MYNTVEKSLING

Cirkeln, KTH

31 Jan. 02

Myntveksling.

Innledning

1 Innledning: *Myntveksling* er et navn vi gir til en lang rekke problemer og resultater som forkommer i mange deler av matematikken, og i mange anvendelser av matematikken. Det er lett å forstå problemene og å eksperimentere med dem, og de er både interessante og inspirerende, og gir et godt inntrykk av hva mange matematikere sysler med. Også teoretisk kan man komme et stykke på vei med elementære midler, som de fleste gymnaselever behersker. Det er imidlertid langt mellom generelle resultater, og man kommer fort til forskningsfronten. Området har derfor aldrig blitt sentralt i matematikken selvom mange matematikere har arbeidet med det.

Problemet

2 Problemet: Vi antar at du har et ubegrenset antall mynter av valørene a og b. Det mest generelle spørsmålet er: Hvilke beløp kan du veksle til deg?

3 Eksempel: Før vi presiserer problemet er det bra å se på noen eksempler:

a	**b**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	**g**	**n**
2	**3**	0	*	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	**1**	**1**
2	**4**	0	*	2	*	4	*	6	*	8	*	10	*	12	*	14	*	16	∞	∞
2	**5**	0	*	2	*	4	5	6	7	8	9	10	11	12	13	14	15	16	**3**	**2**
2	**7**	0	*	2	*	4	*	6	7	8	9	10	11	12	13	14	15	16	**5**	**3**
2	**9**	0	*	2	*	4	*	6	*	8	9	10	11	12	13	14	15	16	**7**	**4**

3	**4**	0	*	*	3	4	*	6	7	8	9	10	11	12	13	14	15	16	**5**	**3**
3	**5**	0	*	*	3	*	5	6	*	8	9	10	11	12	13	14	15	16	**7**	**4**
3	**6**	0	*	*	3	*	*	6	*	*	9	*	*	12	*	*	15	*	∞	∞
3	**7**	0	*	*	3	*	*	6	7	*	9	10	*	12	13	14	15	16	**11**	**6**
3	**8**	0	*	*	3	*	*	6	*	8	9	*	11	12	*	14	15	16	**13**	**7**

felles divisor

Vi observerer først at om a og b har en **felles divisor** finnes det uendelig mange beløp vi ikke kan veksle til oss. Alle beløp vi veksler må nemlig være delbare med den felles divisoren. Videre ser vi at det virker som om vi kan få alle beløp over en viss størrelse om a og b ikke har en felles divisor.

Oppdatert

4 Oppdatert problem: Om myntverdiene a og b ikke har noen felles divisor, kan vi da veksle alle beløp over en viss størrelse? Om det er slik, kan du finne en formel for det største beløpet $g(a,b)$ som *ikke* kan veksles. Kan du videre finne en formel for antallet beløp $n(a,b)$ som ikke kan veksles.

Gjetning

5 Gjetning: Før du kikker på svaret er det viktig at du regner mange eksempel. Hva tyder eksemplene på? Kan du gjette en formel som gjelder for $g(a,b)$ og $n(a,b)$? Først når du selv har gjettet et svare bør du gå videre i disse notatene:

Svar

6 Svar: *Vi har*

$$g(a,b) = ab - b - a, \quad \textit{og} \quad n(a,b) = \frac{(a-1)(b-1)}{2}.$$

Symmetri

7 Symmetri: Se på eksemplene. Ser du noen *symmetrier* mellom tall p, q slik at $ab-b-a = p+q$? Symmetrien gir et mer *komplett resultat.*

Hovedresultat

8 Setning: *La a og b være positive heltall som ikke har noen felles divisor. La $\mathcal{M}(a,b)$ bestå av alle tall på formen $ma+nb$ for noen ikke negative heltall m og n. For hvert par av heltall p og q slik at*

$$ab - b - a = p + q$$

vil et av tallene p eller q tilhøre $\mathcal{M}(a,b)$, mens det andre ikke tilhører $\mathcal{M}(a,b)$. Spesielt ser vi:

(1) *Ved å ta $p < 0$ får vi at alle tall q slik at $q > ab-b-a$ tilhøre $\mathcal{M}(a,b)$.*
(2) *Ved å sette $p = 0$ får vi at $ab-a-b$ ikke tilhører $\mathcal{M}(a,b)$.*
(3) *Ved å ta $0 \le p \le ab-a-b$ ser vi at det er nøyaktig $(a-1)(b-1)/2$ av tallene $0, 1, \ldots, ab-a-b$ som ikke tilhører $\mathcal{M}(a,b)$. Og følgelig vil nøyaktig $(a-1)(b-1)/2$ av disse tallene tilhøre $\mathcal{M}(a,b)$.*

Bevis. Desverre går beviset i omvendt rekkeføge av påstandene i Setningen. Vi viser først påstandene (1), (2) og (3) og bruker disse påstandene til å vise den første delen av Setningen.

(1) Vi har at $ab-a-b$ ikke er i $\mathcal{M}(a,b)$ for om $ab-a-b = ma+nb$ vil vi ha at $ab = (m+1)a + (n+1)b$, så b deler $m+1$ og a deler $n+1$. Men da er $ab = (m+1)a + (n+1)b \ge 2ab$ som er umulig.

(2) For å vise at alle tall $ab-a-b+p$ med $p > 0$ er i $\mathcal{M}(a,b)$ rekker det å vise at de er i $\mathcal{M}(a,b)$ for $p = 1, 2, \ldots, a$. Dette er fordi, om et tall c er i $\mathcal{M}(a,b)$, så vil også $c + ra$ være i $\mathcal{M}(a,b)$ for alle heltall r.

En relasjon

$$ab - a - b + p = am + nb$$

er det samme som en relasjon

$$b(a - 1 - n) = (m + 1)a - p.$$

For hver $n = 0, 1, \ldots, a - 1$ finnes det klart nøyaktig et tall m_n slik at $b(a - 1 - n) = (m_n + 1)a - p_n$ der $1 \leq p_n \leq a$. Om $n \neq n'$ vil $p_n \neq p_{n'}$ fordi, om de var like får vi at $b(n' - n) = b(a-1-n) - b(a-1-n') = (m_n+1)a - p_n - (m_{n'}+1)a - p_{n'} = a(m_n - m_{n'})$. Men siden a og b ikke har noen felles divisor og vi har at $b(n'-n) = a(m_n - m_{n'})$ må da a dele $n'-n$. Men dette er umulig ettersom $|n'-n| < a$. Når n gjennomløper $0, 1, \ldots, a-1$ vil derfor p gjennomløpe $1, 2, \ldots, a$. Derfor ligger alle tallene $ab - a - b + p$ med $p = 1, 2, \ldots, a$ i $\mathcal{M}(a, b)$.

(3) Vi ser nu på relasjonen

$$ab - a - b - p = ma + nb$$

der p er et heltall $0 \leq p \leq ab - a - b$. Ettersom vi for alle disse verdiene av p har $0 \leq ma+nb \leq ba-a-b$, vil vi ha at $0 \leq n \leq a-2$, for om $n \geq a - 1$ vil $nb \geq (a - 1)b = ab - b > ab - b - a$, som er umulig. Ettersom $b(a - 1 - n) > a$ når $0 \leq n \leq a - 2$ får vi at det finnes entydige tall m_n og p_n slik at $b(a-1-n) = (m_n+1)a+p_n$ med $0 < p_n \leq a - 1$. Mer at når $0 \leq n \leq a - 2$ så kan ikke $p_n = 0$ fordi da vil $b(a - 1 - n) = (m_n + 1)a$ og dette er umulig fordi $0 < a - 1 - n < a$ og fordi a og b ikke har noen felles divisor. Vi skriver

$$b(a - 1 - n) = (m_n + 1 - 1)a + qa + p_n \qquad \text{for } q = 0, 1, \ldots, m_n$$

og får at vi på denne måten har funnet alle tall $qa + p_n$ slik at $ba - b - a - qa - p_n$ er i $\mathcal{M}(a, b)$.

For hvert tall n har vi $m_n + 1$ slike tall p_n, $a + p_n$, $2a + p_n$, $\cdots$, $m_n a + p_n$. Vi har følgelig $m_0 + 1 + m_1 + 1 + \cdots + m_{a-2} + 1$ slike tall. Men vi har at

$$\sum_{n=0}^{a-2} b(a - 1 - n) = \sum_{n=0}^{a-2} (m_n + 1)a + \sum_{n=0}^{a-2} p_n.$$

Som ovenfor innser vi at $p_0, p_1, \ldots, p_{a-2}$ er ulike tall, og derfor er tallene $1, \ldots, a - 1$ i noe rekkefølge. Vi får derfor at $b(a - 1)^2 - b(a - 1)(a - 2)/2 = \sum_{n=0}^{a-2}(m_n + 1)a + a(a - 1)/2$. Derfor vil $\sum_{n=0}^{a-2}(m_n + 1)a = (a - 1)((2b(a - 1) - b(a - 2) - a)/2) = ((a - 1)b - 1)/2a$. Det er altså $(a - 1)(b - 1)/2$ tall på formen $ab - a - b - qa - p_n$ som tilhører $\mathcal{M}(a, b)$, og som er mellom 0 og $ab - a - b$. Når $ab - a - b$ ikke er i $\mathcal{M}(a, b)$ kan heller ikke $qa + p_n$ være i $\mathcal{M}(a, b)$ ettersom $ab - a - b = (m_n + 1 - q)a + qa + p_n$, og tallene på formen $qa + p_n$ er derfor alle tallene som ikke er i $\mathcal{M}(a, b)$.

Generalisering

9 Generalisering: Dersom landet har 3 myntsorter a, b og c kan man stille de tilsvarende spørsmålene, men problemene for tre myntsorter er mye vanskeligere å svare på. Vi betegner med $g(a, b, c)$ det største tallet som *ikke* kan veksles, når dette finnes, og med $n(a, b, c)$ antallet priser som ikke kan veksles.

(1) Eksperimenter med tre myntsorter, f.eks. ved å la a og b være som i første del av oppgaven og variere c. Bestem $g(a, b, c)$ og $n(a, b, c)$ i disse tilfellene.

(2) Kan du ved å starte med tilfellet med 2 myntsorter vise for hvilke myntsorter a, b og c tallet $g(a, b, c)$ eksisterer?

(3) Kan du av eksperimentene i del (1) gjette en øvre grense for $g(a, b, c)$ når denne eksisterer? F.eks. kan du undersøke om $g(a, b, c) \leq abc$ når $g(a, b, c)$ finnes. Kan du finne bedre grenser?

(4) Her har du en tabell over noen kjente øvre grenser for $g(a, b, c)$ når vi har $a < b < c$, og d er største felles divisor for a og b:

T. Skolem (1930)	$(a-1)(b+c-1)-1$
I. Schur (1935)	$(a-1)(c-1)-1$
A. Brauer (1942)	$ab/d + dc - a - b - c$
M. Lewin (1972)	$[(c-2)^2/2] - 1$
M. Lewin (1973)	$[\frac{1}{2}(c-2)(b-2)] - 1$
J. Roberts (1956)	$a(c-a-2+[a/(c-a)]) + (b-a-1)(c-a-1)$
Y. Vitek (1975)	$(c-2)\lfloor \frac{a}{2} - 1 \rfloor$ for a, b, c inkongruente (mod a)

Sett inn i formlene for en del verdier av a, b og c og sammenlign med den virkelige verdien for $g(a, b, c)$. Grensene ovenfor og referenser til originalarbeidene kan du finne i [3] i litteraturlisten.

(5) Kan du finne noe samband mellom tallene $g(a, b, c)$ og $n(a, b, c)$?

Det er ganske komplisert å finne eksplisitte uttrykk for $g(a, b, c)$ og $n(a, b, c)$ når disse finnes. Slike uttrykk ble først funnet for noen år siden og er ganske involverte. I [2] i litteraturlisten er endel av dette arbeidet beskrevet og du kan der finne videre referenser til annen litteratur om du er interessert.

(6) Kan du finne noen eksplisitte uttrykk for $g(a, b, c)$ eller for $n(a, b, c)$. Kanskje du kan bestemme eksplisitte uttrykk for spesielle verdier av a, b og c, som f.eks. $b = a + d$ og $c = a + 2d$ for noe heltall d?

For fire og flere myntsorter er du ved *forskningsfronten.* Kan du si noe i dette tilfellet?

10 Litteratur:

[1] Gardiner, A., *Discover Mathematics.* Oxford Science Publ. 1987.

[2] Selmer, E.S., To populære problemer i tallteorien. I Myntveksling, II Frankering. *Normat* 29 (1981).
[3] Smoryński, C., Skolem's solution to a problem of Frobenius. *The mathematical intelligencer* 3 (1981), s 123–132.
[4] Vitek, Y., *Bounds for a linear diophantine problem of Froebenius, II.* Canad. J. Math. 28 (1976), s 1280–1288.