VOORBEREIDINGEN VAKANTIECURSUS 2023

FRITS BEUKERS

1. Introductie

Deze aantekeningen zijn ter voorbereiding op de Vakantiecursus 2023 voor leraren. Tijdens de cursus zullen we veronderstellen dat de cursisten bekend met zijn met het begrip *modulo rekenen*. Paragrafen 2 en 3 van deze tekst gaan over dit onderwerp en bevatten al het basismateriaal dat wij nodig hebben. U wordt gevraagd kennis te nemen van de beweringen van de stellingen. Voor de volledigheid hebben we ook hun bewijzen toegevoegd. U mág deze bewijzen overslaan, ze horen niet tot de basiskennis voor deze cursus.
Paragraaf 4 gaat over het computerprogramma PARI dat we tijdens de cursus zullen gebruiken.

2. Congruenties

Het modulo rekenen, ook wel congruentie rekenen genoemd, is een techniek in de getaltheorie die eenvoudig te begrijpen en buitengewoon effectief is. We starten met een positief geheel getal M en zeggen dat twee getallen a, b gelijk zijn modulo M als a en b een veelvoud van M verschillen. Notatie: $a \equiv b (\text{mod } M)$. We zeggen ook wel dat a congruent is met b modulo M.
Voorbeelden:

$$256 \equiv 6(\text{mod } 10), \quad 32433 \equiv 33(\text{mod } 100), \quad 40 \equiv 5(\text{mod } 7), \quad 67 \equiv 39(\text{mod } 7).$$

Een andere manier om $a \equiv b(\text{mod } M)$ te omschrijven, is te zeggen dat a en b bij deling door M dezelfde rest opleveren. In het laatste voorbeeld hebben zowel 67 als 39 rest 4 bij deling door 7.
De belangrijkste eigenschap van het rekenen met congruenties is dat de som of het product van twee getallen a en b hetzelfde blijft modulo M als we a of b met een veelvoud van M verschuiven. Bijvoorbeeld, stel dat we de rest van 43×51 bij deling door 7 willen uitrekenen. We gaan 43, en daarna 51, met veelvouden van 7 veranderen. Daarbij verandert de rest modulo 7 van het product niet. Dus,

$$43 \times 51 \equiv 1 \times 51 \equiv 1 \times 2 \equiv 2(\text{mod } 7).$$

Dit is uiteraard veel makkelijker dan eerst 43×51 uitrekenen en dan door 7 delen. Dezelfde opmerking geldt bij het optellen van twee getallen. Bijvoorbeeld:

$$43 + 51 \equiv 1 + 51 \equiv 1 + 2 \equiv 3(\text{mod } 7).$$

We kunnen dit wat formaliseren door het begrip *restklassen modulo M* in te voeren. Kies een willekeurig geheel getal r. De restklasse $r(\text{mod } M)$ bestaat uit alle gehele getallen n met $n \equiv r(\text{mod } M)$. Op deze manier wordt de verzameling gehele getallen opgedeeld in de M restklassen $r(\text{mod } M)$ met $r = 0, 1, 2, \ldots, M-1$. Hier ziet u de restklassen modulo 5.

0(mod 5)	...	-15	-10	-5	0	5	10	15	...
1(mod 5)	...	-14	-9	-4	1	6	11	16	...
2(mod 5)	...	-13	-8	-3	2	7	12	17	...
3(mod 5)	...	-12	-7	-2	3	8	13	18	...
4(mod 5)	...	-11	-6	-1	4	9	14	19	...

Merk trouwens op dat de restklasse 1(mod 5) hetzelfde is als 6(mod 5), en als -4(mod 5),etc. Met onze zojuist beschreven schuiftechniek zien we dat het product van een getal uit 2(mod 5) met een getal in 3(mod 5) altijd in de klasse 1(mod 5) terechtkomt. Verder komt hun som altijd in de klasse 0(mod 5) terecht.
We krijgen een optelling en vermenigvuldiging van de restklassen modulo M door af te spreken dat

$$a(\text{mod } M) + b(\text{mod } M) = a + b(\text{mod } M) \quad \text{en} \quad a(\text{mod } M)b(\text{mod } M) = ab(\text{mod } M).$$

De restklassen modulo M worden ook wel *congruentieklassen* modulo M genoemd.
In de youtube video `https://www.youtube.com/watch?v=oLA53mMVzws` van Wiskunde D online wordt dit in 12 minuten allemaal nog eens duidelijk uitgelegd, met een toepassing. Hier is een eerste toepassing.

Stelling 2.1. *Elk positief geheel getal is modulo* 9 *gelijk aan de som van zijn cijfers.*

Bijvoorbeeld 5761 is modulo 9 gelijk aan 1. De som van zijn cijfers, $5+7+6+1 = 19$ is ook 1 modulo 9. De verklaring is de volgende. Start met

$$5761 = 5 \times 10^3 + 7 \times 10^2 + 6 \times 10 + 1$$

en bekijk deze gelijkheid modulo 9. We weten dat 10 modulo 9 gelijk is aan 1, dus kunnen we de 10 overal vervangen door 1. We krijgen,

$$5761 \equiv 5 \times 1 + 7 \times 1 + 6 \times 1 + 1 \equiv 5 + 7 + 6 + 1(\text{mod } 9).$$

In het algemeen gaat het bewijs precies op deze manier.

Bewijs. Stel dat de cijfers van n gegeven worden door $n_k, n_{k-1}, \ldots, n_1, n_0$. Met andere woorden:

$$n = n_k \times 10^k + n_{k-1} \times 10^{k-1} + \cdots + n_1 \times 10 + n_0.$$

Als we dit getal modulo 9 bekijken, dan mogen we 10 overal vervangen door 1. We krijgen dan

$$n \equiv n_k + n_{k-1} + \cdots + n_1 + n_0(\text{mod } 9),$$

precies onze bewering. □

Opmerkingen:

- Een speciaal gevolg is dat een getal deelbaar is door 9 precies dan als de som van zijn cijfers dat is. Deze simpele test staat bekend als de *negenproef*.
- Dezelfde redenatie kunnen we ook modulo 3 houden om te zien dat een getal deelbaar is door 3 als de som van zijn cijfers dat ook is.

3. Congruenties modulo een priemgetal p

In de vorige paragraaf hebben we gekeken naar optelling en vermenigvuldiging modulo M. Het blijkt dat delen modulo een willekeurige M niet zo eenvoudig is. Daarom beperken we ons in deze paragraaf tot rekenen modulo een priemgetal p, waarbij deling wel mogelijk is.

We beginnen met een belangrijke observatie. Kies een priemgetal p en een getal a dat niet deelbaar is door p. Start met de rij getallen

$$1, 2, 3, \ldots, p-1$$

vermenigvulding ze allemaal met a en bekijk ze modulo p,

$$a, 2a, 3, \ldots, (p-1)a \pmod{p}.$$

Bijvoorbeeld $p = 7$ en $a = 3$. We beginnen met het rijtje

$$1, 2, 3, 4, 5, 6$$

vermenigvuldigen elk getal in het rijtje met 3,

$$3, 6, 9, 12, 15, 18$$

en kijken modulo 7,

$$3, 6, 2, 5, 1, 4 \pmod{7}.$$

We zien dat we het rijtje $1, 2, 3, 4, 5, 6$ weer terug hebben gekregen, maar dan in een andere volgorde. Dat gebeurt ook bij algemene p en a.

Stelling 3.1. *Stel p is priem en a een getal niet deelbaar door p. Dan zijn de verzamelingen $\{1, 2, \ldots, p-1\}$ en $\{a, 2a, \ldots, (p-1)a\}$ modulo p gelijk.*

Bewijs. Dit is niet moeilijk in te zien. Elk a-voud $a \times r$ met $0 < r < p$ is modulo p gelijk aan één van de getallen $1, 2, \ldots, p-1$. Er kan niet gelden dat $a \times r \equiv 0 \pmod{p}$ omdat noch a, noch r deelbaar is door p. Als twee a-vouden $a \times r$ en $a \times s$ gelijk zijn modulo p betekent dit dat p een deler is van hun verschil $a(r-s)$. Omdat p geen deler van a is, moet p dus $r - s$ delen. Omdat $-p < r - s < p$ kan dit alleen als $r = s$.
Conclusie, de getallen $a, 2a, \ldots (p-1)a$ zijn modulo p allen verschillend en moeten dus de restklassen $\{1, 2, \ldots, p-1\} \pmod{p}$ opvullen. □

Een gevolg van Stelling 3.1 is de volgende beroemde stelling.

Stelling 3.2 (Kleine stelling van Fermat)**.** *Stel dat p een priemgetal is en a een getal niet deelbaar door p. Dan geldt:*

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

Bewijs. We weten uit Stelling dat de verzamelingen $\{1, 2, \ldots, p-1\}$ en $\{a, 2a, \ldots, (p-1)a\}$ modulo p hetzelfde zijn. Dus zijn ook de producten van hun elementen gelijk modulo p. Met andere woorden,

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

Verzamel de factoren a uit het product links bij elkaar en schrijf $1 \times 2 \times \cdots \times (p-1)$ als $(p-1)!$. We vinden

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

De priem p deelt dus het verschil $(p-1)!(a^{p-1} - 1)$. Omdat p niet $(p-1)!$ deelt moet p dus een deler zijn van $a^{p-1} - 1$. Conclusie: $a^{p-1} \equiv 1 \pmod{p}$. □

Fermat's kleine stelling wordt ook uitgelegd in de Engelstalige Youtube film

`https://www.youtube.com/watch?v=w0ZQvZLx2KA`

Merk op dat, als $a^{p-1} \equiv 1 \pmod{p}$, dan geldt na vermenigvuldiging met a dat $a^p \equiv a \pmod{p}$. Opmerkelijk genoeg is dit ook waar als a deelbaar is door p. Immers, beide zijden a^p en a zijn deelbaar door p en dus ook hun verschil. We vinden hiermee,

Stelling 3.3 (Kleine stelling van Fermat, versie 2)**.** *Stel dat p priem is. Dan geldt voor elk geheel getal a dat $a^p \equiv a (\mathrm{mod}\ p)$.*

Dit is vrijwel de eerste niet-triviale stelling over priemgetallen in de geschiedenis van de getaltheorie.

NB Als $m > 1$ niet priem is dan gebeurt het *nooit* dat $a^m \equiv a (\mathrm{mod}\ m)$ voor alle gehele getallen a.

4. Het computerprogramma PARI

Rond 1986 startte een groep Franse wiskundigen uit Bordeaux een getaltheorie calculator. De naam van hun project is PARI en het is nog steeds actief. Eén van de features was dat er geen beperking op de getalgrootte bestond. Het rekenen met getallen van 100 cijfers is even gemakkelijk als rekenen met getallen van bijvoorbeeld 6 cijfers, een beperking die de meeste andere wiskunde-programmas destijds hadden. In de loop van de tijd is PARI uitgebreid met talloze functies uit de getaltheorie, waaronder zeer geavanceerde. Wij zullen er slechts een paar van gebruiken.
Er zijn verschillende manieren om met PARI te werken:

(1) Online, `https://pari.math.u-bordeaux.fr/gp.html`. U kunt gewoon naar de webpagina gaan en beginnen.
(2) Voor Android smartphone of tablet de PARI app 'Paridroid' downloaden via Google play. Bij opstarten van de app verschijnt er een terminalscherm met een paar knoppen.
(3) Op PC of laptop (zowel Windows als Mac) downloaden en installeren,

    `https://pari.math.u-bordeaux.fr/download.html`

    Bij het opstarten van PARI verschijnt er een zwart terminalscherm met een prompt (> of ?).
    Moeite met installeren in Windows? dan is de volgende youtube link handig,

    `https://www.youtube.com/watch?v=cdZLq11mJD4`

    Voor de Mac of linux,

    `https://www.youtube.com/watch?v=ZYuwJKmCClY`

Als eerste probeersel kunt u een willekeurige berekening met gehele getallen invoeren. Bijvoorbeeld $2 * 3$ (2 maal 3) of het meer ambitieuze 2^{100} (intikken met 2^100) en dan gevolgd door de 'enter'-toets op PC of het 'evaluate'-knopje op de app of online. Probeer nog eens wat berekeningen te doen. Voor een aantal basisvaardigen kun je

`https://www.youtube.com/watch?v=RQLqQHu7i0Y`

raadplegen. Niet alles wat daar behandeld wordt zullen we gebruiken, maar het is misschien wel handig om met PARI vertrouwd te raken.
In deze cursus zullen we slechts een paar getaltheoretische functies gebruiken namelijk **prime, isprime, nextprime** en **factor**.

- **prime**(n) geeft het n-de priemgetal. Probeer maar **prime**(10000).
- **isprime**(n) geeft het antwoord 1 als n priem is en 0 anders. Probeer maar **isprime**(18) of **isprime**(19). Of **isprime**(2^127-1).
- **nextprime**(n) geeft het kleinste priemgetal $\geq n$.
  Probeer bijvoorbeeld **nextprime**(10^10).

– **factor**(n) geeft de ontbinding van n in priemfactoren. Als n meer dan 100 cijfers bevat dan kan het zijn dat PARI er (te) lang over doet! Ontbinding in priemfactoren is lastig. Probeer eens **factor**(2^67-1). In 1903 meldde Frank Nelson Cole dat deze ontbinding hem 'three years of Sundays' gekost had.

In PARI kunnen we ook congruentierekenen en daar zullen we veel gebruik van maken. Voor een getal x modulo M bestaat een apart datatype: $\mathrm{Mod}(x, M)$. Typ bijvoorbeeld eerst in $a = \mathrm{Mod}(2, 137)$ en daarna $b = \mathrm{Mod}(6, 137)$. Reken vervolgens uit $a + b$ en $a * b$. Hier krijgen we gewoon $\mathrm{Mod}(8, 137)$ en $\mathrm{Mod}(12, 137)$, zoals verwacht. Eén van de belangrijkste bewerkingen is het snelle machtsverheffen. Bijvoorbeeld a^137 geeft $\mathrm{Mod}(2, 137)$, zoals voorspeld door de kleine stelling van Fermat. Probeer hetzelfde ook eens met grotere getallen.
NB: we hebben in deze paragraaf meteen gebruik gemaakt van het feit dat we aan variabelen, zoals a, b een waarde kunnen toekennen en verder met a, b rekenen zonder steeds hun waarden te hoeven intikken.
Voor de echte liefhebbers is er een uitgebreide tutorial op

`https://pari.math.u-bordeaux.fr/pub/pari/manuals/2.13.0/tutorial.pdf`

Helaas is de leercurve is bijzonder steil op misschien de eerste twee paragrafen na. Ik zet hem er hier bij voor de volledigheid. Wij zullen deze tutorial verder niet nodig hebben.