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

Prov i matematik
MaKand, fristående
Algebra II
2022–03–10

Skrivtid: 8.00-13.00. Tillåtna hjälpmedel: Skrivdon. Lösningarna skall åtföljas av förklarande text. För betygen 3, 4 och 5 krävs 18, 25 resp. 32 poäng inklusive eventuella bonuspoäng.

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

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

b) Polynomen $\overline{6}x^3 - \overline{1}x + \overline{1}$ och $\overline{5}x + \overline{1}$ är lika i $\mathbb{Z}_3[x]$.

c) Ringarna $\mathbb{Z}_{36}$, $\mathbb{Z}_4 \times \mathbb{Z}_9$ och $\mathbb{Z}_6 \times \mathbb{Z}_6$ är alla isomorfa med varandra.

d) $(m, d) = (44, 3)$ och $(m, e) = (44, 7)$ är ett par av fungerande RSA-nycklar (även om talen m, e, d är för små för att utgöra en *säker* RSA-nyckel).

e) Låt a och b vara två irreducibla element i ett integritetsområde R. Då är ab aldrig ett irreducibelt element.

(10 poäng)

2. **a)** Vad säger Eulers sats?

b) Beräkna $\varphi(44)$.

c) Beräkna $9^{10} \pmod{44}$.

d) Faktorisera $x^5 - x$ i irreducibla faktorer i $\mathbb{Z}_5[x]$.

(5 poäng)

3. Låt R vara en kommutativ ring. Ett element e kallas för idempotent om $e^2 = e$.

a) Visa att $eR = \{er \mid r \in R\} \subseteq R$, där e är idempotent, tillsammans med additionen och multiplikationen från R utgör en ring där det additivt neutrala elementet är 0_R och det multiplikativt neutrala elementet är e.

b) Är eR en delring av R?

(5 poäng)

4. **a)** Återge definitionen av en ringhomomorfism.

b) Ge ett exempel på en ringhomomorfism (som inte är f från Uppgift 6) och visa att ditt exempel är en ringhomomorfism.

c) Visa att det inte finns någon ringhomomorfism mellan $\mathbb{Z}_5$ och $\mathbb{Z}_3$.

(5 poäng)

Fortsätter på nästa sida!

5. Låt R vara en ändlig kommutativ ring, d.v.s. $|R| < \infty$. Låt $I \subseteq R$ vara ett ideal.

a) Varje element i R/I är en ekvivalensklass $a + I$, för något $a \in R$. Visa att alla dessa ekvivalensklasser innehåller lika många element.

b) Visa att $|R/I| = \dfrac{|R|}{|I|}$.

(5 poäng)

6. **a)** Avbildningen $f : \mathbb{Z}_{44} \to \mathbb{Z}_{11}, a+44\mathbb{Z} \mapsto a+11\mathbb{Z}$ är en ringhomomorfism, där $a+n\mathbb{Z}$ betecknar a:s restklass modulo n. Visa att f är surjektiv (d.v.s. en epimorfism) och att $\mathrm{Ker}(f) = \langle 11 + 44\mathbb{Z} \rangle$.

b) Visa att $\mathbb{Z}_{44}/\langle 11 + 44\mathbb{Z}\rangle \cong \mathbb{Z}_{11}$.

c) Visa att $\langle 11 + 44\mathbb{Z}\rangle$ är ett maximalt ideal i $\mathbb{Z}_{44}$.

Du får använda påståendena i de föregående deluppgifterna även om du inte lyckats bevisa dem.

(5 poäng)

7. Faktorisera det Gaussiska heltalet $-30 + 110i$ i irreducibla faktorer. (5 poäng)

Lycka till!

Lösningar till tentamen i Algebra II 2022–03–10

Lösning till problem 1. **a)** Falskt! $\mathbb{Z}[x]$ är inte en huvudidealring, då t.ex. $\langle 2, x\rangle$ inte är ett huvudideal: Varje Euklidisk ring är en huvudidealring, så därför kan inte $\mathbb{Z}[x]$ heller vara en Euklidisk ring.

b) Sant! Två polynom är lika om deras koefficienter är lika. I $\mathbb{Z}_3$ har vi $\overline{6} = \overline{0}$, $\overline{-1} = \overline{5}$ och $\overline{1} = \overline{1}$. Alltså är samtliga koefficienter lika, och polynomen är därmed lika.

c) Falskt! Vi vet att $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ om och endast om $\text{sgd}(m, n)) = 1$. Eftersom $\text{sgd}(6, 6) = 6 > 1$ (och $36 = 6 \cdot 6$) så gäller $\mathbb{Z}_{36} \ncong \mathbb{Z}_6 \times \mathbb{Z}_6$. Däremot gäller $\mathbb{Z}_{36} \cong \mathbb{Z}_4 \times \mathbb{Z}_9$ eftersom $36 = 4 \cdot 9$ och $\text{sgd}(4, 9) = 1$.

d) Falskt! $44 = 2^2 \cdot 11$ är inte kvadratfritt, vilket är ett nödvändigt villkor för m i en RSA-nyckel.

e) Sant! Om a och b är irreducibla så är de framförallt icke-inverterbara. Alltså är ab en produkt av två icke-inverterbara element och kan därför inte vara irreducibelt.

Lösning till problem 2. **a)**

Sats (Eulers sats)**.** Om $\text{sgd}(a, m) = 1$, så har vi

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

b) Eftersom $\text{sgd}(2^2, 11) = 1$ så gäller:

$$\varphi(44) = \varphi(2^2 \cdot 11) = \varphi(2^2) \cdot \varphi(11) = (2^2 - 2^1) \cdot 10 = 20.$$

Här har vi även använt att om p är ett primtal och $k \in \mathbb{Z}_{>0}$ så gäller $\varphi(p^k) = p^k - p^{k-1}$.

c) Eftersom $\text{sgd}(3, 44) = 1$ gäller enligt Eulers sats $9^{10} = (3^2)^{10} = 3^{20} = 3^{\varphi(44)} \equiv 1 \pmod{44}$.

d) Enligt Fermats lilla sats gäller $a^5 \equiv a \pmod 5$ för alla heltal a. Alltså är alla element $\overline{a} \in \mathbb{Z}_5$ ett nollställe till $x^5 - x$. Eftersom $\mathbb{Z}_5[x]$ är ett integritetsområde (då $\mathbb{Z}_5$ är en kropp) så säger Faktorsatsen för integritetsområden att

$$x^5 - x = x(x - \overline{1})(x - \overline{2})(x - \overline{3})(x - \overline{4})g(x)$$

för något $g(x) \in \mathbb{Z}_5[x]$. Men eftersom vi är i ett integritetsområde så gäller

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$$

och vi får därför ekvationen

$$5 = \deg(x^5 - x) = \deg(x(x - \overline{1})(x - \overline{2})(x - \overline{3})(x - \overline{4})) + \deg(g(x)) = 5 + \deg(g(x)).$$

Alltså är $\deg(g(x)) = 0$, vilket betyder att $g(x) = c$ för något $c \in \mathbb{Z}_5$. Men koefficienten framför x^5 i högerledet blir då c, vilket betyder att om vi jämför med högerledet så ser vi att c måste vara lika med 1. Alltså gäller

$$x^5 - x = x(x - \overline{1})(x - \overline{2})(x - \overline{3})(x - \overline{4}).$$

Till sist så ser vi att samtliga faktorer $x - \overline{a}$ är icke-inverterbara eftersom de inverterbara elementen i $\mathbb{Z}_5[x]$ är precis de nollskilda konstanta polynomen. Om $x - \overline{a} = p(x)q(x)$ så måste någon av $p(x)$ och $q(x)$ vara ett nollskilt konstant polynom för att summan av graderna ska bli 0. Men då är något av polynomen $p(x)$ och $q(x)$ inverterbara enligt tidigare kommentar, och alltså är $x - \overline{a}$ irreducibel. Alltså är

$$x^5 - x = x(x - \overline{1})(x - \overline{2})(x - \overline{3})(x - \overline{4})$$

en faktorisering i irreducibla element.

Lösning till problem 3. **a)** Vi börjar med att visa att eR är sluten under addition och multiplikation, så att $+, \cdot$ verkligen är funktioner med definitionsmängd $eR \times eR$ och målmängd eR. Antag att $er, es \in eR$ är två godtyckliga element. Då gäller:

$$er + es = e(r + s) \in eR, \quad er \cdot es = e(ers) \in eR.$$

Nu kan vi kontrollera att alla ringaxiom gäller.

- **i)** Additivt neutralt element: Eftersom $e \cdot 0_R = 0_R$, så gäller $0_R \in eR$. Men då gäller $er + 0_R = er = 0_R + er$ för alla $er \in eR$, eftersom $eR \subseteq R$.
- **ii)** Additivt invers: Eftersom $e \cdot (-r) = -er$, så gäller $-er \in eR$ för alla $er \in R$. Alltså har alla element i eR en additiv invers som ligger i eR.
- **iii)** Additiv associativtitet. Eftersom vi har additiv associativitet för alla element i R, så måste det även gälla för delmängden $eR \subseteq R$.
- **iv)** Additiv kommutativitet. Eftersom vi har additiv kommutativitet för alla element i R, så måste det även gälla för delmängden $eR \subseteq R$.
- **v)** Multiplikativt neutralt element: För varje element $er \in eR$ gäller $e \cdot er = e^2 r = er = e^2 r = er \cdot e$. Alltså är e det multiplikativit neutrala elementet.
- **vi)** Multiplikativ associativtitet. Eftersom vi har multiplikativ associativitet för alla element i R, så måste det även gälla för delmängden $eR \subseteq R$.
- **vii)** Distributivitet: Eftersom vi har distributivitet för alla element i R, så måste det även gälla för delmängden $eR \subseteq R$.

Alltså är alla ringaxiom uppfyllda, och eR är därmed en ring där det additivt neutrala elementet är 0_R och det multiplikativt neutrala elementet är e.

b) eR är endast en delring av R om $e = 1_R$, och då är $eR = R$. I övriga fall, alltså om $e \neq 1_R$, så är det multiplikativt neutrala elementet i eR och R inte samma. Alltså är eR inte en delring av R om $e \neq 1_R$.

Lösning till problem 4. **a)** En ringhomomorfism är en funktion $f : R \to S$ mellan två ringar R och S så att följande gäller för varje $a, b \in R$:

- **i)** $f(a +_R b) = f(a) +_S f(b)$,
- **ii)** $f(a \cdot_R b) = f(a) \cdot_S f(b)$,
- **iii)** $f(1_R) = 1_S$.

b) Låt R vara en godtycklig ring. Då är $\mathrm{Id}_R : R \to R, a \mapsto a$, en ringhomomorfism. Vi ser att $\mathrm{Id}_R(a + b) = a + b = \mathrm{Id}_R(a) + \mathrm{Id}_R(b)$ och $\mathrm{Id}_R(a \cdot b) = a \cdot b = \mathrm{Id}_R(a) \cdot \mathrm{Id}_R(b)$ för alla $a, b \in R$, samt $\mathrm{Id}_R(1_R) = 1_R$. Alltså är Id_R en ringhomomorfism.

c) Antag att $f : \mathbb{Z}_5 \to \mathbb{Z}_3$ är en ringhomomorfism. Vi vet att kärnan är ett ideal, och att $\mathbb{Z}_5$ endast har två ideal då det är en kropp; nollidealet och hela ringen. Men eftersom ettan avbildas på ettan (som ju inte är lika med noll), så ligger inte ettan i kärnan. Alltså måste kärnan vara nollidealet. Det betyder dock att avbildningen är injektiv, och $\mathbb{Z}_5$ är då isomorf med bilden av f, som är en delring av $\mathbb{Z}_3$. Detta är dock omöjligt då $\mathbb{Z}_5$ innehåller fler element än $\mathbb{Z}_3$. Alltså finns det ingen ringhomomorfism från $\mathbb{Z}_5$ till $\mathbb{Z}_{\not\neq}$.

Antag att $f : \mathbb{Z}_3 \to \mathbb{Z}_5$ är en ringhomomorfism. Då måste $1_{\mathbb{Z}_3} = 1 + 3\mathbb{Z}$ avbildas på $1_{\mathbb{Z}_5} = 1 + 5\mathbb{Z}$ och $0_{\mathbb{Z}_3} = 0 + 3\mathbb{Z}$ avbildas på $0_{\mathbb{Z}_5} = 0 + 5\mathbb{Z}$. Men eftersom

$$1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} = 0_{\mathbb{Z}_3},$$

så gäller

$$f(1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3}) = f(0_{\mathbb{Z}_3}) = 0_{\mathbb{Z}_5}.$$

Men samtidigt måste följande gälla:

$$\begin{aligned} f(1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3} + 1_{\mathbb{Z}_3}) &= f(1_{\mathbb{Z}_3}) + f(1_{\mathbb{Z}_3}) + f(1_{\mathbb{Z}_3}) + f(1_{\mathbb{Z}_3}) + f(1_{\mathbb{Z}_3}) + f(1_{\mathbb{Z}_3}) \\ &= 1_{\mathbb{Z}_5} + 1_{\mathbb{Z}_5} + 1_{\mathbb{Z}_5} + 1_{\mathbb{Z}_5} + 1_{\mathbb{Z}_5} + 1_{\mathbb{Z}_5} = 1_{\mathbb{Z}_5}. \end{aligned}$$

Men $1_{\mathbb{Z}_5} \neq 0_{\mathbb{Z}_5}$, så vi har en motsägelse. Alltså finns ingen ringhomomorfism från $\mathbb{Z}_3$ och $\mathbb{Z}_5$. Observera att vi även kan använda ett liknande resonemang för att bevisa att det inte finns någon ringhomomorfism från $\mathbb{Z}_5$ till $\mathbb{Z}_3$.

Lösning till problem 5. **a)** Låt $a \in R$ vara ett godtyckligt element och titta på ekvivalensklassen $a + I$. Ett element b ligger i $a + I$ om och endast om $b - a \in I$, d.v.s. om och endast om det finns ett $c \in I$ så att $b - a = c \Leftrightarrow b = a + c$. Vi kan alltså skriva $a + I = \{a + c \mid c \in I\}$. Observera att det inte förekommer några upprepningar i denna mängd eftersom $a + c = a + d \Rightarrow c = d$. Vi har alltså en bijektion mellan element i $a + I$ och I. Alltså innehåller $a + I$ lika många element som I, d.v.s. $|a + I| = |I|$. Eftersom a valdes godtyckligt gäller detta för alla ekvivalensklasser $a + I$.

b) Vi vet att varje element i R tillhör precis en ekvivalensklass, och varje ekvivalensklass innehåller precis $|I|$ element. Vidare vet vi att antalet ekvivalensklasser är precis antalet element i R/I, eftersom elementen i R/I är precis ekvivalensklasserna. Alltså gäller $|R| = |I| \cdot |R/I|$, eftersom vi delat in alla element i $|R/I|$ mängder, och varje mängd innehåller $|I|$ element. Men då $0 < |I| \leq |R| < \infty$, så kan vi dividera båda sidor i likheten med $|I|$, och vi får då

$$|R/I| = \frac{|R|}{|I|}.$$

Lösning till problem 6. **a)** Vi visar först att f är surjektiv. För varje restklass $a + 11\mathbb{Z} \in \mathbb{Z}_{11}$, så är a ett heltal (som vi kan anta uppfyller $0 \leq a < 11$), och vi har då restklassen $a + 44\mathbb{Z} \in \mathbb{Z}_{44}$ som avbildas på just $a + 11\mathbb{Z} \in \mathbb{Z}_{11}$.

Vi visar sedan att $\operatorname{Ker}(f) \subseteq \langle 11 + 44\mathbb{Z}\rangle$. Ett element $a + 11\mathbb{Z}$ ligger i kärnan om och endast om $a + 11\mathbb{Z} = 0 + 11\mathbb{Z}$. Detta är ekvivalent med att $a \in 11\mathbb{Z}$, alltså att $a = 11b$, för något $b \in \mathbb{Z}$. Om detta gäller så har vi $a + 44\mathbb{Z} = 11b + 44\mathbb{Z} = (11 + 44\mathbb{Z})(b + 44\mathbb{Z}) \in \langle 11 + 44\mathbb{Z}\rangle$. Vi har alltså visat att $\operatorname{Ker}(f) \subseteq \langle 11 + 44\mathbb{Z}\rangle$.

Vi visar till sist att $\langle 11 + 44\mathbb{Z}\rangle \subseteq \operatorname{Ker}(f)$. Antag att $a + 44\mathbb{Z} \in \langle 11 + 44\mathbb{Z}\rangle$. Då finns det $b + 44\mathbb{Z}$ så att $a+44\mathbb{Z} = (11+44\mathbb{Z})(b+44\mathbb{Z}) = 11b+44\mathbb{Z}$. Men vi har $f(a+44\mathbb{Z}) = f(11b+44\mathbb{Z}) = 11b+11\mathbb{Z} = 0 + 11\mathbb{Z}$. Vi har alltså visat att $\langle 11 + 44\mathbb{Z}\rangle \subseteq \operatorname{Ker}(f)$. Därmed gäller $\operatorname{Ker}(f) = \langle 11 + 44\mathbb{Z}\rangle$.

b) Enligt Noethers första isomorfisats så gäller det för varje ringhomomorfism $f : R \to S$ att $R/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$. Vi visade precis att f är surjektiv, och därför gäller $\operatorname{Im}(f) = \mathbb{Z}_{11}$, och vi visade även att $\operatorname{Ker}(f) = \langle 11 + 44\mathbb{Z}\rangle$. Alltså gäller enligt Noethers första isomorfisats att $\mathbb{Z}_{44}/\langle 11 + 44\mathbb{Z}\rangle \cong \mathbb{Z}_{11}$.

c) Vi har en sats som säger att om R är en kommutativ ring och $I \subseteq R$ är ett ideal, så är I maximalt om och endast om R/I är en kropp. Eftersom $\mathbb{Z}_{44}/\langle 11 + 44\mathbb{Z}\rangle \cong \mathbb{Z}_{11}$ och $\mathbb{Z}_{11}$ är en kropp (då 11 är ett primtal), så är även $\mathbb{Z}_{44}/\langle 11+44\mathbb{Z}\rangle$ en kropp (eftersom denna egenskap bevaras under isomorfi). Men det betyder att idealet vi kvotade med, d.v.s. $\langle 11 + 44\mathbb{Z}\rangle$ är ett maximalt ideal.

Lösning till problem 7. Vi börjar med att bryta ut $\operatorname{sgd}(30, 110) = 10$:

$$-30 + 110i = 10(-3 + 11i).$$

Sedan faktoriserar vi den största gemensamma delaren i primtal:

$$10 = 2 \cdot 5.$$

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 $2 \not\equiv 3 \pmod 4$ och $5 \not\equiv 3 \pmod 4$ så vet vi att 2 och 5 kan skrivas som en summa av två kvadrater och vi får därför:

$$2 = 1^2 + 1^2 = (1 + i)(1 - i), \quad 5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i).$$

Eftersom att både $1 + i$ och $1 - i$ har normen 2 som är ett primtal så är dessa faktorer irreducibla. På samma sett ser vi att både $1 + 2i$ och $1 - 2i$ har normen 5 som är ett primtal, så även dessa faktorer är irreducibla. Sammanfattningsvis är faktoriseringen av 10 i irreducibla faktorer följande:

$$10 = (1 + i)(1 - i)(1 + 2i)(1 - 2i).$$

Nu går vi vidare och faktoriserar $-3+11i$. Vi börjar med att faktorisera $N(-3+11i)$ i irreducibla faktorer:

$$N(-3+11i) = (-3)^2 + 11^2 = 9 + 121 = 130 = 2 \cdot 5 \cdot 13 = (1+i)(1-i)(1+2i)(1-2i)(2+3i)(2-3i).$$

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 $q|z \vee \overline{q}|z$. Detta betyder att $-3+11i$ kommer innehålla 3 irreducibla faktorer.

Vi testar först om $1+i$ delar $-3+11i$:

$$\frac{-3+11i}{1+i} = \frac{(-3+11i)(1-i)}{(1+i)(1-i)} = \frac{(-3+11)+(11+3)i}{2} = \frac{8+14i}{2} = 4+7i.$$

Vi ser att $1+i$ delar $-3+11i$ och att kvoten är $4+7i$. Men $4+7i$ är inte irreducibelt eftersom $N(4+7i) = 65$ som inte är ett primtal.

Vi testar nu om $1+2i$ delar $4+7i$:

$$\frac{4+7i}{1+2i} = \frac{(4+7i)(1-2i)}{(1+2i)(1-2i)} = \frac{(4+14)+(7-8)i}{5} = \frac{18-i}{5} \notin \mathbb{Z}[i].$$

Alltså delar $1+2i$ INTE $4+7i$. Vi testar med konjugatet $1-2i$ istället. Observera att vi nu vet att $1-2i$ måste dela $4-7i$.

$$\frac{4+7i}{1-2i} = \frac{(4+7i)(1+2i)}{(1-2i)(1+2i)} = \frac{(4-14)+(7+8)i}{5} = \frac{-10+15i}{5} = -2+3i.$$

Vi ser att $1-2i$ delar $4+7i$ och att kvoten är $-2+3i = -(2-3i)$ är irreducibelt! Vi har alltså:

$$-3+11i = -(1+i)(1-2i)(2-3i).$$

Sammantaget får vi föjande faktorisering i irreducibla faktorer:

$$-30+110i = -(1+i)(1-i)(1+2i)(1-2i)(1+i)(1-2i)(2-3i) = i(1+i)^3(1+2i)(1-2i)^2(2-3i).$$