Ein Satz über Binomialkoeffizienten modulo *p* (Primzahl) im Pascalschen Dreieck

Sei *p* eine Primzahl. Wir betrachten im Pascalschen Dreieck die Binomialkoeffizienten modulo *p*. Die Zeilen im Pascalschen Dreieck nummerieren wir bei 0 beginnend (0.Zeile, 1.Zeile, usw.).

Wir betrachten die Binomialkoeffizienten $\binom{m}{k}$ einer Zeile *m*, die sich nicht am Rand befinden, d.h. $1 \leq k \leq m\text{-}1$. Wir wollen diese Koeffizienten «innere Binomialkoeffizienten» nennen.

Satz:

Genau die Zeilen *m* (Zeilennummerierung bei 0 beginnend!) mit $m = p^r, r \in \mathbb{N} \setminus \{0\}$, haben die Eigenschaft, dass alle inneren Binomialkoeffizienten dieser Zeile modulo *p* gleich 0 sind.

Beweis:

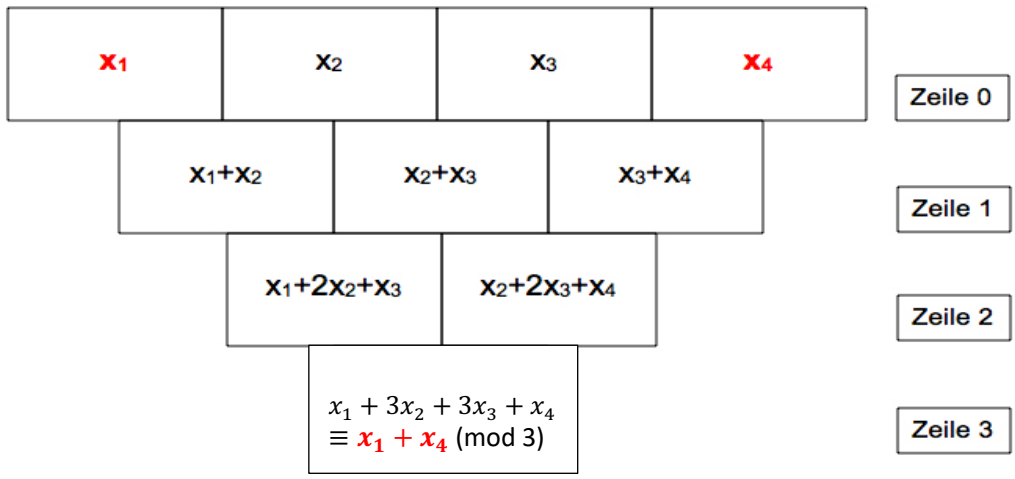
Wir führen den Beweis mit der Primzahl $p = 3$. Die Verallgemeinerung auf beliebige Primzahlen ist dann offensichtlich.

$\Rightarrow$:

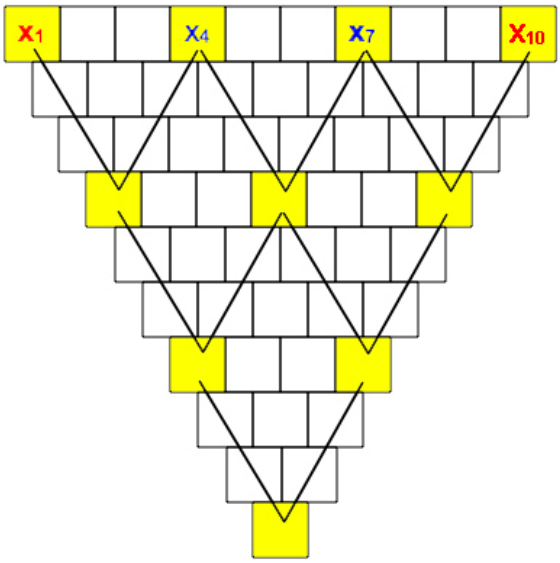
Dass die Zeilen mit den Nummern $3^r, r \in \mathbb{N} \setminus \{0\}$, die behauptete Eigenschaft haben, zeigen wir wie folgt:

Wir bilden eine kopfstehende Pyramide mit den Zeilen 0 bis $m = 3$. Die Grundzeile hat somit $m + 1 = 4$ Kästchen.

Zeile 0 wird mit den Werten x_1, x_2, x_3, x_4 (modulo 3) versehen. Wir vervollständigen die übrigen Kästchen gemäss folgendem Bildungsgesetz: Der Wert eines Kästchens direkt unterhalb zweier Kästchen ist die Summe der Werte dieser beiden Kästchen, jedoch immer modulo 3 gerechnet! Man sieht sofort, dass der Wert an der unteren Spitze gleich $x_1 + 3x_2 + 3x_3 + x_4$ ist, was modulo 3 gleich $x_1 + x_4$ ist = Summe der Eckwerte von Zeile 0.



Nun setzen wir 3 solche Pyramiden mit je einem Feld Überlappung zusammen und ergänzen das Ganze zu einer neuen Pyramide, die nun aus den Zeilen 0 bis 9 besteht (und in der 0. Zeile 9 + 1 = 10 Kästchen aufweist):



Picken wir nur die gelben Felder heraus, haben wir erneut die Situation von oben: eine gelbe Pyramide mit Zeilen 0 bis *m* = 3, die dem geforderten Bildungsgesetz (Wert eines gelben Feldes = Summe der beiden darüber liegenden gelben Felder) gehorcht.
Das unterste Feld ist folglich ebenfalls allein aus den Eckwerten von Zeile 0 zu berechnen, nämlich als Summe $x_1 + x_{10}$.

Dieses Vorgehen wiederholen wir nun mit obiger Pyramide und erhalten eine nächste Pyramide mit den Zeilen 0 bis *m* = 27, dann eine mit den Zeilen 0 bis *m* = 81, usw.
Jede dieser Pyramiden hat die Eigenschaft, dass der Wert der unteren Spitze sich allein als Summe der Eckwerte von Zeile 0 ergibt (immer modulo 3 gerechnet).

Andererseits ist der Wert an der unteren Pyramidenspitze bei einer Pyramide mit den Zeilen 0 bis *m* = 3^r ($r \neq 0$) auch gleich

$$x_1 + \binom{3^r}{1} x_2 + \ldots + \binom{3^r}{3^r - 1} x_{3^r} + x_{3^r+1} = x_1 + x_{3^r+1} .$$

Daraus folgt, dass modulo 3 die inneren Binomialkoeffizienten (gelb) gleich 0 sind, d.h. diese Koeffizienten sind durch 3 teilbar.

⇐:
Seien im Pascalschen Dreieck modulo 3 alle inneren Binomialkoeffizienten einer bestimmten Zeile *m* gleich 0. Wir zeigen: Dann ist *m* eine Dreierpotenz. Sicher ist *m* durch 3 teilbar, denn $\binom{m}{1} = m$ soll ja modulo 3 gleich 0, somit durch 3 teilbar sein. Wir müssen also nur noch Zeilennummern untersuchen, die Vielfache von 3 sind.

Sei *m* = $a \cdot 3^r$, *r* maximal, d.h. *a* und 3^r sind teilerfremd.

Annahme: *a* sei > 1.
Dann ist $\binom{a \cdot 3^r}{3^r}$ wegen *a* > 1 sicher ein innerer Binomialkoeffizient.
Wie wir gleich zeigen werden, teilt 3 jedoch diesen Koeffizienten nicht, er ist also modulo 3 nicht gleich 0 im Widerspruch zur Voraussetzung, dass *alle* inneren Binomialkoeffizienten modulo 3 gleich 0 sind. Folglich muss *a* = 1 sein und *m* ist eine Dreierpotenz.

Wir müssen somit noch zeigen: 3 ist kein Teiler von $\binom{a \cdot 3^r}{3^r}$.

Dazu eine **Bemerkung**: Sei $c \in \mathbb{N}, 1 \leq c \leq 3^r - 1$. In der Primfaktorzerlegung haben dann $a \cdot 3^r - c$ und $3^r - c$ gleich viele Faktoren 3, nämlich je so viele wie c sie hat. Begründung: 3^r enthält die «Maximaldosis» an Faktoren 3, in der Differenz mit *c* ist der grösste gemeinsame Teiler enthalten; dieser enthält nur noch so viele Faktoren 3 wie c sie besitzt, sofern *c* ≤ $3^r - 1$ ist.

Ein Beispiel hierzu: 45 - 1 hat 0 Faktoren 3, weil 1 ebenfalls 0 Faktoren 3 hat; 45 - 3 hat einen Faktor 3, weil 3 auch einen Faktor 3 hat; 45 - 6 hat einen Faktor 3, weil 6 auch nur einen hat.

Es ist $\binom{a \cdot 3^r}{3^r} = \frac{a \cdot 3^r}{3^r} \cdot \frac{a \cdot 3^r - 1}{3^r - 1} \cdot \frac{a \cdot 3^r - 2}{3^r - 2} \cdot \ldots (3^r \; Faktoren)$. In jedem Bruchfaktor dieses Terms haben Zähler und Nenner gemäss obiger Bemerkung gleich viele Faktoren 3 (natürlich ev. auch keine). Alle Faktoren 3 kürzen sich somit vollständig heraus (*a* enthält auch keinen Faktor 3, da teilerfremd zu 3^r).
Deshalb kann 3 den Koeffizienten $\binom{a \cdot 3^r}{3^r}$ nicht teilen. □

Ein Beispiel mit *r* = 2 und *a* = 5:
$\binom{45}{9} = \frac{45}{9} \cdot \frac{44}{8} \cdot \frac{43}{7} \cdot \frac{42}{6} \cdot \frac{41}{5} \cdot \frac{40}{4} \cdot \frac{39}{3} \cdot \frac{38}{2} \cdot \frac{37}{1} = \frac{5}{1} \cdot \frac{44}{8} \cdot \frac{43}{7} \cdot \frac{14}{2} \cdot \frac{41}{5} \cdot \frac{40}{4} \cdot \frac{13}{1} \cdot \frac{38}{2} \cdot \frac{37}{1}$.
Alle Faktoren 3 haben sich herausgekürzt; $\binom{45}{9}$ ist nicht durch 3 teilbar.

Korollar:
Wir betrachten im Pascalschen Dreieck die *inneren* Binomialkoeffizienten $\binom{m}{k}$ einer Zeile *m* (Nummerierung der Zeilen bei Zeile 0 beginnend), also diejenigen, die sich nicht an den äussersten Rändern befinden, d.h. $1 \leq k \leq m-1$.

Behauptung:
Der grösste gemeinsame Teiler (ggT) der inneren Binomialkoeffizienten einer Zeile *m* im Pascalschen Dreieck ist

- *p*, falls $m = p^r, r \in \mathbb{N} \setminus \{0\}$
- 1 sonst.

Beweis:
Sei zunächst *m* keine reine Primzahlpotenz.
Annahme: Sei der grösste gemeinsame Teiler *d* der inneren Binomialkoeffizienten der Zeile *m* grösser als 1.
Sei *p* ein Primfaktor von *d*.
Dann teilt *p* als Teil des ggT alle inneren Binomialkoeffizienten der Zeile *m*.
Nach dem Satz oben ist dann jedoch $m = p^r$ = reine Primzahlpotenz:
Widerspruch zur Voraussetzung. Folglich ist die Annahme falsch; es folgt *d* =1.

Sei nun $m = p^r$.
Der ggT der inneren Binomialkoeffizienten der Zeile *m* ist dann wegen $\binom{p^r}{1} = p^r$ eine reine Potenz von *p*. Wir zeigen, dass es sich nur um die erste Potenz, *p* selber, handeln kann:
$\binom{p^r}{p^{r-1}}$ ist durch *p*, jedoch nicht durch eine höhere Potenz von *p* teilbar:

$$\binom{p^r}{p^{r-1}} = \frac{p^r}{p^{r-1}} \cdot \frac{p^r - 1}{p^{r-1} - 1} \cdot \frac{p^r - 2}{p^{r-1} - 2} \cdot \ldots (p^{r-1}\ Faktoren)$$
$$= p \cdot \frac{p^r - 1}{p^{r-1} - 1} \cdot \frac{p^r - 2}{p^{r-1} - 2} \cdot \ldots\ (p^{r-1}\ Faktoren)$$

Wir kürzen den ersten Faktor zu *p*. Die übrigen Bruchfaktoren enthalten im Zähler und Nenner wieder je gleich viele Faktoren *p* (Überlegung wie im Beweis zum Satz oben), die sich alle wegkürzen. Wir haben ganz links den Faktor *p*; in den nachfolgenden Bruchfaktoren ist *p* nicht mehr enthalten.

Damit ist der ggT der inneren Binomialkoeffizienten der Zeile $m = p^r$ gleich *p.*

□