# Lösningsförlag till inlämningsuppgifter vecka 4

**Uppgift 1** Bestäm den multiplikativa ordningen av $m$ i $\mathbf{Z}_n$ genom att beräkna så få potenser som möjligt.

*Lösning:* För att $m$ skall ha någon multiplikativ ordning över huvud taget måste $m$ vara inverterbart i $\mathbf{Z}_n$. Det kan vi avgöra med Euklides algoritm. I vårt fall är $m = 690326$ och $n = 47447713$ och vi får att $\mathrm{sgd}(m, n) = 1$, exempelvis med ett Java-programeller med hjälp av *Maple*.

Eftersom Lagranges sats ger att ordningen av ett element i en grupp måste dela gruppens ordning får vi att ordningen av $m$ måste dela $\phi(n)$, som är ordningen av gruppen av inverterbara element i $\mathbf{Z}$. För att bestämma $\phi(n)$ behöver vi faktorisera $n$. Vi ser att det måste finnas någon primfaktor som är högst $7000$ om $n$ inte är ett primtal självt. Med en enkel programslinga kan vi hitta faktorerna $4799$ och $9887$. Dessa är båda primtal eftersom vi inte hittade några andra faktorer som var mindre än $100$. Vi får $\phi(n) = (4799 - 1)(9887 - 1) = 47433028$ och om vi faktoriserar detta tal får vi $2^2 \cdot 2399 \cdot 4943$. Låt $p = 2399$ och $q = 4943$. Faktorerna i $47433028$ är nu $1, 2, 4, p, q, 2p, 2q, 4p, 4q, pq, 2pq, 4pq$. Vi kan nu använda samma program som i RSA-uppgiften från förra veckan för att bestämma dessa potenser av $m$ modulo $n$. Vi får

$$\begin{aligned}
690326^{1} &\equiv 690326 \pmod{47447713} \\
690326^{2} &\equiv 32604617 \pmod{47447713} \\
690326^{4} &\equiv 21961554 \pmod{47447713} \\
690326^{p} &\equiv 19858261 \pmod{47447713} \\
690326^{2p} &\equiv 13557176 \pmod{47447713} \\
690326^{4p} &\equiv 1439701 \pmod{47447713} \\
690326^{q} &\equiv 398083310 \pmod{47447713} \\
690326^{2q} &\equiv 18953380 \pmod{47447713} \\
690326^{4q} &\equiv 40141221 \pmod{47447713} \\
690326^{pq} &\equiv 47447712 \pmod{47447713} \\
690326^{2pq} &\equiv 1 \pmod{47447713}
\end{aligned}$$

och därmed är ordningen av $m$ lika med $2pq = 23716514$.

**Uppgift 2** Polynomet $p(x)$ i $\mathbf{Z}_5[x]$ ger rest $r(x)$ vid division med $x^3 + x^2 + 1$ och rest $q(x)$ vid division med $x^3 + 2x + 2$. Ange $p(x)$ om graden är högst $5$.

*Lösning:* I vårt fall är $q(x) = 2x^2 + 3x + 4$ och $r(x) = x^2 + 4x + 4$. Låt $f(x) = x^3 + x^2 + 1$ och $g(x) = x^3 + 2x + 2$. Vi söker nu $p(x)$ så att $p(x) = k(x)f(x) + q(x)$ samtidigt som $p(x) = l(x)g(x) + r(x)$. Genom att dra det ena uttrycket från det andra får vi att

$$k(x)f(x) - l(x)g(x) = r(x) - q(x)$$

Nu vill vi först och främst skriva den största gemensamma delaren mellan $f(x)$ och $g(x)$ som $a(x)f(x) + b(x)g(x)$. Detta gör vi genom Euklides algoritm för polynom.

$$\begin{aligned} x^3 + x^2 + 1 &= 1 \cdot (x^3 + 2x + 2) + (x^2 + 3x + 4) \\ x^3 + 2x + 2 &= (x - 3)(x^2 + 3x + 4) + 2x + 4 \\ x^2 + 3x + 4 &= (3x + 3)(2x + 4) + 2 \end{aligned}$$

och baklänges ger detta att

$$\begin{aligned} 2 &= (x^2 + 3x + 4) - (3x + 3)(2x + 4) = \\ &= (x^2 + 3x + 4) - (3x + 3)((x^3 + 2x + 2) - (x - 3)(x^2 + 3x + 4)) \\ &= (3x^2 + 4x + 2)(x^2 + 3x + 4) - (3x + 3)(x^3 + 2x + 2) = \\ &= (3x^2 + 4x + 2)((x^3 + x^2 + 1) - (x^3 + 2x + 2)) - (3x + 3)(x^3 + 2x + 2) \\ &= (3x^2 + 4x + 2)(x^3 + x^2 + 1) - (3x^2 + 2x)(x^3 + 2x + 2) \end{aligned}$$

För att få en lösning till ekvationen $k(x)f(x) - l(x)g(x) = r(x) - q(x)$ multiplicerar vi $2 = (3x^2+4x+2)(x^3+x^2+1)-(3x^2+2x)(x^3+2x+2)$ med $(r(x)-q(x))/2 = 3(x^2+4x+4)-3(2x^2+3x+4) = 2x^2+3x$. Vi får då att $k(x) = (3x^2+4x+2)(2x^2+3x) = x^4+2x^3+x^2+x$ och därmed är $p(x) = (x^4+2x^3+x^2+x)(x^3+x^2+1)+(2x^2+3x+4) = x^7+3x^6+3x^5+3x^4+3x^3+3x^2+x+2$. Eftersom detta polynom inte har grad högst fem måste vi ta resten vid division med den mintsta gemensamma multipel av $f(x)$ och $g(x)$, dvs $f(x)g(x)$. Vi får $f(x)g(x) = x^6+2x^4+x^5+2x^3+2x+2$ och polynomdivision av $x^7+3x^6+3x^5+3x^4+3x^3+3x^2+x+2$ med $x^6+2x^4+x^5+2x^3+2x+2$ ger resten $p(x) = 4x^5+4x^4+x^3+2x^2+3x$.

Vi kan också kontrollera att resten vid division med $f(x)$ och $g(x)$ ger resterna $q(x)$ respektive $r(x)$.

**Uppgift 3** Avgör om gruppen $G$ som har elementen $\{0, 1, 2, 3, 4, 5, 6, 7\}$ och grupptabell enligt nedan är isomorf med symmetrigruppen för en kvadrat.

*Lösning:* I vårt fall är den givna grupptabellen

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 2 | 4 | 0 | 6 | 1 | 7 | 3 | 5 |
| 1 | 4 | 2 | 1 | 5 | 0 | 3 | 7 | 6 |
| 2 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 3 | 6 | 7 | 3 | 2 | 5 | 4 | 0 | 1 |
| 4 | 1 | 0 | 4 | 7 | 2 | 6 | 5 | 3 |
| 5 | 7 | 6 | 5 | 1 | 3 | 0 | 4 | 2 |
| 6 | 3 | 5 | 6 | 0 | 7 | 1 | 2 | 4 |
| 7 | 5 | 3 | 7 | 4 | 6 | 2 | 1 | 0 |

Symmetrigruppen för en kvadrat består av åtta element. Identitetselementet, $e$, tre rotationer $r_1$, $r_2$, $r_3$ som roterar ett kvarts varv medsols, ett halvt varv medsols och tre kvarts varv medsols, samt fyra speglingar, $s_1$, $s_2$, $s_3$ och $s_4$.

Om vår grupp skall vara isomorf med symmetrigruppen för en kvadrat måste vi kunna identifiera element med motsvarande egenskaper i vår grupp. Identitetselementet är lätt att finna, eftersom det uppfyller $e * a = a * e$ för alla $a$ i gruppen. Om vi tittar i grupptabellen ser vi att $2 * a = a * 2$ för alla element $a$, och $2$ måste vara identitetselementet. I symmetrigruppen för en kvadrat gäller att $a^2 = e$ för alla element utom kvartsvarvsrotationerna. Genom att se var det inte står $2$ på diagonalen ser vi att $5$ och $7$ måste motsvara kvartsvarvsrotationerna. Kvadraten på dessa skall bli rotation ett halvt varv och vi ser då att detta måste motsvara $0$. Resterande fyra element, $1, 3, 4$ och $6$ måste svara mot speglingarna. Vi kan välja speglingarna i symmetrigruppen i en sådan ordning att $s_2 = r_1 s_1$, $s_3 = r_1 s_2$ och $s_4 = r_1 s_3$. Om vi antar att $r_1$ svarar mot $5$ och $s_1$ mot $1$ får vi då att $s_2$ måste svara mot $5 * 1 = 6$, $s_3$ mot $5 * 6 = 4$ och $s_4$ mot $5 * 4 = 3$. Vi har nu en kandidat till isomorfi som ges av

| $a$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ |
|---|---|---|---|---|---|---|---|---|
| $f(a)$ | $r_2$ | $s_1$ | $e$ | $s_4$ | $s_3$ | $r_1$ | $s_2$ | $r_3$ |

Om vi ställer upp den tabell vi får från vår tabell med hjälp av denna bijektion och ändrar ordningen mellan raderna och kolonnerna får vi

| | $2$ | $5$ | $0$ | $7$ | $1$ | $6$ | $4$ | $3$ |
|---|---|---|---|---|---|---|---|---|
| $2$ | $2$ | $5$ | $0$ | $7$ | $1$ | $6$ | $4$ | $3$ |
| $5$ | $5$ | $0$ | $7$ | $2$ | $6$ | $4$ | $3$ | $1$ |
| $0$ | $0$ | $7$ | $2$ | $5$ | $4$ | $3$ | $1$ | $6$ |
| $7$ | $7$ | $2$ | $5$ | $0$ | $3$ | $1$ | $6$ | $4$ |
| $1$ | $1$ | $3$ | $4$ | $6$ | $2$ | $7$ | $0$ | $5$ |
| $6$ | $6$ | $1$ | $3$ | $4$ | $5$ | $2$ | $7$ | $0$ |
| $4$ | $4$ | $6$ | $1$ | $3$ | $0$ | $5$ | $2$ | $7$ |
| $3$ | $3$ | $4$ | $6$ | $1$ | $7$ | $0$ | $5$ | $2$ |

| | $e$ | $r_1$ | $r_2$ | $r_3$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $r_1$ | $r_2$ | $r_3$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ |
| $r_1$ | $r_1$ | $r_2$ | $r_3$ | $e$ | $s_2$ | $s_3$ | $s_4$ | $s_1$ |
| $r_2$ | $r_2$ | $r_3$ | $e$ | $r_1$ | $s_3$ | $s_4$ | $s_1$ | $s_2$ |
| $r_3$ | $r_3$ | $e$ | $r_1$ | $r_2$ | $s_4$ | $s_1$ | $s_2$ | $s_3$ |
| $s_1$ | $s_1$ | $s_4$ | $s_3$ | $s_2$ | $e$ | $r_3$ | $r_2$ | $r_1$ |
| $s_2$ | $s_2$ | $s_1$ | $s_4$ | $s_3$ | $r_1$ | $e$ | $r_3$ | $r_2$ |
| $s_3$ | $s_3$ | $s_2$ | $s_1$ | $s_4$ | $r_2$ | $r_1$ | $e$ | $r_3$ |
| $s_4$ | $s_4$ | $s_3$ | $s_2$ | $s_1$ | $r_3$ | $r_2$ | $r_1$ | $e$ |

Den senare känner vi igen som grupptabellen för symmetrigruppen av en kvadrat, exempelvis från lösningarna av förra årets inlämningsuppgifter.