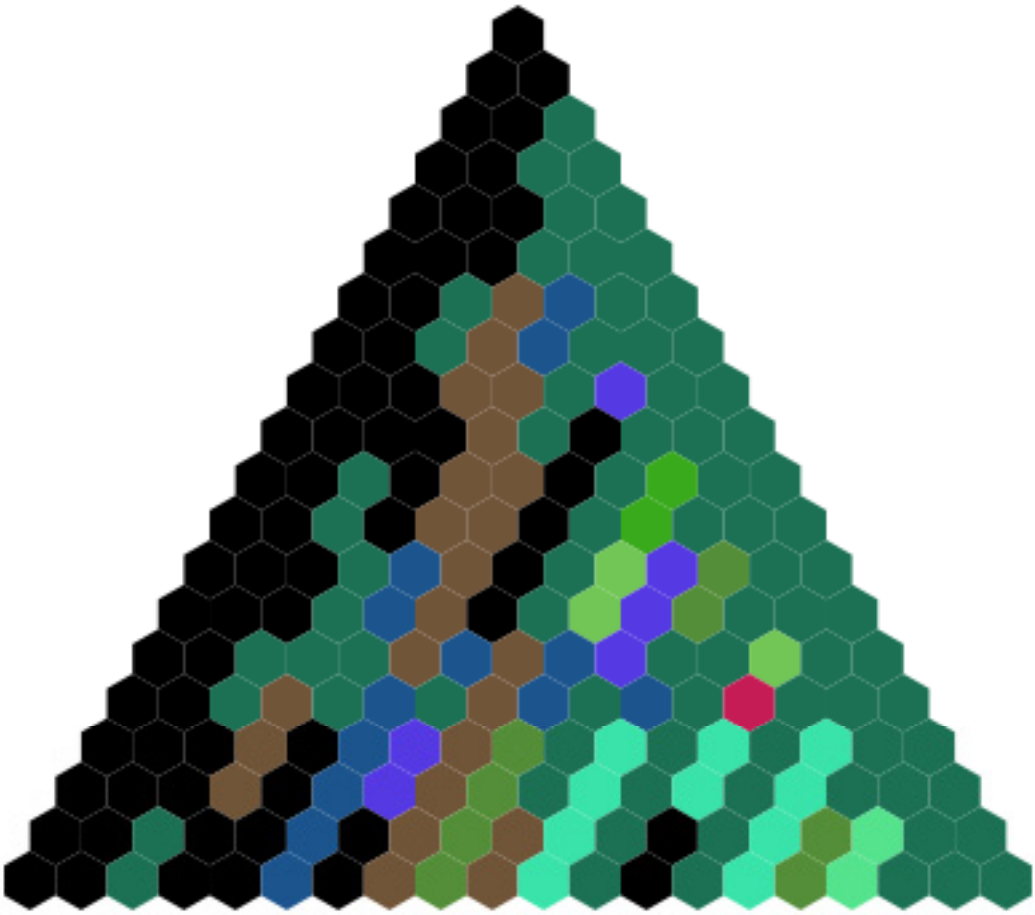
Modulo *n*

5 Binomialkoeffizienten modulo *k*

Wir tragen nun $\operatorname{mod}\left(\binom{n}{k}, k\right)$ ein und färben entsprechend.



Modulo *k*



Farben modulo *k*

Sind Strukturen erkennbar?

6 Zahlentheoretisches

Wir zeigen: Für eine Primzahl p und $0 < k < p^j$ gilt:

$$\operatorname{mod}\left(\binom{p^j}{k}, p\right) = 0$$

Es ist:

$$\binom{p^j}{k} = \frac{p^j\left(p^j-1\right)\left(p^j-2\right)\cdots\left(p^j-(k-1)\right)}{1\cdot 2\cdots k}$$

Wir müssen zeigen, dass dieser Ausdruck mindestens einen Primfaktor p enthält.

Wegen $0 < k < p^j$ können die Zahlen im Nenner einzeln höchstens die einschlägige Primfaktorpotenz p^{j-1} enthalten. Wenn nun eine der Zahlen $i \in \{1,2,\ldots,k-1\}$ eine solche Primfaktorpotenz p^l mit $l < j$ enthält, dann ist dies auch für die Zahl $p^j - i$ im Zähler der Fall. Wir können diese Primfaktorpotenz also herauskürzen. Sollte k selber

eine solche Primfaktorpotenz enthalten, so können wir diese aus p^j im Zähler herauskürzen, und es bleibt im Zähler noch mindestens ein Primfaktor p übrig.

7 Der kleine Satz von Fermat

Der kleine Satz von Fermat besagt: Für eine Primzahl p und eine natürlich Zahl a gilt:

$$\operatorname{mod}\left(a^p, p\right) = a$$

Beispiel: Es sei $p = 5$. Interessant sind nur die Zahlen $a \in \{1,2,3,4,5\}$. Tabelle:

a	1	2	3	4	5
a^5	1	32	243	1024	3125
$\operatorname{mod}\left(a^5, 5\right)$	1	2	3	4	$0 \equiv 5$

Der Beweis geht induktiv über a. Zunächst ist $\operatorname{mod}\left(1^p, p\right) = 1$.

Sei nun $\operatorname{mod}\left(a^p, p\right) = a$. Dann ist:

$$(1+a)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = \underbrace{\binom{p}{0} a^0}_{1} + \sum_{k=1}^{p-1} \binom{p}{k} a^k + \underbrace{\binom{p}{p} a^p}_{a^p}$$

Wir haben oben gesehen, dass für eine Primzahl p und $0 < k < p$ der Binomialkoeffizient $\binom{p}{k}$ den Primfaktor p enthält. Damit enthält auch die Summe $\sum_{k=1}^{p-1} \binom{p}{k} a^k$ den Primfaktor p und es gilt:

$$\operatorname{mod}\left((1+a)^p, p\right) = \operatorname{mod}\left(\left(1+a^p\right), p\right) = 1 + \operatorname{mod}\left(a^p, p\right) = 1 + a$$