Dis1 2008-09
Ugeopgave 1

Rasmus Sylvester Bryder

20. februar 2009

1 F08 opgave 1

(i)

Der skal gøres rede for at [2] er en primisk restklasse i $\mathbb{Z}/49$, og den inverse dertil skal findes.

Altså skal gælde, at 2 er primisk med 49 (da [2] skal være en primisk restklasse modulo 49). Hvis 2 er primisk med 49, må der gælde at $(2, 49) = 1$.

Idet $1 = 25 \cdot 2 + (-1) \cdot 49$, gælder ifølge TAL(3.9), at 2 og 49 er primiske. Da så $0 \leq 2 < 49$ og $(2, 49) = 1$ kan vi ved TAL(6.11) slutte, at [2] er en primisk restklasse i $\mathbb{Z}/49$, og at den derfor er invertibel.

Af ligningen ovenfor ses da den inverse til [2], nemlig $[25] = [2]^{-1}$, da $25 \cdot 2 = 50 \equiv 1 \pmod{49}$.

(ii)

Der skal findes en løsning i $\mathbb{Z}$ til kongruenssystemet

$$x \equiv 7 \pmod{100}, \quad x \equiv 10 \pmod{49}.$$

Da $49 = 7^2$ og $100 = 2^2 \cdot 5^2$ er primiske, ved vi ved Den Kinesiske Restklassesætning, at der eksisterer en løsning modulo 4900. Da der skal gælde for x, at $x \equiv 7 \pmod{100}$, er x da på formen $x = 7 + 100k$, hvor $k \in \mathbb{Z}$. Da dette x også skal opfylde kongruensligningen $x \equiv 10 \pmod{49}$, skal der altså findes k så

$$7 + 100k \equiv 10 \pmod{49}.$$

Der skal pr. TAL(6.6) gælde, at $49|7 + 100k - 10$, dvs. $49|100k - 3$ eller $100k \equiv 3 \pmod{49}$. Da $49|2499$ (fordi $49 \cdot 51 = 2499$), gælder også at $49|2499k$ eller $49|2500k - k$ for alle $k \in \mathbb{Z}$, så der gælder, at

$$k \equiv 2500k = 25 \cdot 100k \equiv 25 \cdot 3 = 75 \equiv 26 \pmod{49},$$

da $100k \equiv 3 \pmod{49}$, og vi benyttede vores regneregler for restklasser. Altså er alle k på formen $k = 26 + 49l$, hvor $l \in \mathbb{Z}$, og dermed er alle x, som er løsninger til kongruenssystemet, på formen $x = 7 + 100(26 + 49l) = 2607 + 4900l$, hvor $l \in \mathbb{Z}$, og alle løsninger opfylder $x \equiv 2607 \pmod{4900}$. $x = 2607$ er altså en løsning til kongruenssystemet.

(iii)

Der skal findes en løsning i $\mathbb{Z}$ til kongruenssystemet

$$x \equiv 7 \pmod{100}, \quad x \equiv 10 \pmod{49}, \quad x \equiv 2 \pmod{3}.$$

Vi kender alle løsninger til de to første kongruensligninger fra (ii), nemlig $x = 2607 + 4900l$. Da 3 og $4900 = 2^2 \cdot 5^2 \cdot 7^2$ er primiske, eksisterer en løsning til de tre ligninger modulo 14700. De før fundne x skal nu tillige opfylde ligningen $x \equiv 2 \pmod{3}$. Altså skal vi finde de $l \in \mathbb{Z}$ for hvilke gælder, at $2607 + 4900l \equiv 2 \pmod{3}$, eller

$$4900l \equiv 2 - 2607 = 2 - 3 \cdot 869 \equiv 2 \pmod{3},$$

når vi benytter vores regneregler for restklasser. Da $3|4899$ (da $3 \cdot 1633 = 4899$), gælder også $3|4899l$ eller $3|4900l - l$ for $l \in \mathbb{Z}$, så

$$l \equiv 4900l \equiv 2 \pmod{3};$$

altså er alle l på formen $l = 2 + 3m$, hvor $m \in \mathbb{Z}$, hvormed alle x, der opfylder alle tre ligninger, er på formen $x = 2607 + 4900(2 + 3m) = 12407 + 14700m$, hvor $m \in \mathbb{Z}$. Altså er $x = 12407$ en løsning til kongruenssystemet.

2 GRP1: opgave 17

Lad $G = \mathrm{Perm}(\mathbb{C})$ være gruppen af alle bijektive afbildninger på $\mathbb{C}$, også kaldt den fulde permutationsgruppe på $\mathbb{C}$. For et givet $n \in \mathbb{N}$ ligger afbildningerne $\delta(z) = e^{2\pi i/n} z$ og $\sigma(z) = \overline{z}$ i G.

Notationen $ab \rightsquigarrow a \circ b$ benyttes fremover. Vi skal vise, at de $2n$ afbildninger $\mathrm{id}, \delta, \delta^2, \ldots, \delta^{n-1}, \sigma, \delta\sigma, \delta^2\sigma, \ldots, \delta^{n-1}\sigma$ udgør en undergruppe på G.

Vi ved at mængden H med disse $2n$ afbildninger er en delmængde af G, da identitetsafbildningen id, δ og σ ligger i G; de forskellige sammensætninger δ^k og $\delta^k\sigma$ for $k = 2, \ldots, n-1$ er også bijektive, da en sammensætning af bijektive afbildninger på $\mathbb{C}$ selv er en bijektiv afbildning på $\mathbb{C}$ pr. GRP(1.13), så $H \subseteq G$.

Vi skal nu undersøge, om det neutrale element for G ligger i H, om H er stabil og om der for alle x i H gælder at x^{-1} ligger i H.

Neutralt element. Da vi ved, at id er neutralt element for G, og at $\mathrm{id} \in H$, gælder altså, at det neutrale element id ligger i H.

Stabil. Vi skal nu undersøge om H er stabil, altså om når vi benytter sammensætningskompositionen på alle afbildninger i H derpå igen får afbildninger i H. Vi ser da, at der er 4 typer afbildninger i H: id, σ, δ^k for $k = 1, \ldots, n-1$, og $\delta^k\sigma$ for $k = 1, \ldots, n-1$.

Sammensætter vi id med en vilkårlig afbildning α i H, vil vi da få, at $\mathrm{id} \circ \alpha = \alpha = \alpha \circ \mathrm{id}$, da id jo er den identiske afbildning. Når vi tager alle 7 tilfælde af sammensætninger med id væk, da alle disse jo ligger i H, er der derfor "kun" følgende tilfælde tilbage at undersøge:

1. $\sigma\sigma$
2. $\sigma\delta^k$ for $k = 1, \ldots, n-1$
3. $\sigma\delta^k\sigma$ for $k = 1, \ldots, n-1$
4. $\delta^k\sigma$ for $k = 1, \ldots, n-1$

5. $\delta^j\delta^k$ for $j,k = 1,\ldots,n-1$
6. $\delta^j\delta^k\sigma$ for $j,k = 1,\ldots,n-1$
7. $\delta^k\sigma\sigma$ for $k = 1,\ldots,n-1$
8. $\delta^j\sigma\delta^k$ for $j,k = 1,\ldots,n-1$
9. $\delta^j\sigma\delta^k\sigma$ for $j,k = 1,\ldots,n-1$

Det er en kedsommelig proces, men vi kan lette arbejdet ved at indse nogle små tricks i G.

Da $\delta(z) = e^{2\pi i/n}z$, er

$$\delta^k(z) = \underbrace{(e^{2\pi i/n})\cdots(e^{2\pi i/n})}_{k} z = (e^{2\pi i/n})^k z = e^{2\pi ki/n}z.$$

Specielt er $\delta^n(z) = e^{2\pi i}z = (-1)^2 z = z$, så $\delta^n = \mathrm{id}$. Vores k-potenser svarer altså til at opløfte alt foran z i k'te. En anden sammenhæng er at

$$\delta^j\delta^k(z) = e^{2\pi ji/n}e^{2\pi ki/n}z = e^{2\pi(j+k)i/n}z = \delta^{j+k}(z).$$

Endvidere da $e^{2\pi(-k)i/n}e^{2\pi ki/n}z = e^0 z = z$, fungerer det altså også for negative potenser – her får vi endda at den inverse til δ^k er δ^{-k}, da så $\delta^k\delta^{-k} = \mathrm{id}$. Vi ser også her, at $\delta^0(z) = e^0 z = z$, så $\delta^0 = \mathrm{id}$.

Desuden gælder også at $\delta^{ab} = (\delta^a)^b$, da

$$(\delta^a)^b(z) = \underbrace{(e^{2\pi ai/n})\cdots(e^{2\pi ai/n})}_{b} z = e^{(2\pi ai/n)b}z = e^{2\pi abi/n}z = \delta^{ab}(z).$$

Om σ kan vi sige, at da $\sigma\sigma$ konjugerer $z \in \mathbb{C}$ dobbelt, er $\sigma\sigma(z) = z$, så $\sigma^2 = \mathrm{id}$, og $\sigma = \sigma^{-1}$.

Da G er en gruppe, gælder der for σ og δ ved GRP(1.4.3), at $(\sigma\delta)^{-1} = \delta^{-1}\sigma^{-1} = \delta^{-1}\sigma$. Lad os nu undersøge sammensætningen $\sigma\delta\sigma\delta$; ved indsættelse af $z \in \mathbb{C}$ fås ved brug af regneregler for konjugerede (Kalkulus 3.1.5) og GRP(1.13):

$$\begin{aligned}
\sigma\delta\sigma\delta(z) &= \sigma\delta\sigma(e^{2\pi i/n}z) = \sigma\delta(\overline{e^{2\pi i/n}z}) = \sigma(e^{2\pi i/n}\overline{e^{2\pi i/n}z}) \\
&= \overline{e^{2\pi i/n}\overline{e^{2\pi i/n}z}} = \overline{e^{2\pi i/n}\overline{e^{2\pi i/n}}\,\overline{z}} = \overline{e^{2\pi i/n}}\;\overline{e^{2\pi i/n}}\,\overline{\overline{z}} \\
&= \overline{e^{2\pi i/n}}e^{2\pi i/n}z = |e^{2\pi i/n}|z = z,
\end{aligned}$$

da $e^{2\pi i/n}$ ved GRP(1.13) er en enhedsrod og har længden 1. Men så er $\sigma\delta\sigma\delta = (\sigma\delta)(\sigma\delta) = \mathrm{id}$, så $(\sigma\delta)^{-1} = \sigma\delta$. Men da vi også havde, at $(\sigma\delta)^{-1} = \delta^{-1}\sigma$, er da $\sigma\delta = \delta^{-1}\sigma$ (hvilket var vinket givet på ugesedlen).

Da for et $k = 1,\ldots,n-1$ gælder $\delta^k\delta^{n-k} = \delta^{k+(n-k)} = \delta^n = \mathrm{id}$, må $\delta^{-k} = \delta^{n-k}$, hvor $n-k = 1,\ldots,n-1$. Med forrige betragtninger har vi så, at

$$\sigma\delta^k = \sigma\underbrace{\delta\cdots\delta}_{k} = \delta^{-1}\sigma\underbrace{\delta\cdots\delta}_{k-1} = \ldots = (\delta^{-1})^k\sigma = \delta^{-k}\sigma = \delta^{n-k}\sigma$$

Og nu begynder vi så at lege lidt med associativiteten – idet vi lader $j,k = 1,\ldots,n-1$ være givet, har vi:

1. Vi fandt jo, at $\sigma\sigma = \mathrm{id}$; da $\mathrm{id} \in H$, er $\sigma\sigma \in H$.

2. Da $\sigma\delta^k = \delta^{n-k}\sigma \in H$, hvor $n-k \in \{1,\ldots,n-1\}$, er $\sigma\delta^k \in H$.

3. Da $\sigma\delta^k\sigma = (\sigma\delta^k)\sigma = (\delta^{n-k}\sigma)\sigma = \delta^{n-k}(\sigma\sigma) = \delta^{n-k} \in H$, er $\sigma\delta^k\sigma \in H$.

4. $\delta^k\sigma \in H$ var oplyst da vi definerede H.

5. Da $\delta^j\delta^k = \delta^{j+k}$, hvor $j,k = 1,\ldots,n-1$, ved vi fra GRP(1.13) at eksponenten $j+k$ kan erstattes af sin principale rest r modulo n i tilfælde af at $j+k > n-1$, da koefficienten i δ^{j+k} måtte være en af de n enhedsrødder til ligningen $z^n = 1$, hvorpå $j+k \equiv r \pmod{n}$ for $0 \leq r < n$.

Da $0 \leq r < n$, dvs. $1 \leq r \leq n-1$ (i hvilket tilfælde $j+k \in \{1,\ldots,n-1\}$) eller $r = 0$ – dvs. at δ^{j+k} enten er en af δ-potenserne eller $\delta^0 = \mathrm{id}$, hvormed $\delta^j\delta^k \in H$.

6. Da vi benytter samme fif som i **5.**, ved vi, at $\delta^j\delta^k\sigma = \delta^{j+k}\sigma \in H$, da enten $\delta^{j+k}\sigma = \delta^s\sigma$ hvor $s = 1,\ldots,n-1$ eller $\delta^{j+k}\sigma = \delta^0\sigma = \sigma$, som begge ligger i H.

7. Da $\delta^k\sigma\sigma = \delta^k(\sigma\sigma) = \delta^k \in H$ giver det sig selv.

8. Da $\delta^j\sigma\delta^k = \delta^j\delta^{n-k}\sigma = \delta^{j+(n-k)}\sigma$, har vi ved samme argument som for **5.**, at enten $\delta^{j+(n-k)}\sigma = \delta^s\sigma$ hvor $s = 1,\ldots,n-1$ eller $\delta^{j+(n-k)}\sigma = \delta^0\sigma = \sigma$, som begge ligger i H.

9. Da $\delta^j\sigma\delta^k\sigma = (\delta^j\sigma)(\delta^k\sigma) = (\delta^j\sigma)(\sigma\delta^{n-k}) = \delta^j(\sigma\sigma)\delta^{n-k} = \delta^j\delta^{n-k} = \delta^{j+(n-k)}$, kan vi igen benytte argumentet fra **5.**, hvorpå vi har enten, at $\delta^{j+(n-k)} = \delta^s$ hvor $s = 1,\ldots,n-1$ eller $\delta^{j+(n-k)} = \delta^0 = \mathrm{id}$, som begge ligger i H.

Da kan vi konkludere, at H er stabil! (Gudskelov.)

Inverse elementer. Vi skal nu blot finde de inverse til de 4 typer afbildninger som nævnt før, og undersøge om de ligger i H.

Da $\mathrm{id}^{-1} = \mathrm{id}$ i G, ligger den inverse til id altså i H. Ligeså har vi $\sigma^{-1} = \sigma \in H$.

Vi påstår, at $(\delta^k)^{-1} = \delta^{n-k}$ for $k = 1,\ldots,n-1$. Dette ses, da $\delta^k\delta^{n-k} = \delta^{k+n-k} = \delta^n = \mathrm{id}$ og $\delta^{n-k}\delta^k = \delta^{n-k+k} = \delta^n = \mathrm{id}$, hvorpå $(\delta^k)^{-1} \in H$ for $k = 1,\ldots,n-1$, da $\delta^{n-k} \in H$ for samme.

Ligeså påstår vi, at $(\delta^k\sigma)^{-1} = \delta^k\sigma$. Thi da vi fandt at $\delta^k\sigma = \sigma\delta^{n-k}$, er

$$(\delta^k\sigma)(\sigma\delta^{n-k}) = \delta^k(\sigma\sigma)\delta^{n-k} = \delta^k\delta^{n-k} = \delta^n = \mathrm{id}$$

og

$$(\sigma\delta^{n-k})(\delta^k\sigma) = \sigma(\delta^{n-k}\delta^k)\sigma = \sigma\delta^n\sigma = \sigma\sigma = \mathrm{id},$$

hvorpå $(\delta^k\sigma)^{-1} \in H$ for $k = 1,\ldots,n-1$, da $\delta^k\sigma \in H$.

"Go ahead. Make my day." Derpå har vi vist, at $H \subseteq G$, at det neutrale element ligger i H, at H er stabil og at alle elementer i H har en invers i H. Derpå er H en undergruppe af G.

3 GRP2: opgave 4

Ved $x \mapsto 7x + 3$ bestemmes en bijektiv afbildning $\sigma : \mathbb{Z}/10 \to \mathbb{Z}/10$. Tallet i, hvor $i = 1, \ldots, 10$, identificeres med sin restklasse modulo 10. Da opfattes σ som en permutation i S_{10}.

Idet tallene i $\mathbb{Z}$ ligeledes opfattes som restklasser modulo 10, kan σ angives i direkte notation ved at indsætte tallene $i = 1, \ldots, 10$ i σ, hvorpå den tilsvarende restklasse modulo 10 er $\sigma(i)$ og $\sigma(i)$ opskrives for alle givne i i parenteser adskilt af kommaer.

Da er

$$\sigma = (10, 7, 4, 1, 8, 5, 2, 9, 6, 3),$$

da $\sigma(1) = 7 \cdot 1 + 3 = 10$, $\sigma(2) = 7 \cdot 2 + 3 = 17 = 10 + 7$, osv.

Da enhver permutation kan opskrives som et produkt af disjunkte cykler, kan vi ligeså gøre sådan for σ. Vi starter ved $i = 1$; det bringer os til det 1. tal i den direkte notation, 10, som er det næste element i cyklen. Da har vi videre $\sigma(10) = 3$, $\sigma(3) = 4$ og $\sigma(4) = 1$, og da vi dermed er nået tilbage hvor vi startede i denne cykel, kan cyklen sluttes. Dernæst undersøges 2 og så videre; med denne fremgangsmetode får vi, at

$$\sigma = (1\ 10\ 3\ 4)(2\ 7)(5\ 8\ 9\ 6),$$

og da ingen af cyklerne har fælles elementer, er cyklerne disjunkte og σ opskrevet som produkt af disse.