KUNGL
TEKNISKA
HÖGSKOLAN

Algebra och kryptografi — Facit till udda uppgifter

Tomas Ekholm
Niklas Eriksen
Magnus Rosenlund

Matematiska institutionen, 2002

Grupper.

Lösning 1.1. Vi väljer att studera varje element i $G \cup H$ för sig självt. De möjliga fallen är: $a \in G \setminus H$, $a \in H \setminus G$, och $a \in G \cap H$.

(a) Antag att $a \in G \setminus H$. Vi får ett bidrag till termen $|G|$ med 1, däremot inget bidrag till $|H|$. I högerledet får vi endast bidrag med 1 till termen $G \cup H$. Detta visar att för varje element i $G \setminus H$ ökar höger- och vänsterled med 1.
(b) Fallet $a \in H \setminus G$ följer analogt med ovanstående fall.
(c) Antag att $a \in G \cap H$. Eftersom $a \in G$ och $a \in H$ får vi ett bidrag till vänsterledet med 2. Detsamma gäller för högerledet.

Vi har visat likheten.

Lösning 1.3. Genom att multiplicera med inverser på ömse sidor om likhetstecknet får vi

$$\begin{aligned} 2 * (x * 3) &= 7 \\ x * 3 &= 2^{-1} * 7 \\ x &= (2^{-1} * 7) * 3^{-1}. \end{aligned}$$

Ur definitionen $a * b = a + b + ab$ ser vi att $0 = e = a * a^{-1} = a + a^{-1} + aa^{-1}$ ger $a^{-1} = \frac{-a}{a+1}$. Därmed får vi

$$\begin{aligned} x = (2^{-1} * 7) * 3^{-1} &= \left(-\frac{2}{3} * 7\right) * \left(-\frac{3}{4}\right) \\ &= \left(-\frac{2}{3} + 7 + \left(-\frac{2}{3}\right)7\right) * \left(-\frac{3}{4}\right) \\ &= \frac{5}{3} * \left(-\frac{3}{4}\right) = \frac{5}{3} - \frac{3}{4} - \frac{5}{3}\frac{3}{4} = -\frac{1}{3}. \end{aligned}$$

Lösning 1.5. Vi vill visa att $(H \cap K, *)$ är en grupp.

(a) Vi visar att $H \cap K$ är sluten under operationen $*$. Låt $a, b \in H \cap K$. Eftersom $a, b \in H$ finns $a * b \in H$ och eftersom $a, b \in K$ finns $a * b \in K$. Detta visar att $a * b \in H \cap K$ och att $H \cap K$ är sluten under operationen $*$.
(b) Identiteten $e \in G$ finns både i H och K, därmed även i $H \cap K$.
(c) Låt $a \in H \cap K$. Detta ger att $a^{-1} \in H$ och $a^{-1} \in K$, d.v.s. $a^{-1} \in H \cap K$.

Enligt sats 1.12 har vi att $H \cap K$ är en delgrupp av G.

Kvotgrupper.

Lösning 2.1. Vi använder direkt definitionen, d.v.s. vi visar att $\sim$ är reflexiv, symmetrisk och transitiv.

(a) (Reflexivitet) Vi ser att $a \sim a$ ty $a^{-1} * a = e \in H$.
(b) (Symmetri) Antag att $a \sim b$. Vi vill visa att $b \sim a$, d.v.s. $b^{-1} * a \in H$. Vi vet från antagandet att $a^{-1} * b \in H$. Inversen till $a^{-1} * b$ är $b^{-1} * a$ och $b^{-1} * a \in H$ eftersom H är en grupp.
(c) (Transitivitet) Antag att $a \sim b$ och $b \sim c$. Vi vill visa att $a \sim c$, d.v.s. $a^{-1} * c \in H$. Vi vet från antagandet att $a^{-1} * b \in H$ och att $b^{-1} * c \in H$. Eftersom H är en grupp är $a^{-1} * c = (a^{-1} * b) * (b^{-1} * c) \in H$.

Detta visar att $\sim$ är en ekvivalensrelation.

Lösning 2.3. (a) Vi visar att $\mathbb{Z}_a$ är en sluten mängd under operationen $+_a$. Låt $x, y \in \mathbb{Z}_a$. Om $x + y < a$ följer att $x + y \in \mathbb{Z}_a$. Om $x + y \geqslant a$ följer att $x +_a y = x + y - a$ vilket ger att $0 \leqslant x + y - a \leqslant a - 2$. Den senare olikheten följer av att $x+y-a \leqslant (a-1)+(a-1)-a = a-2$. I alla fall har vi $x+_a y \in \mathbb{Z}_a$.
(b) Antag att $x, y, z \in \mathbb{Z}_a$. Om $x+y+z \in \mathbb{Z}_a$ följer att $(x+_a y)+_a z = x+_a (y+_a z)$. Fallen om $x + y + z - a$ eller $x + y + z - 2a$ ligger i $\mathbb{Z}_a$ följer analogt.
(c) Identiteten är 0.
(d) Inversen till $x \in \mathbb{Z}_a$ är $a - x$.

Vi är klara; $(\mathbb{Z}_a, +_a)$ är en grupp.

Lösning 2.5. Det står klart att varje x svarar mot några värden på c och d. Antalet sätt att välja c och d är ab och det finns ab tal x i intervallet $0 \leqslant x \leqslant ab - 1$. Detta visar att det finns lika många x som det finns par av c och d. Om vi visar att det finns maximalt ett x för varje par av värden på c och d så följer det att det finns exakt ett x för varje par av värden på c och d.

Antag nu att det finns två tal x_1 och x_2 så att $0 \leqslant x_1 \leqslant ab - 1$, $0 \leqslant x_2 \leqslant ab - 1$, $x_1 \equiv x_2 \equiv c \pmod{a}$ och $x_1 \equiv x_2 \equiv d \pmod{b}$. Av detta följer att a delar $x_1 - x_2$ och b delar $x_1 - x_2$. Detta innebär att $x_1 - x_2$ innehåller alla primtalsfaktorer i a och alla i b och eftersom de var relativt prima så har de inga gemensamma sådana faktorer. Alltså måste $x_1 - x_2$ innehålla alla primtalsfaktorer i ab, så ab delar $x_1 - x_2$. Alltså måste skillnaden mellan x_1 och x_2 antingen vara noll eller större än $ab - 1$. Eftersom vi antagit att både x_1 och x_2 ligger mellan noll och $ab - 1$ följer att $x_1 = x_2$.

Därmed ser vi att det finns maximalt ett tal x som uppfyller alla kriterier. Av vårt inledande resonemang följer att det finns exakt ett tal x som uppfyller kriterierna.

Homomorfier och isomorfier av grupper.

Lösning 3.1. Vi ska visa att ϕ är bijektiv, d.v.s. att ϕ är surjektiv och injektiv. För att visa surjektivitet ska vi visa att det för varje $y \in \mathbb{Q}$ finns ett $x \in \mathbb{Q}$ så att $\phi(x) = y$. För varje $y \in \mathbb{Q}$ har vi att $x = 17y \in \mathbb{Q}$ och $\phi(x) = \phi(17y) = \frac{17y}{17} = y$. Detta visar att ϕ är surjektiv. För att visa injektivitet ska vi visa att två olika element i $\mathbb{Q}$ alltid avbildas på olika element i $\mathbb{Q}$. Låt $x_1, x_2 \in \mathbb{Q}, x_1 \neq x_2$. Då har vi $\phi(x_1) = \frac{x_1}{17} \neq \frac{x_2}{17} = \phi(x_2)$, alltså är ϕ injektiv. Detta visar att ϕ är bijektiv.

Lösning 3.3. Lagranges sats säger att antalet element i en delgrupp H av en grupp G måste dela antalet element i G. Eftersom det finns 7 element i G och 7 är ett primtal är de enda möjligheterna att en delgrupp har 1 eller 7 element. Alla delgrupper måste innehålla e_G, alltså är delgrupperna e_G och G.

Lösning 3.5. Låt $n, m \in \mathbb{Z}$. Då har vi $\phi(n+m) = n+m = \phi(n)+\phi(m)$. Detta visar att ϕ är en homomorfi.

Lösning 3.7. Låt $g_1, g_2 \in G$. Då har vi $\phi(g_1 g_2) = (g_1 g_2)^{-1} = (g_2)^{-1}(g_1)^{-1} = \phi(g_2)\phi(g_1)$. Men $\phi(g_2)\phi(g_1) \neq \phi(g_1)\phi(g_2)$ (i allmänhet) eftersom G inte är abelsk. Detta visar att ϕ inte är en homomorfi.

Symmetriska gruppen.

Lösning 4.1. Vi börjar med att skriva π på cykelform. Vi tar ett godtyckligt element, 1, och ser att det avbildas på 4. Detta avbildas i sin tur på 3, som avbildas på 7 som avbildas på 1. Första cykeln är alltså (1 4 3 7). Vi kan sedan se att 2 avbildas på sig själv, så det bildar en egen cykel. Detsamma gäller 5. Slutligen ser vi att 6 avbildas på 8 och vice versa. Därmed har vi $\pi = (1\ 4\ 3\ 7)(2)(5)(6\ 8) = (1\ 4\ 3\ 7)(6\ 8)$.

Att skriva σ på enradsnotation är inte så svårt. Vi ser att 1 avbildas på 4 (från andra cykeln), att 2 avbildas på 1 (också från andra cykeln), att 3 avbildas på 5 (första cykeln), och så vidare. Observera att de ej utskrivna elementen 6 och 8 avbildas på sig själva. Vi får slutligen $\sigma = 4\ 1\ 5\ 2\ 7\ 6\ 3\ 8$.

Det är en smaksak om man vill beräkna produkterna i cykelnotation eller enradsnotation. Ska vi beräkna $\sigma\pi$ ser vi att $\sigma(\pi(1)) = \sigma(4) = 2$, att $\sigma(\pi(2)) = \sigma(2) = 1$ och så vidare. Vi får till slut $\sigma\pi = 2\ 1\ 3\ 5\ 7\ 8\ 4\ 6 = (1\ 2)(4\ 5\ 7)(6\ 8)$. På samma sätt ser vi att $\pi\sigma = 3\ 4\ 5\ 2\ 1\ 8\ 7\ 6 = (1\ 3\ 5)(2\ 4)(6\ 8)$.

Potenser av samma permutation räknar man enklast i cykelnotation. Man märker snart att på samma sätt som $\sigma = \sigma^1$ hoppar 1 steg fram i varje cykel, så hoppar σ^k k steg fram i varje cykel. För $\sigma = (3\ 5\ 7)(4\ 2\ 1)$ innebär två steg fram från 1 att vi landar på 2, två steg fram från 2 att vi landar på 4, två steg fram från 3 att vi landar på 7, o.s.v.. Vi får $\sigma^2 = (3\ 7\ 5)(4\ 1\ 2)$. Hoppar vi istället tre steg fram i cykler av längd tre, så kommer vi tillbaka till det element vi hoppade från. Det innebär i detta fall att 1 avbildas på 1, att 2 avbildas på 2 och så vidare. Vi har alltså att $\sigma^3 = e$.

Lösning 4.3. Om vi låter $\pi(i)$ vara den plats som i skrivs på, så svarar ställningen mot permutationen

$$(1\ 9\ 14\ 4\ 13\ 8\ 12\ 11)(2)(3\ 7\ 5)(6\ \square\ 10\ 15).$$

Avståndsfunktionen $d(\pi) = 16 - 4 = 12$, så detta är en jämn permutation. Men den tomma rutan har flyttats tre steg från sin startplats, så för att komma dit har den sammanlagt flyttats ett udda antal steg. Ställningen går alltså inte att uppnå.

Lösning 4.5. Vi betraktar permutationen $(a_1\ a_2\ \dots\ a_k)$. Vi vill skriva den som en produkt av $k-1$ transpositioner. I exemplet har detta gjorts genom att elementet a_i skrivs i transposition $i-1$ och transposition i från vänster räknat, utom a_1 och a_2 som skrivs enbart i första respektive sista transpositionen. Vi gör detta även här och får

$$(a_1\ a_2)(a_2\ a_3)(a_3\ a_4)\dots(a_{k-1}\ a_k).$$

Vi måste visa att denna nya permutation, som helt klart är en produkt av $k-1$ transpositioner, är samma som den tidigare permutationen. Vi räknar nu transpositionerna från höger, eftersom det är i den ordningen som de verkar. Vi ser att a_1 avbildas på a_2, eftersom a_1 inte påverkas förrän i sista transpositionen. Vi ser även att a_2 avbildas på a_3 eftersom a_2 inte påverkas förrän i näst sista transpositionen och sedan påverkas inte a_3 något. På samma sätt ser vi att alla element $a_1, a_2, \dots, a_{k-1}$ bara avbildas en gång, och då till efterföljande. Slutligen har vi a_k som kommer att avbildas i samtliga transpositioner på närmast föregående element. Efter $k-1$ transpositioner har det landat på a_1, vilket var vad vi ville. Alltså är permutationerna lika och vi har skrivit $(a_1\ a_2\ \dots\ a_k)$ som en produkt av $k-1$ transpositioner.

Lösning 4.7. Den tomma rutan kan alltid flyttas fritt på spelplanen i de riktningar som inte begränsas av kanter, så om planen är sammanhängande kan den flyttas helt fritt. Den påverkar då de brickor som ligger längs den stig den vandrar.

Vill vi flytta en bricka ska vi placera den tomma rutan på den sida om brickan som vi vill flytta brickan åt, och sedan byta plats på brickan och den tomma rutan. Vill vi sedan fortsätta att flytta brickan i samma riktning måste vi först flytta den tomma rutan runt brickan. Detta är möjligt oavsett var på spelplanen brickan befinner sig.

Förflyttning av en bricka påverkar alltså inte bara brickorna längs den stig vi flyttar brickor, utan också de brickor som ligger precis bredvid stigen, åtminstone på ena sidan. Förutom dessa påverkas inga brickor.

Ringar och kroppar.

Lösning 5.1. $3 \cdot 4 = 12 \equiv 5 \pmod 7$. Detta visar att $3 \cdot 4 = 5$ i $(\mathbb{Z}_7, +, \cdot)$.

Lösning 5.3. Vi kan t.ex. ta $(\mathbb{Z}_6, +, \cdot)$. Då har vi att $2, 3 \in \mathbb{Z}_6$ och $2 \cdot 3 = 6 \equiv 0 \pmod 6$, d.v.s. $2 \cdot 3 = 0$ i $(\mathbb{Z}_6, +, \cdot)$.

Lösning 5.5. Låt $a \in R$ vara en enhet och antag att inversen a^{-1} till a ej är unik. Det innebär att det finns ett annat element $b \in R$ så att $b \cdot a = 1 = a \cdot b$. Men då får vi $b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = 1 \cdot a^{-1} = a^{-1}$. Alltså är a^{-1} unik.

Fermats lilla sats.

Lösning 6.1. Vi har att

$$\begin{aligned} 9^{28} &\equiv (9^2)^{14} \equiv 81^{14} \equiv (-3)^{14} \equiv 3^{14} \equiv (3^3)^4 \cdot 9 \\ &\equiv 27^4 \cdot 9 \equiv (-1)^4 \cdot 9 \equiv 9 \pmod{28}. \end{aligned}$$

Eftersom vi fick $9^{28} \equiv 9 \pmod{28}$ vet vi inte om 28 är ett primtal. Vi fortsätter med nästa beräkning.

$$\begin{aligned} 10^{28} &\equiv (10^2)^{14} \equiv 100^{14} \equiv (16)^{14} \equiv (16^2)^7 \equiv (256)^7 \equiv 4^7 \\ &\equiv (4^3)^2 \cdot 4 \equiv 64^2 \cdot 4 \equiv 8^2 \cdot 4 \equiv 256 \equiv 4 \pmod{28}. \end{aligned}$$

Eftersom vi här fick $10^{28} \not\equiv 10 \pmod{28}$ inser vi att 28 inte kan vara ett primtal. I så fall hade Fermats sats varit falsk.

Beräkningarna ovan kan också genomföras med den metod med upprepad kvadrering som gås igenom i kapitlet om RSA.

Lösning 6.3. Vi har att

$$\begin{aligned} (a+b)^4 &= \binom{4}{0}a^4b^0 + \binom{4}{1}a^3b^1 + \binom{4}{2}a^2b^2 + \binom{4}{3}a^1b^3 + \binom{4}{4}a^0b^4 \\ &= \frac{4!}{4!0!}a^4 + \frac{4!}{3!1!}a^3b + \frac{4!}{2!2!}a^2b^2 + \frac{4!}{1!3!}ab^3 + \frac{4!}{0!4!}b^4 \\ &= \frac{24}{24}a^4 + \frac{24}{6}a^3b + \frac{24}{2\cdot 2}a^2b^2 + \frac{24}{6}ab^3 + \frac{24}{24}b^4 \\ &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4. \end{aligned}$$

På samma sätt får vi att

$$\begin{aligned} (2a+3b)^3 &= \binom{3}{0}(2a)^3(3b)^0 + \binom{3}{1}(2a)^2(3b)^1 + \binom{3}{2}(2a)^1(3b)^2 + \binom{3}{3}(2a)^0(3b)^3 \\ &= \frac{3!}{3!0!}(2a)^3 + \frac{3!}{2!1!}(2a)^2(3b) + \frac{3!}{1!2!}(2a)(3b)^2 + \frac{3!}{0!3!}(3b)^3 \\ &= \frac{6}{6}8a^3 + \frac{6}{2}4a^23b + \frac{6}{2}2a9b^2 + \frac{6}{6}27b^3 \\ &= 8a^3 + 36a^2b + 54ab^2 + 27b^3. \end{aligned}$$

Lösning 6.5. Vi väljer $a = b = 1$ och får

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = (1+1)^n = 2^n.$$

Lösning 6.7. Elementen i $U(\mathbb{Z}_m)$ bildar en multiplikativ grupp, så vi ser som i det andra beviset av Fermats lilla sats att om vi låter u vara produkten av alla element i $U(\mathbb{Z}_m)$ får vi

$$u \equiv a^{|U(\mathbb{Z}_m)|} u \pmod{m}.$$

Om vi multiplicerar med a och inversen till u, så får vi

$$a^{|U(\mathbb{Z}_m)|+1} \equiv a \pmod{m}.$$

RSA-kryptering.

Lösning 7.1. Meddelandet 6 krypteras genom att beräkna $6^7 \pmod{35}$. Vi får

$$6^7 \equiv (6^2)^3 \cdot 6 \equiv 36^3 \cdot 6 \equiv 1^3 \cdot 6 \equiv 6 \pmod{35}.$$

För att kryptera 17 beräknar vi

$$17^7 \equiv (17^2)^3 \cdot 17 \equiv 289^3 \cdot 17 \equiv 9^3 \cdot 17 \equiv 81 \cdot 153 \equiv 11 \cdot 13 \equiv 143 \equiv 3 \pmod{35}.$$

Vi ser då direkt att om vi dekrypterar 3 så ska vi få 17.

Lösning 7.3. Om $n = 187$ kan vi snabbt beräkna att $p = 11$ och $q = 17$ (eller tvärtom). Vi får därmed $m = 160$. Euklides algoritm ger nu d:

$$160 = 6 \cdot 23 + 22$$
$$23 = 1 \cdot 22 + 1$$

Vi får

$$1 = 23 - 22 = 23 - (160 - 6 \cdot 23) = 7 \cdot 23 - 160.$$

Vi kan välja $d = 7$.

Nu återstår bara att beräkna $2^7 \pmod{187}$. Vi får $2^7 \equiv 128 \pmod{187}$. Det skickade meddelandet är alltså 128.

Lösning 7.5. Vi antar att $\text{sgd}(b, q) = d > 1$. Då fås att $a = pb + q = pb'd + q'd = (pb' + q')d$, så d delar a. Men eftersom vi redan visste att d delar b så följer att $\text{sgd}(a, b) \geqslant d$. Vi har fått en motsägelse. Det enda antagandet som kan vara fel är att $\text{sgd}(b, q) = d > 1$, så vi måste ha $\text{sgd}(b, q) = 1$.

Lösning 7.7. Om man känner till p kan $q = n/p$ lätt beräknas, och vice versa. Med hjälp av dessa beräknar man lätt $m = (p-1)(q-1)$ och sedan d med Euklides algoritm.

Om man känner m kan man utnyttja att $n - m = pq - (p-1)(q-1) = p + q - 1$ samt att $(x-p)(x-q) = x^2 - (p+q)x + pq$. Vi får alltså att $(x-p)(x-q) = x^2 - (n-m+1)x + n$ och genom att finna lösningarna till $x^2 - (n-m+1)x + n = 0$ finner vi p och q. Sedan beräknas d enkelt.

Om man känner d kan man utnyttja att $ed - 1$ är en multipel av m. Detta innebär att $p - 1$ och $q - 1$ är delare till $ed - 1$. Vi kan samla alla delare till $ed - 1$, addera ett till var och en av dem och testa att dela n med dem. I allmänhet har inte $ed - 1$ så många delare att det tar särskilt lång tid att göra.