Lösningsförslag

Dugga 2 på Grunk 91MA13/92MA13 den 2024-11-18 kl 08.00-12.00

---

1. (a) $\frac{1}{13}\binom{14}{5} = \frac{1}{13} \cdot \frac{14\cdot 13\cdot 12\cdot 11\cdot 10}{5\cdot 4\cdot 3\cdot 2\cdot 1} = \frac{14\cdot 12\cdot 11\cdot 10}{(5\cdot 2)\cdot(4\cdot 3)} = 14 \cdot 11 = 140 + 14 = 154.$

   (b) Räknereglerna för argument ger $\arg(z) = 9\arg(1+i) + \arg(\sqrt{3}+i) - \arg(5i) = 9\frac{\pi}{4} + \frac{\pi}{6} - \frac{\pi}{2} = \frac{\pi(27+2-6)}{12} = \frac{23\pi}{12}$. Argumentet definieras upp till multipler av 2π, så andra svar är möjliga, t.ex. $-\frac{\pi}{12}$.

   (c) Båda sidorna är positiva så $2^{x+3} = e^x \Leftrightarrow \ln(2^{x+3}) = \ln(e^x) \Leftrightarrow (x+3)\ln(2) = x \Leftrightarrow x\ln(2) + 3\ln(2) = x \Leftrightarrow x(\ln(2) - 1) = -3\ln(2) \Leftrightarrow x = \frac{3\ln(2)}{1-\ln(2)}$.

   Svar: $a)\ 154 \qquad b)\ \frac{23\pi}{12} \qquad c)\ x = \frac{3\ln(2)}{1-\ln(2)}$.

2. (a) Vi använder att $\cos(x) = \sin(\frac{\pi}{2} - x)$, att $\sin$ och $\arcsin$ är udda funktioner, att $\sin(x) = \sin(\pi - x)$, och att $x \in [-\frac{\pi}{2}, \frac{\pi}{2}] \Leftrightarrow \arcsin(\sin(x)) = x$. Vi får $\arcsin(\cos(\frac{6\pi}{5})) = \arcsin(\sin(\frac{\pi}{2} - \frac{6\pi}{5})) = \arcsin(\sin(\frac{5\pi-12\pi}{10})) = \arcsin(\sin(-\frac{7\pi}{10})) = -\arcsin(\sin(\frac{7\pi}{10})) = -\arcsin(\sin(\pi - \frac{7\pi}{10})) = -\arcsin(\sin(\frac{3\pi}{10})) = -\frac{3\pi}{10}$.

   (b) Tangens för dubbla vinkeln ger $\tan(2\alpha) = \frac{2\tan(\alpha)}{1-\tan^2(\alpha)} = \frac{2\tan(\arctan(\sqrt{2}-1))}{1-\tan^2(\arctan(\sqrt{2}-1))} = \frac{2(\sqrt{2}-1)}{1-(\sqrt{2}-1)^2} = \frac{2\sqrt{2}-2}{1-(2-2\sqrt{2}+1)} = \frac{2\sqrt{2}-2}{2\sqrt{2}-2} = 1$. Så $\tan(2\alpha) = 1$ ger att $2\alpha = \frac{\pi}{4} + k\pi$ och att $\alpha = \frac{\pi}{8} + \frac{k\pi}{2}$ där k är något heltal. Men eftersom $0 < \alpha < \frac{\pi}{2}$ så måste $k = 0$ och $\alpha = \frac{\pi}{8}$.

   Svar: $a)\ -\frac{3\pi}{10} \qquad b)\ \frac{\pi}{8}$.

3. (a) Vi ser att $x > 3$ för att alla logaritmer ska vara definierade. För sådana x kan i vi exponentiera bägge led vilket ger
   $\ln(x) + \ln(x-3) = 2\ln(2) + \ln(7) \Rightarrow x(x-3) = 2^2 \cdot 7 \Leftrightarrow x^3 - 3x - 28 = 0 \Leftrightarrow (x - \frac{3}{2})^2 - \frac{9}{4} - \frac{112}{4} = 0 \Leftrightarrow (x - \frac{3}{2})^2 - (\frac{11}{2})^2 = 0 \Leftrightarrow (x - \frac{14}{2})(x + \frac{8}{2}) = 0 \Leftrightarrow (x-7)(x+4) = 0 \Leftrightarrow x = 7$ eller $x = -4$. Men enligt villkoret ovan är endast $x = 7$ en lösning.
   Svar: $x = 7$ är ekvationens enda lösning.

   (b) Vi utgår från högerledet och förenklar tills vi får vänsterledet med Eulers formler:

$$\cos^2(x) - \sin^2(x) = \left(\frac{e^{ix} + e^{-ix}}{2}\right)^2 - \left(\frac{e^{ix} - e^{-ix}}{2i}\right)^2 = \frac{e^{2ix} + 2 + e^{-2ix}}{4} - \frac{e^{2ix} - 2 + e^{-2ix}}{-4}$$

$$= \frac{e^{2ix} + 2 + e^{-2ix} + e^{2ix} - 2 + e^{-2ix}}{4} = \frac{2e^{2ix} + 2e^{-2ix}}{4} = \frac{e^{2ix} + e^{-2ix}}{2} = \cos(2x).$$

4. Eftersom $\arccos$ är strängt avtagande är också f det. Definitionsmängden till $\arccos$ är $[-1, 1]$ så f är definierad när $-1 \leq 2x + 3 < 1 \Leftrightarrow -4 \leq 2x \leq -2 \Leftrightarrow -2 \leq x \leq -1$. Så $D_f = [-2, -1]$ Eftersom värdemängden till $\arccos$ är $[0, \pi]$ så ges värdemängden till f av $V_f = [-5, \pi - 5]$. För att ta fram ett uttryck för inversen sätter vi $y = f(x)$ och löser ut x som funktion av y. För $x \in D_f$ och $y \in V_f$ har vi

$$y = f(x) \Leftrightarrow y = \arccos(2x+3) - 5 \Leftrightarrow y + 5 = \arccos(2x+3)$$

$$\Leftrightarrow \cos(y+5) = 2x + 3 \Leftrightarrow x = \frac{\cos(y+5) - 3}{2}$$

Svar: $D_f = [-2, -1]$, $V_f = [-5, \pi - 5]$, och $f^{-1}(y) = \frac{\cos(y+5)-3}{2}$.

5. Vi skriver om vänsterledet med hjälpvinkelmetoden. Vi ansätter

$$2\sin(x) - \sqrt{12}\cos(x) = C\sin(x+v).$$

Eftersom $\sin(x+v) = \sin(x)\cos(v) + \cos(x)\sin(v)$ så får vi villkoren $C\sin(v) = -\sqrt{12}$ och $C\cos(v) = 2$. Trigonometriska ettan ger $C^2 = 2^2 + (-\sqrt{12})^2 = 16$, så vi kan ta $C = 4$. Våra ekvationer blir $\sin(v) = -\frac{\sqrt{12}}{4} = -\frac{\sqrt{3}}{2}$ och $\cos(v) = \frac{1}{2}$, så vi kan ta $v = -\frac{\pi}{3}$. Vi har nu visat att $2\sin(x) - \sqrt{12}\cos(x) = 4\sin(x - \frac{\pi}{3})$, så ekvationen i uppgiften övergår till

$$4\sin(x-\tfrac{\pi}{3}) = 4\sin(3x) \Leftrightarrow \sin(x-\tfrac{\pi}{3}) = \sin(3x) \Leftrightarrow \begin{cases} x - \frac{\pi}{3} = 3x + 2k\pi \\ \text{eller} \\ x - \frac{\pi}{3} = \pi - 3x + 2k\pi \end{cases}$$

$$\Leftrightarrow \begin{cases} -2x = \frac{\pi}{3} + 2k\pi \\ \text{eller} \\ 4x = \frac{4\pi}{3} + 2k\pi \end{cases} \Leftrightarrow \begin{cases} x = -\frac{\pi}{6} - k\pi \\ \text{eller} \\ x = \frac{\pi}{3} + \frac{k\pi}{2} \end{cases} \quad \text{där } k \in \mathbb{Z}.$$

Här kan vi dock se att de x mellan 0 och 2π som löser den övre ekvationen är $\frac{5\pi}{6}$ och $\frac{11\pi}{6}$, medan de x mellan 0 och 2π som löser den nedre ekvationen är $\frac{\pi}{3}$, $\frac{5\pi}{6}$, $\frac{4\pi}{3}$, och $\frac{11\pi}{6}$. Så alla lösningar till den övre ekvationen ingår i lösningarna för den nedre, så vi kan förkota svaret till:
Svar: Ekvationens lösningar är $\frac{\pi}{3} + \frac{k\pi}{2}$ där $k \in \mathbb{Z}$.

6. Vi inför $\frac{z}{2} - 5 = re^{iv}$ där $r \geq 0$. Ekvationen kan då skrivas $r^4e^{4iv} = -\frac{81}{4}$. Absolutbeloppet av högerledet är $\frac{81}{4}$ och ett argument för högerledet är π, så ekvationen kan skrivas $r^4e^{4iv} = \frac{81}{4}e^{i\pi}$. Vi jämför belopp och argument på bägge sidor och får ekvationssystemet

$$\begin{cases} r^4 = \frac{81}{4} \\ 4v = \pi + 2k\pi \end{cases} \Leftrightarrow \begin{cases} r = \left(\frac{81}{4}\right)^{\frac{1}{4}} = \frac{3}{\sqrt{2}} \\ v = \frac{\pi}{4} + \frac{k\pi}{2} \end{cases}$$

där $k = 0, 1, 2, 3$, vilket ger $v \in \{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$. Vi går tillbaka till vår ursprungliga variabel z genom att beräkna sinus och cosinus för dessa vinklar v.
Eftersom $\frac{z}{2} - 5 = re^{iv}$ får vi $\frac{z}{2} = 5 + re^{iv}$ och

$$z = 10 + 2re^{iv} = 10 + 2\frac{3}{\sqrt{2}}e^{iv} = 10 + 3\sqrt{2}(\cos(v) + i\sin(v))$$

vilket efter insättning av de fyra vinklarna v ovan ger

$$z = 10 + 3\sqrt{2}(\cos(v) + i\sin(v)) = 10 + 3\sqrt{2}(\pm\tfrac{1}{\sqrt{2}} \pm i\tfrac{1}{\sqrt{2}}) = 10 \pm 3 \pm 3i.$$

Svar: Ekvationen har lösningarna $13 + 3i$, $13 - 3i$, $7 + 3i$, och $7 - 3i$.

7. (a) Linjen genom A och B har riktningskoefficient $\frac{-1-1}{-1-0} = 2$ och skär y-axeln i punkten A, så linjen har ekvation $y = 2x + 1$. Vi substituerar detta värde i ekvationen för den elliptiska kurvan och får ekvationen

$$(2x+1)^2 = x^3 - x + 1 \Leftrightarrow 4x^2 + 4x + 1 = x^3 - x + 1 \Leftrightarrow x^3 - 4x^2 - 5x = 0$$

$$\Leftrightarrow x(x^2 - 4x - 5) = 0 \Leftrightarrow x((x-2)^2 - 3^2) = 0 \Leftrightarrow x(x+1)(x-5) = 0.$$

Lösningarna $x = 0$ och $x = -1$ motsvarar punkterna A och B, den tredje skärningspunkten mellan kurvan och linjen motsvarar $x = 5$ vilket enligt linjens ekvation ger $y = 11$. Så tredje skärningspunkten är $(5, 11)$, och dess spegelbilden i x-axeln är $(5, -11)$.
Svar: $A \oplus B = (5, -11)$.

(b) Man kan här beräkna båda sidorna explicit och se att både vänsterledet och högerledet blir $B = (-1, -1)$, så svaret är ja. Men man kan också resonera geometriskt: Låt alltid P' betyda spegelbilden av en punkt P i x-axeln. Enligt definitionen så ligger A, B, och $(A \oplus B)'$ på samma linje. På grund av symmetri ligger därför även A', B', och $(A \oplus B)$ på samma linje vilket visar att $(A \oplus B) \oplus C = (A \oplus B) \oplus A' = (B')' = B$. På samma vis, eftersom B, C, och $(B \oplus C)'$ ligger på samma linje så ligger även B', C' och $B \oplus C$ på samma linje, så $A \oplus (B \oplus C) = C' \oplus (B \oplus C) = (B')' = B$.
Svar: Ja, $(A \oplus B) \oplus C = B = A \oplus (B \oplus C)$.

Kommentar för den som är intresserad: Denna definition av addition på elliptiska kurvor är användbar eftersom den faktiskt uppfyller den accosicativa lagen

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

för *alla* punkter A, B, C på kurvan (för att additionen alltid ska bli definierad får man trixa lite i specialfallen när punkterna är varandras spegelbilder eller när linjen mellan dem tangerar kurvan).

Tillämpningar inom kryptografi bygger på att det är relativt lätt att givet A och B på kurvan beräkna $R = A \oplus kB = A \oplus \big(\underbrace{B \oplus B \oplus \cdots \oplus B}_{k}\big)$, för varje heltal k (kryptering). Men givet R och A och k är det mycket svårt att beräkna B (dekryptering), även för en dator. I praktiken ersätter man även de reella talen med en *ändlig kropp* $\mathbb{Z}_p$, så att kurvan består av alla heltalspar som uppfyller kurvans ekvation modulo ett stort primtal p.

Den som är nyfiken kan läsa mer här:
`https://en.wikipedia.org/wiki/Elliptic_curve#The_group_law`

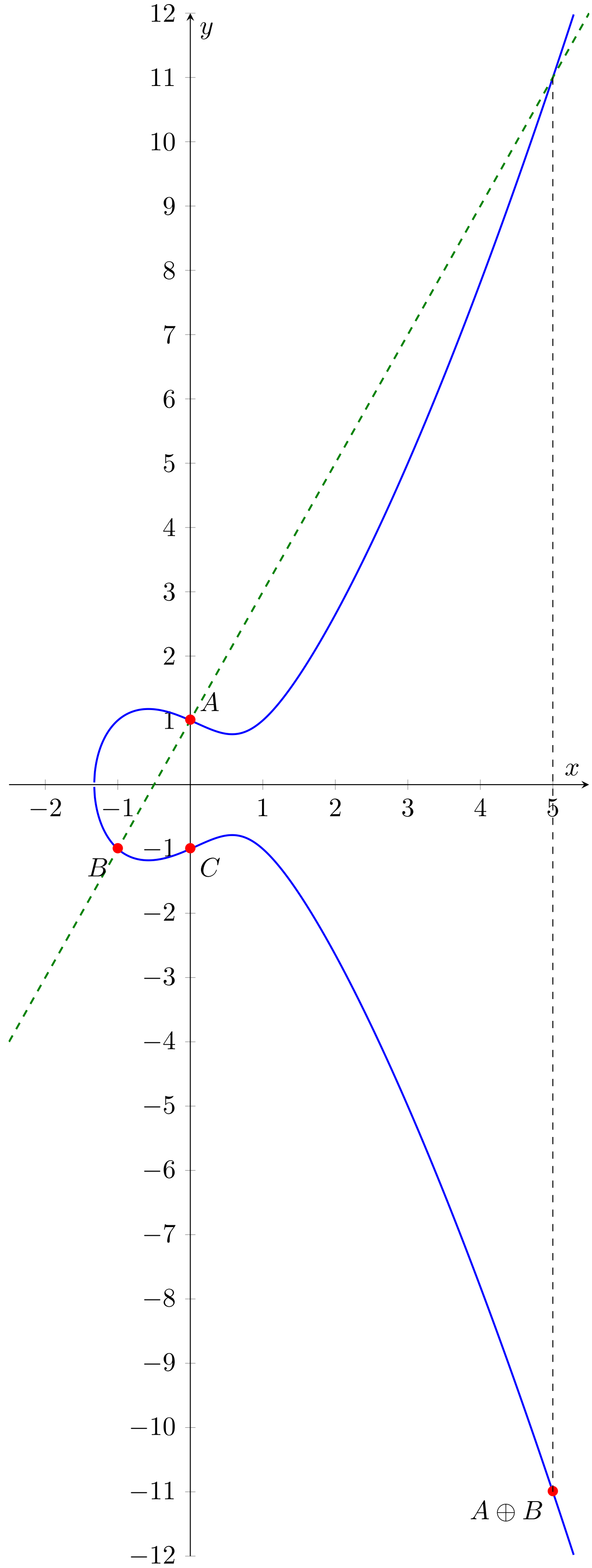

Illustration av lösningen till 7 a), vi ser att bilden stämmer med vår algebraiska lösning: $A \oplus B = (5, -11)$.