Proefstuderen Wiskunde,
Universiteit van Amsterdam, December 2021

Bewijzen, Geheimen, Priemgetallen (en waar ze te vinden)

Jeroen Zuiddam

1. Priemgetallen en waar ze te vinden

Priemgetallen zijn een cruciaal ingrediënt in de moderne cryptografie. De studie van priemgetallen gaat duizenden jaren terug en vormt nog altijd een centraal onderwerp in de wiskunde. Laten we eerst de definitie herhalen:

Definitie. Zij n een natuurlijke getal[1]. We noemen n een *priemgetal* als $n \geq 2$ en de enige delers van n zijn 1 en n.

De definitie roept direct allerlei vragen op. Hoeveel priemgetallen zijn er? Hoe zijn de priemgetallen verdeeld over alle natuurlijke getallen? Gegeven een getal, kunnen we snel (met een eenvoudig na te gaan criterium, of een eenvoudig uit te voeren algoritme) bepalen of het een priemgetal is? Laten we dat laatste het *priemtestprobleem* noemen. Ons doel is om het priemtestprobleem beter te begrijpen en een aloritme te beshrijven die het probleem oplost, een *priemtest* (primality test, in het Engels).

Hier is een eerste oplossing voor het priemtestprobleem, een simpel algoritme dat we (in het Engels) *exhaustive search* kunnen noemen. We zeggen er vooraf meteen bij dat dit algoritme niet computationeel efficiënt is, en dus zullen we hierna op zoek gaan naar iets slimmers.[2] (Waar we allerlei wiskunde voor nodig hebben.) Gegeven een getal n, om te testen of n een priemgetal is, kunnen we de definitie volgen en voor elke getal $2 \leq m \leq n-1$ kijken of m een deler is van n. Als we zo'n deler vinden dan is n duidelijk niet priem, en anders wel. Omdat dit algoritme bijna letterlijk is gebaseerd op de (bovenstaande) definitie van een priemgetal is het duidelijk dat het algoritme correct is.

Opgave 1. Kun je simpele verbeteringen bedenken voor bovenstaande algoritme, die het algoritme versnellen?

We gaan in de komende opgaven toewerken naar de *Fermat priemtest*, een simpele test (die wel computationeel efficiënt is) om te kijken of een getal een priemgetal is, met grote kans. Voordat we de Fermat priemtest kunnen bespreken, bespreken we wat basistheorie over priemgetallen, binomiaalcoefficiënten, en modulorekenen, en in het bijzonder de Kleine stelling van Fermat.

2. Oneindigheid van de priemgetallen

Om te beginnen: hoeveel priemgetallen zijn er? *A priori* zou het kunnen zijn dat er een eindige lijst (verzameling) $L = \{p_1, p_2, \ldots, p_k\}$ van priemgetallen is. Als dat het geval is dan is het priemtestprobleem makkelijk: gegeven een getal n, om te testen of n een priemgetal is, kijken

[1] De natuurlijke getallen zijn de getallen $1, 2, 3, 4, \ldots$

[2] De reden dat dit algoritme niet efficiënt is, is dat het exponentieel veel stappen kost in termen van de $\log_2(n)$ bits dat het kost om n te beschrijven. Het algoritme kost namelijk grofweg n stappen, wat exponentieel is in $\log_2(n)$. Als efficiënt algoritme beschouwen we elk algoritme dat polynomiaal in $\log_2(n)$ veel stappen gebruikt, dus bijvoorbeeld $(\log_2(n))^2$ stappen.

we simpelweg of n in de eindige lijst L voorkomt. Zo ja, dan is n priem en anders niet. Dit zou een extreem efficiënt algoritme opleveren. Echter, dit idee werkt niet, vanwege de volgende stelling (al meer dan tweeduizend jaar oud):

Stelling. *Er zijn oneindig veel priemgetallen.*

We herhalen het bewijs.

Bewijs. Dit is een zogenaamd "bewijs uit het ongerijmde", wat betekent dat we het tegenovergestelde (de negatie) van de bewering aannemen en daaruit een tegenspraak afleiden, zodat de originele bewering waar moet zijn. Dus, stel dat er *eindig* veel priemgetallen zijn (zeg het aantal is k) en noem deze priemgetallen $p_1, p_2, \ldots, p_k$. Neem nu het product van deze getallen en tel daar 1 bij op,

$$N = p_1 \cdot p_2 \cdots p_k + 1.$$

Het getal N kan geen priemgetal zijn, want dan zou het gelijk moeten zijn aan één van de p_i. (Waarom kan N niet gelijk zijn aan een van deze p_i?) Dus N heeft minstens één deler die ongelijk is aan 1 en ongelijk aan N. Van al die delers, laat q de kleinste zijn. Dan moet q een priemgetal zijn. (Waarom?) Aangezien, per aanname, $p_1, \ldots, p_k$ alle priemgetallen zijn, vinden we dat q gelijk is aan een p_i. Nu observeren we twee dingen: $q = p_i$ is een deler van N en $q = p_i$ is een deler van $p_1 \cdot p_2 \cdots p_k$. We concluderen hieruit dat q een deler is van het verschil $N - p_1 \cdot p_2 \cdots p_k = 1$. (Ga na: als een getal q twee getallen a en b deelt, dan deelt q ook het verschil $a - b$.) Maar q is ook niet gelijk aan 1. Dit geeft de gewenste tegenspraak. □

Nu we weten dat er oneindig veel priemgetallen, zijn er nog preciezere vragen die natuurlijk opkomen, bijvoorbeeld: hoe zijn de priemgetallen verspreid over de natuurlijk getallen? Hier is veel onderzoek over gedaan, waar we niet over in detail zullen treden, maar de intuïtie is: als je een willekeurig getal kies, dan is de kans vrij groot dat het een priemgetal is. Een simpele (vrij grove) versie van die uitspraak die makkelijk te onthouden is, is als volgt:

Stelling ("Postulaat van Bertrand")**.** *Voor elk natuurlijk getal n is er een priemgetal dat tussen n en $2n$ ligt.*

(We zullen het bewijs hier niet geven. Voor een mooi bewijs van dit resultaat zie het boek "Proofs from the book" van Aigner en Ziegler.)

Met andere woorden, als je een priemgetal zoekt van grootte ongeveer n, dan kun je over de getallen $n, n+1, n+2, \ldots, 2n$ lopen, en kom je sowieso minstens één priemgetal tegen. Om te herkennen welk van deze getallen een priemgetal is, hebben we echter uiteraard een methode nodig om te testen of een getal priem is, het doel dat we ons eerder hebben gesteld.

Opgave 2. Ga na dat het Postulaat van Bertrand waar is voor $n \leq 50$. Hier zijn alle priemgetallen onder de 50:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

3. Hoofdstelling van de rekenkunde

Nu brengen we in herinnering de belangrijke Hoofdstelling van de rekenkunde (net als de oneindigheid van de priemgetallen is deze stelling al meer dan tweeduizend jaar oud), die zegt dat priemgetallen de "bouwstenen" van de natuurlijke getallen zijn, in de volgende zin:

Stelling (Hoofdstelling van de rekenkunde)**.** *Elk natuurlijk getal is te schrijven als product van priemgetallen, en deze schrijfwijze is uniek op volgorde na.*

(We hebben een schets van het bewijs voor existentie in het hoorcollege gezien, en zullen het bewijs van uniciteit overslaan, alhoewel dat wel elementair is.)

Het schrijven van een natuurlijk getal als product van priemgetallen heet een *priemontbinding*. De Hoofdstelling van de rekenkunde zegt dat ieder natuurlijk getal een priemontbinding heeft en dat de priemontbinding uniek is, op volgorde na van de factoren in het product.

Opgave 3. In de definitie van priemgetallen wordt het getal 1 niet priem genoemd. Kun je, met de Hoofdstelling van de rekenkunde in het achterhoofd, een goed argument vinden dat we 1 inderdaad niet priem moeten noemen?

Opgave 4. Gebruik de Hoofdstelling van de rekenkunde om te bewijzen dat $\sqrt{2}$ geen rationaal getaal is. Dat will zeggen: bewijs dat $\sqrt{2}$ niet geschreven kan worden als een breuk $\frac{a}{b}$ voor natuurlijke getallen a en b. Hint: Probeer een bewijs uit het ongerijmde. Dus: neem aan dat $\sqrt{2}$ *wel* kan worden geschreven als $\sqrt{2} = \frac{a}{b}$ voor natuurlijke getallen a en b. Probeer vervolgens door algebraïsche manipulatie een gelijkheid te maken van natuurlijke getallen en vervolgens een tegenspraak af te leiden door middel van de Hoofdstelling van de rekenkunde.

4. Freshman's dream

We gaan nu een lemma bewijzen dat vaak Freshman's dream (droom van de eerstejaars student) wordt genoemd. Hiervoor gebruiken we de belangrijke Binomiaalstelling. De Binomiaalstelling geeft aan wat er gebeurt als we een uitdrukking van de vorm $(x+y)^n$ uitschrijven als één grote som. Om dit te kunnen bespreken hebben we het combinatorische begrip binomiaalcoëfficiënten nodig.

Definitie (Faculteit en binomiaalcoëfficiënten)**.** Voor elk natuurlijk getal n gebruiken we de notatie $n!$ voor het product van de getallen 1 tot en met n, dus $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$. We spreken $n!$ uit als n faculteit. Voor natuurlijke getallen n en k met $k \leq n$ definiëren we de getallen

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

De getallen $\binom{n}{k}$ heten *binomiaalcoëfficiënten* en we spreken $\binom{n}{k}$ ook wel uit als n *choose* k (in het Engels).

Opgave 5. In deze opgave bekijken we wat de betekenis is van de faculteit en de binomiaalcoëfficiënten.

(a) Stel je voor dat je n verschillende boeken hebt (of andere objecten) die je op een rij wilt zetten. Bewijs dat dit op $n!$ verschillende manieren kan.

(b) Stel nu dat je k kopieën hebt van een boek en $n-k$ kopieën van een ander boek. Kopieën van hetzelfde boek kun je niet van elkaar onderscheiden. Je wilt nu deze boeken op volgorde zetten. Bewijs dat dit op $\binom{n}{k}$ verschillende manieren kan.

De binomiaalcoëfficiënten spelen een prominente rol in de Binomiaalstelling:

Stelling (Binomiaalstelling)**.** $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ *voor alle natuurlijke getallen* x, y, n

Opgave 6. Bewijs de Binomiaalstelling. Kijk of je Opgave 5 (b) kunt gebruiken.

Nu we de Binomiaalstelling hebben, zijn we klaar om naar het bewijs van de Freshman's dream te kijken. (De Freshman's dream hebben we weer nodig in het bewijs van de Kleine stelling van Fermat.) Herinner je onze notatie van modulorekenen: Voor natuurlijke getallen a, b, n schrijven we

$$a \pmod{n} = b$$

als b gelijk is aan de *rest* van a gedeeld door n. Dus bijvoorbeeld: $21 \pmod{7} = 0$ want 21 wordt gedeeld door 7 zonder rest, en $14 \pmod{3} = 2$ want $14 = 4 \times 3 + 2$, dat will zeggen, 3 deelt 14 met rest 2. Met andere woorden, de uitdrukking $a \pmod{n}$ geeft aan wat overblijft als we zo vaak mogelijk n van a aftrekken (zonder negatief te gaan). Merk op dat $0 \leq a \pmod{n} < n$. (Waarom?)

Lemma (Freshman's dream[3])**.** *Voor alle natuurlijke getallen x en y en priemgetallen p, geldt dat $(x+y)^p \pmod p = x^p + y^p \pmod p$.*

Opgave 7. We bewijzen Freshman's dream in twee stappen. Zij p een priemgetal.

(a) Bewijs dat de binomiaalcoëfficiënten $\binom{p}{1}$, $\binom{p}{2}$, ..., $\binom{p}{p-1}$ een veelvoud zijn van p. Met andere woorden, alle binomiaalcoefficiënten $\binom{p}{k}$ zijn een veelvoud van p, behalve de "eerste en de laatste", waarvoor geldt $\binom{p}{0} = \binom{p}{p} = 1$.

(b) Concludeer dat $(x+y)^p \pmod p = x^p + y^p \pmod p$. Gebruik (a) en de Binomiaalstelling.

5. De Kleine stelling van Fermat en de Fermat priemtest

We herhalen de Kleine stelling van Fermat en bespreken het bewijs. Dan bespreken we de Fermat priemtest. Hier gebruiken we de notatie voor modulorekenen zoals hiervoor gedefinieerd. In het bewijs zullen we de Freshman's dream gebruiken die we eerder hebben bewezen.

Stelling (Kleine stelling van Fermat)**.** *Voor elk priemgetal p en voor elke natuurlijk getal $0 \leq a \leq p$ geldt $a^p \pmod p = a$.*

Merk op dat de stelling duidelijk waar is voor $a = 0$ en $a = 1$.

Bewijs. Dit is een bewijs dat gebruikt maakt van een belangrijke bewijsmethode genaamd "inductie". (In eerste instantie kan deze methode wat ingewikkeld lijken. In de opleiding oefenen we er veel meer mee.) Eerst merken we op dat de bewering van de stelling duidelijk waar is voor $a = 0$. Dit heet de "basisstap" van de inductie. Nu gaan we een zogenaamde "inductiestap" bewijzen. Hiervoor *nemen we aan* dat de bewering waar is voor de waarde $a = k$ voor een of andere k. Ons doel is om hieruit de bewering voor de waarde $a = k+1$ af te leiden. De inductiestap kunnen we herhaaldelijk toepassen (vanaf de basisstap) zodat de bewering waar moet zijn voor alle waardes van a. Preciezer gezegd: we nemen aan dat $k^p \pmod p = k \pmod p$ (de "inductiehypothese") en we gaan bewijzen dat $(k+1)^p \pmod p = k+1 \pmod p$. Pak de uitdrukking $(k+1)^p$ en pas de Freshman's dream toe om te krijgen dat

$$(k+1)^p \pmod p = k^p + 1^p \pmod p.$$

Het is duidelijk dat $1^p = 1$ en vanwege de inductiehypothese weten we dat de gelijkheid $k^p \pmod p = k \pmod p$ geldt. Nu gebruiken we het simpelle feit dat $(x \pmod p) + (y \pmod p) \pmod p = x + y \pmod p$. Hiermee vinden we

$$(k+1)^p \pmod p = (k \pmod p) + 1 \pmod p = k+1 \pmod p.$$

Dit is wat we wilde bewijzen. □

De Kleine stelling van Fermat is het hoofdingrediënt voor de Fermat priemtest. De Fermat priemtest gaat als volgt.

Fermat priemtest. Gegeven een getal n, kies enkele waarden $0 \leq a \leq n$ en voor iedere waarde kijk of $a^n \pmod n = a$. Als dat zo is, zeg: "waarschijnlijk priem". Als we een a vinden met $a^n \pmod n \neq a$, zeg: "niet priem".

Inderdaad volgt uit de Kleine stelling van Fermat dat: als n niet priem is, dan is de uitvoer van de Fermat priemtest correct. Het vergt meer werk om te zien dat de Fermat priemtest "meestal" goed werkt als n wel priem is (we laten dat liggen voor een andere keer).

[3] De naam van dit lemma komt van een fout (dream) die schijnbaar veel gemaakt wordt door nieuwe studenten die denken dat $(x+y)^p = x^p + y^p$, dus zonder de mod p.

6. Carmichaelgetallen, en andere tests

Zoals gezegd, helaas werkt de Fermat priemtest niet altijd. Namelijk er zijn getallen n die niet priem zijn, maar waarvoor wel geldt dat $a^n \bmod n = a$ voor all natuurlijke getallen $0 \leq a \leq n$. Deze interessante getallen heten *Carmichaelgetallen*. Deze getallen zijn "relatief zeldzaam", maar kunnen ook niet genegeerd worden wanneer we daadwerkelijk priemgetallen nodig hebben. Er zijn geavanceerdere priemtesten die preciezer zijn, en sinds 2002 is er zelfs een efficiënte priemtest die geen enkele wikkeleurigheid (randomness) gebruikt (Agrawal–Kayal–Saxena, "PRIMES is in P").

Opgave 8. Het getal $n = 561$ is het kleinste Carmichaelgetal. Ga voor een aantal waarden van a na dat $n = 561$ inderdaad aan $a^n = a \bmod n$ voldoet terwijl het geen priemgetal is (met een rekenmachine of door te programmeren).

7. Extra en anders: De Sylvester–Gallai stelling

In deze laatste uitdagende opgave gaan we iets heel anders doen, namelijk een geometrische stelling bewijzen (want wiskunde gaat over meer dan getallen).

Opgave 9. Bewijs de Sylvester–Gallai stelling: Gegeven zijn een *eindig* aantal punten in het vlak. Stel dat elke lijn die door twee punten gaat, ook door een derde punt gaat. Dan moeten alle punten op één lijn liggen. Hint: neem aan van niet, en construeer een tegenspraak. Geldt de stelling nog als we de aanname "eindig" weglaten?

Uitwerkingen

We geven hier (niet altijd volledige) uitwerkingen van bovenstaande opgaven.
Voor vragen of opmerkingen, stuur een email naar j.zuiddam@uva.nl (Versie 10 december 2021)

Opgave 1. Kun je simpele verbeteringen bedenken voor de naieve priemtest, die het algoritme versnellen?

Uitwerking. Ik heb hier twee verbeteringen in gedachten die het algoritme versnellen (maar de verbeterde algoritmes kosten alsnog exponentieel veel stappen).

In het originele algoritme kijken we voor elk getal m met $2 \leq m \leq n-1$ of het een deler is van n. Het is echter voldoende om voor elk getal m met $2 \leq m \leq \sqrt{n}$ te kijken of het een deler is van n. Namelijk, als m een deler is van n, dan is ook n/m een deler van n. We hoeven dus niet zowel voor m als n/m te kijken of het een deler is van n. Nu observeren we dat of $m \leq \sqrt{n}$ of $n/m \leq \sqrt{n}$ (of allebei). Het is dus inderdaad voldoende om alleen voor de getallen m met $2 \leq m \leq \sqrt{n}$ te kijken of ze n delen.

De tweede verbetering is om vantevoren een lijst L te maken van alle priemgetallen tot een bepaalde grootte c. Dus bijvoorbeeld, laat L de lijst zijn van alle priemgetallen die kleiner zijn dan $c = 1000$. Om te kijken of n priem is kijken we eerst voor elk priemgetal p in de lijst L of p ons getal n deelt. (Zo ja, dan is n niet priem.) Daarna kijken we voor elke getal m met $c \leq m \leq n-1$ of m een deler is van n. (Zo ja, dan is n niet priem; zo nee, dan is n wel priem.)

Opgave 2. Ga na dat het Postulaat van Bertrand waar is voor $n \leq 50$. Hier zijn alle priemgetallen onder de 50:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Uitwerking. Het doel is om te bewijzen dat voor elk getal $1 \leq n \leq 50$ geldt dat er een priemgetal p is zodat $n \leq p \leq 2n$. Dus bijvoorbeeld, voor $n = 1$, vinden we het priemgetal $p = 2$ waarvoor geldt $n = 1 \leq p \leq 2 \cdot 1 = 2 \cdot n$. Nu is er een manier om tegen dit probleem aan te kijken wat het iets makkelijker maakt om het na te gaan. Namelijk, het is voldoende (ga na) om te bewijzen dat het verschil tussen opeenvolgende priemgetallen hoogstens een factor 2 is. Met andere woorden, ons doel is om te bewijzen dat voor elke priemgetal $p \leq 50$ er een priemgetal q is zodat $p \leq q \leq 2p$. Dit kunnen we eenvoudig nagaan voor bovenstaande lijst van priemgetallen $p \leq 50$. (Bijvoorbeeld voor $p = 2$ vinden we $2 \leq q = 3 \leq 2 \cdot 2$ en voor $p = 13$ vinden we $13 \leq q = 17 \leq 2 \cdot 13$. Je ziet dat we zelfs vrij veel keuze hebben voor q.)

Opgave 3. In de definitie van priemgetallen wordt het getal 1 niet priem genoemd. Kun je, met de Hoofdstelling van de rekenkunde in het achterhoofd, een goed argument vinden dat we 1 inderdaad niet priem moeten noemen?

Uitwerking. Het argument dat ik in gedachte heb, heeft te maken met de *uniciteit* in de Hoofdstelling van de rekenkunde: de priemontbinding van elke getal is *uniek*. Echter, als we 1 ook een priemgetal noemen, dan kunnen we 1 arbitrair vaak in elke priemontbinding voor laten komen (bijvoorbeeld $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3$) waardoor deze niet meer uniek is. Natuurlijk zouden we dit op kunnen lossen door in de Hoofdstelling van de rekenkunde te zeggen: Elk natuurlijk getal is te schrijven als product van priemgetallen, de deze schrijfwijze is uniek op volgorde en producten met 1 na, maar dan hebben we een veel langere en minder simpele stelling.

Opgave 4. Gebruik de Hoofdstelling van de rekenkunde om te bewijzen dat $\sqrt{2}$ geen rationaal getaal is. Dat will zeggen: bewijs dat $\sqrt{2}$ niet geschreven kan worden als een breuk $\frac{a}{b}$ voor natuurlijke getallen a en b. Hint: Probeer een bewijs uit het ongerijmde. Dus: neem aan dat $\sqrt{2}$ *wel* kan worden geschreven als $\sqrt{2} = \frac{a}{b}$ voor natuurlijke getallen a en b. Probeer vervolgens door algebraïsche manipulatie een gelijkheid te maken van natuurlijke getallen en vervolgens een tegenspraak af te leiden door middel van de Hoofdstelling van de rekenkunde.

Uitwerking. Stel dat $\sqrt{2}$ wel rationaal is, dus er bestaan natuurlijke getallen a, b zodat $\sqrt{2} = a/b$. Vermenigvuldig met b aan beide kanten en kwadrateer beide kanten om te krijgen dat $2b^2 = a^2$. We passen de Hoofdstelling van de rekenkunde toe om b en a te ontbinden in priemfactoren, zeg

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$
$$b = q_1^{m_1} \cdot q_2^{m_2} \cdots q_\ell^{m_\ell}.$$

waarbij p_i en q_i priemgetallen zijn, en n_i, m_i natuurlijke getallen. Dan zijn (vanwege de uniciteit in de Hoofstelling van de rekenkunde) de priemontbindingen van b^2 en a^2 gelijk aan

$$a = p_1^{2n_1} \cdot p_2^{2n_2} \cdots p_k^{2n_k}$$
$$b = q_1^{2m_1} \cdot q_2^{2m_2} \cdots q_\ell^{2m_\ell}.$$

Per aanname hebben we

$$2b^2 = a^2.$$

Dit geeft

$$2 \cdot q_1^{2m_1} \cdot q_2^{2m_2} \cdots q_\ell^{2m_\ell} = p_1^{2n_1} \cdot p_2^{2n_2} \cdots p_k^{2n_k}.$$

Nu zien we dat aan de linkerkant van de gelijkheid het priemgetal 2 met een oneven macht voorkomt, terwijl het aan de rechterkant van de gelijkheid met een even macht voorkomt (kan 0 zijn). Dit is een tegenspraak (weer vanwege de uniciteit van de Hoofdstelling van de rekenkunde). Dus was de aanname dat $\sqrt{2}$ rationaal is onjuist.

Opgave 5. In deze opgave bekijken we wat de betekenis is van de faculteit en de binomiaalcoëfficiënten.

(a) Stel je voor dat je n verschillende boeken hebt (of andere objecten) die je op een rij wilt zetten. Bewijs dat dit op $n!$ verschillende manieren kan.

(b) Stel nu dat je k kopieën hebt van een boek en $n-k$ kopieën van een ander boek. Kopieën van hetzelfde boek kun je niet van elkaar onderscheiden. Je wilt nu deze boeken op volgorde zetten. Bewijs dat dit op $\binom{n}{k}$ verschillende manieren kan.

Uitwerking. (a) We willen n verschillen boeken op een rij zetten. We doen dit door één voor één een boek te kiezen. Voor het eerste boek hebben we n mogelijkheden. Na het kiezen van het eerste boek hebben we $n-1$ boeken over. Dus, voor het kiezen van het tweede boek hebben we $n-1$ mogelijkheiden. Op dezelfde manier hebben we voor het kiezen van het derde book $n-2$ mogelijkheden. Dit herhalen we totdat we na $n-1$ boeken te kiezen nog 1 boek over hebben. (Daar hebben we slechts 1 keuze.) Het totale aantal mogelijke keuzes is het product van het aantal mogelijkheiden in elke stap: $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$, oftewel $n!$.

(b) Noem $f(n,k)$ het aantal mogelijke manieren om n boeken op een rij te zetten als de collectie boeken bestaat uit k kopieën van boek (genaamd x) en $n-k$ kopieën van een ander boek (genaamd y). We willen bewijzen dat $f(n,k) = \binom{n}{k}$. Stel we hebben deze boeken op een rij gezet op één van de $f(n,k)$ mogelijke manieren. Als we de k kopieën van boek x nummeren (1 tot k) en de $n-k$ kopieëen van boek y ook nummeren (1 tot $n-k$), zodat ze niet meer identiek zijn, dan krijgen we $k!$ mogelijke manieren om de genummerde kopieëen van x te ordenen en $(n-k)!$ mogelijke maniereen om de genummerde kopieëen van y te ordenen. We vinden van $n! = f(n,k)k!(n-k)!$ en dus $f(n,k) = \frac{n!}{k!(n-k)!} = \binom{n}{k}$.

Opgave 6. Bewijs de Binomiaalstelling. Kijk of je Opgave 5 (b) kunt gebruiken.

Uitwerking. We schrijven de macht $(x+y)^n$ uit tot

$$(x+y)(x+y)\cdots(x+y).$$

We willen dit product verder uitwerken als een grote som. De termen van deze som ontstaan door uit iedere factor $(x+y)$ het element x of y te kiezen, en van al die keuzes het product te nemen. Bijvoorbeeld,

$$(x+y)(x+y)(x+y) = xxx + xyy + yxy + yyx + xxy + xyx + yxx + yyy$$

en omdat $xxy = xyx = yxx = x^2y$ en $xyy = yxy = yyx = y^2x$ krijgen we

$$(x+y)(x+y)(x+y) = x^3 + 3x^2y + 3xy^2 + y^2.$$

Merk op dat xyy, yxy, yyx precies alle mogelijkheden zijn om één kopie van x en twee kopieën van y op een rij te zetten, en er zijn $\binom{3}{1} = 3$ verschillende mogelijkheden daarvoor (Opgave 5 (b)). Op dezelfde manier zijn xxy, xyx, yxx precies alle mogelijkheden om twee kopieën van x en één kopie van y op een rij te zetten, en er zijn $\binom{3}{2} = 3$ verschillende mogelijkheden daarvoor.

In het algemeen, correspondeert de $k$de term in de uitwerking van $(x+y)^n$ met $x^k y^{n-k}$ maal het aantal mogelijke manieren om k kopieën van x en $n-k$ kopieën van y op een rij te zetten, wat geeft

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

Opgave 7. We bewijzen Freshman's dream in twee stappen. Zij p een priemgetal.

(a) Bewijs dat de binomiaalcoëfficiënten $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ een veelvoud zijn van p. Met andere woorden, alle binomiaalcoefficiënten $\binom{p}{k}$ zijn een veelvoud van p, behalve de "eerste en de laatste", waarvoor geldt $\binom{p}{0} = \binom{p}{p} = 1$.

(b) Concludeer dat $(x+y)^p \pmod p = x^p + y^p \pmod p$. Gebruik (a) en de Binomiaalstelling.

Uitwerking. (a) Het is duidelijk dat $\binom{p}{0} = \binom{p}{p} = 1$. Neem $1 \le k \le p-1$ een geheel getal. We vinden

$$\begin{aligned}\binom{p}{k} &= \frac{p!}{k!(p-k)!} = \frac{p(p-1)(p-2)\cdots 2\cdot 1}{k(k-1)(k-2)\cdots 2\cdot 1\cdot (p-k)(p-k-1)\cdots 2\cdot 1} \\ &= \frac{p(p-1)\cdots(k+1)}{(p-k)(p-k-1)\cdots 2\cdot 1}.\end{aligned}$$

Merk nu op dat als we de noemer $(p-k)(p-k-1)\cdots 2$ schrijven als product van priemgetallen $q_1 q_2 \cdots q_r$, dan moeten alle q_i strict kleiner zijn dan p, en dus kunnen ze p niet delen. Dus moeten ze het product $(p-1)\cdots(k+1)$ delen. Dit betekent dat $\binom{p}{k}$ van de vorm $p\ell$ is waarbij ℓ een natuurlijk getal is. Met andere woorden, $\binom{p}{k}$ is een veelvoud van p.

(b) We weten al van Opgave 6 dat

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

Van (a) weten we dat $\binom{p}{k}$ deelbaar is door p voor $1 \le k \le p-1$. Wanneer we modulorekenen "negeren" we veelvouden van p, en dus krijgen we

$$(x+y)^p \pmod p = \binom{p}{0} y^p + \binom{p}{p} x^p \pmod p = y^p + x^p \pmod p.$$

Opgave 8. Het getal $n = 561$ is het kleinste Carmichaelgetal. Ga voor een aantal waarden van a na dat $n = 561$ inderdaad aan $a^n \pmod{561} = a$ voldoet terwijl het geen priemgetal is (met een rekenmachine of door te programmeren).

Uitwerking. We vinden dat $3 \cdot 11 \cdot 17 = 561$, dus 561 is zeker geen priemgetal.

Kies een getal a, bijvoorbeeld $a = 2$. Om te verifiëren dat $a^{561} \pmod{561} = 561$, lijkt het in eerste instantie alsof we het gigantische getal 2^{561} moeten berekenen, dan daarop de operatie "$\pmod{561}$" moeten toepassen en dan moeten kijken of het antwoord gelijk is aan 561. Gelukkig is er een slimme manier om $2^{561} \pmod{561}$ te berekenen zonder 2^{561} te berekenen. Veel softwarepaketten kunnen dit en dit werkt als volgt (met een methode die "repeated squaring" heet). De methode is dat we elke macht x^n (voor x en n natuurlijke getallen) recursief kunnen schrijven als

$$x^n = \begin{cases} (x^2)^{n/2} & \text{als } n \text{ even is} \\ x(x^2)^{(n-1)/2} & \text{als } n \text{ oneven is.} \end{cases}$$

We kunnen dit herhaaldelijk toepassen om a^n te schrijven als een product van machten van a. Bijvoorbeeld, $x^5 = x \cdot x^4 = x \cdot (x^2)^2$. Bovendien geldt (ga na) dat $(a \cdot b) \pmod{n} = (a \pmod{n}) \cdot (b \pmod{n})$ voor elke natuurlijke getallen a, b. We hebben dus ook

$$x^n \pmod{n} = \begin{cases} (x^2 \pmod{n})^{n/2} \pmod{n} & \text{als } n \text{ even is} \\ x(x^2 \pmod{n})^{(n-1)/2} \pmod{n} & \text{als } n \text{ oneven is.} \end{cases}$$

Dit ziet er ingewikkeld uit, maar wat het betekent is dat we in de berekening van x^n de tussenresultaten altijd $\pmod{n}$ mogen nemen. Dit zorgt ervoor dat de tussenresultaten nooit groter dan n worden. Bijvoorbeeld, $x^5 \pmod{n} = x \cdot ((x^2 \pmod{n})^2 \pmod{n}) \pmod{n}$ (Probeer dit eens te programmeren.)

Opgave 9. Bewijs de Sylvester–Gallai stelling: Gegeven zijn een *eindig* aantal punten in het vlak. Stel dat elke lijn die door twee punten gaat, ook door een derde punt gaat. Dan moeten alle punten op één lijn liggen. Hint: neem aan van niet, en construeer een tegenspraak. Geldt de stelling nog als we de aanname "eindig" weglaten?

Uitwerking. Het bewijs van deze stelling is zeker niet makkelijk te vinden en was lang onbekend. Voor een volledige uitwerking van het bewijs verwijzen we naar deze lecture notes van Yuval Wigderson: `http://web.stanford.edu/~yuvalwig/math/teaching/BeyondEuclidNotes.pdf` (in het Engels)