Pascal's tafel modulo priemmachten bekeken

Bachelorscriptie

July 21, 2014

Auteur:
Judith van Dulst
3470822

Begeleider:
prof. dr. F. Beukers

Universiteit Utrecht

Inhoud

1 Inleiding

De driehoek van Pascal begint met op de 0-de rij een 1. In elke volgende rij is elk getal de som van de twee getallen die er schuin boven staan. De driehoek gaat er dan als volgt uit zien

Rij											
0					1						
1				1		1					
2			1		2		1				
3		1		3		3		1			
4	1		4		6		4		1		
5	1	5		10		10		5		1	

enzovoort

In de driehoek van Pascal zijn de binomiaal coëfficiënten te vinden. In de n-de rij op de k+1-de plek is $\binom{n}{k}$ te vinden. Met $\binom{n}{k}$ kunnen we het aantal mogelijkheden vinden om k elementen te kiezen uit een verzameling van n elementen. Volgens de optelregel van de driehoek van Pascal zou dus moeten gelden

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

Dit is te verklaren door naar een verzameling van n elementen te kijken en bekijk hieruit 1 willekeurig element. Dit elementen kan wel of niet gekozen worden. Als het element niet gekozen wordt moeten er nog k elementen uit de overige $n-1$ elementen gekozen worden. Dit wordt gegeven door $\binom{n-1}{k}$. Als het element wel gekozen wordt moeten er nog $k-1$ elementen gekozen worden uit de overige $n-1$ elementen. Dit wordt gegeven door $\binom{n-1}{k-1}$. Dus de regel volgt.
Er geldt $\binom{0}{0} = 1$. Uit een verzameling van 0 elementen kan slechts op 1 manier 0 elementen gekozen worden.
Hiermee zien we dat inderdaad de binomiaal coëfficiënten af te lezen zijn in de driehoek van Pascal.

In deze scriptie gaan we kijken naar de driehoek van Pascal, en daarmee ook de binomiaal coëfficiënten, maar dan modulo priemmachten bekeken.

2 Opbouw

In deze scriptie bekijken we de initiatormethode om Pascal's tafel modulo op te bouwen. We bekijken eerst de priemgetallen 2 en 3, om daarna te onderzoeken of we deze methode kunnen generaliseren voor een willekeurig priemgetal.

Na het bekijken van een willekeurig priemgetal rijst de vraag of we deze methode ook kunnen gebruiken voor machten van priemgetallen. Eerst zullen we dit onderzoeken voor modulo 4 en daarna voor p^2 met p een willekeurig priemgetal.

3 Pascal's tafel

Voor de initiatormethode die we gaan bekijken is het handiger om Pascal's driehoek in een andere vorm te bekijken. We gebruiken hiervoor Pascal's tafel. Pascal's tafel bouwen we op door horizontaal k te zetten en verticaal l. Op plek (k, l) komt $\binom{k+l}{k}$.

	0	1	2	$\cdots$	k
0	$\binom{0}{0}$	$\binom{1}{1}$	$\binom{2}{2}$	$\cdots$	$\vdots$
1	$\binom{1}{0}$	$\binom{2}{1}$	$\binom{3}{2}$	$\cdots$	$\vdots$
2	$\binom{2}{0}$	$\binom{3}{1}$	$\binom{4}{2}$	$\cdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
l	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\binom{k+l}{k}$

Zo wordt Pascal's tafel

1	1	1	...	$\binom{k}{k}$
1	2	2	...	$\vdots$
1	3	6	...	$\vdots$
$\vdots$	...	...	$\ddots$	$\vdots$
$\binom{n-k}{k}$	...	...	...	$\binom{n}{k}$

waarbij $n = k + l$.

4 Stelling van Lucas

Om de initiatormethode modulo p te kunnen bewijzen hebben we de stelling van Lucas nodig. Deze luidt als volgt.

Stelling 4.1 (Stelling van Lucas) *Stel* $n = n_0 + n_1 p + n_2 p^2 + ... + n_d p^d$ *en* $m = m_0 + m_1 p + m_2 p^2 + ... + m_d p^d$ *waarin* $0 \leq m_i, n_i \leq p - 1$ *voor alle* i.
Dan geldt

$$\binom{n}{m} \equiv \binom{n_o}{m_o}\binom{n_1}{m_1}...\binom{n_d}{m_d} (mod\ p)$$

Om deze stelling te bewijzen zullen we eerst twee andere stellingen bewijzen die we hiervoor nodig hebben.

Stelling 4.2 *Stelling:*

$$\binom{p}{k} \equiv 0\ \ als\ 0 < k < p$$

Bewijs:

$$\binom{p}{k} = \frac{p!}{(p-k!)k!}$$

$p! = p(p-1)...2 \cdot 1$ dus $p \mid p!$, maar $p \not\mid (p-k)!$ aangezien $p-k < p$ en $p \nmid k!$ aangezien $k < p$. Hieruit volgt dat p niet boven en onder de deelstreep weggedeeld kan worden en dus $p \mid \binom{p}{k}$. De stelling volgt. □

Stelling 4.3

$$(x+1)^{p^r} \equiv x^{p^r} + 1 (mod\ p)$$

Bewijs:

$$(x+1)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1} + ... + \binom{p}{p-1}x + \binom{p}{p}$$

Uit stelling 1 volgt:

$$\begin{aligned} (x+1)^p &\equiv \binom{p}{0}x^p + \binom{p}{p} (\text{mod p}) \\ &\equiv x^p + 1 (\text{mod p}) \end{aligned}$$

Dan:

$$\begin{aligned} & (x+1)^{p^r} \\ = \quad & ((x+1)^p)^{p^{r-1}} \\ \equiv \quad & (x^p+1)^{p^{r-1}} (\text{mod p}) \\ \equiv \quad & ((x^p+1)^p)^{p^{r-2}} (\text{mod p}) \\ \equiv \quad & (x^{p^2}+1)^{p^{r-2}} (\text{mod p}) \\ \equiv \quad & ... \\ \equiv \quad & x^{p^r} + 1 (\text{mod p}) \end{aligned}$$

□

Met deze twee stellingen kunnen we nu de stelling van Lucas bewijzen.

Bewijs:

We hebben $n = n_0 + n_1 p + n_2 p^2 + ... + n_d p^d$ en $m = m_0 + m_1 p + m_2 p^2 + ... + m_d p^d$ met $0 \leq m_i, n_i \leq p-1$
Bekijk

$$\begin{aligned} \sum_{k=0}^{n} \binom{n}{k} x^k &= (x+1)^n \\ &= (x+1)^{n_0}(x+1)^{n_1 p}...(x+1)^{n_d p^d} \end{aligned}$$

Uit stelling 2 volgt nu:

$$\begin{aligned} &\equiv (x+1)^{n_0}(x^p+1)^{n_1}....(x^{p^d}+1)^{n_d} (\text{mod p}) \\ &\equiv \sum_{a_0=0}^{n_o} \tbinom{n_o}{a_0} x^{a_0} \sum_{a_1=0}^{n_1} \tbinom{n_1}{a_1} x^{a_1 p}... \sum_{a_d=0}^{n_d} \tbinom{n_d}{a_d} x^{a_d p^d} \end{aligned}$$

Er geldt dat $\binom{n_i}{a_i} = 0$ als $a_i > n_i$. We zien dat $n_i \leq p-1$. Dit geeft:

$$\equiv \sum_{a_0=0}^{p-1} \binom{n_o}{a_0} x^{a_0} \sum_{a_1=0}^{p-1} \binom{n_1}{a_1} x^{a_1 p}... \sum_{a_d=0}^{p-1} \binom{n_d}{a_d} x^{a_d p^d}$$

Aan de linkerkant van de gelijkheid is $\binom{n}{m}$ de coëfficiënt van x^m. Nu zijn we geïnteresseerd in de coëfficiënt van x^m aan de rechterkant van de gelijkheid.

Dit betekent dat we $a_0, a_1, ..., a_d$ moeten vinden, zo dat

$$m = a_0 + a_1 p + ... + a_d p^d$$

Elke som loopt tot $p-1$. Hieruit volgt $0 \leq a_0 \leq p-1$. Dus we moeten $a_i = m_i$ kiezen.
De coëfficiënt van $x^{m_i p^i}$ is $\binom{n_i}{m_i}$. De coëfficiënt van x^m wordt

$$\binom{n_0}{m_0}\binom{n_1}{m_1}...\binom{n_d}{m_d}$$

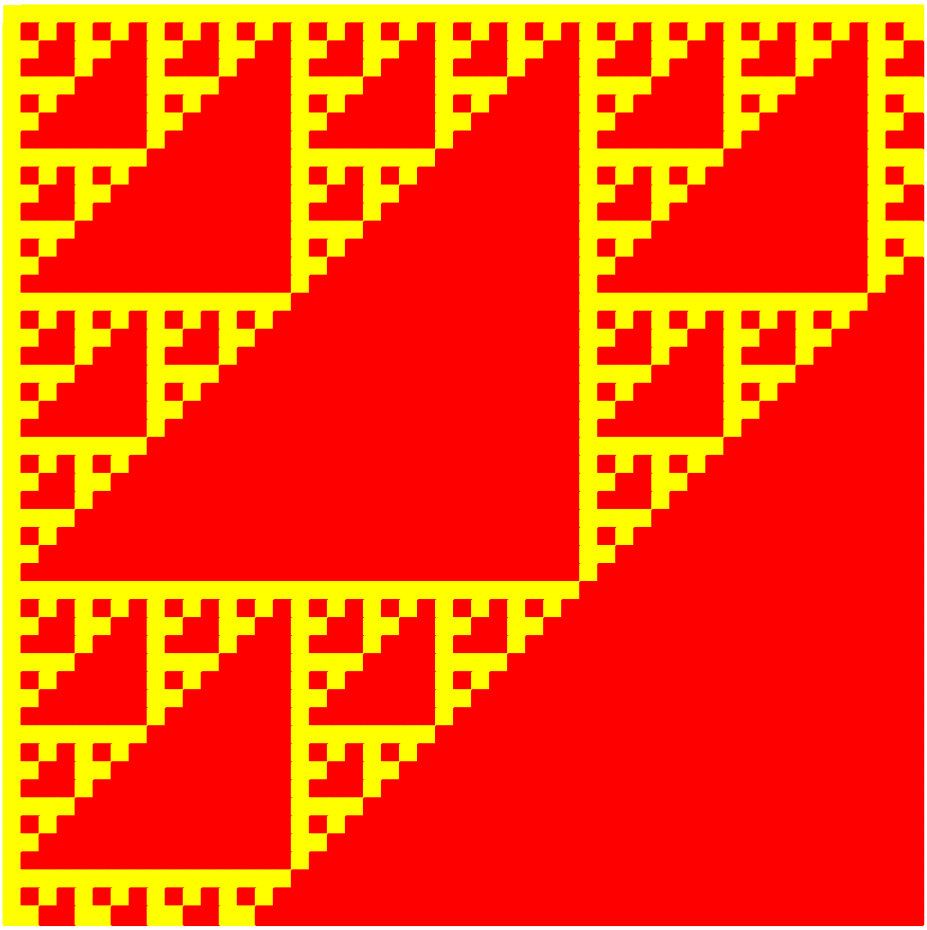
Dit geeft:

$$\binom{n}{m} = \binom{n_0}{m_0}\binom{n_1}{m_1}...\binom{n_d}{m_d} (\text{mod } p)$$

□

5 Modulo 2

We bekijken Pascal's tafel modulo 2:



Een geel vierkant betekent 1 (mod 2) en een rood vierkant betekent 0(mod 2).

Stelling 5.1 *De tafel van pascal modulo 2 kan als volgt opgebouwd worden. Begin met de volgende initiator*

$$\begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$$

Merk op dat de initiator Pascal's tafel modulo 2 is waarbij we k en l van 0 tot 1 laten lopen.
Nu kan de tafel verder opgebouwd worden door elke 0 te vervangen door:

$$\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}$$

En elke 1 te vervangen door:

$$\begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$$

Zo zou de eerste stap dus geven

$$\begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{matrix}$$

En de tweede stap

$$\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}$$

Bewijs: Bekijk $\binom{n}{k}$. Deze staat in de tafel op plaats (k, l). Elk getal wordt vervangen door een 2×2-vierkant. Dus (k, l) komt terecht op

$$\begin{matrix} (2k, 2l) & (2k+1, 2l) \\ (2k, 2l+1) & (2k+1, 2l+1) \end{matrix}$$

Oftewel $\binom{k+l}{k} = \binom{n}{k}$ komt terecht op

$$\begin{matrix} \binom{2k+2l}{2k} & \binom{2k+1+2l}{2k+1} \\ \binom{2k+2l+1}{2k} & \binom{2k+1+2l+1}{2k+1} \end{matrix}$$

wat gelijk is aan

$$\begin{matrix} \binom{2n}{2k} & \binom{2n+1}{2k+1} \\ \binom{2n+1}{2k} & \binom{2n+2}{2k+1} \end{matrix}$$

Er geldt dat $n = n_0 + n_1 \times 2 + n_2 \times 2^2 + ...$ en $k = k_0 + k_1 \times 2 + k_2 \times 2^2 + ...$ dus $2n = 0 + n_0 \times 2 + n_1 \times 2^2 + n_2 \times 2^3 + ...$ en $2k = 0 + k_0 \times 2 + k_1 \times 2^2 + k_2 \times 2^3 + ...$

Bekijk nu $\binom{2n+n_0}{2k+k_0}$ met $n_0 \leq 2$, $k_0 \leq 1$ en $n_0 \geq k_0$.
Stel dat $n_0 < 2$. Dan

$$\binom{2n+n_0}{2k+k_0} = \binom{[2n+n_0/2]}{[2k+k_0/2]}\binom{n_o}{k_0} \equiv \binom{n}{k}\binom{n_0}{k_0} (\text{mod } 2)$$

In dit geval kun je dus de waarde van $\binom{n}{k}$ vermenigvuldigen met de waarde van de initiator op deze plaats.

Stel nu dat $n_0 \geq 2$ Dan

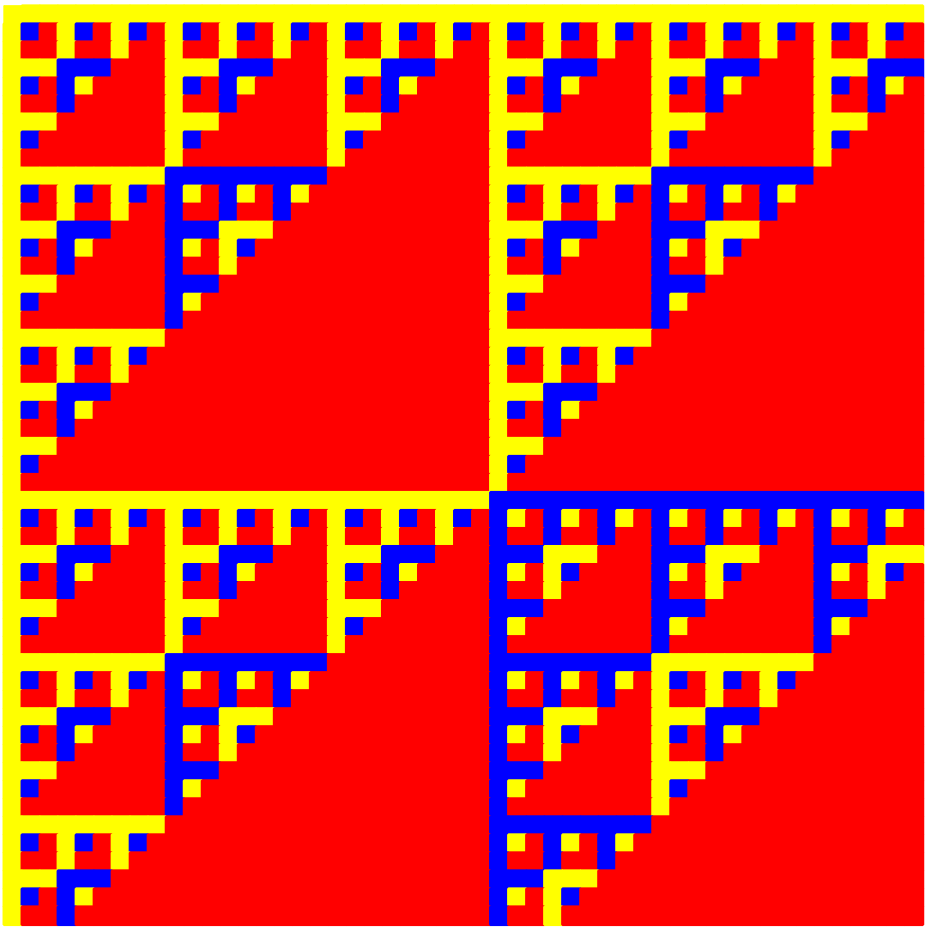
$$\binom{2n+n_0}{2k+k_0} = \binom{[2n+n_0/2]}{[2k+k_0/2]}\binom{n_o-2}{k_0} \equiv \binom{n+1}{k} \times 0 \equiv 0 (\text{mod } 2)$$

In de initiator staat op de plaatsen waarvoor geldt dat $n_0 \geq 2$ een 0. Ook in dit geval kunnen we dus de waarde van $\binom{n}{k}$ vermenigvuldigen met de waarde van de initiator op deze plaats.

□

6 Modulo 3

We bekijken Pascal's tafel modulo 3:



Een rood vierkant betekent 0(mod 3), een geel vierkant betekent 1(mod 3) en een blauw vierkant betekent 2(mod 3).

Stelling 6.1 *De tafel van pascal modulo 3 kan als volgt worden opgebouwd. Begin met de volgende intitiator*

$$\begin{matrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 0 \end{matrix}$$

Merk op dat de initiator de tafel van pascal modulo 3 is waarbij k en l van 0 tot 2 lopen.
Nu kan de tafel verder opgebouwd worden door elke 0 te vervangen door:

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

Elke 1 te vervangen door:

$$\begin{matrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 0 \end{matrix}$$

En elke 2 te vervangen door:

$$\begin{matrix} 2 & 2 & 2 \\ 2 & 1 & 0 \\ 2 & 0 & 0 \end{matrix}$$

Deze stelling volgt uit stelling 7.1 die voor willekeurige priegetallen p geldt.

7 Modulo p

De initiator methode die we hebben gezien bij modulo 2 en modulo 3 kunnen we generaliseren voor een priemgetal p.

Stelling 7.1 *Pascal's tafel modulo p kunnen we als volgt opbouwen. Neem als initiator het $p \times p$ - vierkant met $\binom{k+l}{k} (mod\ p)$ op plek (k, l)*
Vervang daarna elk getal α door het $p \times p$ - vierkant dat onstaat door elk getal in de initiator te vermenigvuldigen met α.

Bewijs:

Elk getal wordt vervangen door een $p \times p$-vierkant. Dan komt $\binom{n}{k}$ terecht op:

$$\begin{array}{cccc} \binom{pn}{pk} & \binom{pn+1}{pk+1} & \cdots & \binom{pn+(p-1)}{pk+(p-1)} \\ \binom{pn+1}{pk} & \binom{pn+2}{pk+1} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \binom{pn+(p-1)}{pk} & \cdots & \cdots & \binom{pn+(2p-2)}{pk+(p-1)} \end{array}$$

Bekijk nu $\binom{pn+n_0}{pk+k_0}$.
Stel $n_0 < p$

$$\binom{pn+n_0}{pk+k_0} \equiv \binom{[(pn+n_0)/p]}{[(pk+k_0)/p]}\binom{n_0}{k_0} \equiv \binom{n}{k}\binom{n_0}{k_0} (\text{mod p})$$

Vermenigvuldig dus de waarde van $\binom{n}{k}$ met de waarde van de initiator op deze plaats.

Stel $n_0 \geq p$.

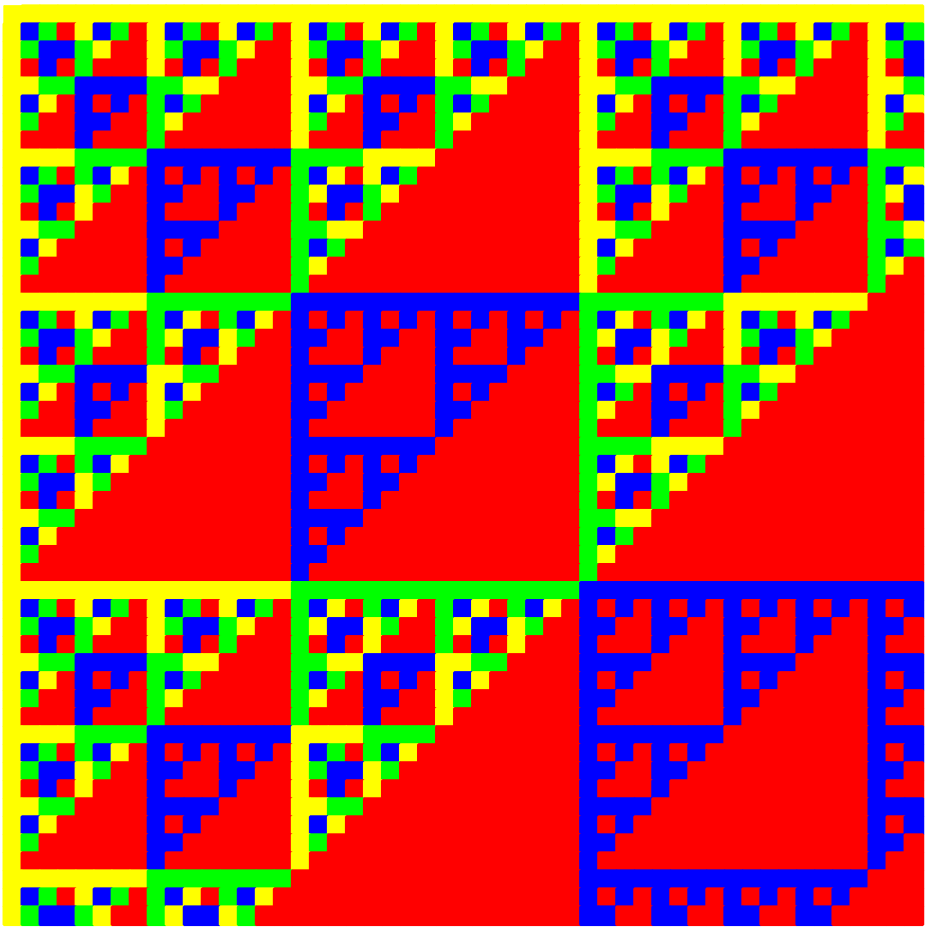
$$\binom{pn+n_0}{pk+k_0} \equiv \binom{[(pn+n_0)/p]}{[(pk+k_0)/p]}\binom{n_0-p}{k_0} \equiv \binom{n+1}{k} \times 0 \equiv 0 (\text{mod p})$$

Er geldt dat $\binom{n_0-p}{k_0} \equiv 0$, want $n_0 = k_0 + l_0 \Rightarrow n_0 - p = k_0 + l_0 - p < k_0$.

Op de plaatsen in de initiator waarvoor geldt dat $n_0 \geq p$ staat een 0. Dus ook in dit geval kunnen we de waarde van $\binom{n}{k}$ vermenigvuldigen met de waarde van de initiator op deze plaats. $\square$

8 Modulo 4

We bekijken Pascal's tafel modulo 4:



Een rood vierkant betekent 0(mod 4), een geel vierkant betekent 1(mod 4), een blauw vierkant betekent 2(mod 4) en een groen vierkant betekent 3(mod 4).

Stelling 8.1 *Pascal's tafel modulo 4 kan als volgt worden opgebouwd. Begin met de volgende initiator*

$$\begin{matrix} 1 & 1 \\ 1 & 2 \end{matrix}$$

Elk getal wordt vervangen door een 2×2-vierkant. Door welk vierkant een getal wordt vervangen hangt af van de waarden van k en l modulo 2. Dit wordt weergegeven in onderstaande tabel.

$k \equiv 0(mod\ 2)$ $l \equiv 0(mod\ 2)$	$k \equiv 1(mod\ 2)$ $l \equiv 0(mod\ 2)$	$k \equiv 0(mod\ 2)$ $l \equiv 1(mod\ 2)$	$k \equiv 1(mod\ 2)$ $l \equiv 1(mod\ 2)$
1 1 *1 2*	*1 1* *3 0*	*1 3* *1 0*	*1 1* *1 2*

Vermenigvuldig zo'n vierkant met de waarde van $\binom{n}{k}$ om te vinden door welk vierkant $\binom{n}{k}$ vervangen moet worden.

Let op: Als $k \equiv l \equiv 1(\text{mod } 2)$ dan volgt uit de stelling van Lucas dat $\binom{n}{k} \equiv 0(\text{mod } 2)$. Dus in dit geval geldt dat $\binom{n}{k} \equiv 0(\text{mod } 4)$ of $\binom{n}{k} \equiv 2(\text{mod } 4)$. Dit betekent dat $\binom{n}{k} \equiv -\binom{n}{k}$. Hierdoor zal het soms lijken alsof de twee bewijzen voor deze stelling niet overeen komen, terwijl dit wel het geval is.

Om de initiatormethode voor modulo 4 te kunnen bewijzen hebben we een nieuwe stelling nodig. De stelling van Lucas konden we enkel gebruiken voor priemgetallen. De volgende stelling kunnen we gebruiken voor machten van priemgetallen.

Eerst voeren we een aantal notaties in. $N_0 = n - p^q[n/p^q] = n - n_q p^q$, K_0 en L_0 worden op eenzelfde manier gedefiniëerd en $(n!)_p$ is het product van de getallen $\leq n$ die niet deelbaar zijn door p. Verder definiëren we

$$\epsilon \equiv \begin{cases} 1 \text{ als } p=2, q \geq 3 \\ -1 \text{ anders} \end{cases}$$

en

$$\alpha = \begin{cases} 0 \text{ als } K_0 + L_0 < p^q \\ 1 \text{ als } K_0 + L_0 \geq p^q \end{cases}$$

Stelling 8.2

$$\binom{n}{k} = (\epsilon)^\alpha \frac{(N_0!)_p}{(K_0!)_p (L_o!)_p} \frac{([k/p] + [l/p])!}{[k/p]![l/p]!} \text{ als } k_0 + l_0 < p$$

en

$$\binom{n}{k} = (\epsilon)^{\alpha} \frac{(N_0!)_p}{(K_0!)_p (L_o!)_p} \frac{([k/p]+[l/p])!}{[k/p]![l/p]!} p([k/p]+[l/p]+1) \text{ als } k_0 + l_0 \geq p$$

Bewijs:

We bekijken $n!$ en we delen dit op in factoren die deelbaar zijn door p en factoren die niet deelbaar zijn door p. Zo krijgen we

$$n! = \prod_{\substack{r=1 \\ p \nmid r}}^{n} r \prod_{\substack{r=1 \\ p \mid r}}^{n} r$$

We bekijken eerst de factoren die wel deelbaar zijn door p

$$\begin{aligned} \prod_{\substack{r=1 \\ p \mid r}}^{n} r &= p \cdot 2p \cdot 3p \cdots [n/p]p \\ &= p^{[n/p]} \cdot 1 \cdot 2 \cdot 2 \cdots [n/p] \\ &= p^{[n/p]} [n/p]! \end{aligned}$$

Voor de factoren die niet deelbaar zijn door p krijgen we:

$$\begin{aligned} \prod_{\substack{r=1 \\ p \nmid r}}^{n} r &= \prod_{\substack{r=1 \\ p \nmid r}}^{n_q p^q} r \prod_{\substack{r=1 \\ p \nmid r}}^{n-n_q p^q} (n_q p^q + r) \\ &= \prod_{\substack{r=1 \\ p \nmid r}}^{n_q p^q} r \prod_{\substack{r=1 \\ p \nmid r}}^{N_0} (n_q p^q + r) \end{aligned}$$

Er geldt dat

$$\prod_{\substack{r=1 \\ p \nmid r}}^{p^q} r = \epsilon \equiv \begin{cases} 1 (\text{mod } p^q) \text{ als } p=2, q \geq 3 \\ -1 (\text{mod } p^q) \text{ anders} \end{cases}$$

en dus

$$\prod_{\substack{r=1 \\ p \nmid r}}^{n_q p^q} r \equiv (\epsilon)^{n_q} (\text{mod } p^q)$$

Voor de andere factor geldt

$$\begin{aligned} \prod_{\substack{r=1 \\ p \nmid r}}^{N_0} (n_q p^q + r) &\equiv \prod_{\substack{r=1 \\ p \nmid r}}^{N_0} r \\ &\equiv (N_0!)_p (\text{mod } p^q) \end{aligned}$$

Zo vinden we dus voor $n!$

$$n! = p^{[n/p]}[n/p]!\tilde{N} \text{ met } \tilde{N} \equiv (\epsilon)^{n_q}(N_0!)_p (\text{mod } p^q)$$

Op analoge manier zijn uitdrukkingen voor k en l te vinden

$$\begin{aligned} k! = p^{[k/p]}[k/p]!\tilde{K} \text{ met } \tilde{K} \equiv (\epsilon)^{k_q}(K_0!)_p (\text{mod } p^q) \\ l! = p^{[l/p]}[l/p]!\tilde{L} \text{ met } \tilde{L} \equiv (\epsilon)^{l_q}(L_0!)_p (\text{mod } p^q) \end{aligned}$$

Dit kunnen we gebruiken om een uitdrukking te vinden voor $\binom{n}{k}$

$$\binom{n}{k} = \frac{n!}{k!l!} \equiv p^{[n/p]-[k/p]-[l/p]} \frac{[n/p]!}{[k/p]![l/p]!} (\epsilon)^{n_q - k_q - l_q} \frac{(N_0!)_p}{(K_0!)_p (L_0!)_p} (\text{mod } p^q)$$

Schrijf nu

$$\begin{aligned} n = p[n/p] + n_0 \quad 0 \leq n_0 < p \\ k = p[k/p] + k_0 \quad 0 \leq k_0 < p \\ l = p[l/p] + l_0 \quad 0 \leq l_0 < p \end{aligned}$$

Dan

$$[n/p] - [k/p] - [l/p] = \begin{cases} 0 \text{ als } k_0 + l_0 < p \\ 1 \text{ als } k_0 + l_0 \geq p \end{cases}$$

Hieruit volgt

$$p^{[n/p]-[k/p]-[l/p]}\frac{[n/p]!}{[k/p]![l/p]!} \equiv \begin{cases} p^0 \frac{[n/p]!}{[k/p]![l/p]!} \equiv \frac{([k/p]+[l/p])!}{[k/p]![l/p]!} \text{ als } k_0+l_0<p \\ p^1 \frac{[n/p]!}{[k/p]![l/p]!} \equiv p([k/p]+[l/p]+1)\frac{([k/p]+[l/p])!}{[k/p]![l/p]!} \text{ als } k_0+l_0\geq p \end{cases}$$

Dan

$$(n_q - k_q - l_q)p^q = (n - N_0) - (k - K_0) - (l - L_0) = -(N_0 - K_0 - L_0)$$

dus

$$\alpha = n_q - k_q - l_q = -\frac{N_0 - K_0 - L_0}{p^q} = \begin{cases} 0 \text{ als } K_0+L_0<p^q \\ 1 \text{ als } K_0+L_0\geq p^q \end{cases}$$

We vinden dat

$$\binom{n}{k} = (\epsilon)^\alpha \frac{(N_0!)_p}{(K_0!)_p(L_o!)_p}\frac{([k/p]+[l/p])!}{[k/p]![l/p]!} \text{ als } k_0+l_0<p$$

en

$$\binom{n}{k} = (\epsilon)^\alpha \frac{(N_0!)_p}{(K_0!)_p(L_o!)_p}\frac{([k/p]+[l/p])!}{[k/p]![l/p]!}p([k/p]+[l/p]+1) \text{ als } k_0+l_0\geq p$$

Er geldt dat $n = p[n/p] + n_0 = [n/p^q]p^q + N_0$. Dus $N_0 \equiv p[n/p] + n_0 (\text{mod } p^q)$. Dit geldt ook voor K_0 en L_0.

□

Met deze stelling kunnen we nu de initiator methode bewijzen voor modulo 4.

In dit bewijs zijn alle equivalenties modulo 4, tenzij anders aangegeven.

Bewijs:

We hebben

$$\begin{aligned} n &= 2[n/2] + n_0 \\ k &= 2[k/2] + k_0 \\ l &= 2[l/2] + l_0 \end{aligned}$$

We gaan bekijken $\binom{2n+\beta+\gamma}{2k+\beta}$. Stel eerst dat $\beta + \gamma < 2$ Dan

$$\begin{aligned} 2n + \beta + \gamma = (\beta + \gamma) + 2(n_0 + 2[n/2]) \quad & (2n + \beta + \gamma)_0 \equiv \beta + \gamma + 2n_0 \\ 2k + \beta = \beta + 2(k_0 + 2[k/2]) \quad & (2k + \beta)_0 \equiv \beta + 2k_0 \\ 2l + \gamma = \gamma + 2(l_0 + 2[l/2]) \quad & (2l + \gamma)_0 \equiv \gamma + 2l_0 \end{aligned}$$

Dit geeft

$$\binom{2n+(\beta+\gamma)}{2k+\beta} \equiv (-1)^{\alpha} \frac{((\beta+\gamma+2n_0)!)_2}{((\beta+2k_0)!)_2((\gamma+2l_0)!)_2} \binom{n}{k}$$

Er geldt

$$\alpha = \begin{cases} 1 & \text{als } k \equiv l \equiv 1 (\text{mod } 2) \\ 0 & \text{anders} \end{cases}$$

Zo vinden we

$$\binom{2n}{2k} \equiv \begin{cases} -\binom{n}{k} & \text{als } k \equiv l \equiv 1 (\text{mod } 2) \\ \binom{n}{k} & \text{anders} \end{cases}$$

$$\binom{2n+1}{2k+1} \equiv \begin{cases} -\binom{n}{k} & \text{als } k \equiv 0 (\text{mod } 2) \text{ en } l \equiv 1 (\text{mod } 2) \\ \binom{n}{k} & \text{anders} \end{cases}$$

$$\binom{2n+1}{2k} \equiv \begin{cases} -\binom{n}{k} & \text{als } k \equiv 1 (\text{mod } 2) \text{ en } l \equiv 0 (\text{mod } 2) \\ \binom{n}{k} & \text{anders} \end{cases}$$

Stel nu dat $\beta = \gamma = 1$ Dan

$$\begin{aligned} 2n+2 = 0 + 2(1 + n_0 + 2n_1) \quad & (2n+2)_0 \equiv 2 + 2n_0 \\ 2k+1 = 1 + 2(k_0 + 2k_1) \quad & (2k+1)_0 \equiv 1 + 2k_0 \\ 2l+1 = 1 + 2(l_0 + 2l_1) \quad & (2l+1)_0 \equiv 2 + 2l_0 \end{aligned}$$

Dan

$$\binom{2n+2}{2k+1} \equiv (-1)^{\alpha} \frac{(2+2n_0)!_2}{(1+2k_0)!_2(1+2l_0)!_2} 2(k+l+1) \binom{n}{k}$$

Er geldt

$$\alpha = \begin{cases} 0 & \text{als } k \equiv l \equiv 0 (\text{mod } 2) \\ 1 & \text{anders} \end{cases}$$

Zo vinden we

$$\binom{2n+2}{2k+1} \equiv \begin{cases} 2\binom{n}{k} & \text{als } k \equiv l (\text{mod } 2) \\ 0 & \text{als } k \not\equiv l (\text{mod } 2) \end{cases}$$

□

De initiatormethode modulo 4 kunnen we ook bewijzen door te kijken naar coëfficiënten.

Bewijs:

Om $\binom{2n}{2k}$ te bepalen zijn we op zoek naar de coëfficiënt van x^{2k} in $(1+x)^{2n}$.

$$(1+x)^{2n} = (1+2x+x^2)^n \equiv (1+x^2)^n + n(2x)(1+x^2)^{n-1} (\text{mod } 4)$$

Alle overige termen bevatten minstens twee keer de factor $2x$ en zijn dus gelijk aan $0(\text{mod } 4)$. De coëfficiënt van x^{2k} in $(1+x^2)^n$ is gelijk aan $\binom{n}{k}$. De term $n(2x)(1+x^2)^{n-1}$ geeft enkel oneven machten van x en draagt dus niet bij aan de coëfficiënt van x^{2k}.
We vinden

$$\binom{2n}{2k} \equiv \binom{n}{k} (\text{mod } 4)$$

Om $\binom{2n+1}{2k}$ te bepalen zijn we op zoek naar de coëfficiënt van x^{2k} in $(1+x)^{2n+1}$

$$\begin{aligned}
(1+x)^{2n+1} &= (1+x)^{2n}(1+x) \\
&= (1+2x+x^2)^n(1+x) \\
&\equiv (1+x)((1+x^2)^n) + n(2x)(1+x^2)^{n-1}) (\text{mod } 4) \\
&\equiv (1+x^2)^n + n(2x)(1+x^2)^{n-1} + x(1+x^2)^n + n(2x^2)(1+x^2)^{n-1} (\text{mod } 4)
\end{aligned}$$

De coëfficiënt van x^{2k} in $(1+x^2)^n + n(2x)(1+x^2)^{n-1}$ is $\binom{n}{k}$. De term $x(1+x^2)^n$ geeft enkel oneven machten van x dus draagt niet bij aan de coëfficiënt van x^{2k}. De coëfficiënt van x^{2k} in $n(2x^2)(1+x^2)^{n-1}$ is $2n\binom{n-1}{k-1} = 2n\frac{(n-1)!}{(k-1)!(n-k)!} = 2k\frac{n!}{k!(n-k)!} = 2k\binom{n}{k}$
Stel $k \equiv 0(\text{mod } 2)$. Dan

$$\binom{2n+1}{2k} \equiv \binom{n}{k} + 2k\binom{n}{k} \equiv \binom{n}{k} (\text{mod } 4)$$

Stel $k \equiv 1(\text{mod } 2)$. Dan

$$\binom{2n+1}{2k} \equiv \binom{n}{k} + 2k\binom{n}{k} \equiv -\binom{n}{k} (\text{mod } 4)$$

Om $\binom{2n+1}{2k+1}$ te bepalen zijn we op zoek naar de coëfficiënt van x^{2k+1} in $(1+x)^{2n+1}$

$$(1+x)^{2n+1} \equiv (1+x^2)^n + n(2x)(1+x^2)^{n-1} + x(1+x^2)^n + n(2x^2)(1+x^2)^{n-1} (\text{mod } 4)$$

De term $(1+x^2)^n$ geeft enkel even machten van x, $n(2x)(1+x^2)^{n-1}$ geeft $2n\binom{n-1}{k} = 2n\frac{(n-1)!}{(n-k-1)!k!} = 2(n-k)\frac{n!}{(n-k)!k!} = 2(n-k)\binom{n}{k}$, $x(1+x^2)^n$ geeft $\binom{n}{k}$ en $n(2x^2)(1+x^2)^{n-1}$ geeft enkel even machten.

Stel $n \equiv k (\text{mod } 2)$. Dan

$$\binom{2n+1}{2k+1} \equiv \binom{n}{k} + 2(n-k)\binom{n}{k} \equiv \binom{n}{k} (\text{mod } 4)$$

Stel $n \not\equiv k (\text{mod } 2)$. Dan

$$\binom{2n+1}{2k+1} \equiv \binom{n}{k} + 2(n-k)\binom{n}{k} \equiv -\binom{n}{k} (\text{mod } 4)$$

Om $\binom{2n+2}{2k+1}$ te bepalen zijn we op zoek naar de coëfficiënt van x^{2k+1} in $(1+x)^{2n+2}$

$$(1+x)^{2n+2} \equiv (1+x^2)^n + n(2x)(1+x^2)^{n-1} + 2x(1+x^2)^n + n(4x^2)(1+x^2)^{n-1} + x^2(1+x^2)^n + n(2x^3)(1+x^2)^{n-1}$$

De term $(1+x^2)^n + n(2x)(1+x^2)^{n-1}$ geeft $2(n-k)\binom{n}{k}$, $2x(1+x^2)^n$ geeft $2\binom{n}{k}$, $n(4x^2)(1+x^2)^{n-1} \equiv 0 (\text{mod } 4)$, $x^2)^{n-1}$ geeft enkel even machten en $n(2x^3)(1+x^2)^{n-1}$ geeft $2n\binom{n-1}{k-1} = 2n\frac{(n-1)!}{(n-k)!(k-1)!} = 2k\frac{n!}{(n-k)!k!} = 2k\binom{n}{k}$

Stel $n = equiv1 (\text{mod } 2)$. Dan

$$\binom{2n+2}{2k+1} \equiv 2n\binom{n}{k} + 2\binom{n}{k} \equiv 2\binom{n}{k} (\text{mod } 4)$$

Stel $n \equiv 0 (\text{mod } 2)$. Dan

$$\binom{2n+2}{2k+1} \equiv 2n\binom{n}{k} + 2\binom{n}{k} \equiv 0 (\text{mod } 4)$$

□

9 Modulo p^2

Na modulo 4 bekeken is te vermoeden dat deze methode te generaliseren is voor modulo p^2. Dit gaan we onderzoeken.
We beginnen dan met een $p \times p$-vierkant en onderzoeken of we dan weer elk getal door een $p \times p$-vierkant vervangen afhankelijk van de waarde van k en l modulo p.

Alle onderstaande equivalenties zijn modulo p^2, tenzij anders aangegeven.

We gaan $\binom{pn+\beta+\gamma}{pk+\beta}$ bekijken. Stel eerst dan $\beta + \gamma < p$. Dan

$$\begin{aligned} pn + \beta + \gamma = \beta + \gamma + p(n_0 + p[n/p]) \quad & N_0 \equiv \beta + \gamma + pn_0 \\ pk + \beta = \beta + p(k_0 + p[k/p]) \quad & K_0 \equiv \beta + pk_0 \\ pl + \gamma = \gamma + p(l_0 + p[l/p]) \quad & L_0 \equiv \gamma + pl_0 \end{aligned}$$

Dit geeft

$$\binom{pn + (\beta+\gamma)}{pk + \beta} \equiv (-1)^\alpha \frac{(\beta + \gamma + pn_0)!_p}{(\beta + pk_0)!_p (\gamma + pl_0)!_p} \binom{n}{k}$$

Behalve α hangt de waarde alleen af van n_0, k_0 en l_0. Om α te bepalen bekijken we $K_0 + L_0 = \beta + pk_0 + \gamma + pl_0$ We weten $\beta + \gamma \leq p - 1$. Dus $K_0 + L_0 < p^2$ als

$$p + pk_0 + pl_0 - 1 < p^2$$

$$p + pk_0 + pl_0 \leq p^2$$

$$1 + k_0 + l + 0 \leq p$$

We weten ook dat $0 \leq \beta + \gamma$. Dus $K_0 + L_0 \geq p^2$ als

$$pk_0 + pl_0 \geq p^2$$

$$k_0 + l_0 \geq p$$

$$1 + k_0 + l_0 > p$$

We zien dus dat ook de waarde van α af hangt van k_0 en l_0. Het is dus genoeg om de waarden van k en l modulo p te weten.

Nu moeten we ook nog het geval bekijken waarin $p \leq \beta + \gamma \leq 2p - 2$ Dan

$$\begin{aligned} pn + \beta + \gamma = (\beta + \gamma - p) + p(1 + n_0 + p[n/p]) \quad & N_0 \equiv \beta + \gamma + pn_0 \\ pk + \beta = \beta + p(k_0 + p[k/p]) \quad & K_0 = \beta + pk_0 \\ pl + \gamma = \gamma + p(l_0 + p[l/p]) \quad & L_0 = \gamma + pl_0 \end{aligned}$$

Dit geeft

$$\binom{pn+\beta+\gamma}{pk+\beta} \equiv (-1)^{\alpha} \frac{(\beta+\gamma+pn_0)!_p}{(\beta+pk_0)!_p)(\gamma+pl_0)} p(n+1)\binom{n}{k}$$

We bekijken $p(n+1)$ modulo p^2 dus hoeven we alleen de waarde van n modulo p te weten. Dus nu hangt alles behalve α af van de waarden van k en l modulo p.
Om α te bepalen kijken we weer naar $K_0 + L_0 = \beta + pk_0 + \gamma + pl_0$. We weten dat $\beta + \gamma \geq p$. Dus $K_0 + L_0 \geq p^2$ als

$$p + pk_0 + pl_0 \geq p^2$$

$$1 + k_0 + l_0 \geq p$$

We weten ook dat $\beta + \gamma \leq 2p - 2$. Dus $K_0 + L_0 < 2p^2$ als

$$2p - 2 + pk_0 + pl_0 < p^2$$

$$2p - 1 + pk_0 + pl_0 \leq p^2$$

$$2 - \frac{1}{p} + pk_0 + pl_0 \leq p^2$$

$$1 + pk_0 + pl_0 < p^2$$

De laatste stap volgt uit $2 - \frac{1}{p} > 1$. We zien dus dat het voor α ook genoeg is om de waarden van k en l modulo p te weten.

10 Conclusie

We hebben gezien dat de initiatormethode te gebruiken is voor willekeurige priemgetallen. Hierna hebben we gekeken naar kwadraten van priemgetallen. We hebben precies bekeken hoe dit werkt voor modulo 4. Ook hebben we onszelf ervan overtuigd dat we op eenzelfde manier deze methode kunnen gebruiken kwadraten van willekeurige priemgetallen.

11 Referenties

Andrew Granville, *Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995) CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253-276
Brad Wilson, *Asymptotic behavior of Pascal's triangle modulo a prime*, Acta Arithetica LXXXIII.2 (1998), pp. 105-116
Andrew Granville, *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's Triangle*, The American Mathematical Monthly 99, (1992), pp. 317-331