LÖSNINGSFÖRSLAG TILL

Tentamen i kursen LGMA50: Algebra och Talteori VT2019
Den 21 Mars 2019 kl 14:00-18:00 Jonathan Nilsson

---

1. Hitta alla heltal x, y som uppfyller $12x + 7y = 250$ och $x \geq 0$ och $y \geq 0$. [6p]

Vi använder Euklides algoritm för att hitta $gcd(12, 7)$:
$12 = 7 + 5$, $7 = 5 + 2$, $5 = 2 \cdot 2 + 1$. Alltså är gcd 1 och jobbar vi igenom stegen baklänges får vi

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7 = 3 \cdot (12 - 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7.$$

Efter multiplikation med 250 har vi därför $750 \cdot 12 - 1250 \cdot 7 = 250$. Så en lösning till $12x + 7y = 250$ är $(x, y) = (750, -1250)$. Enligt sats ges alla lösningar till ekvationen av

$$(x, y) = (750 + 7k, -1250 - 12k) \text{ för } k \in \mathbb{Z}.$$

Vi har nu

$$x \geq 0 \Leftrightarrow 750 + 7k \geq 0 \Leftrightarrow 7k \geq -750 \Leftrightarrow k \geq -107$$

och

$$y \geq 0 \Leftrightarrow -1250 - 12k \geq 0 \Leftrightarrow -1250 \geq 12k \Leftrightarrow k \leq -105.$$

Vi har alltså tre möjliga värden på k: $-105, -106, -107$. Sätter vi in dessa värden i vår allmänna lösning får vi tre lösningar på uppgiften.

Svar:

$$(x, y) = (15, 10)$$

$$(x, y) = (8, 22)$$

$$(x, y) = (1, 34)$$

[6p] 2. Hitta alla lösningar till följande ekvationssystem

$$\begin{cases} x \equiv 3 \mod 4 \\ x \equiv 2 \mod 5 \\ x \equiv 4 \mod 9. \end{cases}$$

Om vi kallar modulus för $n_1 = 4$, $n_2 = 5$, $n_3 = 9$ så har vi $M = n_1 n_2 n_3 = 180$. Vi inför också $N_i = M/n_i$ så att $N_1 = 45$, $N_2 = 36$, $N_3 = 20$.

Om $b_i N_i \equiv 1 \mod n_i$ (b_i är alltså invers till N_i i $\mathbb{Z}_{n_i}$) så blir då

$$x = 3 \cdot b_1 \cdot N_1 + 2 \cdot b_2 \cdot N_2 + 4 \cdot b_3 \cdot N_3$$

en lösning till systemet.

Vi behöver därför hitta inverserna b_i. Eftersom talen är små är det lätt att hitta inverser:

$b_1 \cdot 45 \equiv 1 \mod 4 \Leftrightarrow b_1 \cdot 1 \equiv 1 \mod 4$. Vi väljer $b_1 = 1$.

$b_2 \cdot 36 \equiv 1 \mod 5 \Leftrightarrow b_2 \cdot 1 \equiv 1 \mod 5$. Vi väljer $b_2 = 1$.

$b_3 \cdot 20 \equiv 1 \mod 9 \Leftrightarrow b_3 \cdot 2 \equiv 1 \mod 9$. Vi väljer $b_3 = 5$.

Formeln ovan ger då lösningen $x = 3 \cdot 1 \cdot 45 + 2 \cdot 1 \cdot 36 + 4 \cdot 5 \cdot 20 = 607$.

Eftersom 4, 5, och 9 är parvis relativt prima säger Kinesiska restklassatsen att systemet har en unik lösning modulo $M = 180$. Slutligen är $607 \equiv 67 \mod 180$.

Svar: Systemets lösningar är $x \equiv 67 \mod 180$.
Eller med andra ord, lösningarna ges av alla heltal $x = 67 + 180k$ för $k \in \mathbb{Z}$.

3. Hitta heltal a och b så att $a^2 + b^2 = 1117$ genom att använda Fermats nedstigningsprocedur, där du utgår från likheten $224^2 + 95^2 = 53 \cdot 1117$. [6p]

Vi följer standardalgoritmen. Vi hittar tal med minimala absolutbelopp som är kongruenta med 224 respektive 95 modulo 53. Vi får $u = 12$ och $v = -11$. Då blir $u^2 + v^2 = 265 = 5 \cdot 53$. Vi har nu

$$(12^2 + (-11)^2)(224^2 + 95^2) = 5 \cdot 53^2 \cdot 1117.$$

Och efter vi skrivit om vänsterledet med formeln $(A^2+B^2)(u^2+v^2) = (uA+vB)^2+(uB-vA)^2$ får vi $1643^2 + 3604^2 = 5 \cdot 53^2 \cdot 1117$. Delar vi med 53^2 får vi till slut

$$31^2 + 68^2 = 5 \cdot 1117.$$

Vi upprepar nu hela algoritmen en gång till. Vi reducerar 31 och 68 modulo 5 och får $u = 1$ och $v = -2$ vilket ger $u^2 + v^2 = 5$ och som tidigare: $105^2 + 130^2 = (1^2 + (-2)^2)(31^2 + 68^2) = 5^2 \cdot 1117$. Där den vänstra likheten använde formeln ovan. Division med 5^2 ger slutligen $21^2 + 26^2 = 1117$.

Svar: Vi har $1117 = 21^2 + 26^2$.

[10p]4. Besvara följande korta frågor, endast svaret krävs.

(a) Beräkna $(3x+7)\cdot(5x+9)$ i ringen $\mathbb{Z}_{11}[x]$

(b) Är $(\mathrm{Mat}_{2\times 2}(\mathbb{R}),+)$ en grupp?

(c) Har ekvationen $x^2 \equiv 56 \mod 83$ någon lösning?

(d) Beräkna $\phi(5^4\cdot 3^3)$

(e) Beräkna $\sigma(7^2\cdot 3^3)$

(f) Beräkna 5^{321} modulo 7, svara med ett tal mellan 0 och 7.

(g) Hitta alla lösningar till ekvationen $2x \equiv 6 \mod 8$.

(h) Är $(\mathbb{Z}_3[x],+,\cdot)$ är en kropp?

(i) Är $3+10i$ ett Gaussiskt primtal?

(j) Skriv $\begin{pmatrix}1&2&3&4&5&6\\5&2&6&1&4&3\end{pmatrix} \in S_6$ som en produkt av transpositioner.

(a) $(3x+7)\cdot(5x+9) = 4x^2+7x+8$

(b) Ja.

(c) Nej, ty $(\frac{56}{83}) = (\frac{4}{83})(\frac{2}{83})(\frac{7}{83}) = 1\cdot(-1)\cdot(-1)(\frac{83}{7}) = (\frac{-1}{7}) = -1$.

(d) $\phi(5^4\cdot 3^3) = \phi(5^4)\phi(3^3) = (5^4-5^3)(3^3-3^2) = 500\cdot 18 = 9000$.

(e) $\sigma(7^2\cdot 3^3) = (1+7+7^2)(1+3+3^2+3^3) = 57\cdot 40 = 2280$.

(f) Med Fermats lilla: $5^{321} = 5^{53\cdot 6+3} = (5^6)^{53}5^3 \equiv 5^3 \equiv 6 \mod 7$.

(g) $x=3$ och $x=7$ (snabbast är att testa alla $x=0,1,\ldots,7$)

(h) Nej. (exempelvis saknar polynomet x invers i ringen)

(i) Ja. (ty $10^2+3^2 = 109$ är ett primtal)

(j) $\begin{pmatrix}1&2&3&4&5&6\\5&2&6&1&4&3\end{pmatrix} = (1,5,4)(3,6) = (1,4)\circ(1,5)\circ(3,6)$.

5. Hitta ett heltal x mellan 0 och 250 som uppfyller $x^{79} \equiv 47 \mod 250$. [6p]

Vi följer standardalgoritmen, vi börjar med att hitta positiva heltal k och z som uppfyller $79k - z\phi(250) = 1$. Vi har $\phi(250) = \phi(5^3)\phi(2) = (125-25)\cdot 1 = 100$. Med Euklides algoritm har vi

$$100 = 79 + 21, \quad 79 = 3 \cdot 21 + 16, \quad 21 = 16 + 5, \quad 16 = 3 \cdot 5 + 1.$$

Arbetar vi oss genom stegen baklänges får vi

$$1 = 16 - 3 \cdot 5 = 16 - 3(21 - 16) = \cdots = 19 \cdot 79 - 15 \cdot 100.$$

Alltså får vi direkt en lösning $(k, z) = (19, 15)$ som uppfyller villkoren. Vi upphöjer därför båda led i den usprungliga ekvationen med 19 och får

$$47^{19} \equiv x^{15\phi(250)+1} \equiv (x^{\phi(250)})^{15} \cdot x \equiv x \mod 250.$$

Så vi tar $x \equiv 47^{19} \mod 250$. Vi använder successiv kvadrering för att beräkna denna potens:

$$47^1 \equiv 47 \quad 47^2 \equiv 209 \quad 47^4 \equiv 181 \quad 47^8 \equiv 11 \quad 47^{16} \equiv 121 \quad \text{(allt modulo 250)}$$

Vi skriver 19 som en summa av olika 2-potenser: $19 = 16 + 2 + 1$. Vi har nu

$$47^{19} \equiv 47^{16+2+1} \equiv 47^{16}47^2 47^1 \equiv 121 \cdot 209 \cdot 47 \equiv 83 \mod 250.$$

Svar: $x = 83$ uppfyller $x^{79} \equiv 47 \mod 250$.

[6p] 6. Nedan visas en delvis ifylld tabell för en binär operation $\star$ på mängden $M = \{a, b, c, d\}$. Fyll i resten av tabellen på så vis att $(M, \star)$ blir associativ, kommutativ, har ett identitetselement, och saknar ett nollelement. Detta går att göra på precis ett sätt. Blir $(M, \star)$ en grupp? Motivera dina slutsatser!

$\star$	a	b	c	d
a			a	
b	b			
c			a	c
d				

Från tabellen framgår direkt att varken a, b, eller c är identitetselement. Alltså är d identitetselement och vi kan fylla i d's rad och kolonn i tabellen. Kommutativiteten säger också att tabellen ska vara symmetrisk med avseende på diagonalen. Vi fyller i detta och får

$\star$	a	b	c	d
a		b	a	a
b	b			b
c	a		a	c
d	a	b	c	d

Eftersom $\star$ är associativ har vi $a \star (c \star c) = (a \star c) \star c$ vilket enligt tabellen ger $a \star a = a$.

Vidare har vi via associativitet $(b \star a) \star c = b \star (a \star c)$ vilket ger $b \star c = b$ och därför också $c \star b = b$ och vi kan fylla i detta i tabellen. Nu återstår bara att hitta $b \star b$.

Associativiteten ger $(b \star b) \star a = b \star (b \star a) = b \star b$, vilket betyder att $b \star b$ måste vara a eller b. Men om $b \star b = b$ blir b ett nollelement i $(M, \star)$ så vi måste ha $b \star b = a$. Därmed är tabellen klar. $(M, \star)$ är inte en grupp, t.ex. saknar a invers eftersom ingenting multiplicerat med a blir identitetselementet d.

Svar: $(M, \star)$ har följande tabell:

$\star$	a	b	c	d
a	a	b	a	a
b	b	a	b	b
c	a	b	a	c
d	a	b	c	d

Detta är inte en grupp.