De kleine stelling van Fermat

Moderne getaltheorie:
deelbaarheidscriteria, rekenen met resten,
stellingen van Fermat, Euler en Gauss

Overzicht collegestof & encyclopedische toevoegingen

mc.vanhoorn@wxs.nl

Inhoudsopgave

Inleiding (1)
opmerking vooraf

- Het centrale begrip in dit college is **deelbaarheid**.
- Als je twee natuurlijke getallen op elkaar deelt, kan de deling uitkomen. Dan is het ene getal deelbaar op het andere.
- Het kan ook zijn dat de deling niet uitkomt. Dan is er een rest ≠ 0
- Dit is de essentie.

- Verder is er een nieuwe notatie, de modulo-notatie:

  $$a = b \text{ (modulo } n\text{)}$$

- Dit betekent precies hetzelfde als:
- **bij deling door *n* hebben *a* en *b* dezelfde rest**

- Als $a = b \pmod{n}$ heten a en b **congruent modulo *n***

Inleiding (2)

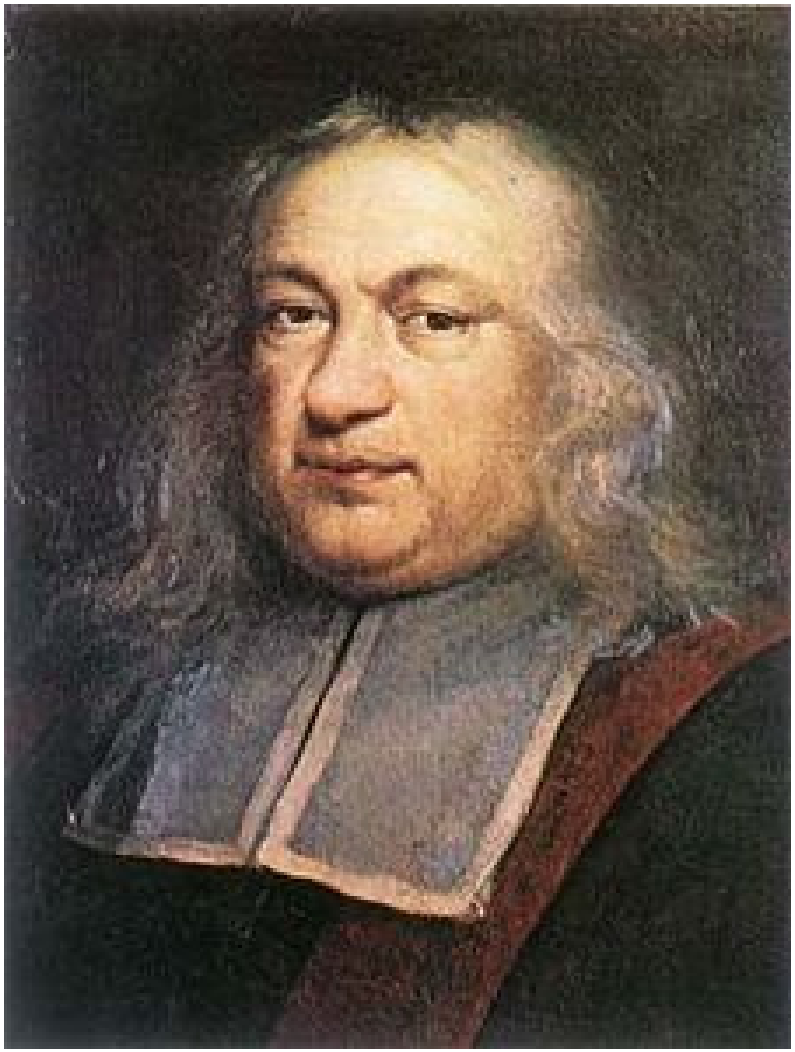
- Getaltheorie is net als meetkunde een zeer oude tak van wiskunde.
- Door de eeuwen heen kreeg de getaltheorie weinig externe toepassingen, de eigenschappen van getallen werden vrijwel uitsluitend toegepast binnen de getaltheorie.
- De laatste decennia is dat geheel veranderd.
- Opmerking. De thans voorliggende presentatie over de kleine stelling van Fermat c.a. heeft mede een encyclopedisch karakter, tijdens het college zal niet alles expliciet worden besproken.

Inleiding (3)

- Pierre de Fermat (1607-1665)

- Was werkzaam als jurist.

- Leverde bijdragen aan:
- - waarschijnlijkheidsrekening,
- - optica (brekingsindex),
- - analytische meetkunde,
- - analyse (bepaling maxima en minima van sommige functies),
- - getaltheorie.



Inleiding (4)

- Fermat werd beroemd door het zgn. vermoeden van Fermat, ook wel de grote stelling van Fermat.
- Deze luidt als volgt:

- **de vergelijking $a^n + b^n = c^n$ heeft geen oplossing voor *n* groter dan 2 (*a*, *b*, *c* en *n* zijn natuurlijke getallen)**

- Nadat door de eeuwen heen naar een bewijs was gezocht werd in 1994 een bewijs van Andrew Wiles (1953) erkend.
- Meer hierover in het college van Jaap Top.

De stelling (1)

- **De <u>kleine</u> stelling van Fermat** zegt het volgende:

- **Laat *p* een priemgetal zijn en *a* een natuurlijk getal dat geen factor *p* bevat, dan geldt dat $a^{p-1} = 1 \pmod{p}$**

- (De notatie: **= 1 modulo *p***
- Betekent precies hetzelfde als: **heeft rest 1 bij deling door *p***)

- Voorbeelden:
- $6^4 = 1 \pmod 5$, $10^6 = 1 \pmod 7$, $28^{28} = 1 \pmod{29}$
- In het laatste geval is narekenen niet eenvoudig.

- De stelling wordt ook wel geformuleerd als $a^p = a \pmod p$
- De stelling moet natuurlijk nog wel worden bewezen. Volgt.

De stelling (2)

- Het omgekeerde van de stelling geldt niet. Dus: laat *a* en *n* twee natuurlijke getallen zijn waarvoor $a^{n-1} = 1 \pmod{n}$; dan hoeft het niet zo te zijn dat *n* een priemgetal is.

- Er zijn namelijk tegenvoorbeelden:
- $2^{340} = 1 \pmod{341}$, terwijl $341 = 11 \times 31$

- En voor alle *a* geldt $a^{560} = 1 \pmod{561}$, terwijl $561 = 3 \times 11 \times 17$; dit met de voorwaarde dat de ggd van *a* en 561 gelijk is aan 1, m.a.w. *a* bevat geen factoren 3, 11 of 17

- De geldigheid van deze tegenvoorbeelden moet natuurlijk nog wel worden bewezen. Zie hierna.

De stelling (3)
bewijs 1e tegenvoorbeeld

- Gesteld werd: $2^{340} = 1 \pmod{341}$
- Dit moet nog worden bewezen, wat als volgt kan.

- Ten eerste is $2^5 = 32 = 1 \pmod{31}$,
- zodat $2^{340} = (2^5)^{68} = 1^{68} = 1 \pmod{31}$
- Ten tweede is $2^5 = 32 = -1 \pmod{11}$,
- zodat $2^{340} = (2^5)^{68} = (-1)^{68} = 1 \pmod{11}$
- Hierbij is van belang dat machtsverheffen een geoorloofde bewerking is, namelijk omdat het hier herhaald vermenigvuldigen is.
- We hebben nu gevonden dat $2^{340} - 1$ deelbaar is door 31 en door 11, en dus door $11 \times 31 = 341$
- De conclusie is dat $2^{340} = 1 \pmod{341}$

De stelling (4)
bewijs 2e tegenvoorbeeld

- Bewezen moet worden: $a^{560} = 1 \pmod{561}$ als a geen factoren 3, 11 of 17 bevat:

- $a^2 = 1$ modulo 3 (Fermat), dus $a^{560} = 1 \pmod 3$
- $a^{10} = 1$ modulo 11 (Fermat), dus $a^{560} = 1 \pmod{11}$
- $a^{16} = 1$ modulo 17 (Fermat), dus $a^{560} = 1 \pmod{17}$
- We hebben nu gevonden dat $a^{560} - 1$ deelbaar is door 3, door 11 en door 17, en dus door 561
- Met andere woorden: $a^{560} = 1 \pmod{561}$

Voorbeelden van de modulo-notatie (1)

het nieuwe ISBN

Het vijfde element van het ISBN is het controlecijfer. Dit wordt berekend met behulp van de algoritme modulus 10.

Elk van de eerste 12 cijfers van het ISBN wordt afwisselend vermenigvuldigd met 1 en 3. Het controlecijfer is gelijk aan 10 min de rest die overblijft nadat de som van de gewogen producten van de eerste 12 cijfers gedeeld is door 10, met één uitzondering. Als deze berekening resulteert in een duidelijk controlecijfer van 10, is het controlecijfer 0.

Volg deze stappen om het controlecijfer voor het ISBN 978-0-11-000222-? te berekenen:

Stap 1: Bepaal de som van de gewogen producten voor de eerste twaalf cijfers van het ISBN (zie de volgende tabel).

	Prefix			**Registratie-groep**	**Registrator**		**Publicatie**						**Controle-cijfer**	**Som**
ISBN	9	7	8	0	1	1	0	0	0	2	2	2	?	
Gewicht	1	3	1	3	1	3	1	3	1	3	1	3	-	
Product	9	21	8	0	1	3	0	0	0	6	2	6	-	56

Stap 2: Deel de som van de gewogen producten van de eerste twaalf cijfers van het ISBN berekend in stap 1 door 10, en bepaal de rest.

56 / 10 = 5 rest = 6

Stap 3: Trek de rest die is berekend in stap 2 af van 10. Het resulterende verschil is de waarde van het controlecijfer, met één uitzondering. Als uit stap 2 de rest 0 is, is het controlecijfer 0.

10 – 6 = 4

Controlecijfer = 4

ISBN = 978-0-11-000222-4

De volgende wiskundige formule is een alternatieve manier om het controlecijfer te berekenen:

Controlecijfer = mod 10 (10 – [mod 10 {som van gewogen producten van de eerste twaalf ISBN cijfers}])

Controlecijfer = mod 10 (10 – [mod 10 {56}])

Controlecijfer = 4

Voorbeelden van de modulo-notatie (2)

de berekening van de paasdatum volgens Gauss

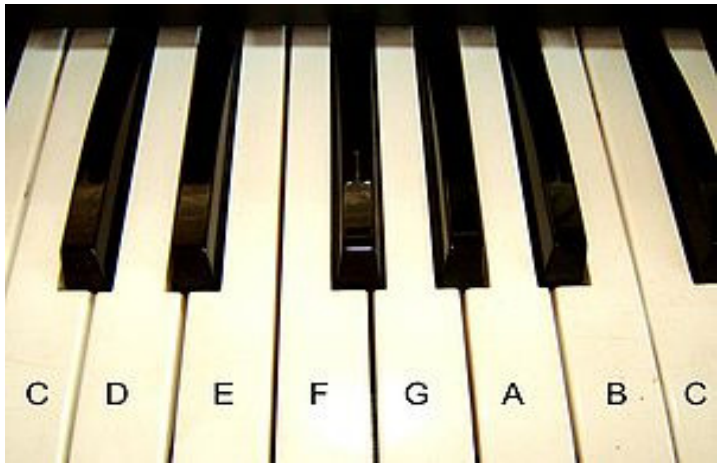
- Recept voor de berekening:
- Gebruik voor de 20ste en 21ste eeuw de getallen $M = 24$ en $N = 5$
- Neem de zo klein mogelijke resten a, b, c, d en $e > 0$ zó dat:
- a = jaartal (mod 19), b = jaartal (mod 4) en c = jaartal (mod 7),
- daarna $d = 19a + M \pmod{30}$ en $e = 2b + 4c + 6d + N \pmod 7$
- Dan valt eerste paasdag op $22 + d + e$ maart of op $d + e - 9$ april

- Toepassing op 2009:
- In 2009 is $a = 14$, $b = 1$ en $c = 0$, dus $d = 20$ en $e = 1$
- Dus eerste paasdag 2009 valt op 43 maart = 12 april

Voorbeelden van de modulo-notatie (3)

toonladders

- De bekende tonale toonladder, beginnend met de c, herhaalt zich voortdurend. Men is gewend de toonladder slechts één keer te noteren: c’ = c (mod octaaf)
- Elk tweetal tonen staat in een bepaalde toonhoogte-verhouding tot elkaar. De c die een octaaf hoger is heeft een toonhoogte die gelijk is aan tweemaal de toonhoogte van de oorspronkelijke c.
- Hier wordt niet ingegaan op kwesties als: is de cis identiek met de des?



Deelbaarheidscriteria (1)

priemgetallen als factor van 99999……9

- Inmiddels bekend: $10^6 = 1 \pmod 7$
- Dit is hetzelfde als: 1.000.000 heeft rest 1 bij deling door 7
- En dus geldt: **999.999 is deelbaar door 7**; reken na!
- Op dezelfde manier wordt afgeleid: **9.999.999.999.999.999 is deelbaar door 17**; reken na!

- N.B. Ook hier een kanttekening: $10^{p-1} = 1 \pmod p$ geldt voor alle priemgetallen p ongelijk aan 2 en 5, maar het kan voorkomen dat $10^m = 1 \pmod p$, waarbij m kleiner is dan p-1
- Voorbeelden:
- $10^{10} = 1 \pmod{11}$, maar ook is $10^2 = 1 \pmod{11}$, immers 99 is deelbaar door 11
- $10^{12} = 1 \pmod{13}$, maar ook is $10^6 = 1 \pmod{13}$; reken na!

Deelbaarheidscriteria (2)

priemgetallen als factor van 99999……9

- **Stelling: laat *p* een priemgetal zijn ongelijk 2 en 5, dan bestaat er een getal van de vorm 99999……9 dat deelbaar is door *p***
- Bewijs: dit blijkt direct uit $10^{p-1} = 1 \pmod{p}$

- Opmerking. Dit is een existentiebewijs, hiermee wordt niet elke exponent *m* verkregen waarvoor $10^{m} = 1 \pmod{p}$

- Reflectie. Door de kleine stelling van Fermat kun je eigenschappen van vaak zeer grote getallen afleiden, zonder dat je die grote getallen zelf berekent.

Deelbaarheidscriteria (3)

de 9-proef en de 3-proef

- Alle getallen van de vorm 99999……9 zijn deelbaar door 9, immers gelijk aan 9 x 11111……1. Deze eigenschap kan worden gebruikt om de **geldigheid van de 9-proef te bewijzen**.

- Voorbeeld: is het getal 1665 deelbaar door 9?
- Om dit te onderzoeken gebruiken we dat $10^n - 1 = 0 \pmod 9$, m.a.w. $10^n = 1 \pmod 9$ voor alle natuurlijke getallen n:
- $1665 = 1 \times 1000 + 6 \times 100 + 6 \times 10 + 5 =$
- $= 1 \times 1 + 6 \times 1 + 6 \times 1 + 5 \times 1 \pmod 9 =$
- $= (1 + 6 + 6 + 5) \pmod 9 =$
- $= 18 = 0 \pmod 9$
- Dus 1665 is deelbaar door 9

- In het algemene geval gaat het net zo.

Deelbaarheidscriteria (4)

de 9-proef en de 3-proef

- **Conclusie: een getal is deelbaar door 9 precies dan als de som van de cijfers van het getal deelbaar is door 9.**
- Dit heet **de 9-proef**.
- Zo is er ook **de 3-proef**. Bewijs zelf.

- De 9-proef in modulo-taal:
- **getal = som der cijfers van het getal (mod 9)**

- Voorbeeld:
- De rest van 1607 bij deling door 9 is 5, zo ook de rest van 1060007 bij deling door 9, en de rest van 100600000007 bij deling door 9

- Voor de rest bij deling door 3 geldt dezelfde eigenschap, d.w.z. de rest van 100600000007 bij deling door 3 is 2

Deelbaarheidscriteria (5)

de 11-proef

- Merk het volgende op:
- $10^1 = -1 \pmod{11}$, $10^2 = 1 \pmod{11}$, $10^3 = -1 \pmod{11}$, $10^4 = 1 \pmod{11}$, enzovoort.
- Bewijs dat dit zo doorgaat; gebruik: $10 = -1 \pmod{11}$.

- Onderzoek nu de **deelbaarheid door 11** van een willekeurig getal als volgt (neem weer 1665):
- $1665 = (1 \times 1000) + (6 \times 100) + (6 \times 10) + 5 =$
- $= (1 \times -1) + (6 \times 1) + (6 \times -1) + 5 \pmod{11} =$
- $= -1 + 6 - 6 + 5 \pmod{11} = 4 \pmod{11}$
- Dus 1665 is niet deelbaar door 11

- In het algemene geval gaat het net zo.

Deelbaarheidscriteria (6)

de 11-proef

- **Conclusie: een getal is precies dan deelbaar door 11 als de alternerende som der cijfers deelbaar is door 11.**
- Dit heet **de 11-proef**.

- Voorbeelden:
- 16654 is deelbaar door 11, want $1 - 6 + 6 - 5 + 4 = 0$
- 1006006005004 is deelbaar door 11

- Ook:
- 273812 is deelbaar door 11,
- want $2 - 7 + 3 - 8 + 1 - 2 = -11 = 0 \pmod{11}$

Deelbaarheidscriteria (7)

een eerste 7-proef

- Een deelbaarheidscriterium voor andere getallen dan 9 en 11 is iets lastiger. Hier als voorbeeld **deelbaarheid door 7**.
- Bekend: $10^6 = 1 \pmod 7$, m.a.w. 999.999 is deelbaar door 7
- Ook geldt: $10^3 = -1 \pmod 7$, want 1001 is deelbaar door 7
- Er is net zo'n rij te maken als bij 11: $10^3 = -1 \pmod 7$, $10^6 = 1 \pmod 7$, $10^9 = -1 \pmod 7$, $10^{12} = 1 \pmod 7$, enzovoort

- Onderzoek nu de deelbaarheid door 7 van een willekeurig getal als volgt (neem 16654):
- $16654 = (16 \times 1000) + 654 =$
- $= (16 \times -1) + 654 \pmod 7 = -16 + 654 = 638 = 1 \pmod 7$
- Dus 16654 is niet deelbaar door 7
- 16653 is wel deelbaar door 7

Repeterende breuken (1)

- Bekend is: 1/3 = 0,3333....
- De decimale ontwikkeling van 1/3 wordt verkregen door herhaald uitvoeren van een staartdeling. De decimale ontwikkeling van 1/3 is een voorbeeld van een repeterende breuk, omdat deze decimale ontwikkeling steeds dezelfde cijfers bevat. De decimale ontwikkeling van 1/3 is onbegrensd.
- Om de 'gewone' waarde van 0,3333…. te vinden kan de ontwikkeling worden geschreven als meetkundige reeks:
- 0,3333…. = 0,3 + 0,03 + 0,003 + 0,0003 + …..
- De eerste term is 0,3 en de reden (constante verhouding) is 0,1 en dus is de som van de oneindige reeks: 0,3/(1-0,1) = 0,3/0,9 = 1/3

- **Stelling. (a) Elke gewone breuk heeft een repeterende decimale ontwikkeling. (b) Omgekeerd stelt elke repeterende decimale ontwikkeling een gewone breuk voor.**

Repeterende breuken (2)

- Bewijs van de stelling.
- (a) De decimale ontwikkeling van een gewone breuk wordt verkregen door herhaald een staartdeling uit te voeren. Omdat er slechts eindig veel verschillende resten mogelijk zijn moeten ergens in de rij gelijke uitkomsten voorkomen. Maar dan zijn vanaf die gelijke uitkomsten de volgende uitkomsten ook gelijk.
- Voorbeeld: 3/7 = 0,1428571428571……
- (b) Bij elke repeterende decimale ontwikkeling kan een **meetkundige reeks** worden gevonden waarvan de som eindig is, en wel gelijk aan een gewone breuk.
- Voorbeeld: 0,2545454545….. = 0,25 + 0,0045 + 0,000045 + ….. =
- = 1/4 + 0,0045/(1 – 0,01) = 1/4 + 0,0045/0,99 = 1/4 + 1/220 = 14/55
- Of: 0,25454545….. = 0,2 + 0,054(1 – 0,01) = 1/5 + 6/110 = 14/55

Repeterende breuken (3)

- Opmerking:
- De decimale ontwikkeling van een gewone breuk is niet eenduidig.
- Voorbeeld: 1/3 = 0,33333…….
- Dus 1 = 3 x 1/3 = 0,99999…..
- De conclusie is dat 1,00000….. = 0,99999…
- Zo is ook 1/4 = 0,2500000…. = 0,2499999….

- De schrijfwijze 0,9999999…….. levert een methode om breuken met teller 1 decimaal te ontwikkelen.
- Voorbeeld. Bekend is dat 999999 deelbaar is door 7
- Om precies te zijn is 999999 : 7 = 142857
- Hieruit volgt: 1/7 = 0,142857142857……..

- Zo ook 999999 : 21 = (0)47619, dus 1/21 = 0,047619047619……
- en 999 : 37 = (0)27, dus 1/37 = 0,027027……..

Meer deelbaarheidscriteria (1)

een tweede 7-proef

- Het bewijs van de 11-proef kan op een andere manier worden gegeneraliseerd als eerder gedaan, als volgt:
- $10 = 3 \pmod 7$,
- vermenigvuldig met 10 resp. 3: $10^2 = 9 = 2 \pmod 7$
- nogmaals, en herhaald: $10^3 = 6 \pmod 7$
- $10^4 = 4 \pmod 7$
- $10^5 = 5 \pmod 7$
- $10^6 = 1 \pmod 7$
- $10^7 = 3 \pmod 7$.
- Het patroon gaat zich na zes stappen herhalen.

- Deze structuur lijkt op die van de decimale ontwikkeling.
- Vraag: hoe kan het dat in beide gevallen een patroon zich na zes stappen gaat herhalen?

Meer deelbaarheidscriteria (2)

een tweede 7 proef

- Uit het voorgaande volgt een criterium voor deelbaarheid door 7, als volgt:
- Neem 16653 en splits dit in eenheden, tientallen, honderdtallen enz:
- $16653 = (1 \times 10000) + (6 \times 1000) + (6 \times 100) + (5 \times 10) + (3 \times 1) =$
- $= (1 \times 4) + (6 \times 6) + (6 \times 2) + (5 \times 3) + (3 \times 1) \pmod 7 =$
- $= 4 + 36 + 12 + 15 + 3 = 70 = 0 \pmod 7$
- Dus 16653 is deelbaar door 7

- Onderzoek op deze wijze de deelbaarheid door 7 van:
- 2009, 999999, 142857
- Welk van deze getallen is ook deelbaar door 49?

Meer deelbaarheidscriteria (3)

een derde 7-proef

- **Recept voor een derde 7-proef**: neem een getal, hak het laatste cijfer eraf, en trek dit 2 x af van het getal dat je overhoudt. Als dit deelbaar is door 7, is het oorspronkelijke getal deelbaar door 7.

- Voorbeelden:
- 126 is deelbaar door 7, want $12 - 2 \times 6 = 0$
- 1001 is deelbaar door 7, want $100 - 2 \times 1 = 98 = 0 \pmod 7$

- Is 999.999 deelbaar door 7? Oplossing:
- $99999 - 2 \times 9 = 99981$,
- $9998 - 2 \times 1 = 9996$,
- $999 - 2 \times 6 = 987$,
- $98 - 2 \times 7 = 84 = 0 \pmod 7$
- Dus 999.999 is deelbaar door 7

Meer deelbaarheidscriteria (4)

een derde 7-proef

- Bewijs van het kloppen van de derde 7-proef:
- Een willekeurig getal is te schrijven als [*AB*], waarbij *B* het laatste cijfer voorstelt en *A* het getal is dat je overhoudt na weglating van het laatste cijfer. (Dus in 1665 is $A = 166$ en $B = 5$)
- het getal [*AB*] is: $10 \times A + B$,
- trek $2 \times B$ af van *A*: $A - 2 \times B$
- Je hebt nu twee getallen, namelijk $10 \times A + B$ en $A - 2 \times B$
- …….
- Opdracht: vul dit bewijs aan om tot de onderstaande conclusie te kunnen komen.

- **De conclusie luidt: $[AB] = 10 \times A + B = 0 \pmod 7$ precies dan als $A - 2 \times B = 0 \pmod 7$.**

Meer deelbaarheidscriteria (5)
slot

- Voor elk natuurlijk getal dat geen factoren 2 en 5 bevat gelden soortgelijke deelbaarheidscriteria als voor 7.
- Zo is het tweede criterium ook mogelijk voor deelbaarheid door 21: ga na dat $10^1 = 10 \pmod{21}$, $10^2 = 16 \pmod{21}$, $10^3 = 13 \pmod{21}$, $10^4 = 4 \pmod{21}$, $10^5 = 19 \pmod{21}$, $10^6 = 1 \pmod{21}$, en gebruik dit om na te gaan dat 1665524 deelbaar is door 21

- Als er wel één of meer factoren 2 of 5 in het spel zijn geldt een tweeledig criterium. Voorbeeld: een getal is deelbaar door 6 precies dan als het deelbaar is door 2 én door 3. Net zo: een getal is deelbaar door 35 als het deelbaar is door 5 én door 7.

- Zo kán het met 21 ook: ga na dat 1665524 deelbaar is door 3 en door 7.

Talstelsels (1)

- Het thans gangbare getallenstelsel is een **positioneel stelsel met grondtal 10**, d.w.z. de positie van een cijfer geeft de waarde van het cijfer aan, en het aantal verschillende cijfers is 10. Misschien is het aantal vingers een bron geweest voor het grondtal 10.
- Zo heeft het cijfer 1 in 12345 de waarde 1×10^4.
- Andere talstelsels zijn mogelijk. Het grondtal 60 ziet men terug in het aantal minuten in een uur. Zeer bekend is het 2-tallige (binaire of digitale) systeem door de uitgebreide toepassing in de elektronica.

- Niet-positionele stelsels zijn mogelijk, zoals het systeem van de **Romeinse cijfers**. Dit systeem is in Europa eeuwenlang in zwang geweest. Met de komst van modernere wetenschap heeft het decimale systeem het verdrongen. Hierbij valt de naam van **Simon Stevin**, die decimale breuken gebruikte. Deze worden beschouwd als een natuurlijke uitbreiding van systeem met grondtal 10.

- Het gebruik van een positioneel stelsel in Europa is te danken aan de invloed van **Arabische wiskundigen** (via Italië, Spanje).

Talstelsels (2)

- **Deelbaarheid hangt niet af van een talstelsel**. Een priemgetal blijft een priemgetal, hoe je het ook wilt schrijven.
- **De eerder genoemde deelbaarheidscriteria hangen af van het talstelsel**. Zo hebben de getallen van de vorm 99999……9 alleen een speciale betekenis bij het grondtal 10.

- Voorbeeld. Neem als grondtal het getal 8, dat dan dus geschreven wordt als 10. Er zijn nu 8 cijfers: 0, 1, 2, 3, 4, 5, 6 en 7
- De achttallige notatie 12345 betekent in het tientallige stelsel:
- $1 \times 8^4 + 2 \times 8^3 + 3 \times 8^2 + 4 \times 8^1 + 5 \times 8^0 =$
- $= 1 \times 4096 + 2 \times 512 + 3 \times 64 + 4 \times 8 + 5 \times 1 = 5349$

- Zo is de rij 7, 77, 777, 7777, …. (achttallig) gelijk aan de rij 7, 63, 511, 4095, …. (tientallig). Al deze getallen zijn deelbaar door 7.

Talstelsels (3)

deelbaarheidscriteria in het achttallig stelsel

- Beschouw het achttallig stelsel. Het grondtal is acht, nu geschreven als 10. De telrij ziet er als volgt uit: 1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17, 20, 21, ….
- Altijd moet duidelijk zijn in welk talstelsel wordt gewerkt. Terugrekenen naar het tientallig stelsel gaat als volgt:
- 511 (achttallig) = $5 \times 8^2 + 1 \times 8 + 1 = 329$ (tientallig)
- Omgekeerd 511 (tientallig) = $7 \times 8^2 + 7 \times 8 + 7 = 777$ (achttallig)

- **Stelling. In het achttallig stelsel is elk oneven getal een deler van een getal van de vorm 7777….7**
- Bewijs: elk oneven getal *n* heeft met 8 een ggd gelijk aan 1. Dus geldt de stelling van Euler: $8^{\varphi(n)} = 1$ (modulo *n*), m.a.w. $8^{\varphi(n)}-1$ is deelbaar door *n* ; dus is juist een getal 7777….7 deelbaar door *n*.
- Over de stelling van Euler volgt verderop meer.

Talstelsels (4)

deelbaarheidscriteria in het achttallig stelsel

- **Stelling. In het achttallig stelsel is een getal deelbaar door 7 precies dan als de som der cijfers deelbaar is door 7.**
- Bewijs. Net als het bewijs van de 9-proef in het tientallig stelsel
- Voorbeeld: 511 (achttallig) is deelbaar door 7, want 5 + 1 + 1 = 7

- **Stelling. In het achttallig stelsel is een getal deelbaar door negen precies dan als de alternerende som der cijfers deelbaar is door negen.**
- Bewijs. Net als het bewijs van de 11-proef in het tientallig stelsel. In het achttallig stelsel is negen = 11.
- Voorbeeld: 515 (achttallig) is deelbaar door negen, want 5 - 1 + 5 = 11 (achttallig) = 9 (tientallig)
- Controle: 515 (achttallig) = 333 (tientallig)

Talstelsels (5)

een achttallige staartdeling

- Tientallig is de uitkomst van de deling 9215 : 95 gelijk aan 97
- Achttallig correspondeert dit met de deling 21777 : 137
- Een achttallige staartdeling verloopt als volgt
- 137 / 21777 \ 141
- 137
- 607
- 574
- 137
- 137
- 0
- Dus achttallig is 21777 : 137 = 141
- Inderdaad is 141 (achttallig) = 97 (tientallig)

Eigenschappen van de rij van Fibonacci (1)

- Leonardo van Pisa of Fibonacci (1170? – 1250?) is bekend vanwege de getallenrij die naar hem genoemd is:
- 0, 1, 1, 2, 3, 5, 8, 13, 21, ……. . hierin heeft de 0 het rangnummer 0
- Elk getal in de rij is de som van de beide voorgaande getallen.
- In formule: $f_{n+1} = f_{n-1} + f_n$
- Zo liggen alle volgende getallen vast.

- Uit de formule volgt dat je ook kunt **terugrekenen**: $f_{n-1} = f_{n+1} - f_n$
- Zo liggen alle voorafgaande getallen vast.

Eigenschappen van de rij van Fibonacci (2)

- **Stelling: Neem een willekeurig natuurlijk getal *m* > 1**
- **Dan is er een getal met rangnummer > 0 in de rij van Fibonacci dat deelbaar is door *m*; zelfs zijn er oneindig veel getallen in de rij met deze eigenschap.**

- Eerst een voorbeeld.
- Neem m = 8; de resten modulo 8 van de getallen in de rij van Fibonacci zijn: **0, 1,** 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, **0, 1,** 1, 2, ……..
- Duidelijk is dat de resten zich na enige tijd gaan herhalen. Dit is logisch, omdat het aantal verschillende resten eindig is. Waar het om gaat is: ook **het aantal paren resten is eindig**. Er moet dus zeker een keer een paar opvolgende getallen voorkomen dat al eerder in de rij voorkwam. In dit geval blijkt dat het paar (0, 1) al eerder was voorgekomen.

Eigenschappen van de rij van Fibonacci (3)

- Bewijs van de stelling:
- Maak de rij van de resten modulo *m*: 0, 1, 1, 2, 3, ……..
- Beschouw de **opeenvolgende paren** van deze resten modulo *m*: (0, 1), (1, 1), (1, 2), (2, 3), …….
- Er zijn eindig veel paren en dus zit er een herhaling in de rij van de paren, m.a.w. voor zekere waarden van *j* en *k*, waarbij aangenomen mag worden dat $j < k$, geldt: $(f_j, f_{j+1}) = (f_k, f_{k+1}) \pmod{m}$
- Dan kan men vanaf deze paren terugrekenen, net zo lang tot men bij f_0 is. Dat gaat dus in *j* stappen: $f_0 = 0 = f_{k-j} \pmod{m}$
- Met andere woorden: f_{k-j} is deelbaar door *m*, waarbij $k-j > 0$
- Door de herhaling in de rij zijn oneindig veel getallen in de rij deelbaar door *m*

Eigenschappen van de rij van Fibonacci (4)

- Voorbeelden
- $f_{18} = 2584$ is deelbaar door 19, en vervolgens zijn ook f_{36}, f_{54}, …. deelbaar door 19
- $f_8 = 21$ is deelbaar door 7, en vervolgens zijn ook f_{16}, f_{24}, ….. deelbaar door 7
- $f_5 = 5$ is deelbaar door 5, en vervolgens zijn ook f_{10}, f_{15}, …… deelbaar door 5

- **Stelling.**
- **Voor een priemgetal $p \neq 5$ is òf f_{p-1}, òf f_{p+1} deelbaar door p.**
- Voor een bewijs: zie na de behandeling van binomiaalcoëfficiënten.

- Voorbeeld: $f_{14} = 377$ is deelbaar door 13. Maar ook is reeds: $f_7 = 13$; de stelling bewijst dus een existentie.

Binomiaalcoëfficiënten (1)

de driehoek van Pascal

- 1
- 1 1
- 1 2 1
- 1 3 3 1
- 1 4 6 4 1
- 1 5 10 10 5 1
- 1 6 15 20 15 6 1
- 1 7 21 35 35 21 7 1

- Dit schema heet de driehoek van Pascal. Genoemd naar Blaise Pascal (1623-1662). De Chinezen kenden dit schema 2000 jaar geleden al. Het kan naar believen worden voortgezet.
- Aardig is dat de rij van Fibonacci in de driehoek van Pascal zit! (Hoe?)
- De getallen in het schema zijn de coëfficiënten in de uitwerking van machten van een tweeterm, bijvoorbeeld:
- $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

Binomiaalcoëfficiënten (2)
de driehoek van Pascal

- De getallen in de driehoek heten **binomiaalcoëfficiënten**. Het getal op plaats k in rij n wordt berekend door n! te delen door $k!(n-k)!$, waarbij k loopt van 0 t/m n, en $n = 0, 1, 2, 3, \ldots\ldots$
- $(a+b)^n$ uitgeschreven met behulp van deze coëfficiënten heet het **binomium van Newton**.

- **Stelling.**
- **Als n een priemgetal is, zijn alle binomiaalcoëfficiënten, behalve die voor $k = 0$ en $k = n$, deelbaar door n.**
- Bewijs. Het gaat om de binomiaalcoëfficiënten voor $k = 1, \ldots\ldots, n-1$
- Voor deze waarden van k liggen k en $n-k$ beide tussen 0 en n, en dus bevat noch k, noch $n-k$ het priemgetal n
- Om een binomiaalcoëfficiënt te berekenen moet een deling worden uitgevoerd. Daarbij blijft de priemfactor n in de teller dus altijd staan voor $k = 1, \ldots\ldots\ldots, n-1$ QED

Binomiaalcoëfficiënten (3)

de driehoek van Pascal

- **Stelling.**
- **Is p een priemgetal, dan is $(a + b)^p = a^p + b^p \pmod p$**
- Bewijs. Alle overige coëfficiënten zijn gelijk aan 0 modulo *p*
- QED

- Bovengenoemde eigenschap van de binomiaalcoëfficiënten wordt ook gebruikt in het bewijs van een eigenschap van de Fibonacci-rij, die nog moest worden bewezen.
- Namelijk:
- **zij *p* een priemgetal ≠ 5, dan is òf f_{p-1}, òf f_{p+1} deelbaar door *p***

- Dit bewijs wordt hierna geschetst. Het geval $p = 2$ wordt buiten beschouwing gelaten. Voor dit geval is direct te zien dat de eigenschap geldt. Dus is in het volgende verhaal *p* oneven en ≠ 5.

Bewijs van een eigenschap van de Fibonacci-rij (1)

- De Fibonacci-rij ziet er als volgt uit: 0, 1, 1, 2, 3, 5, 8, ……..
- Vaak wordt de rij gedefinieerd door de twee begintermen 0 en 1 en de recursieve betrekking $f_{n+2} = f_n + f_{n+1}$
- Er bestaat een expliciete formule voor de *n*-de term:
- $\boldsymbol{f_n = (1/\sqrt{5}).\{(½ + ½\sqrt{5})^n - (½ - ½\sqrt{5})^n\}}$ **(*)**
- Deze formule wordt hier bekend verondersteld.

- Op het vorige blad staat om welke eigenschap van de Fibonacci-rij het gaat. In het bewijs wordt ook de **formule van Kepler** gebruikt:
- $\boldsymbol{f_{n-1}.f_{n+1} - f_n^2 = (-1)^n}$
- Deze formule wordt hier niet bewezen.

- Het bewijs met *n* = priemgetal *p* verloopt als volgt.

Bewijs van een eigenschap van de Fibonacci-rij (2)

- Schrijf eerst formule (*) anders:
- $2^p.f_p = (1/\sqrt{5}).\{(1 + \sqrt{5})^p – (1 - \sqrt{5})^p\}$
- Werk vervolgens de vormen tussen de haakjes uit en constateer dat dan alle termen met $\sqrt{5}$ tot een even macht tegen elkaar wegvallen;
- over blijft: $2^p.f_p = (1/\sqrt{5}).\{2.p.(\sqrt{5}) + …….. + 2.p.(\sqrt{5})^{p-2} + 2.(\sqrt{5})^p\}$
- Werk de accolades weg: $2^p.f_p = 2.p + ……. 2.p.(\sqrt{5})^{p-3} + 2.(\sqrt{5})^{p-1}$
- Nu zijn de exponenten van $\sqrt{5}$ even geworden (p is immers oneven), en dus kunnen de worteltekens verdwijnen:
- $2^p.f_p = 2.p + …….. 2.p.5^{½p-1½} + 2.5^{½p-½}$
- De exponenten zijn hier gehele getallen.
- De laatste vergelijking bestaat volledig uit gehele getallen en dus kan alles modulo p worden genomen;
- dan vallen rechts alle termen weg op de laatste na:

Bewijs van een eigenschap van de Fibonacci-rij (3)

- $2^p.f_p = 2.5^{½p-½} \pmod p$
- Nu volgt uit de kleine stelling van Fermat dat $2^p = 2 \pmod p$, en bovendien mag links en rechts door 2 worden gedeeld omdat $p \neq 2$
- Het resultaat is: $f_p = 5^{½p-½} \pmod p$
- In de formule van Kepler komt f_p^2 voor, dit is dus:
- $f_p^2 = 5^{p-1} \pmod p$
- Maar nu zegt de kleine stelling van Fermat dat, als $p \neq 5$:
- $5^{p-1} = 1 \pmod p$, zodat: $f_p^2 = 1 \pmod p$
- Dit invullen in de formule van Kepler, samen met $(-1)^p = -1$:
- $f_{p-1}.f_{p+1} - 1 = -1 \pmod p$, zodat $f_{p-1}.f_{p+1} = 0 \pmod p$
- Omdat p een priemgetal is, is nu f_{p-1} of f_{p+1} deelbaar door p;
- Zij kunnen niet beide deelbaar zijn door p, want in dat geval zou wegens de recursieformule ook f_p deelbaar zijn door p, waaruit zou volgen dat alle getallen in de Fibonacci-rij deelbaar zijn door p. QED

Bewijs van de kleine stelling van Fermat (1)

rekenen met resten: vermenigvuldigen

- **Modulo een priemgetal kunnen vermenigvuldigingen worden uitgevoerd. Dit geldt zelfs modulo een willekeurig natuurlijk getal.**
- Eerst een voorbeeld:
- We weten: $12 = 5 \pmod 7$, zo ook $30 = 2 \pmod 7$
- Nu is $12 \times 30 = 360 = 3 \pmod 7$,
- en ook $5 \times 2 = 10 = 3 \pmod 7$
- Dus $12 \times 30 = 5 \times 2 \pmod 7$

- Het bovenstaande geldt algemeen:
- **Als $h = i \pmod n$ en $j = k \pmod n$, dan $h \times j = i \times k \pmod n$**
- Bewijs: $h = i + l \times n$ en $j = k + m \times n$,
- dus $h \times j = i \times k + \{i \times m \times n + k \times l \times n + l \times m \times n^2\} =$
- $= i \times k + 0 \pmod n$

Bewijs van de kleine stelling van Fermat (2)

rekenen met resten: delen

- **Modulo een priemgetal *p* kunnen delingen worden uitgevoerd**. Dit wordt als volgt bewezen:
- Stel: $k \times m = k \times n \pmod{p}$, waarin k, m en n resten ongelijk aan 0 zijn. Het gaat erom te delen door k, m.a.w. te bewijzen dat $m = n \pmod{p}$.
- Nu volgt: $k \times (m - n) = 0 \pmod{p}$
- Omdat p een priemgetal is, moet k of $m - n$ deelbaar zijn door p ; maar k is ongelijk aan 0 (mod p), is dus niet deelbaar door p. Dan moet $m - n$ deelbaar zijn door p, anders gezegd $m = n \pmod{p}$.
- Dit is juist wat bewezen moest worden.
-
- Opmerking. Modulo een niet-priemgetal mag delen niet zomaar.
- Voorbeeld: $2 = 8 \pmod{6}$, dus $2 \times 1 = 2 \times 4 \pmod{6}$,
- maar 1 is niet gelijk aan 4 (mod 6)

Bewijs van de kleine stelling van Fermat (3)

rekenen met resten

- Hieronder staat een vermenigvuldigtabel voor de resten modulo 7 die ongelijk aan 0 zijn:

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Bewijs van de kleine stelling van Fermat (4)

rekenen met resten

- Vanwege: 6 = 13 = 20 = 27 = …… (mod 7), en ook : 6 = -1 = -8 = …… (mod 7), kan men zeggen dat de 6 in de tabel staat voor alle resten die er modulo 7 gelijk aan zijn.

- Men spreekt dan ook liever van **restklassen** in plaats van resten. Dus modulo 7 zijn de restklassen ongelijk aan 0 de volgende: 1, 2, 3, 4, 5 en 6

- Opvallend is dat in de tabel in elke rij de restklassen 1, 2, 3, 4, 5 en 6 precies allemaal één keer voorkomen, zij het telkens in een andere volgorde.
- Met andere woorden: als $a \neq 0 \pmod 7$, dan zijn de restklassen 1x*a*, 2x*a*, 3x*a*, 4x*a*, 5x*a* en 6x*a* alle verschillend, en dus in zekere volgorde gelijk aan 1, 2, 3, 4, 5 en 6.

Bewijs van de kleine stelling van Fermat (5)

rekenen met resten

- Laatstgenoemde eigenschap geldt algemeen

- Lemma:
- **Laat p een priemgetal zijn en $a \neq 0 \pmod{p}$. Dan zijn de restklassen $1 \times a$, $2 \times a$, $3 \times a$, …… , $(p-1) \times a$ alle verschillend, en dus in zekere volgorde gelijk aan 1, 2, 3, …… , $p-1$**
- Bewijs:
- Neem aan: $h \times a = k \times a \pmod{p}$, met h en k tussen 0 en p
- Dan volgt: $(h - k) \times a = 0 \pmod{p}$
- Dus bevat òf a, òf $h - k$ een factor p
- a bevat geen factor p, dus $h - k = 0 \pmod{p}$
- Dus $h = k$

Bewijs van de kleine stelling van Fermat (6)

slot

- Laat p een priemgetal zijn en laat a geen factor p bevatten
- Neem nu het product $1 \times a \times 2 \times a \times 3 \times a \times \ldots\ldots \times (p-1) \times a$
- Dit is gelijk aan $1 \times 2 \times 3 \times \ldots\ldots \times (p-1) \times a^{p-1} = (p-1)! \times a^{p-1}$
- Anderzijds is het product $1 \times a \times 2 \times a \times 3 \times a \times \ldots\ldots \times (p-1) \times a$ krachtens het lemma gelijk aan $1 \times 2 \times 3 \times \ldots\ldots \times (p-1) = (p-1)! \pmod{p}$
- Dus geldt: $(p-1)! \times a^{p-1} = (p-1)! \pmod{p}$
- Hier staat links en rechts $(p-1)!$; in dit getal zit geen factor p en dus mag $(p-1)!$ worden weggedeeld.
- Het resultaat is: $a^{p-1} = 1 \pmod{p}$
- QED

De stelling van Euler (1)

de indicatorfunctie

- Definitie. Twee natuurlijke getallen *a* en *b* heten **relatief priem** als hun grootste gemene deler gelijk is aan 1, notatie ggd(*a*, *b*) = 1
- (**Eng.: relatively prime, coprime**)

- Voorbeelden:
- Is *p* een priemgetal, dan zijn alle getallen tussen 0 en *p* relatief priem met *p*.
- Zo zijn de getallen 1 t/m 12 relatief priem met 13

- Van de getallen van 1 t/m 11 zijn alleen de getallen 1, 5, 7 en 11 relatief priem met 12

- De getallen 1, 3, 7 en 9 zijn relatief priem met 10

De stelling van Euler (2)

de indicatorfunctie

- Definitie. De **indicatorfunctie van Euler** is de functie die aan een gegeven natuurlijk getal *m* toevoegt het **aantal resten** tussen 0 en *m* dat relatief priem is met m.
- Notatie: ***m* -> *φ*(*m*)**
- $\varphi(5) = 4$ $\varphi(9) = 6$ $\varphi(13) = 12$
- $\varphi(2) = 1$ $\varphi(6) = 2$ $\varphi(10) = 4$ $\varphi(14) = 6$
- $\varphi(3) = 2$ $\varphi(7) = 6$ $\varphi(11) = 10$ $\varphi(15) = 9$
- $\varphi(4) = 2$ $\varphi(8) = 4$ $\varphi(12) = 4$ $\varphi(16) = 8$
- Merk op dat $\varphi(p) = p-1$ voor elk priemgetal p

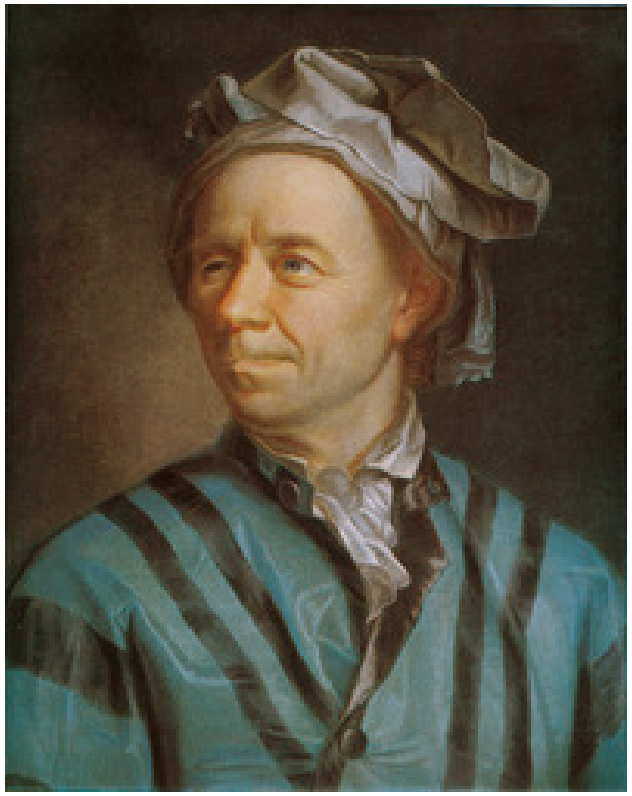
- **Stelling. Ligt *a* tussen 0 en *m* en is *a* relatief priem met *m*, dan is ook *m-a* relatief priem met *m*.**
- Bewijs. $a = m - (m-a)$. Zou $m-a$ een deler met m gemeenschappelijk hebben, dan zou dit ook een deler van a moeten zijn.
- Opmerking. In deze stelling mag de voorwaarde dat a tussen 0 en m ligt vervallen, mits negatieve getallen worden ingecalculeerd.

De stelling van Euler (3)

- Leonhard Euler (1707-1783) leverde een grote bijdrage aan vrijwel alle takken van de wiskunde.

- Hij beschreef de indicatorfunctie en generaliseerde daarmee de kleine stelling van Fermat.

- **Stelling van Euler:**
- **Zijn *m* en *a* natuurlijke getallen met (*m*, *a*) = 1, dan is $a^{\varphi(m)} = 1 \pmod{m}$**



De stelling van Euler (4)

rekenen met de resten die meetellen

- Hieronder staat een vermenigvuldigtabel van de resten modulo 9 die meetellen bij de bepaling van $\varphi(9)$
- De resten 3 en 6 tellen niet mee.

x	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

De stelling van Euler (5)
bewijsvoering

- De resten modulo 9 die met 9 een ggd gelijk aan 1 hebben vormen een gesloten systeem met een eenheidselement, waarin vermenigvuldiging en deling kunnen worden gedefinieerd.

- Is a een willekeurig getal met $(a, 9) = 1$, dan zijn de resten $1 \times a$, $2 \times a$, $4 \times a$, $5 \times a$, $7 \times a$ en $8 \times a$ modulo 9 in zekere volgorde gelijk aan 1, 2, 4, 5, 7 en 8. Zie de vermenigvuldigtabel.
- M.a.w.: $1 \times a \times 2 \times a \times 4 \times a \times 5 \times a \times 7 \times a \times 8 \times a = 1 \times 2 \times 4 \times 5 \times 7 \times 8 \pmod 9$

  Ook is: $1 \times a \times 2 \times a \times 4 \times a \times 5 \times a \times 7 \times a \times 8 \times a = 1 \times 2 \times 4 \times 5 \times 7 \times 8 \times a^6$

  Dus: $1 \times 2 \times 4 \times 5 \times 7 \times 8 \times a^6 = 1 \times 2 \times 4 \times 5 \times 7 \times 8 \pmod 9$

  Delen door $1 \times 2 \times 4 \times 5 \times 7 \times 8$ mag, dus volgt $a^6 = 1 \pmod 9$

  Omdat $\varphi(9) = 6$ is de stelling van Euler bewezen voor dit geval.

  In het algemene geval gaat het bewijs op precies dezelfde manier.

De stelling van Euler (6)
voorbeelden

- $\varphi(9) = 6$, dus $10^6 = 1 \pmod 9$
- Hier staat niets anders dan dat 999.999 deelbaar is door 9
- $\varphi(21) = 12$, dus $10^{12} = 1 \pmod{21}$
- Hier staat dat 999.999.999.999 deelbaar is door 21
- Eerder bleek al eens dat 999.999 deelbaar is door 7 ; dit getal is dus ook al deelbaar door 21

- $\varphi(49) = 42$, dus $10^{42} = 1 \pmod{49}$
- Hier staat: het getal dat uit 42 negens bestaat is deelbaar door 49
- In hoeverre er een getal van de vorm 99999…..9 bestaat dat minder dan 42 cijfers telt en deelbaar is door 49 is zo niet te zeggen.
- In dit geval blijkt er niet een dergelijk getal te bestaan.

Kwadraatresten (1)

- Het laatste cijfer van een kwadraat kan zijn: 0, 1, 4, 5, 6, 9
- Dit blijkt door de kwadraten van de getallen van 0 t/m 9 te nemen, dit zijn immers de getallen modulo 10.
- De 6 getallen 0, 1, 4, 5, 6, 9 heten de **kwadraatresten** modulo 10

- De laatste twee cijfers van een kwadraat kunnen zijn: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96
- Deze 22 getallen zijn de kwadraatresten modulo 100

- Zo blijkt bij elk natuurlijk getal dat sommige resten kwadraatresten zijn en andere niet.
- Voorbeeld: 0, 1, 2, 4 zijn de kwadraatresten modulo 7
- Vaak richt de aandacht zich op **kwadraatresten ≠ 0 en modulo een priemgetal**.

Kwadraatresten (2)

- **Stelling. Zij p een oneven priemgetal en $a \neq 0 \pmod{p}$.**
- **Dan geldt:**
- **(1e) $a \neq -a$, en a en $-a$ hebben dezelfde kwadraatrest modulo p**
- **(2e) het aantal kwadraatresten $\neq 0$ modulo p is $(p-1)/2$**
- Bewijs. (1e) Neem aan dat $p > 2$ en $a \neq 0$ (modulo p);
- $a \neq -a$ (modulo p), want anders zou $2a = 0$ (modulo p) zijn.
- Algemeen geldt dat $(-a)^2 = a^2$, of vanwege $-a = p-a \pmod{p}$
- natuurlijk ook $(p-a)^2 = p^2 - 2pa + a^2 = 0 + a^2 \pmod{p}$
- (2e) Uit (1e) blijkt dat van de p-1 resten modulo p die $\neq 0$ zijn ten hoogste de helft een kwadraatrest kan zijn.
- Stel nu $b^2 = a^2 \pmod{p}$
- Dan is $b^2 - a^2 = (b-a)(b+a) \pmod{p}$
- Delen is toegestaan, dus $b = a \pmod{p}$, of $b = -a \pmod{p}$
- Er zijn twee mogelijkheden en dus $(p-1)/2$ kwadraatresten $\neq 0$

Kwadraatresten (3)

een stelling over Pythagoreïsche drietallen

- Definitie. Een **Pythagoreïsch drietal** is een drietal natuurlijke getallen *a*, *b* en *c* waarvoor geldt $a^2 + b^2 = c^2$
- Een Pythagoreïsch drietal heet **primitief** als de ggd van *a*, *b* en *c* gelijk is aan 1, d.w.z. als *a*, *b* en *c* geen gemeenschappelijke factoren hebben.
- Voorbeelden van primitieve Pythagoreïsche drietallen: (3, 4, 5),
- (5, 12, 13), (7, 24, 25), (8, 15, 17), (20, 21, 29), (11, 60, 61)

- **Stelling. Laat (*a*, *b*, *c*) een primitief Pythagoreïsch drietal zijn. Dan geldt:**
- **1e. Precies één van de getallen *a* en *b* is deelbaar door 3**
- **2e. Precies één van de getallen *a* en *b* is deelbaar door 4**
- **3e. Precies één van de getallen *a*, *b* en *c* is deelbaar door 5**
- **4e. Precies één van de getallen *a*, *b*, *a*-*b* en *a*+*b* is deelbaar**
- **door 7**

Kwadraatresten (4)

een stelling over Pythagoreïsche drietallen; bewijs

- 1e. Beschouw de resten van a^2, b^2 en c^2 modulo 3. Dit zijn natuurlijk kwadraatresten. De kwadraatresten modulo 3 zijn 0 en 1.
- Voor $a^2 + b^2 = c^2$ vervalt de mogelijkheid $0 + 0 = 0 \pmod 3$, omdat dan alle drie getallen deelbaar door 3 zouden zijn. De mogelijkheid $1 + 1 = 2 \pmod 3$ vervalt omdat 2 geen kwadraatrest modulo 3 is.
- Dus blijven over de volgende mogelijkheden:
- $0 + 1 = 1$ en $1 + 0 = 1 \pmod 3$
- M.a.w.: $a^2 = 0 \pmod 3$ of $b^2 = 0 \pmod 3$, maar niet beide
- Omdat 3 een priemgetal is kan dit slechts als
- $a = 0 \pmod 3$ of $b = 0 \pmod 3$, maar niet beide
- Met andere woorden: precies één van de getallen a en b is deelbaar door 3

- Opdracht: bewijs het 2e, 3e en 4e deel van de stelling.

Kwadraatresten (6)

de lengte van de hypotenusa

- **Stelling. Stel *a*, *b*, *c* is een primitief Pythagoreïsch drietal. Dan bevat het getal *c* uitsluitend priemfactoren van de vorm 4*k*+1 (*k* is een natuurlijk getal).**
- Uitleg. In het college over complexe getallen door Jaap Top (voorjaar 2007) bleek: de som van twee kwadraten die onderling ondeelbaar zijn, bevat aan oneven priemgetallen uitsluitend getallen van de vorm 4*k*+1. Deze stelling werd destijds aangehaald, niet bewezen. Dit college staat nog op de website van Henk Broer.
- Priemgetallen van de vorm $4k + 1$ zijn complex geen priemgetallen, zie: 5 = (2+i)(2-i), 13 = (2+3i)(2-3i), 113 = (7+8i)(7-8i) en dergelijke.

- Hier toegepast: $c^2 = a^2 + b^2$ en *a* en *b* zijn onderling ondeelbaar, *c* is oneven, dus c^2 bevat uitsluitend priemfactoren van de vorm $4k + 1$
- Dan kan ook *c* uitsluitend zulke priemfactoren bevatten.
- Gevolg: de lengte van de hypotenusa in een primitieve rechthoekige driehoek kan nooit factoren 2, 3, 7, 11, 19, 23, 31, 43, …. hebben.

Kwadraatresten (6)

kwadratische reciprociteit

- Bekijk de priemgetallen 7 en 11. De kwadraatresten modulo 7 zijn 0, 1, 2 en 4; 11 = 4 (mod 7), dus **11 is kwadraatrest modulo 7**.
- De kwadraatresten modulo 11 zijn 0, 1, 3, 4, 5 en 9. Dus **7 is geen kwadraatrest modulo 11**.

- Bekijk de priemgetallen 5 en 11. De kwadraatresten modulo 5 zijn 0, 1 en 4; 11 = 1 (mod 5), dus **11 is kwadraatrest modulo 5**. Tegelijk geldt: **5 = 16 (mod 11) is kwadraatrest modulo 11**.

- Bekijk de priemgetallen 11 en 13. De kwadraatresten modulo 13 zijn 0, 1, 3, 4 9, 10 en 12; omdat 13 = 2 (mod 11) geldt: **13 is geen kwadraatrest modulo 11**, en **11 is geen kwadraatrest modulo 13**.

- Een vraag is: is er op voorhand een wetmatigheid aan te wijzen?

Kwadraatresten (7)
kwadratische reciprociteit

- Reeds Leonhard Euler (1707-1783) kwam tot een kwadratische reciprociteitswet, maar kon deze niet bewijzen.
- Ook Adrien-Marie Legendre (1752-1833) kon geen bewijs leveren. Van hem is wel een nog steeds gebruikte notatie afkomstig.
- Carl Friedrich Gauß (1777-1855) publiceerde in 1801 een bewijs, dat hij misschien al in 1796 had gevonden.

Kwadraatresten (8)

kwadratische reciprociteit

- **Symbool van Legendre**. Definitie:

- $\left(\frac{a}{p}\right)$ = 1 als *a* kwadraatrest modulo *p* is, en
  = -1 als *a* geen kwadraatrest modulo *p* is.
  Spreek uit: *a* boven *p*

Kwadratische reciprociteitswet.

Zijn *p* en *q* oneven priemgetallen, dan is:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

De kwadratische reciprociteitswet wordt hier niet bewezen.

Kwadraatresten (9)

kwadratische reciprociteit

- **De kwadratische reciprociteitswet in een andere, gelijkwaardige formulering**:
- Zijn p en q oneven priemgetallen, dan geldt:
- 1^e. Als ten minste één van de getallen p en q van de vorm $4k+1$ is, is p kwadraatrest modulo q als q kwadraatrest modulo p is, en omgekeerd.
- 2^e. Als beide getallen p en q van de vorm $4k-1$ (oftewel $4k+3$) zijn, is p kwadraatrest modulo q als q geen kwadraatrest modulo p is, en omgekeerd.

- Ga na dat deze formulering hetzelfde betekent als de formulering met behulp van het symbool van Legendre.
- Controleer de eerder gegeven voorbeelden.

Kwadraatresten (10)

kwadratische vergelijkingen

- De kwadratische reciprociteitswet wordt gebruikt om kwadratische restvergelijkingen op te lossen.
- Voorbeeld. Los op: $x^2 = 7 \pmod{31}$
- De vraag is allereerst of er een oplossing is. Omdat $31 = 3 \pmod 7$ **geen** kwadraatrest is en beide priemgetallen 7 en 31 van de vorm $4k+3$ zijn, is 7 **wel** een kwadraatrest modulo 31. Het heeft dus zin te zoeken: $31 + 7 = 38$, $62 + 7 = 69$, $93 + 7 = 100$.
- Dus $x = 10$ of $x = 31 - 10 = 21 \pmod{31}$ (controleer het laatste!)

- Nog een voorbeeld. Los op: $x^2 = 7 \pmod{41}$
- Omdat $41 = 6 \pmod 7$ **geen** kwadraatrest modulo 7 is en omdat 41 van de vorm $4k+1$ is, is 7 **geen** kwadraatrest modulo 41
- De vergelijking heeft dus geen oplossing. Zoekwerk is overbodig.

Niet bewezen stellingen (1)

- Je moet natuurlijk alles bewijzen. Maar dat is in het voorgaande niet gebeurd. Een eenvoudig te formuleren stelling is dat elk priemgetal van de vorm $4k+1$ de som van twee kwadraten is, en omgekeerd, als een priemgetal gelijk is aan de som van twee kwadraten, dan is het van de vorm $4k+1$. Het bewijs van deze stelling vergt meerdere stappen, men noemt het toch ‘elementair’.

- In het bewijs van de kwadratische reciprociteitswet speelt ook weer het onderscheid tussen priemgetallen van de vorm $4k+1$ resp. $4k+3$ mee.

- In meerdere tekstboeken worden stellingen als hier bedoeld goed uitgelegd. Je moet er wel even voor gaan zitten, en zonodig zelf een getallenvoorbeeld maken om een bewijs te doorgronden.

Niet bewezen stellingen (2)

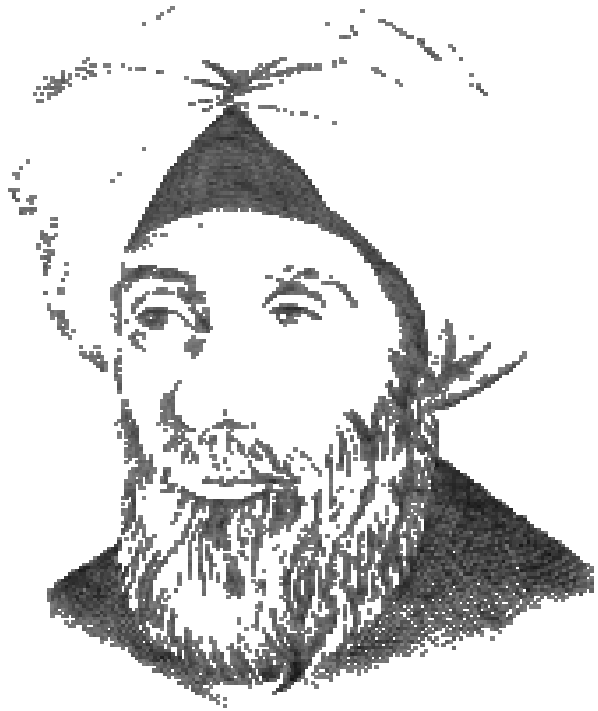
- Er is een groot aantal stellingen die eveneens ‘elementair’ kunnen worden bewezen, maar die in het voorgaande niet genoemd zijn.

- Bijvoorbeeld:
- Er zijn oneindig veel priemgetallen (een heel bekende stelling met een eenvoudig bewijs uit het ongerijmde).
- Er zijn oneindig veel priemgetallen van de vorm $4k+3$
- Er zijn oneindig veel priemgetallen van de vorm $4k+1$

- Heel anders lijkt de **stelling van Wilson**:
- Als p een priemgetal is, is $(p-1)! = -1 \pmod{p}$
- En omgekeerd: als $(m-1)! = -1 \pmod{m}$, dan is m een priemgetal

Geschiedenis van de getaltheorie

- De stelling van Wilson was al bekend aan de Arabische wiskundige al Hasan (Alhazen), die leefde van 965 tot 1039 of 1040.
- Door de eeuwen heen is getaltheorie beoefend, al in de oudst bekende culturen.
- Arabische wiskundigen zorgden voor de overdracht van veel oude en nieuwe resultaten naar Europa.



Onopgeloste problemen

- Legio is het aantal onopgeloste problemen, waarvan de formulering toch ook heel eenvoudig is.

- Voorbeeld. het vermoeden van Goldbach, genoemd naar Christian Goldbach (1690-1764):
- Elk even getal > 2 is te schrijven als de som van twee priemgetallen;
- zie 4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 3 + 7, ……..

- Een ander onopgelost vraagstuk is of er oneindig veel zgn. priemtweelingen bestaan, d.w.z. priemgetallen die 2 van elkaar verschillen:
- 3 en 5, 5 en 7, 11 en 13, ……, 101 en 103, 107 en 109, …….

Literatuur

- André Weil, *Number theory* (Boston 1983).
- mooi boek met historische achtergronden
- Dan Shanks, *Solved and unsolved problems in number theory* (New York 1978).
- dit focust meer op het open karakter van de getaltheorie
- H. Davenport, *The higher arithmetic* (New York 1983).
- handzaam boekje
- Ethan Bolker, *Elementary number theory* (New York 2007).
- een boek met een zgn. algebraische insteek en veel voorbeelden
- Underwood Dudley, *Elementary number theory* (San Francisco 1978).
- kent een geleidelijke opbouw

- Frits Beukers, *Getaltheorie voor beginners* (Epsilon Utrecht ^{3}2005).
- een toegankelijk boek dat alle ‘elementaire’ stof bevat