

Opgave UO:4

1. En færdig formel. Det er en rigtig nød, dvs jeg kan ikke selv bestemme cykelfremstillingen (eller bare cykeltypen) i almindelighed af

$$\sigma = (1\ 2)(1\ 2\ 3)(1\ 2\ 3\ 4) \dots (1\ 2\ 3\ 4 \dots, n).$$

Overraskende nok findes der en ret så simpel formel for permutationen:

$$\sigma(x) = (\text{odd}(x + n) + 1)/2,$$

hvor $\text{odd}(a)$ er den *ulige del* af a (divider a med størst mulig potens af 2). Dette udtryk er fundet af Niels Peter Jørgensen i 1997. Det er nemt at vise formelen ved induktion efter n .

2. Josefus' permutation. Gunnar Forst opdagede i 1998, at permutationen σ hænger tæt sammen med med Josefus-problemet [GKP, s. 8–16]: For et givet n bestemmes *Josefus' permutation*, J , på følgende måde: Sæt tallene $1, \dots, n$ i en ring. Spring over et tal og skub det næste ud af ringen, spring over et og skub det næste ud, og fortsæt indtil alle tallene er skubbet ud. Altså: Spring over tallet 1 og skub tallet 2 ud af ringen. Spring over 3 og skub 4 ud, osv. Sæt så

$$J(y) := \text{det } y\text{'te tal, der skubbes ud.}$$

(*Josefus-problemet* er så at bestemme $J(n)$, altså det tal der bliver sidst tilbage i ringen. I det rigtige Josefus-problem er det hver tredje, der skubbes ud, men det er en anden historie, se neden for.)

Det er ikke så svært at vise, for givet n , at Josefus-permutationen J er bestemt som følgende produkt:

$$J = (1\ 2\ 3 \dots n)(2\ 3 \dots n)(3 \dots n) \dots (n - 1\ n).$$

Idet ω er rækkefølgeombytningen: ombyt 1 og n , 2 og $n - 1$, osv, eller eksplicit:

$$\omega(x) = n + 1 - x,$$

følger det, at

$$J^{-1} = \omega\sigma\omega^{-1}.$$

Med formelen ovenfor for σ får vi derfor et eksplicit udtryk for den inverse Josefus:

$$J^{-1}(y) = n + 1 - [\text{odd}(2n + 1 - y) + 1]/2,$$

og heraf fås videre:

$$J(x) = 2n + 1 - 2^\nu(2n + 1 - 2x), \text{ med } J(x) \geq 1, \text{ størst mulig } \nu.$$

Specielt, for $x = n$, fås formelen for det tal, der bliver skubbet ud til sidst:

$$J(n) = 2n + 1 - 2^\nu.$$

Eksempel, for $n = 10$:

$$J(10) = 21 - 16 \cdot 1 = 5, \quad J(9) = 21 - 4 \cdot 3 = 9, \quad J(8) = 21 - 4 \cdot 5 = 1, \\ J(7) = 21 - 2 \cdot 7 = 7, \text{ osv.}$$

3. Fixpunkter. Det er let at bestemme fixpunkter (svarende til “1-cykler”) ud fra formlen for σ : Antag, for et givet $x \leq n$, at $x + n = 2^\nu u$, hvor u er ulige. Da er x et fixpunkt, hvis og kun hvis $(u + 1)/2 = 2^\nu u - n$, eller:

$$(2^{\nu+1} - 1)u = 2n + 1.$$

Denne ligning kan løses, nødvendigvis med ulige u , præcis når

$$2n + 1 \equiv 0 \pmod{2^{\nu+1} - 1}, \quad \text{og så med } x = \frac{2^\nu + n}{2^{\nu+1} - 1}.$$

Det er altså ét fixpunkt for hvert $\nu = 1, 2, \dots$, hvor kongruenserne kan løses:

$$2n + 1 \equiv 0 \pmod{3}, \quad 2n + 1 \equiv 0 \pmod{7}, \quad 2n + 1 \equiv 0 \pmod{15}, \dots$$

For eksempel, med $2n + 1 = 3 \cdot 5 \cdot 7$, altså $n = 52$, er der 3 fixpunkter.

4. Tilfældet med en 2-potens. Troels Windfeldt Hansen opdagede i 2003 empirisk, at cykeltypen for σ ikke var helt tilfældig, når n er en 2-potens. Fx kunne det “ses”, at når $n = 2^{p-1}$ med et primtal p , så er der ét fixpunkt og ellers lutter p -cykler.

Antag i det følgende, at $n = 2^m$. For at bestemme fixpunkter undersøger kongruenserne ovenfor. Et fixpunkt x svarer til en eksponent ν , så $2n + 1 \equiv 0$, altså $2^{m+1} \equiv -1$, hvor der regnes modulo $2^{\nu+1} - 1$. Da $2^{\nu+1} \equiv 1$, gælder kongruensen $2^{m+1} \equiv -1$ også, når eksponenten $m + 1$ erstattes med sin principale rest r modulo $\nu + 1$. Men af $2^r \equiv -1$ følger, at $2^r + 1$ er delelig med $2^{\nu+1} - 1$, og da $r < \nu + 1$, sker det kun, når $\nu = 1$ og $r = 1$. Af $m + 1 \equiv r \pmod{\nu + 1}$, altså $m + 1 \equiv 1 \pmod{2}$, følger, at m må være lige. Omvendt, hvis m er lige, er der præcis ét fixpunkt, svarende til $\nu = 1$, nemlig $x = (2^m + 2)/3$. Med andre ord: Antallet af fixpunkter er 1, når m er lige, og 0, når m er ulige.

Troels’ resultater var udgangspunkt for overvejelserne om fixpunkter og for de efterfølgende resultater.

5. Sætning. $\sigma^{m+1} = id$.

Bevis. Det er bekvemt at konjugere σ med den bijektive afbildning,

$$\{0, \dots, n - 1\} \rightarrow \{1, \dots, n\}, \quad x \mapsto n - x.$$

Efter denne konjugering får vi følgende udtryk for σ , som permutation af $\{0, \dots, n - 1\}$:

$$(5.1) \quad \sigma(x) = 2n - 1 - \frac{\text{odd}(2n - 1 - x + 1) - 1}{2} - n.$$

Vi identificerer tal x , med $0 \leq x < 2n - 1$, med deres *bitmønstre*, den binære fremstilling af x med $m + 1$ cifre, idet vi skriver cifrene fra venstre, med “konstantleddet” (svarende til $x_0 2^0$) længst mod venstre og den ledene bit x_m (svarende til $x_m 2^m$) til højre. Den ledende bit er 0, når $x < n$, idet der altid medtages $m + 1$ bits. Sammen med x betragtes det *komplementære tal* \bar{x} , der fås af (bitmønstret for) x ved overalt at skifte 0’er med 1’er og vice versa. Aritmetisk er $\bar{x} = 2n - 1 - x$. Det fremgår, at vi kan få $\sigma(x)$ i en række skridt:

- (1) $x \mapsto u = \text{odd}(\bar{x} + 1)$,
- (2) For u ulige: $u \mapsto v = (u - 1)/2$.
- (3) $v \mapsto \sigma(x) = \bar{v} - n$.

For at se effekten af dette på bitmønstrer for x opsøges fra venstre det første 1 i x (antag et øjeblik, at $x > 0$):

$$x = 00 \dots 001y,$$

med k 0'er ($k \geq 0$). Vi finder så $\bar{x} = 11 \dots 110\bar{y}$, $\bar{x} + 1 = 00 \dots 001\bar{y}$, og altså

$$u = \text{odd}(\bar{x} + 1) = 1\bar{y}00 \dots 00,$$

med k ledende 0'er. Videre finder vi

$$v = (u - 1)/2 = \bar{y}00 \dots 000,$$

nu med $k + 1$ 0'er. Herefter fås $\bar{v} = y11 \dots 111$, og endelig slutresultatet,

$$\sigma(x) = \bar{v} - n = y11 \dots 110,$$

med k 1'er. Med andre ord: man får $\sigma(x)$ ved at bortskære den venstre blok i x , til og med det første 1, og så foranstille (til højre) komplementet til den bortskårne blok. Lidt dynamisk kan konstruktionen beskrives som følger: Betragt en uendelig følge af bits opnået ved at gentage skiftevis mønstrer x og det komplementære mønster \bar{x} :

$$x\bar{x}x\bar{x} \dots$$

Lad os vedtage, at en *pointer*, placeret til venstre for et bit i denne følge, *bestemmer* det tal, hvis bitmønster består af de $m + 1$ bits til højre for pointeren. Tallet x bestemmes altså ved at placere pointeren fx lige til venstre for det første bit i følgen.

Af beskrivelsen af $\sigma(x)$ ovenfor fås følgende observation:

Hvis pointeren bestemmer x , så bestemmes $\sigma(x)$ ved at flytte pointeren til højre hen forbi det førstkommande 1.

Denne beskrivelse passer faktisk også for $x = 0$. Her består den uendelige bitfølge af $m + 1$ 0'er efterfulgt af $m + 1$ 1'er, efterfulgt af \dots . Flytningen er hen forbi det første 1, og så efterfølges pointeren af m 1'er og et 0, som bestemmer tallet $n - 1 = 2^m - 1$.

Nu følger det videre, at $\sigma^2(x)$ bestemmes ud fra $\sigma(x)$ ved igen at flytte pointeren forbi det førstkommande 1, og σ^{m+1} fås ved $m + 1$ gentagelser, altså ved $m + 1$ gange at flytte forbi det førstkommande 1. I følgen $x\bar{x}$ til er der lige mange 0'er og 1'er. I følgen $x\bar{x}$ er der altså præcis $m + 1$ 1'er, og det sidste bit i følgen er et 1. Når pointeren er flyttet $m + 1$ gange, er den altså præcis flyttet hen forbi det sidste bit i følgen $x\bar{x}$, og så bestemmer pointeren igen x . Med andre ord: $\sigma^{m+1}(x) = x$.

6. Korollar. *Hvis $n = 2^{p-1}$, hvor p er et ulige primtal, så har σ cykeltypen $1^1 p^k$, hvor $k = (2^{p-1} - 1)/p$.*

Bevis. Det er Troels' conjecture, og det følger umiddelbart. Da $\sigma^p = id$, er hver banelængde divisor i p . Da der kun er et fixpunkt (en 1-cykel), har de øvrige cykler længde p .

7. Cykeltypen. Observationen i beviset for Sætning 5 kan bruges til at bestemme cykeltypen helt, stadig i tilfældet $n = 2^m$. Af sætningen følger, hvis x bestemmer en p -cykel, så er p divisor i $m + 1$ (og naturligvis er $\sigma^p(x) = x$).

Betragt, for $m + 1 = pd$ og et bitmønster x , ligningen $\sigma^p(x) = x$. Den betyder, at når pointeren i følgen $x\bar{x}x\bar{x} \dots$ flyttes p gange (altid til højre, forbi det første 1), så fremkommer

x igen. Lad h være det samlede antal bits, som overspringes ved de p flytninger. Når de p flytninger er gentaget d gange, har vi flyttet $m + 1$ gange, og altså oversprunget de $2(m + 1)$ bits i $x\bar{x}$. Derfor er $dh = 2(m + 1)$. Altså er $h = 2p$. Lad z være blokken af de første p (fra venstre) af de oversprungne bits, og lad w være blokken af de næste p . Da er

$$x\bar{x} = zw \dots zwzw,$$

med d gentagelser at de $2p$ bits zw . Af denne ligning følger, at d må være ulige (ellers ville $x = \bar{x}$), at $w = \bar{z}$, og at x har formen,

$$(*) \quad x = z\bar{z}z\bar{z} \dots z\bar{z}z;$$

hvis $d = 2e - 1$, er der e blokke z og $e - 1$ blokke \bar{z} , begge af længde p .

Med andre ord: *For hver divisor p i $m + 1$, med $m + 1 = dp$, er $\sigma^p(x) = x$, hvis og kun hvis d er ulige og x har formen (*), hvor z er en blok med p bits og højre bit lig 0.*

Der er 2^{p-1} muligheder for et sådant z , og altså i alt 2^{p-1} muligheder for et tal x med $\sigma^p(x) = x$.

Lad nu $\alpha(p)$ betegner antallet af tal $x < n$ for hvilke cyklen bestemt ved x har længde p . Af det foregående fås:

$$\sum_{q|p} \alpha(q) = \begin{cases} 2^{p-1} & \text{hvis } p \mid m + 1 \text{ og } (m + 1)/p \text{ er ulige,} \\ 0 & \text{ellers.} \end{cases}$$

Møbius inversion giver herefter, når $p \mid (m + 1)$,

$$\alpha(p) = \sum'_{q|p} \mu(p/q) 2^{q-1},$$

hvor der summeres over de divisorer q for hvilke $(2m + 1)/q$ er ulige.

Ækvivalent, hvis $m + 1 = 2^v u$, hvor u er ulige, så er $\alpha(p) = 0$ med mindre p er en divisor i $m + 1$ af formen $2^v v$. I det sidste tilfælde er

$$\alpha(2^v v) = \sum_{w|v} \mu(v/w) 2^{2^v w-1}.$$

Antallet af p -cykler er $\alpha(p)/p$.

8. Eksempel. For $n = 2^9 = 512$ er $m + 1 = 10 = 2 \cdot 5$, så der er 2- og 10-cykler, nemlig, for $v = 1$:

$$\frac{1}{2} \mu(1) 2^{2-1} = 1 \quad \text{2-cykler,}$$

og for $v = 5$:

$$\frac{1}{10} ((-1) 2^{2-1} + 2^{10-1}) = 51 \quad \text{10-cykler.}$$

9. Tilfældet med en 2-potens minus 1. Lasse Nielsen opdagede i 2003, at der for vilkårligt n gælder, at tallene $x_k = n - (2^k - 1)$, for $k = 0, 1, \dots$ og $x_k \geq 1$, ligger i samme cykel:

$$x_k \mapsto x_{k-1} \mapsto \dots \mapsto n - 3 \mapsto n - 1 \mapsto n = x_0;$$

længden af den største cykel, der forekommer i σ er altså altid mindst lig med $k + 1$, hvor k er den hele del af tallet $\log_2 n$.

Antag, at $n = 2^m - 1$. Lasse Nielsen opdagede videre (empirisk), at *i cykelfremstillingen af σ forekommer i dette tilfælde p -cykler for alle $p = 1, \dots, m$, og ikke for andre p .*

For at vise denne påstand konjugerer vi σ som i (5.1), men denne gang i intervallet $1 \leq x \leq n$ med $\omega(x) = n + 1 - x$. Nu bliver permutationen, defineret for $1 \leq x \leq 2^m - 1$:

$$\sigma(x) = 2n + 1 - \frac{\text{odd}(2n + 1 - x) - 1}{2} - (n + 1).$$

Her er $2n + 1 = 2^{m+1} - 1$, så med betegnelserne fra beviset oven for er

$$\sigma(x) = \bar{u} - 2^m, \quad \text{hvor } u = (\text{odd}(\bar{x}) - 1)/2.$$

Tallene i intervallet svarer til bitmønstre med $m + 1$ bits og ledende bit 0, med undtagelse af lutter 0'er. Er

$$x = 11 \dots 10y0$$

med k 1'er, fås $\bar{x} = 00 \dots 01\bar{y}1$, og $\text{odd}(\bar{x}) = 1\bar{y}100 \dots 0$, og $u = \bar{y}100 \dots 00$, og altså

$$\sigma(x) = y011 \dots 10.$$

Med andre ord:

Betragt den uendelige periodiske følge af bits $xxx \dots$. Hvis pointeren bestemmer x (fx i stillingen yderst til venstre), så bestemmes $\sigma(x)$ ved at flytte pointeren hen forbi det førstkommande 0.

Beskrivelsen passer også for $x = 2^m - 1$, som er fixpunkt, svarende til bitmønstret $11 \dots 110$.

Af beskrivelsen ses, at hvis der er k 0'er i bitmønstret for x , så er $\sigma^k(x) = x$. Der kan højst være m 0'er (idet lutter 0'er er udelukket). Desuden ses, at for $x = 1 \dots 100 \dots 0$ med p 0'er bliver perioden præcis p . Hermed er Lasses observation eftervist.

Antallet af p -cykler kan bestemmes således: Lad $M_\lambda(d)$ være mængden af bit-mønstre af længde d , med ledende (højre) bit 0, og med λd 0'er, og ikke bestående af lutter 0'er, og lad $\beta_\lambda(d)$ være antallet af sådanne mønstre. Antallet er naturligvis kun positivt, når λd er et naturligt tal strengt mindre end d ; og i det tilfælde er

$$\beta_\lambda(d) = \binom{d-1}{\lambda d-1}.$$

Lad $\beta_\lambda^{\text{prim}}(d)$ betegne antallet af mønstre i $M_\lambda(d)$, som er *primitive*, dvs ikke har formen $zz \dots z$, hvor $z \in M_\lambda(e)$ med en ægte divisor $e \mid d$. Det er klart, at $\beta_\lambda(d) = \sum_{e \mid d} \beta_\lambda^{\text{prim}}(e)$, så ved Möbius-inversion fås:

$$\beta_\lambda^{\text{prim}}(e) = \sum_{d \mid e} \mu(e/d) \beta_\lambda(d).$$

Det følger af beskrivelsen ovenfor, når $1 \leq x \leq 2^m - 1$, at x har periode p under σ , hvis og kun hvis bitmønstret x har formen $zz \dots z$, hvor z er et primitivt mønster med p 0'er. For $1 \leq p \leq m + 1$ er antallet af tal x med periode p altså lig med summen,

$$\sum_{e \mid m+1} \beta_{p/e}^{\text{prim}}(e).$$

Der er kun bidrag, når $e > p$, så summen bliver:

$$\sum_{d|e|(m+1)} \mu(d) \beta_{p/e}(e/d) = \sum_{d|e|(m+1)} \mu(d) \binom{e/d-1}{p/d-1},$$

hvor der i summen kun medtages led, når $e > p$ og $d \mid p$; specielt er $e > 1$. Antallet af p -cykler fås fra summen ved at dividere med k .

Bemærk, at summen altid har et led svarende til $e = m + 1$ og $d = 1$, nemlig følgende:

$$\binom{m}{p-1}.$$

Hvis $m + 1$ er et primtal, er der ikke andre led. I dette tilfælde er antallet af p -cykler altså lig med

$$\frac{1}{p} \binom{p}{k-1}.$$

10. Eksempel. $n = 2^9 - 1 = 511$ giver $m + 1 = 10$ med divisorer $e = 10, 5, 2$ idet $e > 1$.

$$p = 9, (e, d) = (10, 1): \binom{9}{8}/9 = 1.$$

$$p = 8, (e, d) = (10, 1), (10, 2): \left(\binom{9}{7} - \binom{4}{3}\right)/8 = 4.$$

$$p = 7, (e, d) = (10, 1): \binom{9}{6}/7 = 12.$$

$$p = 6, (e, d) = (10, 1), (10, 2): \left(\binom{9}{5} - \binom{4}{2}\right)/6 = 20.$$

$$p = 5, (e, d) = (10, 1), (10, 5): \left(\binom{9}{4} + \binom{4}{0} + \binom{4}{1}\right)/5 = 25.$$

$$p = 4, (e, d) = (10, 1), (10, 2), (5, 1): \left(\binom{9}{3} - \binom{4}{1} + \binom{4}{3}\right)/4 = 21.$$

$$p = 3, (e, d) = (10, 1), (5, 1): \left(\binom{9}{2} + \binom{4}{2}\right)/3 = 14.$$

$$p = 2, (e, d) = (10, 1), (10, 2), (5, 1): \left(\binom{9}{1} - \binom{4}{0} + \binom{4}{1}\right)/2 = 6.$$

$$p = 1, (e, d) = (10, 1), (5, 1), (2, 1): \left(\binom{9}{0} + \binom{4}{0} + \binom{4}{0}\right)/1 = 3.$$

11. Den rigtige Josefus. Den generelle udfordring, se [GKP, s. 79–81], er følgende: Stil tallene $1, 2, \dots, n$ i ringen og skub hvert q 'te tal ud (tilfældet ovenfor er $q = 2$, Josefus' oprindelige problem svarer til $q = 3$). Lad $J_q = J_{q,n}$ være permutationen i S_n bestemt ved at $J_q(x)$ er lig med det x 'te tal, der skubbes ud. Findes der en formel for permutationen J_q ?

Som ovenfor ses, at

$$J_q = (1\ 2\ 3 \dots n)^{q-1} (2\ 3 \dots n)^{q-1} \dots (n-1\ n)^{q-1},$$

og heraf:

$$J_q^{-1} = \omega \sigma_q \omega^{-1},$$

hvor

$$\sigma_q = \sigma_{q,n} = (1\ 2)^{q-1} (1\ 2\ 3)^{q-1} \dots (1\ 2\ 3 \dots n)^{q-1}$$

Findes der en formel for σ_q , som tillader at bestemme σ_q^{-1} ?

Det er let at bestemme et rekursivt udtryk: Hold q fast, og prøv med et udtryk af formen

$$\sigma_{q,n}(x) = f(x + (q-1)n).$$

Induktivt kan antages, for $1 \leq x \leq n - q$, at

$$\sigma_{q,n}(x) = \sigma_{q,n-1}(x+q-1) = f(x+q-1 + (q-1)(n-1)) = f(x + (q-1)n),$$

så ligningen gælder, når bare den gælder for $n - q < x \leq n$. For $x = n - q + 1$ er $\sigma_{q,n}(x) = n$, så kravet her er

$$f(n-q+1 + (q-1)n) = n, \quad \text{altså } f(qn - q + 1) = n.$$

For $n - q + 1 < x \leq n$ er $x = n - a$ med $0 \leq a < q - 1$, og her er $\sigma_{q,n}(n - a) = \sigma_{q,n-1}(q - 1 - a) = f(q - 1 - a + (q - 1)(n - 1))$; kravet er

$$f(-a + qn) = f(-a + (q - 1)n), \text{ for } 0 \leq a < q - 1.$$

Erstattes n med $t + 1$ i det første krav, og n med t i de øvrige, er betingelserne:

$$f(qt - a) = f((q-1)t - a) \text{ for } a = 0, \dots, q - 2, \quad f(qt + 1) = t + 1.$$

Eksempel. For $q = 2$ fås $f(2t) = f(t)$, $f(2t + 1) = t$, hvorefter $f(x) = [\text{odd}(x) + 1]/2$.

Og for $q = 3$ fås:

$$f(3t - 1) = f(2t - 1), \quad f(3t) = f(2t), \quad f(3t + 1) = t + 1.$$

Man får altså $f(z)$ ved først at reducere, gentagne gange, argumentet z med de to operationer $3t - 1 \mapsto 2t - 1$ og $3t \mapsto 2t$ indtil der fremkommer et tal $\equiv 1 \pmod{3}$; denne reduktion kunne betegnes $\text{odd}_3(z)$. Med denne betegnelse er $f(z) = (\text{odd}_3(z) + 2)/3$, og altså

$$\sigma_3(x) = \frac{\text{odd}_3(x + 2n) + 2}{3}.$$

Den ovenfor af reduktionen ovenfor, $2t \mapsto 3t$ og $2t - 1 \mapsto 3t - 1$, kan fås ved at multiplicere med $3/2$ og runde op; med en ikke-standard notation kan den betegnes $\lceil 3/2 \rceil$. Med denne notation bestemmes den inverse sådan:

$$x = \sigma_3^{-1}(y) = \lceil 3/2 \rceil^v (3y - 2) - 2n,$$

med v mindst mulig og $x \geq 1$ (eller v størst og $x \leq n$). For den konjugerede, $J_3 = \omega \sigma_3^{-1} \omega^{-1}$, fås:

$$J_3(y) = 3n + 1 - \lceil 3/2 \rceil^v (3n + 1 - 3y);$$

specielt, Josefus-tallet er

$$J_3(n) = 3n + 1 - \lceil 3/2 \rceil^v (1).$$

Generaliseringen til $q > 3$ er umiddelbar.

LITTERATUR

[GKP] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics*, Second edition, Addison-Wesley, 1995.