De Chinese reststelling is een stelling binnen de getaltheorie. De stelling werd voor het eerst beschreven in de vierde eeuw door de Chinese wiskundige Sun Tzu in zijn *Sun Tzu Suan Jing* (Rekenkundig handboek van Meester Sun). De stelling werd opnieuw in 1247 gepubliceerd door de Chinese wiskundige Qin Jiushao, in zijn *Wiskundige verhandeling in negen secties*.

■ door Paul Levrie (Toegepaste Ingenieurswetenschappen, Universiteit Antwerpen)

今有物　不知其數　三　三數之　賸二　五

De titel van dit artikel beschrijft een wiskundig probleem dat is terug te vinden als probleem 26 in hoofdstuk 3 van het Chinese boek *Sun Tzu Suan Jing* (het volledige boek is hier te vinden: http://ctext.org/Sun Tzu-suan-jing). Het werk dateert uit de vierde eeuw na Christus, en de auteur is Sun Tzu. De oplossing van het probleem staat er ook bij:

二十三

en je onderscheidt met wat moeite 2 keer 10 plus 3 (= 23). Vrij geformuleerd is het probleem het volgende: we zoeken een getal dat rest 2 geeft bij deling door 3, rest 3 bij deling door 5 en rest 2 bij deling door 7. Het is het oudste probleem van deze soort waar we weet van hebben, en dat het een oplossing heeft, volgt uit de stelling in het onderstaande kader.

We herinneren je er aan dat $x \equiv a_1 \pmod{m_1}$ uitgesproken wordt als 'x is congruent met a_1 modulo m_1', en dat dit gewoon betekent dat bij deling van het gehele getal x door m_1 de rest gelijk is aan a_1. Een voorbeeld zal dit duidelijk maken:

$$38 \equiv 2 \pmod{12},$$

want $38 = 3 \cdot 12 + 2$ (als je 38 kokosnoten in stapeltjes van 12 wil leggen, dan blijven er precies 2 over).

Verder zijn twee getallen *relatief priem* als ze geen gemeenschappelijke deler hebben (behalve 1). Dus 38 en 12 zijn niet relatief priem (gemene deler 2), maar 17 en 25 wel.

TWEE CONGRUENTIES Probleem 26 van Sun Tzu kunnen we nu ook als volgt schrijven: bepaal een getal x dat voldoet aan

$$x \equiv 2 \pmod{3},$$
$$x \equiv 3 \pmod{5},$$
$$x \equiv 2 \pmod{7}.$$

Maar voor we dit oplossen, proberen we een eenvoudiger geval: bepaal een getal x dat voldoet aan

$$x \equiv 3 \pmod{4},$$
$$x \equiv 6 \pmod{7}.$$

Een dergelijk probleem, met twee congruenties, kunnen we grafisch oplossen (zie figuur 1).We tekenen een rooster met als afmetingen de twee moduli, in dit geval dus 4 en 7, en we nummeren de verschillende vakjes, vertrekkend in de linkerbovenhoek met het getal 1, en dan gaan we verder zoals de pijlen in de figuur aangeven: één vakje naar rechts en één naar beneden. Komen we hierbij aan de onderste rand, dan gaan we boven verder. Komen we aan de rechterrand, dan vullen we vanaf

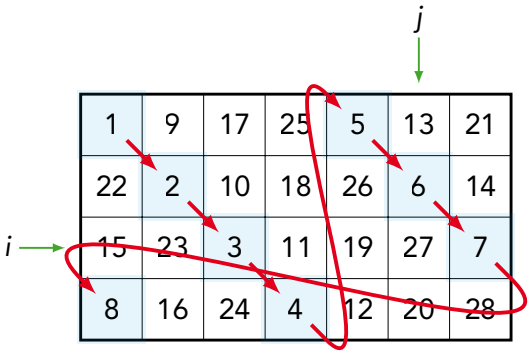
CHINESE RESTSTELLING

Als $m_1, m_2, \ldots, m_k$ positieve gehele getallen zijn die paarsgewijs relatief priem zijn, en als $a_1, a_2, \ldots, a_k$ gehele getallen zijn, dan heeft het stelsel

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\ldots$$
$$x \equiv a_k \pmod{m_k}$$

een oplossing, en die oplossing is uniek modulo m, waarbij $m = m_1 m_2 \cdots m_k$.

五數之 賸三 七 七數之 賸二 問物幾何



Figuur 1

links verder aan.

Merk op dat de getallen die in de i-de rij staan allemaal rest i geven bij deling door 4, en de getallen in de j-de kolom hebben rest j bij deling door 7. (Hierbij laten we even rest 4 toe modulo 4 en ook rest 7 modulo 7.) Dit heeft tot gevolg dat de gezochte x in dit geval het getal is dat staat in de derde rij – vanwege $x \equiv 3 \pmod 4$ – en de zesde kolom – wegens $x \equiv 6 \pmod 7$. We vinden dus $x = 27$, en je kan zelf nagaan dat dit klopt.

Dit rooster levert het bewijs van de Chinese reststelling in het geval van de twee moduli 4 en 7.

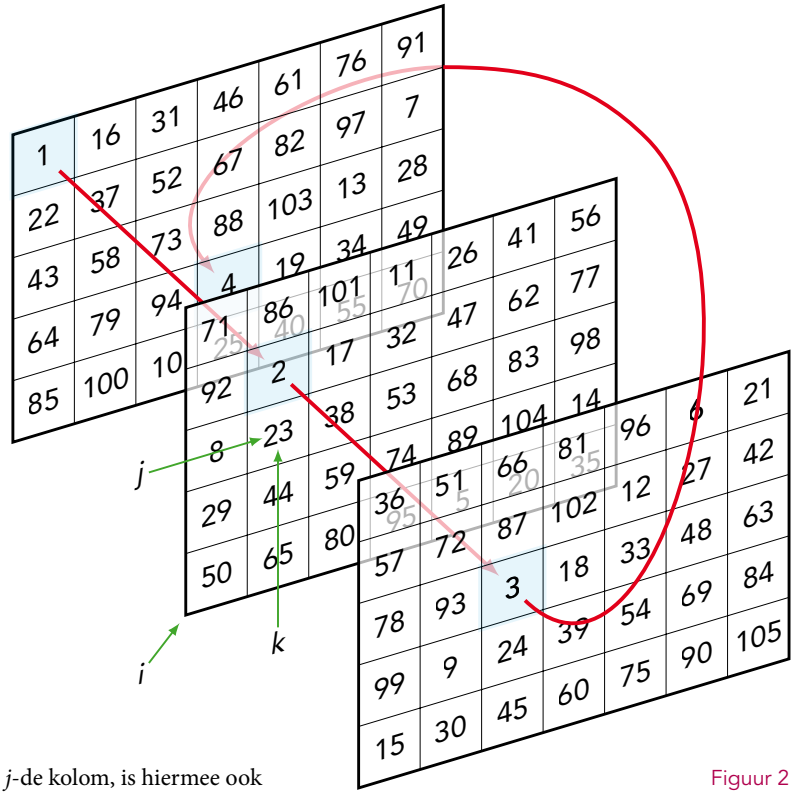
Op dezelfde manier volgt het bewijs voor twee willekeurige moduli m_1 en m_2 als ze relatief priem zijn, want in dat geval krijgen alle vakjes in het overeenkomstige rooster een uniek nummer toebedeeld. Want pas als alle getallen van 1 tot en met $m_1 \cdot m_2$ zijn ingevuld, stopt de bovenstaande procedure. Inderdaad, je kan geen getal meer invullen als je op een vakje stoot dat er al een bevat. Door de gebruikte 'diagonaalmethode' kan dit alleen maar gebeuren als je in het vakje rechtsonder in het rooster bent (zie je waarom?). En daar kan je enkel belanden na een aantal stappen dat een veelvoud is van zowel m_1 (het vakje zit op rij m_1) als van m_2 (het vakje zit in kolom m_2). Als m_1 en m_2 relatief priem zijn, dan gebeurt dit dus na $m_1 \cdot m_2$ stappen. En omdat er precies één getal ligt op de snijding

EEN EIERENPROBLEEM

Een oude vrouw gaat naar de markt om haar eieren te verkopen. Een paard trapt echter op haar eiermand en breekt haar eieren. De eigenaar van het paard wil haar vergoeden, en vraagt hoeveel eieren er in de mand zaten. De vrouw kan zich dat niet herinneren, maar ze weet nog wel dat als ze de eieren er per 6 uitnam, ze 5 eieren overhield, indien ze ze er per 5 uitnam, bleven er 4 over, indien per 4 bleven er 3 over, en per 3 hield ze er 2 over. Hoeveel eieren had de vrouw minstens in haar mand?

Dit probleem is terug te vinden in het boek *Brāhmasphuṭasiddhānta* uit 628 van de Indische wiskundige Brahmagupta. Het verhaaltje is er later rond gebreid.

De eierenkoopvrouw, Hendrick Bloemaert, 1632



Figuur 2

van de i-de rij met de j-de kolom, is hiermee ook bewezen dat er precies één oplossing is modulo $m_1 \cdot m_2$. We hebben dus bewezen dat

$$x \equiv i \pmod{m_1}$$
$$x \equiv j \pmod{m_2}$$

precies één oplossing heeft modulo $m_1 \cdot m_2$ als m_1 en m_2 relatief priem zijn.

DRIE CONGRUENTIES Werken we met drie congruenties, zoals in het probleem van Sun Tzu, dan kunnen we op een soortgelijke manier te werk gaan, maar we hebben wel een dimensie meer nodig. De moduli zijn in dit geval 3, 5 en 7, en we vertrekken dan ook van 3 roosters van 5 op 7 die we, zoals in het vorige voorbeeld, opvullen met de getallen van 1 tot en met 105. Het precieze systeem wordt duidelijk gemaakt in figuur 2.

In het i-de rooster bevinden zich de getallen die rest i geven bij deling door 3. De j-de rij in een rooster bevat de getallen die congruent zijn met j modulo 5, en in de k-de kolom staan de getallen die rest k geven bij deling door 7.

De oplossing van het probleem van Sun Tzu is dus het getal dat in het tweede rooster op de derde rij en in de tweede kolom staat. We vinden daar $x = 23$.

ALGEMENER Met dit systeem kunnen we meer algemeen de Chinese reststelling bewijzen voor drie congruenties met moduli die relatief priem zijn. De argumentatie die we gebruikt hebben in het geval van twee congruenties blijft immers geldig: alle roostervakjes krijgen met deze manier van nummeren een uniek nummer.

Willen we de oplossing wiskundig bepalen, en niet grafisch, dan helpt de volgende redenering. We veronderstellen dat de gezochte oplossing de som is van drie getallen, één per congruentie:

$$x = a + b + c.$$

Als we nu even veronderstellen dat b en c drievouden zijn, dan moeten we a congruent kiezen met 2 om aan de eerste congruentie $x \equiv 2 \pmod 3$ te voldoen:

$$x = a + 3b' + 3c' \text{ en } a \equiv 2 \pmod 3$$
$$\Rightarrow x \equiv 2 \pmod 3.$$

Als we dan bovendien veronderstellen dat a en c vijfvouden zijn, en we kiezen b congruent met 3, dan is er voldaan aan $x \equiv 3 \pmod 5$:

$$x = 5a'' + b + 5c'' \text{ en } b \equiv 3 \pmod 5$$
$$\Rightarrow x \equiv 3 \pmod 5.$$

Ten slotte zorgen we ervoor dat a en b zevenvouden zijn, en kiezen we c congruent met 2:

$$x = 7a''' + 7b''' + c \text{ en } c \equiv 2 \pmod 7$$
$$\Rightarrow x \equiv 2 \pmod 7.$$

Brengen we dit allemaal samen, dan moet
- a een veelvoud zijn van 5 en 7, stel $a = 35A$, met $35A \equiv 2 \pmod 3$;
- b een veelvoud zijn van 3 en 7, stel $b = 21B$, met $21B \equiv 3 \pmod 5$;
- c een veelvoud zijn van 3 en 5, stel $c = 15C$, met $15C \equiv 2 \pmod 7$.

Het gevolg is dat een oplossing van het probleem van Sun Tzu gegeven wordt door

$$x = 35A + 21B + 15C.$$

Rest ons nog de drie volgende kleine problemen op te lossen: bepaal A, B en C zodanig dat

$$35A \equiv 2 \pmod 3,$$
$$21B \equiv 3 \pmod 5,$$
$$15C \equiv 2 \pmod 7.$$

Die kunnen nog verder vereenvoudigd worden, bijvoorbeeld bij de eerste hebben we dat $35A \equiv 2A \pmod 3$, want $35 \equiv 2 \pmod 3$. De congruentie wordt dan: $2A \equiv 2 \pmod 3$. Wat overblijft is dit:

$$2A \equiv 2 \pmod 3,$$
$$B \equiv 3 \pmod 5,$$
$$C \equiv 2 \pmod 7$$

en deze kunnen op zicht opgelost worden: $A = 1$, $B = 3$, en $C = 2$ voldoen. (Voor een andere methode: zie het kader hieronder.) We vinden dan voor x door invullen:

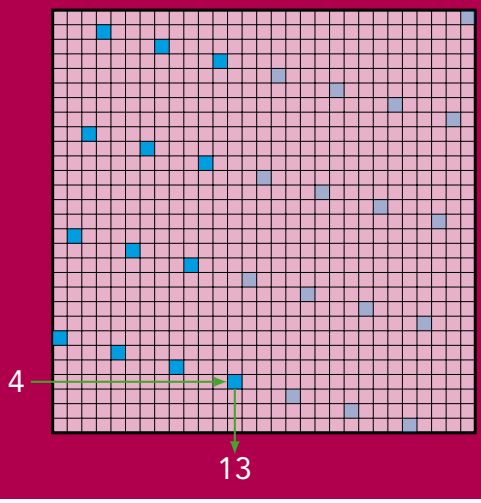
$$x = 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 = 128$$

en modulo $3 \cdot 5 \cdot 7 = 105$ geeft dit de oplossing die we grafisch hebben gevonden. ■

GRAFISCH OPLOSSEN VAN LINEAIRE CONGRUENTIES

Een vergelijking in gehele getallen, van de vorm $ax \equiv c \pmod b$, wordt een lineaire congruentie genoemd. Zo'n lineaire congruentie heeft precies één oplossing die kleiner is dan b, als de getallen a en b relatief priem zijn, dus geen gemeenschappelijke deler hebben. Indien a en b niet te groot zijn, kan je die oplossing grafisch vinden op een blad ruitjespapier.
We bekijken het aan de hand van een voorbeeld:

$$7x \equiv 4 \pmod{29}.$$

Hiervoor bakenen we op het ruitjesblad een vierkant af met zijde 29. En dan beginnen we ruitjes in te kleuren, links onderaan, in de eerste kolom, ruitje 7 hoog. Het volgende ruitje is dan telkens één naar rechts en 7 omhoog, waarbij we op precies dezelfde manier te werk gaan als in figuur 1. Zo wordt er op elke rij en in elke kolom één ruitje ingekleurd.
Als je het ruitje in rij 4 (geteld van onderaan) hebt ingekleurd, dan mag je stoppen. De oplossing van de congruentie is dan het kolomnummer van dit ruitje, in dit geval 13. Dus $x = 13$. Inderdaad:

$$7 \cdot 13 = 91 \equiv 4 \pmod{29}.$$