LÖSNINGSFÖRSLAG TILL

Matematik Göteborgs Universitet

Tentamen i kursen LGMA50: Algebra och Talteori VT2019

Den 12 Juni 2019 kl 8:30-12:30 Jonathan Nilsson

Tillåtna hjälpmedel: En enkel miniräknare. Grafritande, symbolhanterande, eller programmeringsbara räknare är inte tillåtna. Maxpoäng på tentan är 40p. För godkänt krävs minst 20p. För full poäng på en uppgift krävs en fullständig och välmotiverad lösning som går att följa. Skriv tydligt vad ditt svar är på varje uppgift. Börja varje uppgift på en ny sida.
Telefonvakt: Jonathan Nilsson, 0708676282.

---

1. Hitta alla par av heltal (x, y) som uppfyller $217x + 152y = 3$. [4p]

Vi använder Euklides algoritm:
$217 = 152 + 65$
$152 = 2 \cdot 65 + 22$
$65 = 2 \cdot 22 + 21$
$22 = 21 + 1$

Därför är $gcd(217, 152) = 1$. Om vi arbetar igenom stegen baklänges får vi
$1 = 22 - 21 = 22 - (65 - 2 \cdot 22) = -65 + 3 \cdot 22 = -65 + 3 \cdot (152 - 2 \cdot 65)$
$= 3 \cdot 152 - 7 \cdot 65 = 3 \cdot 152 - 7(217 - 152) = 10 \cdot 152 - 7 \cdot 217.$

Multiplicerar vi med 3 får vi $30 \cdot 152 - 21 \cdot 217 = 3$. Därför är $(x, y) = (-21, 30)$ en lösning till den ursprungliga ekvationen. Enligt sats ges alla lösningar därför av $(x, y) = (-21 + 152k, 30 - 217k)$ där $k \in \mathbb{Z}$.

Svar: Alla lösningar ges av $(x, y) = (-21 + 152k, 30 - 217k)$ där $k \in \mathbb{Z}$.

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

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 4 \\ x \equiv 4 \mod 5 \\ x \equiv 3 \mod 7. \end{cases}$$

Vi inför $n_1 = 3$, $n_2 = 4$, $n_3 = 5$, $n_4 = 7$, $M = n_1 n_2 n_3 n_4 = 420$, och $N_i = M/n_i$ alltså $N_1 = 140$, $N_2 = 105$, $N_3 = 84$, $N_4 = 60$. Enligt vår standardmetod blir då

$$x = 1 \cdot b_1 \cdot N_1 + 2 \cdot b_2 \cdot N_2 + 4 \cdot b_3 \cdot N_3 + 3 \cdot b_4 \cdot N_4$$

en lösning till systemet där b_i är inversen till N_i i $\mathbb{Z}_{n_i}$. Att hitta inverserna b_i är lätt eftersom n_i är små:

$$b_1 \cdot 140 \equiv 1 \mod 3 \iff b_1 \cdot 2 \equiv 1 \mod 3 \quad \text{vi tar } b_1 = 2.$$

$$b_2 \cdot 105 \equiv 1 \mod 4 \iff b_2 \cdot 1 \equiv 1 \mod 4 \quad \text{vi tar } b_2 = 1.$$

$$b_3 \cdot 84 \equiv 1 \mod 5 \iff b_3 \cdot -1 \equiv 1 \mod 5 \quad \text{vi tar } b_3 = -1.$$

$$b_4 \cdot 60 \equiv 1 \mod 7 \iff b_4 \cdot 4 \equiv 1 \mod 7 \quad \text{vi tar } b_4 = 2.$$

Med ovanstående formel blir $x = 514$ en lösning systemet. Enligt Kinesiska restklassatsen har systemet en unik lösning modulo $M = 420$ (eftersom n_i är parvis relativt prima) och $514 \equiv 94 \mod 420$. Alltså blir vår slutsats:

Svar: Systemets lösningar ges av $x \equiv 94 \mod 420$. Eller med andra ord: alla heltalslösningar till systemet ges av $x = 94 + 420k$ där $k \in \mathbb{Z}$.

3. Avgör om det finns ett heltal x så att $x^2 + 60x + 1331 \equiv 0 \mod 3221$. [6p]

Vi börjar med att kvadratkomplettera:

$$x^2 + 60x + 1331 \equiv 0 \Leftrightarrow (x+30)^2 - 900 + 1331 \equiv 0 \Leftrightarrow (x+30)^2 \equiv -431,$$

där alla kongruenser är modulo 3221. Med $y = x + 30$ ska vi alltså avgöra om $y^2 \equiv -431 \mod 3221$ är lösbar. Vi ska därför beräkna Legendre-symbolen $(\frac{-431}{3221})$. Eftersom $3221 \equiv 1 \mod 4$ och 431 är ett primtal så har vi:

$$(\frac{-431}{3221}) = (\frac{-1}{3221}) \cdot (\frac{431}{3221}) = 1 \cdot (\frac{3221}{431}) = (\frac{204}{431}) = (\frac{4}{431}) \cdot (\frac{3}{431}) \cdot (\frac{17}{431})$$

Här är första faktorn 1 eftersom 4 är en kvadrat. Eftersom $431 \equiv 3$ och $17 \equiv 1$ mod 4 har vi fortsättningsvis:

$$= 1 \cdot (-1) \cdot (\frac{431}{3}) \cdot (\frac{431}{17}) = -(\frac{2}{3}) \cdot (\frac{6}{17}) = -(-1) \cdot (\frac{2}{17})(\frac{3}{17}) = (\frac{2}{17}) \cdot (\frac{3}{17})$$

Här är $17 \equiv 1 \mod 8$, så första faktorn är 1, och eftersom $17 \equiv 1 \mod 4$ får vi vidare:

$$= 1 \cdot (\frac{17}{3}) = (\frac{2}{3}) = -1.$$

Vi kan därför dra slutsatsen:

Svar: Eftersom $(\frac{-431}{3221}) = -1$ så saknar ekvationen $y^2 \equiv -431 \mod 3221$ lösningar. Därför saknar också den ekvivalenta ekvationen $x^2 + 60x + 1331 \equiv 0 \mod 3221$ lösningar, det finns alltså inga heltal x som uppfyller den givna ekvationen.

[6p] 4. Vi definierar en relation $\sim$ på heltalen $\mathbb{Z}$ genom

$$a \sim b \Longleftrightarrow 4|(b-a) \text{ och } 6|(b-a).$$

Är relationen $\sim$ är reflexiv? symmetrisk? transitiv? en ekvivalensrelation? Hitta också alla x som uppfyller $5 \sim x$.

Vi har $a \sim a$ för alla a eftersom både 4 och 6 delar $a - a = 0$. Alltså är relationen reflexiv.

Eftersom $4|b-a \Leftrightarrow 4|-(b-a) \Leftrightarrow 4|a-b$, och på samma vis $6|b-a \Leftrightarrow 6|a-b$ så gäller $a \sim b \Rightarrow b \sim a$, och relationen är alltså symmetrisk.

Slutligen antar vi att $a \sim b$ och $b \sim c$. Vi har då speciellt $4|b-a$ och $4|c-b$. Med då har vi också $4|(b-a)+(c-b)$ alltså $4|c-a$. På analogt vi får vi också $6|c-a$ vilket tillsammans ger $a \sim c$. Relationen är därför också transitiv.

Relationen har alltså alla tre egenskaper och är en ekvivalensrelation.

Slutligen hittar vi alla heltal x så att $5 \sim x$. Detta betyder att $4|x-5$ och $6|x-5$, vilket i sin tur är ekvivalent med att $x \equiv 1 \mod 4$ och $x \equiv 5 \mod 6$. Första ekvationen ger $x = 1 + 4y$ för $y \in \mathbb{Z}$ och sätter vi in detta i den andra får vi $1 + 4y \equiv 5 \mod 6 \Leftrightarrow 4y \equiv 4 \mod 6 \Leftrightarrow 4y+6z = 4$ för $y, z \in \mathbb{Z}$. Denna diofantiska ekvation har en lösning $(y, z) = (1, 0)$ och eftersom $gcd(4, 6) = 2$ ges alla lösningar av $(y, z) = (1 + 3k, -2k)$ för $k \in \mathbb{Z}$. Detta ger $x = 1 + 4y = 1 + 4(1 + 3k) = 5 + 12k$ för $k \in \mathbb{Z}$, eller med andra ord $x \equiv 5 \mod 12$.

Svar: Relationen är en ekvivalensrelation, den är alltså reflexiv, symmetrisk, och transitiv. Vidare gäller $5 \sim x$ om och endast om $x \equiv 5 \mod 12$.

5. På följande korta uppgifter krävs endast svaret. [6p]

   (a) Gäller $(x+2)|(x^2+x+2)$ i ringen $\mathbb{Z}_4[x]$?

   (b) Är $\alpha = \sqrt{3-2^{\frac{1}{5}}}$ ett algebraiskt heltal?

   (c) Är 2930 ett perfekt tal?

   (d) Är $(\mathbb{Z}_{123}, +, \cdot)$ är en kropp?

   (e) Skriv talet $12-48i$ som en produkt av Gaussiska primtal.

   (f) Beräkna $(1,2,3)\circ(4,5)\circ(3,1,2,4)\circ(5,2)$ i S_5.

På följande korta uppgifter krävs endast svaret.

(a) Ja. (eftersom $(x^2+x+2) = (x+2)(x+3)$)

(b) Ja. (med $p(x) = (x^2-3)^5+2$ fås $p(\alpha) = 0$)

(c) Nej. ($\sigma(2930) = (1+2)(1+5)(1+293) = 5292 \neq 2\cdot 2930$)

(d) Nej. ($3|123$ så 3^{-1} existerar exempelvis ej)

(e) $12-48i = 3(1+i)^2(1-i)^2(1-4i)$.

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

[6p] 6. Hitta ett heltal x mellan 0 och 100 som uppfyller $x^{53} \equiv 69 \mod 100$.

Vi följer standardalgoritmen, vi börjar med att hitta positiva heltal k och z som uppfyller $53k - z\phi(100) = 1$. Vi har $\phi(100) = \phi(5^2)\phi(2^2) = (25-5)\cdot(4-2) = 40$. Med Euklides algoritm har vi

$$53 = 40 + 13, \quad 40 = 3 \cdot 13 + 1 \text{ så } 1 = 40 - 3\cdot(13) = 40 - 3\cdot(53-40) = 4\cdot 40 - 3\cdot 53.$$

Alltså får vi en lösning $(k, z) = (-3, -4)$ till $53k - z\phi(100) = 1$. Alla lösningar ges då av $(k, z) = (-3 + 40t, -4 + 53t)$ för $t \in \mathbb{Z}$. För att få en positiv lösning kan vi t.ex. ta $t = 1$ vilket ger $k = 37$ och $z = 49$.

Vi upphöjer därför båda led i den usprungliga ekvationen med 37 och får

$$69^{37} \equiv x^{49\phi(100)+1} \equiv (x^{\phi(100)})^{49} \cdot x \equiv x \mod 100.$$

Så vi tar $x \equiv 69^{37} \mod 100$. Vi använder successiv kvadrering för att beräkna denna potens, moduloräkningen blir enkel eftersom det är modulo 100:

$$69^1 \equiv 69 \quad 69^2 \equiv 61 \quad 69^4 \equiv 21 \quad 69^8 \equiv 41 \quad 69^{16} \equiv 81 \quad 69^{32} \equiv 61 \text{ (allt mod 100)}$$

Vi skriver 37 som en summa av olika 2-potenser: $37 = 32 + 4 + 1$. Vi har nu

$$69^{37} \equiv 69^{32+4+1} \equiv 69^{32}69^{4}69^{1} \equiv 61 \cdot 21 \cdot 69 \equiv 89 \mod 100.$$

Svar: $x = 89$ uppfyller $x^{53} \equiv 69 \mod 100$.

7. Låt mängden $P(\mathbb{N})$ bestå av alla delmängder till $\mathbb{N}$. Vi definierar en binär operation Δ på $P(\mathbb{N})$ enligt [6p]

$$A\Delta B = (A \cup B)\backslash(A \cap B).$$

Vi har då t.ex. $\{2,3,4,5\}\Delta\{4,5,6\} = \{2,3,6\}$.

(a) Låt $A = \{1,2,3,4\}$, $B = \{2,3,5,6\}$, och $C = \{2,4,6,7\}$.
Beräkna $(A\Delta B)\Delta C$ och $A\Delta(B\Delta C)$.

(b) Visa att $(P(\mathbb{N}), \Delta)$ är en abelsk grupp.

(c) Lös ekvationen $\{2k \mid k \in \mathbb{N}\}\Delta X = \{3k \mid k \in \mathbb{N}\}$. Beskriv explicit vilka heltal som ligger i X.

(d) Definiera $\varphi : P(\mathbb{N}) \to \mathbb{Z}_2$ genom $\varphi(D) = 1$ när $5 \in D$, och $\varphi(D) = 0$ annars. Visa att φ är en grupp-homomorfism.

(a) $(A\Delta B)\Delta C = \{1,4,5,6\}\Delta\{2,4,6,7\} = \{1,2,5,7\}$
$A\Delta(B\Delta C) = \{1,2,3,4\}\Delta\{3,4,5,7\} = \{1,2,5,7\}$

(b) Associativitet är lättast att visa genom att rita Venn-diagram. Vi ser då att $(A\Delta B)\Delta C = A\Delta(B\Delta C)$, båda mängderna är lika med $(A\backslash(B \cup C)) \cup (B\backslash(A \cup C)) \cup (C\backslash(A \cup B)) \cup (A \cap B \cap C)$, eller med andra ord de heltal som ligger i antingen 1 eller 3 av mängderna A, B, C. Identitetselementet är den tomma mängden $\{\} = \varnothing$. Eftersom $A\Delta A = \varnothing$ så är varje element i gruppen sin egen invers. Detta visar att $(P(\mathbb{N}), \Delta)$ är en grupp. Den är abelsk eftersom $A \cup B = B \cup A$ och $A \cap B = B \cap A$ vilket ger $A\Delta B = B\Delta A$.

(c) Eftersom varje mängd är sin egen invers applicerar vi $\{2k \mid k \in \mathbb{N}\}\Delta$ på båda sidorna, och använder associativitet för att få:

$$\{2k \mid k \in \mathbb{N}\}\Delta X = \{3k \mid k \in \mathbb{N}\} \Leftrightarrow X = \{2k \mid k \in \mathbb{N}\}\Delta\{3k \mid k \in \mathbb{N}\}$$

$$= \{x \text{ så att } 2|x \text{ eller } 3|x\}\backslash\{x \text{ så att } 2|x \text{ och } 3|x\}$$

$$= \{x \equiv 0,2,3,4 \mod 6\}\backslash\{x \equiv 0 \mod 6\} = \{x \equiv 2,3,4 \mod 6\}.$$

Mängden X består alltså av alla naturliga tal som modulo 6 är antingen $2, 3$, eller 4.

(d)

$$\varphi(A\Delta B) = \begin{cases} 1 \text{ om } 5 \in A \cup B \text{ men } 5 \notin A \cap B \\ 0 \text{ annars} \end{cases}$$

$$= \begin{cases} 0 \text{ om } 5 \in A \text{ och } 5 \in B \\ 1 \text{ om } 5 \in A \text{ och } 5 \notin B \\ 1 \text{ om } 5 \notin A \text{ och } 5 \in B \\ 0 \text{ om } 5 \notin A \text{ och } 5 \notin B \end{cases} = \varphi(A) + \varphi(B)$$

Alltså har vi $\varphi(A\Delta B) = \varphi(A) + \varphi(B)$ för alla $A, B \in P(\mathbb{N})$, vilket visar att φ är en grupp-homomorfism.