UPPSALA UNIVERSITET
Matematiska institutionen
Elin Persson Westin
076-80 46 726

Prov i matematik
MaKand, fristående
Algebra II
2019–08–31

Skrivtid: 5 timmar. Tillåtna hjälpmedel: Skrivdon. Lösningarna skall åtföljas av förklarande text. För betygen 3, 4 och 5 krävs 18, 25 resp. 32 poäng, inklusive bonuspoäng.

1. Avgör om följande påståenden är sanna eller falska. Ge ett *kort* bevis eller ett motexempel.

a) Om K är en kropp så är även polynomringen $K[x]$ det.

b) Låt R vara ett integritetsområde. $R/\langle p\rangle$ är ett integritetsområde om och endast om p är ett primelement.

c) Polynomet $p(x) = 2x^5 + 24x^2 - 36x - 6$ är irreducibelt i $\mathbb{Q}[x]$.

d) $\mathbb{Z}[x]$ är en Euklidisk ring.

e) Om Alice och Bob vill skicka krypterade meddelanden till varandra genom att använda RSA-algoritmen måste de först träffas för att utbyta nycklar.

(10 poäng)

2. Hitta samtliga heltalslösningar till följande system av kongruenser:

$$\begin{cases} x \equiv 2 \pmod 3 \\ 2x \equiv 6 \pmod 7 \\ x \equiv 5 \pmod{10}. \end{cases}$$

(5 poäng)

3. **a)** Beräkna $\varphi(24)$, där φ är Eulers φ-funktion.

b) Beräkna $4^8 \pmod{24}$. Motsäger ditt svar Eulers sats, varför/varför inte?

c) Hitta alla nollställen i $\mathbb{Z}_{19}$ till polynomet $x^{19} + 18x \in \mathbb{Z}_{19}[x]$.

(5 poäng)

4. Avgör om några av följande ringar är isomorfa.

$$R_1 = \mathbb{Z}_{12}, \quad R_2 = \mathbb{Z}_6 \times \mathbb{Z}_6, \quad R_3 = \mathbb{Z}_2 \times \mathbb{Z}_6, \quad R_4 = \mathbb{Z}_6, \quad R_5 = \mathbb{Z}_2 \times \mathbb{Z}_3.$$

(5 poäng)

5. Låt R vara en kommutativ ring och antag att varje ideal är ett primideal. Visa att R är en kropp. (Hint: titta på idealet $\langle a^2\rangle$.) (4 poäng)

6. Låt $\mathbb{R}[x]$ beteckna ringen av alla reella polynom. Låt $\mathrm{ev}_3 : \mathbb{R}[x] \to \mathbb{R}$ definieras av $\mathrm{ev}_3(p(x)) = p(3)$, dvs utvärdering i det reella talet 3.

a) Visa att ev_3 är en ringhomomorfism.

b) Låt

$$I = \{p \in \mathbb{R}[x] \mid 3 \text{ är en rot till } p\}.$$

Visa att I är ett ideal i $\mathbb{R}[x]$ och att $\mathbb{R}[x]/I \cong \mathbb{R}$.

(6 poäng)

7. Faktorisera det Gaussiska heltalet $24 + 18i$. (5 poäng)

Lycka till!

Lösningar till tentamen i Algebra II 2019–08–31

Lösning till problem 1. **a)** Falskt!

T.ex. polynomet x har ingen multiplikativ invers, och $K[x]$ är således ingen kropp!

b) Sant!

$R/\langle p\rangle$ är ett integritetsområde om och endast om $\langle p\rangle$ är ett primideal. $\langle p\rangle$ är ett primideal om och endast om p är ett primelement.

c) Sant!

Eisensteins kriterium med $p = 3$ ger oss att polynomet är irreducibelt i $Q(\mathbb{Z})[x] \cong \mathbb{Q}[x]$. (Kriteriumet gäller eftersom: $3|(-6), 3|(-36), 3|24, 3 \not| 2, 3^2 \not| (-6)$.)

d) Falskt!

$\mathbb{Z}[x]$ är inte en huvudidealring då t.ex. $\langle x, 2\rangle$ inte är ett huvudideal. Varje Euklidisk ring är en huvudidealring, så $\mathbb{Z}[x]$ kan inte heller vara en Euklidisk ring.

e) Falskt!

För RSA-krytering används två nycklar, den hemliga behåller den som vill ta emot meddelanden för sig själv, men den offentliga nyckeln kan denne sprida offentligt - den kan inte användas för att avkryptera meddelandet, bara kryptera det.

Lösning till problem 2. Vi noterar först att $3, 7, 10$ är parvis relativt prima vilket innebär att vi får använda Kinesiska restsatsen! Vi ansätter därför en lösning x på följande form:

$$x = 70b_1 + 30b_2 + 21b_3.$$

Om vi sätter in detta i systemet får vi:

$$\begin{cases} 70b_1 + 30b_2 + 21b_3 \equiv 2 \pmod 3 \\ 2(70b_1 + 30b_2 + 21b_3) \equiv 6 \pmod 7 \\ 70b_1 + 30b_2 + 21b_3 \equiv 5 \pmod{10} \end{cases} \Leftrightarrow \begin{cases} 70b_1 \equiv 2 \pmod 3 \\ 60b_2 \equiv 6 \pmod 7 \\ 21b_3 \equiv 5 \pmod{10} \end{cases} \Leftrightarrow \begin{cases} 1b_1 \equiv 2 \pmod 3 \\ 4b_2 \equiv 6 \pmod 7 \\ 1b_3 \equiv 5 \pmod{10} \end{cases}$$

$$\Leftrightarrow \begin{cases} b_1 \equiv 2 \pmod 3 \\ 4b_2 \equiv -1 \pmod 7 \\ b_3 \equiv 5 \pmod{10} \end{cases} \Leftrightarrow \begin{cases} b_1 \equiv 2 \pmod 3 \\ 2 \cdot 4b_2 \equiv 2 \cdot (-1) \pmod 7 \\ b_3 \equiv 5 \pmod{10} \end{cases} \Leftrightarrow \begin{cases} b_1 \equiv 2 \pmod 3 \\ b_2 \equiv -2 \pmod 7 \\ b_3 \equiv 5 \pmod{10} \end{cases}$$

Vi får alltså att

$$x = 70 \cdot 2 + 30 \cdot (-2) + 21 \cdot 5 = 185 \equiv -25 \pmod{210}$$

löser systemet. Kinesiska restsatsen ger oss att samtliga lösningar är $x = -25 + 210n$ där $n \in \mathbb{Z}$ (Obs: $210 = 3 \cdot 7 \cdot 10$).

Lösning till problem 3. **a)** Vi vet att om m_1, m_2 är relativt prima så gäller $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$. samt att för ett primtal p gäller $\varphi(p^n) = p^{n-1}(p-1)$. Detta ger oss:

$$\varphi(24) = \varphi(3 \cdot 2^3) = \varphi(3)\varphi(2^3) = 2 \cdot 4 = 8.$$

b)

$$\begin{aligned} 4^8 &\equiv (4^2)^4 \pmod{24} \\ &\equiv (16)^4 \pmod{24} \\ &\equiv ((-8)^2)^2 \pmod{24} \\ &\equiv 64^2 \pmod{24} \\ &\equiv (-8)^2 \pmod{24} \\ &\equiv 16 \pmod{24}. \end{aligned}$$

Detta motsäger INTE Eulers sats, eftersom att satsen säger att om a är RELATIVT PRIMT med m så gäller $a^{\varphi(m)} \equiv 1 \pmod{m}$. Men eftersom att $(4, 24) = 4 \neq 1$ så gäller inte Eulers sats i det här fallet.

c) Fermats lilla sats säger att för varje $a \in \mathbb{Z}$ gäller det att $a^{19} \equiv a \pmod{19}$. Alltså har vi, för varje $a \in \mathbb{Z}_{19}$:

$$a^{19} + 18a = a + 18a = a - a = 0.$$

Alltså är varje element a i $\mathbb{Z}_{19}$ ett nollstället till polynomet.

Lösning till problem 4. Vi börjar med att titta på antalet element i respektive ring:

$$|\mathbb{Z}_{12}| = 12, \quad |\mathbb{Z}_6 \times \mathbb{Z}_6| = 36, \quad |\mathbb{Z}_2 \times \mathbb{Z}_6| = 12, \quad |\mathbb{Z}_6| = 6, \quad |\mathbb{Z}_2 \times \mathbb{Z}_3| = 6.$$

Eftersom att om två ringar är isomorfa så måste de ha samma antalet element har två endast kvar två möjligheter: $\mathbb{Z}_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_6$ och $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Nu tittar vi istället på karaktäristiken. Om två ringar är isomorfa har de samma karaktäristik. Vi vet att karaktäristiken av $R \times S$ är minsta gemensamma multipel av $\text{char}(R)$ och $\text{char}(S)$. Alltså har vi:

$$\text{char}(\mathbb{Z}_{12}) = 12, \quad \text{char}(\mathbb{Z}_2 \times \mathbb{Z}_6) = 6, \quad \text{char}(\mathbb{Z}_6) = 6, \quad \text{char}(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6.$$

Nu har vi endast en möjlighet kvar, nämligen att $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Vi tror att detta är sant och försöker därför hitta en isomorfi. Vi vet att $\varphi(0) = (0, 0)$ och $\varphi(1) = (1, 1)$. Vi har då endast 4 element kvar. Om vi inte har någon bra idé på en isomorfism kan vi alltid använda oss av att $\varphi(a + b) = \varphi(a) + \varphi(b)$. Vi får då:

$$\varphi(2) = (1, 1) + (1, 1) = (2, 2) = (0, 2),$$

$$\varphi(3) = (0, 2) + (1, 1) = (1, 3) = (1, 0),$$

$$\varphi(4) = (1, 0) + (1, 1) = (2, 1) = (0, 1),$$

$$\varphi(5) = (0, 1) + (1, 1) = (1, 2).$$

Vi kan nu kontrollera att även $\varphi(ab) = \varphi(a)\varphi(b)$ gäller, samt att avbildningen är en bijektion. Om vi gör detta har vi visat att φ är en isomorfism, och därmed att $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Vi bör observera att detta avbildning faktiskt kan definieras via $\varphi(a) = (a, a)$. Det är då uppenbart att det är en ringhomomorfism och det är lätt att visa att avbildningen är surjektiv. Eftersom att mängderna har lika många element följer det sedan att det är en bijektion.

Lösning till problem 5. Vi vet att $a^2 \in \langle a^2 \rangle$. Men eftersom att det antagits att alla ideal är primideal så har vi att $a \cdot a \in \langle a^2 \rangle \Rightarrow a \in \langle a^2 \rangle$. Då finns det $r \in R$ så att $a^2 r = a$. Vi vill nu använda den multiplikativa kancelleringslagen, men då måste vi visa att ringen är ett integritetsområde först!

Vi tittar därför på nollidealet. Om $ab \in \{0\}$ så har vi $a \in \{0\}$ eller $b \in \{0\}$, eftersom att även nollidealet är ett primideal. Men det innebär att $ab = 0 \Rightarrow a = 0 \vee b = 0$, eftersom att R även är kommutativ är R ett integritetsområde.

Om $a \neq 0$ får vi då:

$$a^2 r = a \Rightarrow ar = 1.$$

Men detta innebär att varje nollskilt a är inverterbart! Eftersom att R även är kommutativ är R då en kropp.

Lösning till problem 6. **a)** Vi behöver visa att $\text{ev}_3(p+q) = \text{ev}_3(p) + \text{ev}_3(q)$, $\text{ev}_3(pq) = \text{ev}_3(p)\text{ev}_3(q)$ samt att $\text{ev}_3(1) = 1$.

Om vi evaluerar det konstanta polynomet 1 får vi såklart $1 \in \mathbb{R}$. Enligt definitionen av polynomringen har vi även:

$$\text{ev}_3(p + q) = (p + q)(3) = p(3) + q(3) = \text{ev}_3(p) + \text{ev}_3(q),$$

$$\text{ev}_3(pq) = (pq)(3) = p(3)q(3) = \text{ev}_3(p)\text{ev}_3(q).$$

Alltså är ev_3 en ringhomomorfism.

b) Vi har $p \in I$ om och endast om $p(3) = 0$. Om $p, q \in I$ så har vi $(p+q)(3) = p(3)+q(3) = 0+0 = 0$. Alltså har vi $p + q \in I$. Om $p \in I$ och $q \in \mathbb{R}[x]$ har vi $(pq)(3) = p(3)q(3) = 0 \cdot q(3) = 0$. Alltså har vi $pq \in I$. Eftersom att nollpolynomet uppenbarligen ligger i I är mängden även nollskild. Alltså är I ett ideal.

I är dessutom, enligt definition, kärnan av ev_3. Eftersom att för varje reellt tal a har vi det konstanta polynomet a som uppfyller $\mathrm{ev}_3(a) = 0$ så är avbildningen en surjektion. Enligt Noethers första isomorfisats har vi för en ringhomomorfism $\varphi : R \to S$: $R/\ker(\varphi) \cong \mathrm{im}(\varphi)$. Detta ger oss att $\mathbb{R}[x]/I \cong \mathbb{R}$.

Lösning till problem 7. Vi börjar med att bryta ut $(24, 18) = 6$:

$$24 + 18i = 6(4 + 3i).$$

Sedan faktoriserar vi den största gemensamma delaren i primtal:

$$6 = 2 \cdot 3.$$

Kom ihåg följande sats:

Sats. De irreducibla elementen i $\mathbb{Z}[i]$ är:

a) Primtal $p \in \mathbb{N}$ så att $p \equiv 3 \pmod 4$,

b) Gaussiska heltal $a + bi$ sådana att $N(a + bi) = a^2 + b^2$ är ett primtal.

c) Gaussiska heltal som är associerade med de i a) och b).

Eftersom att $3 \equiv 3 \pmod 4$ så är 3 irreducibelt i $\mathbb{Z}[i]$, medan $2 \not\equiv 3 \pmod 4$. Då vet vi dock att 2 kan skrivas som en summa av två kvadrater och vi får därför:

$$2 = 1^2 + 1^2 = (1 + i)(1 - i).$$

Eftersom att både $1 + i$ och $1 - i$ har normen 2 som är ett primtal så är dessa faktorer irreducibla. Sammanfattningsvis är faktoriseringen av 6 i irreducibla faktorer följande:

$$6 = 3(1 + i)(1 - i).$$

Nu går vi vidare och faktoriserar $4+3i$. Vi börjar med att faktorisera $N(4+3i)$ i irreducibla faktorer:

$$N(4 + 3i) = 4^2 + 3^2 = 16 + 9 = 25 = 5^2 = ((1 + 2i)(1 - 2i))^2.$$

Kom ihåg att varje irreducibelt element också är primt och att $N(z) = z\overline{z}$. För varje irreducibel faktor i $N(z)$ har vi $q|z\overline{z} \Rightarrow q|z \vee q|\overline{z}$, och det senare är ekvivalent med $q|z \vee \overline{q}|z$.

Vi testar först om $1 + 2i$ delar $4 + 2i$:

$$\frac{4 + 3i}{1 + 2i} = \frac{(4 + 3i)(1 - 2i)}{(1 + 2i)(1 - 2i)} = \frac{(4 + 6) + (3 - 8)i}{5} = \frac{10 - 5i}{5} = 2 - i = -i(1 - 2i).$$

Vi ser att $1 + 2i$ delar $4 + 3i$ och att kvoten $-i(1 - 2i)$ är irreducibel! Vi har alltså:

$$4 + 3i = -i(1 + 2i)(1 - 2i).$$

Sammantaget får vi föjande faktorisering i irreducibla faktorer:

$$24 + 18i = 3(1 + i)(1 - i)(1 + 2i)(1 - 2i).$$