Bewijzen voor de kleine stelling van Fermat

De kleine stelling van Fermat is een van de meest fundamentele stellingen in de elementaire getaltheorie, en stelt dat voor priemgetallen p en voor willekeurige gehele getallen a er geldt dat $a^p - a$ een veelvoud is van p, of in modulaire notatie:

$$a^p \equiv a \pmod{p}.$$

Zoals we van Pierre de Fermat wel gewoon zijn, heeft hij zijn resultaat nooit bewezen. Hij verkondigde in een brief aan Frénicle de Bessy, naast de feitelijke stelling, slechts het volgende commentaar:

> Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

Wij gaan het risico te langdradig te worden niet uit de weg en zullen de stelling wél bewijzen, bovendien niet één keer maar wel dertien keer!

1. **Modulorekenen** ..... Yucatan De Groote
2. **Binomiaalstelling** ..... Sara Chiers
3. **Telescoping** ..... Ben De Bondt
4. **Kettingen tellen** ..... Jef Laga
5. **Grafentheorie** ..... Jeroen Meulewaeter
6. **Groepentheorie** ..... Jozefien D'haeseleer
7. **Dynamische systemen** ..... Jens Bossaert
8. **Chebyshevpolynomen** .....
9. **Hyperkubussen** ..... Wouter Van Steenberge
10. **Formele machtreeksen** ..... Tim Seynnaeve
11. **Taylorreeksen** ..... Frederik Broucke
12. **Groepacties** ..... Lins Denaux
13. **Ordelemma** ..... Bart Michels

Allereerst merken we een equivalente formulering van de stelling op:

- Voor elk priemgetal p en elk geheel getal a geldt dat $a^p \equiv a \pmod{p}$.
- Voor elk priemgetal p en elk geheel getal a niet deelbaar door p geldt dat $a^{p-1} \equiv 1 \pmod{p}$.

Deze zijn inderdaad equivalent: veronderstel eerst dat $a^p \equiv a \pmod{p}$ en dat a niet deelbaar is door p. Dan heeft a een multiplicatieve inverse a^{-1} modulo p. Na vermenigvuldiging links en rechts volgt dat $a^{p-1} \equiv 1 \pmod{p}$. In de omgekeerde richting kunnen we vermenigvuldigen met a om $a^p \equiv a \pmod{p}$ te vinden, als a niet deelbaar is door p. Als a wel deelbaar is door p dan is $a \equiv 0 \pmod{p}$ en dus zeker $a^p \equiv a \pmod{p}$.

Voor sommige bewijzen zal de equivalente vorm directer te bewijzen blijken; we zullen dus verder geen onderscheid meer maken tussen de twee formuleringen. Daarnaast veronderstellen we soms dat $p \neq 2$, opdat p oneven zou zijn (het geval $p = 2$ is triviaal).

1 Modulorekenen (Yucatan De Groote)

Veronderstel dat p geen deler is van a, en beschouw de verzameling $S := \{1, 2, \ldots, p-1\}$. We beweren dat de verzameling $a \cdot S$ (d.w.z. S puntsgewijze vermenigvuldigd met a), beschouwd modulo p, niets meer is dan een permutatie van S. Met andere woorden, we beweren:

$$S \equiv \{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\} \pmod{p}.$$

Het is alvast duidelijk dat geen enkele van de elementen $i \cdot a$ (met $1 \leq i \leq p-1$) deelbaar zijn door p. Het volstaat dus aan te tonen dat alle elementen van $a \cdot S$ verschillend zijn. Dit volgt uit het feit dat a inverteerbaar is modulo p, want uit $a \cdot i \equiv a \cdot j \pmod{p}$ voor zekere i en j volgt na vermenigvuldiging met de inverse van a inderdaad dat $i \equiv j \pmod{p}$, of dus dat $i = j$.

Door alle elementen van S en $a \cdot S$ te vermenigvuldigen, volgt dan:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (1 \cdot a) \cdot (2 \cdot a) \cdot \cdots \cdot ((p-1) \cdot a) \pmod{p}.$$

Nu nog links en rechts de niet-nul factor $(p-1)!$ wegdelen en dan volgt er dat $1 \equiv a^{p-1} \pmod{p}$. ■

[http://www.artofproblemsolving.com/Wiki/index.php/Fermat's_Little_Theorem#Proof_2_.28Inverses.29]

2 Binomiaalstelling (Sara Chiers)

Dit eenvoudige bewijs steunt op inductie op a en een eigenschap die bekend staat als *freshman's dream*.

De inductiebasis is duidelijk voldaan: $0^p \equiv 0 \pmod{p}$. Veronderstel vervolgens dat $a^p \equiv a \pmod{p}$. Uit de binomiaalstelling weten we:

$$(a+1)^p = a^p + \binom{p}{1} \cdot a^{p-1} + \binom{p}{2} \cdot a^{p-2} + \ldots + \binom{p}{p-1} \cdot a + 1.$$

Merk op dat elke binomiaalcoëfficiënt $\binom{p}{k}$ met $0 < k < p$ een veelvoud is van p, want p deelt de teller maar niet de noemer in de definitie:

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

Modulo p beschouwd vallen de meeste coëfficiënten dus weg uit de binomiaalontbinding van $(a+1)^p$. De inductiehypothese toepassen levert tot slot de gezochte eigenschap voor $a+1$.

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$ ■

[http://www.artofproblemsolving.com/Wiki/index.php/Fermat's_Little_Theorem#Proof_1_.28Induction.29]

3 Telescoping (Ben De Bondt)

Een alternatief gebruik van de binomiaalstelling resulteert in een *telescoping sum*.

$$(a-b)^p - (a-b-1)^p = (a-b)^p - \sum_{i=0}^{p} \binom{p}{i} \cdot (a-b)^i \cdot (-1)^{p-i}.$$

Als we veronderstellen dat p oneven is, dan kunnen we in deze som de term voor $i = p$ schrappen met de voorafgaande term. Merk op dat $p - i$ even is als en slechts als i oneven is, zodat $-(-1)^{p-i} = (-1)^i$.

$$(a-b)^p - (a-b-1)^p = \sum_{i=0}^{p-1} (-1)^i \cdot \binom{p}{i} \cdot (a-b)^i.$$

Enkel voor $i = 0$ is de optredende binomiaalcoëfficiënt geen veelvoud van p, dus modulo p staat er:

$$(a-b)^p - (a-b-1)^p \equiv 1 \pmod{p}.$$

Passen we dit concreet toe voor $b = 0, 1, 2, \ldots$, dan vinden we:

$$\begin{aligned} a^p - (a-1)^p &= 1 + p \cdot h_1, \\ (a-1)^p - (a-2)^p &= 1 + p \cdot h_2, \\ (a-2)^p - (a-3)^p &= 1 + p \cdot h_3, \\ &\vdots \\ 2^p - 1^p &= 1 + p \cdot h_{a-1}, \\ 1^p - 0^p &= 1 + p \cdot h_a. \end{aligned}$$

Hierin zijn h_i zekere gehele getallen. Als we de a vergelijkingen in beide kolommen optellen, vinden we dat $a^p - 0^p = a + p \cdot (h_1 + h_2 + \ldots + h_a)$, zodat p een deler is van $a^p - a$.

[https://sakai.wfu.edu/access/content/group/26f503c9-bec7-4bb7-bdab-82ed8fda9d39/publications/Student/Caroline%20LaRoche%20Turnage%20-%20Thesis.pdf]

4 Kettingen tellen (Jef Laga)

Een kort en elegant bewijs, dat de methode van enkele andere bewijzen combinatorisch uitdrukt.

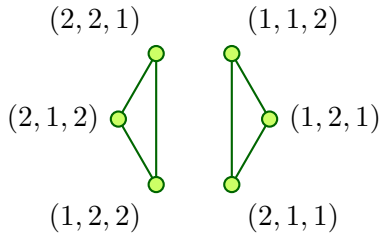
Veronderstel dat we beschikken over kralen in a kleuren en dat we er halskettingen van willen maken met precies p kralen. Eerst rijgen we p kralen op een koord; dit kan op a^p manieren. Voor elk van de kleuren is er precies één koord in uitsluitend die kleur; deze gooien we weg en we houden er $a^p - a$ over. Door de einden van de koorden te verbinden maken we halskettingen. Maar twee koorden die slechts een cyclische permutatie van elkaar verschillen leveren niet te onderscheiden kettingen op. Aangezien er juist p cyclische permutaties zijn van de p kralen op een koord, is het aantal halskettingen $(a^p - a)/p$, wat een geheel getal moet zijn. ■

[http://www.cimat.mx/~mmoreno/teaching/spring08/Fermats_Little_Thm.pdf]

5 Grafentheorie (Jeroen Meulewaeter)

Beschouw volgende graaf. De toppen zijn de sequenties $(a_1, a_2, \ldots, a_p)$ van natuurlijke getallen tussen 1 en a (inclusief), waarvan niet alle elementen gelijk zijn. Het is duidelijk dat er dan juist $a^p - a$ toppen zijn. Twee toppen zijn verbonden door een boog als de bijhorende sequenties over één element cyclisch gepermuteerd zijn, dus wanneer de ene van de vorm $(u_1, u_2, \ldots, u_p)$ is en de andere $(u_p, u_1, \ldots, u_{p-1})$.

Een voorbeeld, waarin $a = 2$ en $p = 3$:



Elke top in deze graaf heeft graad twee, dus elke component van de graaf is een cykel. Bovendien heeft elke cykel lengte p. Het aantal componenten wordt dus gegeven door $(a^p - a)/p$, wat een geheel getal moet zijn. Dit betekent dat p een deler is van $a^p - a$. ■

[http://www.dharwadker.org/pirzada/applications/main.html]

6 Groepentheorie (Jozefien D'haeseleer)

Aangezien p priem is, vormen de getallen $\{1, 2, \ldots, p-1\}$ een groep $(G, \times)$ onder de vermenigvuldiging modulo p, met orde $|G| = p - 1$. Beschouw nu de deelgroep van G voortgebracht door het element a en noem deze H, dus $H \coloneqq \{a, a^2, a^3, \ldots, a^k\}$ met k het kleinste positieve getal zodat $a^k \equiv 1 \pmod{p}$.

De stelling van Lagrange stelt dat de orde van een deelgroep van een eindige groep steeds een deler is van de orde van de groep zelf. Hier is $|H| = k$ dus een deler van $|G| = p - 1$; schrijf $p - 1 = km$. Dan is inderdaad $a^{p-1} = a^{km} = (a^k)^m \equiv 1^m = 1 \pmod{p}$. ■

[http://en.wikipedia.org/wiki/Proofs_of_Fermat's_little_theorem#Proof_using_group_theory]

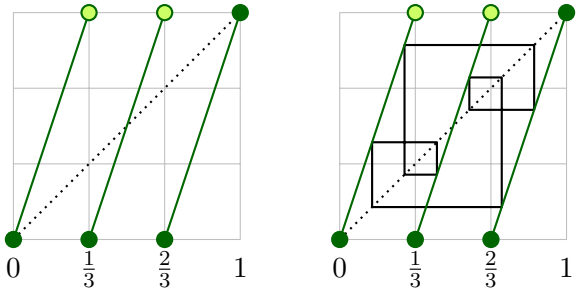
7 Dynamische systemen (Jens Bossaert)

Voor dit bewijs via dynamische systemen definiëren we de volgende familie van functies:

$$T_n(x) : [0,1] \to [0,1] : x \mapsto \begin{cases} \{nx\} = nx - \lfloor nx \rfloor & \text{als } x < 1 \\ 1 & \text{als } x = 1 \end{cases}$$

De *baan* van een punt x onder $T_n(x)$ is de verzameling $\{x, T_n(x), T_n^2(x), T_n^3(x), \ldots\}$. Een eindige baan heet een *cykel*. Het aantal punten in de cykel noemen we de *periode* van x; er geldt dan dat $T_n^k(x) = x$ als en slechts als k een veelvoud is van de periode van x. Een punt x met $T_n(x) = x$ heet een *fixpunt*.

De grafiek van T_3 hieronder verduidelijkt hoe deze functies eruit zien. Rechts staat een illustratie van een cykel van T_3, gegeven door $\frac{1}{7} \mapsto \frac{3}{7} \mapsto \frac{2}{7} \mapsto \frac{6}{7} \mapsto \frac{4}{7} \mapsto \frac{5}{7} \mapsto \frac{1}{7}$. Het is grafisch ook duidelijk dat een fixpunt correspondeert met een snijpunt van de grafiek met de rechte $y = x$, en dat de functie T_n dus precies n fixpunten heeft.



Noteer vervolgens $\mathcal{N}_k(T_n)$ voor het aantal punten van T_n met periode k. Een eerste belangrijk lemma stelt dat $k \mid \mathcal{N}_k$ wanneer $\mathcal{N}_k$ eindig is. Dit geldt omdat punten met eenzelfde periode k kunnen worden gepartitioneerd in equivalentieklassen, waarbij we punten als equivalent beschouwen als ze in dezelfde cykel voorkomen. Het is inderdaad duidelijk dat twee verschillende cykels disjunct moeten zijn. Bovendien zijn al deze equivalentieklassen even groot (met grootte k), waaruit het gestelde volgt.

Een volgende eenvoudige eigenschap betreft de compositie van de functies en stelt dat $T_a \circ T_b = T_{ab}$. Voor $x = 1$ klopt dit uiteraard. Voor $0 \leq x < 1$ vinden we $T_a(T_b(x)) = \{a \cdot \{bx\}\} = \{abx - a\lfloor bx \rfloor\} = \{abx\} = T_{ab}(x)$ aangezien $a\lfloor bx \rfloor$ een geheel getal is.

Nu tellen we het aantal punten x van T_a zodat $T_a^k(x) = x$. Merk op dat deze punten precies de fixpunten zijn van T_a^k, en aangezien $T_a^k = T_{a^k}$ zijn er juist a^k zulke punten. We kunnen deze ook anders tellen; elk punt x met $T_a^k(x) = x$ heeft als periode een deler van x, waaruit de volgende gelijkheid geldt:

$$a^k = \sum_{m|k} \mathcal{N}_m(T_a).$$

Passen we het laatste resultaat toe op een priemgetal p, dan staat er:

$$a^p = \mathcal{N}_1(T_a) + \mathcal{N}_p(T_a) = a + \mathcal{N}_p(T_a).$$

Uit het eerste lemma volgt tot slot dat $p \mid \mathcal{N}_p = a^p - a$: precies wat Fermats kleine stelling beweert! ■

[http://galileo.stmarys-ca.edu/jsauerbe/dynamical.pdf]

8 Chebyshevpolynomen

Dit bewijs is in essentie hetzelfde als het vorige, maar via een andere familie functies. We definiëren:

$$T_n(x) : [-1, 1] \to [-1, 1] : x \mapsto \cos(n \arccos x)$$

Deze functies blijken polynomen te zijn en staan bekend als de Chebyshevpolynomen. Hier geldt eveneens dat $(T_a \circ T_b)(x) = \cos(a \arccos(\cos(b \arccos x))) = \cos(ab \arccos x) = T_{ab}(x)$. Om aan te tonen dat T_n juist n fixpunten heeft, volstaat het de oplossingen van de vergelijking $T_n(\cos\theta) = \cos\theta$ te tellen, want voor elke $x \in [-1, 1]$ bestaat er een unieke $\theta \in [0, \pi]$ met $\cos\theta = x$. Deze vergelijking herleidt zich tot $\cos n\theta = \cos\theta$, die opgelost wordt door $\theta = \frac{2k\pi}{n-1}$ of $\theta = \frac{2l\pi}{n+1}$ met $k, l \in \mathbb{Z}$. Aangezien $\theta \in [0, \pi]$ moeten we k en l tellen zodat volgende voorwaarde voldaan is:

$$0 \leq \frac{2k\pi}{n-1} \leq \pi, \qquad \text{of} \qquad 0 \leq \frac{2l\pi}{n+1} \leq \pi.$$

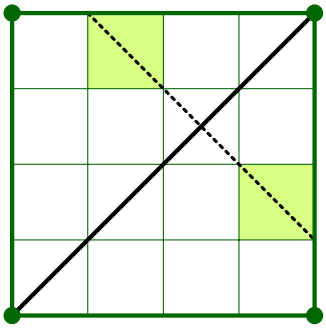
Er zijn precies n keuzen voor k of l waarvoor dit geldt dus T_n heeft precies n fixpunten.

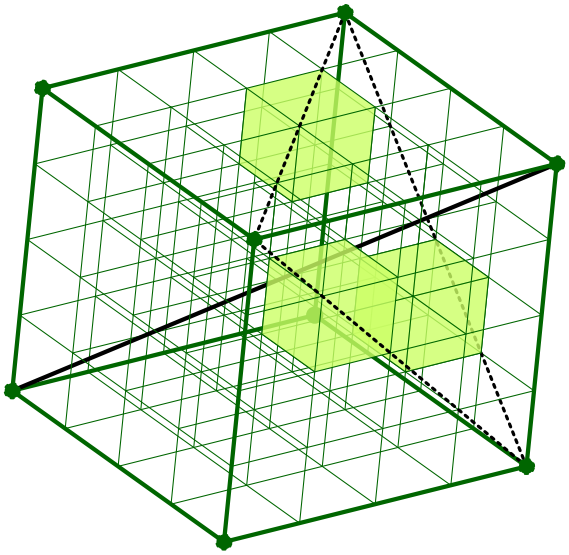
De rest van het bewijs kennen we: we tellen het aantal punten x zodat $T_a^p(x) = x$, dus zodat $T_{a^p}(x) = x$, en daar zijn er dus a^p van. Juist a van deze punten zijn fixpunten van T_a, de overige $a^p - a$ kunnen worden gepartitioneerd volgens hun banen, die allemaal grootte p hebben. Zodus moet $p \mid a^p - a$. ■

[http://cuhkmath.wordpress.com/2014/04/25/a-dynamical-proof-of-fermats-little-theorem/]

9 Hyperkubussen (Wouter Van Steenberge)

Dit bewijs berust opnieuw op een opdeling van a^p objecten in a "bijzondere" en $a^p - a$ "generieke" die gepartitioneerd kunnen worden in groepen van p, dit keer vanuit een meetkundig perspectief. Probeer je een hyperkubus voor te stellen in p dimensies en deel elke zijde ervan in a stukken. Zo delen we de hyperkubus op in a^p subhyperkubusjes. Bijvoorbeeld, voor $p = 2, 3$ en $a = 4$:





Beschouw een ruimtediagonaal van onze hyperkubus, die uiteraard door a kleintjes gaat. De hyperkubus heeft een p-voudige rotatiesymmetrie rond deze as: zo'n rotatie beeldt een deelkubusje af op één van de p kubusjes in een baan van deze symmetrie. Na p rotaties wordt elk van de kubusjes terug op zichzelf afgebeeld. Bovendien kan dit niet in $m < p$ rotaties voor een kubusje buiten de diagonaal, want dan zou $m \mid p$, dus $m = 1$ gezien p priem is, zodat het kubusje gefixeerd wordt door zo'n rotatie en dus op de diagonaal ligt.

De $a^p - a$ deelkubusjes die niet op de diagonaal liggen, kunnen we dus onderverdelen in groepen van p kubusjes die invariant zijn onder deze rotatiesymmetrieën, waaruit $p \mid a^p - a$. ■

Het geval $a < 0$ volgt uit het bewezen geval, maar daarbij gaat de meetkundige interpretatie verloren.

[http://www.artofproblemsolving.com/Wiki/index.php/Fermat's_Little_Theorem#Proof_4_.28Geometry.29]

10 Formele machtreeksen (Tim Seynnaeve)

Dit bewijs in nogal bijzonder, in de zin dat het niet steunt op rechtstreekse eigenschappen van priem- of binomiaalgetallen maar enkel op prutswerk met formele machtreeksen.

Definieer $f(x) = 1 - x - dx^2 + \sum_{k \geq 3} a_k x^k$, met coëfficiënten in $\mathbb{Z}$. Deze kan op een unieke manier geschreven worden als een formeel product van de vorm $f(x) = \prod_{k \geq 1}(1 - m_k x^k)$ met ook m_k in $\mathbb{Z}$.

Inderdaad: reken dit product uit en stel de corresponderende coëfficiënten gelijk aan elkaar, dan wordt elke volgende m_k vastgelegd door een lineaire vergelijking met voor de rest reeds bekende coëfficiënten.

Op dezelfde manier (uitwerken en coëfficiënten gelijkstellen) bestaat er een unieke "inverse" machtreeks $f^{-1}(x)$, zodat $f(x)\cdot f^{-1}(x)=1$, met gehele coëfficiënten. Hier blijkt dat $f^{-1}(x)=1+x+(d+1)x^2+\sum_{k\geq 3}b_kx^k$, wat we ook als een formeel product $f^{-1}(x)=(1+x)\cdot(1+(d+1)x^2)\cdot\prod_{k\geq 3}(1-n_kx^k)$ kunnen schrijven (met n_k in $\mathbb{Z}$).

Vervolgens voeren we de formele logaritmische afgeleide in van een machtreeks $g(x)$ als de machtreeks $(\ln g(x))' \coloneqq g'(x)/g(x)$. Voor twee machtreeksen geldt dat $(\ln g(x)\cdot h(x))' = (\ln g(x))' + (\ln h(x))'$ uit de Leibnizregel voor afgeleiden: $(g(x)\cdot h(x))' = g'(x)\cdot h(x) + g(x)\cdot h'(x)$. In het bijzonder volgt voor inverse machtreeksen dat $(\ln f(x))' + (\ln f^{-1}(x))' = 0$.

Met onze functie $f(x)$ kunnen we zo berekenen:

$$-x\big(\ln f(x)\big)' = \sum_{k\geq 1}\frac{km_kx^k}{1-m_kx^k} = \sum_{N\geq 1}x^N\sum_{s|N}m_{N/s}^s\frac{N}{s}.$$

En analoog met de inverse:

$$x(\ln f(x))' = -x\big(\ln f^{-1}(x)\big)' = \sum_{N\geq 1}x^N\sum_{s|N}n_{N/s}^s\frac{N}{s}.$$

Hieruit halen we de volgende interessante identiteit m.b.t. de twee reeksen:

$$\sum_{s|N}m_{N/s}^s\frac{N}{s} = -\sum_{s|N}n_{N/s}^s\frac{N}{s}.$$

Met inductie kunnen we dan aantonen dat $m_k=-n_k$ voor oneven k, maar niet voor even k. Hier zullen we daar geen tijd aan verspillen en dit als waar aannemen.

Herinner je dat $m_2=d$ en $n_2=-(d+1)$ in ons concrete geval. Pas dan bovenstaande identiteit toe op $N=2p$, met p een oneven priemgetal. De som bevat dan slechts vier termen met $s\in\{1,2,p,2p\}$:

$$2p\cdot m_{2p}+p\cdot m_p^2+2\cdot d^p+1 = -2p\cdot n_{2p}-p\cdot n_p^2+2\cdot(d+1)^p-1.$$

Na herschikken staat er dat $p\cdot(2m_{2p}+2n_{2p}+m_p^2+n_p^2)=2(d+1)^p-2d^p-2$. Aangezien $m_p=-n_p$ wordt dat $p\cdot(m_{2p}+n_{2p}+m_p^2)=(d+1)^p-d^p-1$, oftewel $p\mid(d+1)^p-d^p-1$. Deze uitdrukking sommeren over $d=1,2,\ldots,a-1$ resulteert in $p\mid a^p-a$, de kleine stelling van Fermat! ■

[http://arxiv.org/pdf/0801.0805v3.pdf]

11 Taylorreeksen (Frederik Broucke)

Als we de Taylorontwikkeling van $f(x)=x^{p-1}-1$ berekenen rond $x=1$, vinden we:

$$f(x)=(p-1)\cdot(x-1)+\frac{1}{2!}(p-1)(p-2)\cdot(x-1)^2+\ldots+\frac{1}{(p-1)!}(p-1)!\cdot(x-1)^{p-1}.$$

Wanneer n een veelvoud is van p, is $f(n)$ duidelijk géén veelvoud van p. Beschouw nu $n=kp+c$ met $k,c\in\mathbb{Z}$ en $0<c<p$. Modulo p zal $f(kp+c)\equiv f(c)\pmod p$. Het volstaat dus het gedrag van $f(n)$

te onderzoeken voor $0 < n < p$. Concreet zullen we aantonen dat $p \mid f(n)$ voor alle gehele $0 < n < p$, en dit doen we via een soort "eindige inductie".

Het basisgeval $n = 1$ is triviaal. Veronderstel dat $p \mid f(n)$ voor $0 < n < p - 1$ als inductiehypothese, dan zullen we aantonen dat ook $p \mid f(n + 1)$. De Taylorontwikkeling ingevuld in $x = n + 1$ geeft:

$$f(n+1) = (p-1) \cdot n + \frac{1}{2!}(p-1)(p-2) \cdot n^2 + \ldots + \frac{1}{(p-1)!}(p-1)! \cdot n^{p-1}.$$

Bemerk vervolgens dat we de coëfficiënten kunnen vereenvoudigen modulo p:

$$\binom{p-1}{k} = \frac{(p-1)\ldots(p-k)}{k!} \equiv (-1)^k \pmod{p}.$$

Hieruit leiden we af dat $f(n+1) \equiv -n + n^2 - n^3 + \ldots + n^{p-1} \pmod{p}$, waarin we een meetkundige reeks met ratio $-n$ herkennen. De somformule voor zulke reeksen geeft $f(n+1) \equiv (n^p - n)/(n+1) = n \cdot f(n)/(n+1) \pmod{p}$. Aangezien $0 < n < p-1$ is $n+1$ niet deelbaar door p. De inductiehypothese impliceert dan dat $f(n+1) \equiv 0 \pmod{p}$, oftewel $p \mid f(n+1)$. ■

[http://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Bishop.pdf]

12 Groepacties (Lins Denaux)

Dit bewijs steunt op volgende observatie: voor een groepsactie van een p-groep (een groep met orde p^n) op een eindige verzameling S, is het aantal elementen van S congruent met het aantal fixpunten van deze actie, modulo p. Dit zal volgen uit de baanformule: $|G| = |G_s| \cdot |s^G|$, waarin G_s de stabilisator van s (de deelgroep van groepselementen die s fixeren) en s^G de baan van s (de beelden van s onder de groepsactie) voorstelt. De stabilisator is een deelgroep en heeft dus als orde een macht van p. Er volgt:

$$|s^G| = \frac{|G|}{|G_s|} = \frac{p^n}{p^k} = p^{n-k}.$$

Wanneer s geen fixpunt is, dan is de grootte van s^G verschillend van 1 en dus deelbaar door p. Beschouw dan de som van de lengtes van alle banen in deze actie, modulo p. De elementen die niet gefixeerd worden, leveren dan geen bijdrage in deze som, terwijl de fixpunten één eenheid bijdragen. Er blijft slechts over dat $|S|$ congruent is met het aantal fixpunten modulo p.

Gewapend met deze observatie kunnen we nu de kleine stelling van Fermat bewijzen. Definieer S als de verzameling p-tupels van getallen tussen 1 en a, en beschouw de actie op S van de cyclische groep van orde p door cyclische permutatie. Het is niet moeilijk aan te tonen dat dit wel degelijk een groepsactie vormt en dat $(a_1, \ldots, a_p)$ een fixpunt is als en slechts als $a_1 = \ldots = a_p$. Zodus zijn er juist a fixpunten. Samen met $|S| = a^p$ geeft het zopas bewezen lemma dat $a^p \equiv a \pmod{p}$. ■

[http://users.humboldt.edu/evans/research/fermat.pdf]

13 Ordelemma (Bart Michels)

We zullen bewijzen dat als a en p copriem zijn, de orde $\mathrm{ord}_p(a)$ van a modulo p een deler is van $p - 1$. Dit volstaat voor de kleine stelling van Fermat, want dan is $a^{p-1} = a^{k \cdot \mathrm{ord}_p(a)} \equiv 1^k = 1 \pmod{p}$.

Beschouw de rij $a, a^2, a^3, \ldots$ modulo p. De periode ervan is precies $\mathrm{ord}_p(a)$ en de termen van deze rij kunnen hoogstens $p - 1$ waarden aannemen, waaruit in elk geval al volgt dat $\mathrm{ord}_p(a) \leq p - 1$.

Noteer $k = \mathrm{kgv}(\mathrm{ord}_p(1), \mathrm{ord}_p(2), \ldots, \mathrm{ord}_p(p-1))$. Aangezien de veelterm $x^k - 1$ precies $p-1$ nulpunten heeft modulo p en omdat $\mathbb{Z}/p\mathbb{Z}$ een veld is, is $k \geq p-1$. We zullen bewijzen dat er een getal is van orde k modulo p. Dan is $k \leq p-1$, zodat $k = p-1$ en dus $\mathrm{ord}_p(a) \mid k = p-1$ als $\mathrm{ggd}(a,p) = 1$.

Zij $q_1^{b_1} \cdots q_r^{b_r}$ de priemfactorenontbinding van k. Omdat k het kleinste gemene veelvoud is van de ordes, bestaat voor elke $n \in \{1, \ldots, r\}$ een getal a_n waarvoor $q_n^{b_n} \mid \mathrm{ord}_p(a_n)$, stel $\mathrm{ord}_p(a_n) = m_n q_n^{b_n}$. Dan is $\mathrm{ord}_p(a_n^{m_n}) = q_n^{b_n}$. We beweren dat $\mathrm{ord}_p(a_1^{m_1} \cdots a_r^{m_r}) = k$. Daartoe gebruiken we de volgende eigenschap: Als $\mathrm{ggd}(\mathrm{ord}_u(v), \mathrm{ord}_u(w)) = 1$, dan is $\mathrm{ord}_u(vw) = \mathrm{ord}_u(v)\,\mathrm{ord}_u(w)$. Inderdaad: stellen we $x = \mathrm{ord}_u(v)$, $y = \mathrm{ord}_u(w)$ en $z = \mathrm{ord}_u(vw)$, dan is enerzijds $(vw)^{xy} \equiv 1$ zodat $z \mid xy$. Anderzijds volgt uit $(vw)^z \equiv 1$ dat $v^{yz} \equiv 1$, zodat $x \mid yz$ en dus $x \mid z$. Analoog volgt dat $y \mid z$, zodat $xy \mid z$ en dus $xy = z$.

We kunnen deze eigenschap nu herhaaldelijk toepassen met $v = a_1^{m_1}$ en $w = a_2^{m_2}$, $v = a_1^{m_1} a_2^{m_2}$ en $w = a_3^{m_3}$, $v = a_1^{m_1} a_2^{m_2} a_3^{m_3}$ en $w = a_4^{m_4}$, enzovoort, om te besluiten dat $\mathrm{ord}_p(a_1^{m_1} \cdots a_r^{m_r}) = k$. Merk op dat we meteen ook hebben bewezen dat er een primitieve wortel modulo p bestaat. ■