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

Prov i matematik
MaKand, fristående
Algebra II
2019–06–05

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) Varje kropp är en faktoriell ring.
b) Polynomet $x^4 - 6x + 12$ är ett irreducibelt element i $\mathbb{Z}[x]$.
c) $\{p(x) \in \mathbb{Z}[x] \mid p(0) = 0\}$ är en delring av $\mathbb{Z}[x]$.
d) Om ett reellt polynom saknar nollställen så är det irreducibelt.
e) Mängden av alla jämna heltal är ett ideal i $\mathbb{Z}$.

(10 poäng)

2. Hitta samtliga heltalslösningar till följande system av kongruenser:

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \end{cases}$$

(5 poäng)

3. **a)** Beräkna $\varphi(33)$, där φ är Eulers φ-funktion.
b) Elin behöver hjälp med att skicka och ta emot hemliga meddelanden med hjälp av RSA-kryptering. Hon har valt en offentlig nyckel $(m, e) = (33, 3)$ men har glömt hur hon ska hitta motsvarande hemliga nyckel $(33, d)$. Beräkna d åt Elin.
c) Använd resultatet från antingen a) eller b) för att visa att $a^{21} \equiv a \pmod{33}$ gäller för alla heltal a så att $(a, 33) = 1$.

(5 poäng)

4. Visa att om $\varphi : R \to S$ är en isomorfi så är R faktoriell om och endast om S är faktoriell. Du får anta att du vet att följande gäller:

- R är ett integritetsområde om och endast om S är ett integritetsområde.
- a är irreducibel om och endast om $\varphi(a)$ är irreducibel.
- a är inverterbar om och endast om $\varphi(a)$ är inverterbar.

(5 poäng)

5. **a)** Visa att $\mathbb{Z}_{15}/5\mathbb{Z}_{15} \cong \mathbb{Z}_5$.
b) Visa att $5\mathbb{Z}_{15} \subset \mathbb{Z}_{15}$ är ett maximalt ideal.

(5 poäng)

6. Låt $\mathbb{R}[x]$ vara ringen av reella polynom. Låt I vara idealet $I = \langle 9 - x^2, x^2 + x - 6, 2x + 6 \rangle$.

a) Förklara varför det måste finnas ett reellt polynom $p(x)$ så att $I = \langle p(x) \rangle$.
b) Hitta ett sådant polynom $p(x)$ och visa att $I = \langle p(x) \rangle$.

(5 poäng)

7. Faktorisera det Gaussiska heltalet $315 + 225i$. (5 poäng)

Lycka till!

Lösningar till tentamen i Algebra II 2019–06–05

Lösning till problem 1. **a)** Sant!

Definitionen av en faktoriell ring är följande:

Definition. Vi säger att en ring R är *faktoriell* om R är ett integritetsområde och varje nollskilt icke-inverterbart element $a \in R$ är en produkt av irreducibla element. Denna produkt är unik upp till ordning av faktorerna samt upp till associering.

Varje kropp är ett integritetsområde, och vi har inga nollskilda icke-inverterbara element, alltså är det villkoret trivialt uppfyllt. Alltså är varje kropp faktoriell.

b) Sant!

Vi använder Eisensteins kriterium med $p = 3$:

$$3|a_0, a_0 = 12, \quad 3|a_1, a_1 = (-6), \quad 3|a_2, a_2 = 0, \quad 3|a_3, a_3 = 0, \quad 3 \nmid a_4, a_4 = 1, \quad 3^2 \nmid a_0, a_0 = 12.$$

Satsen (Eisensteins kriterium) ger oss att polynomet är irreducibelt i $\mathbb{Q}[x]$. Eftersom att polynomet är primitivt så är det då även irreducibelt i $\mathbb{Z}[x]$.

c) Falskt!

Sats. Låt R vara en ring och $S \subseteq R$. Då är S en delring om och endast om följande gäller:

(a) $\forall s, t \in S : s + t \in S, s \cdot t \in S, -s \in S$.
(b) $0_R, 1_R \in S$.

Det konstanta polynomet 1 är det multiplikativt neutrala elementet i $\mathbb{R}[x]$, och detta ligger INTE i mängden. Alltså är mängden inte en delring.

d) Falskt!

T.ex. polynomet $(x^2 + 1)(x^2 + 1)$ saknar reella nollställen men det är reducibelt.

e) Sant!

Definition. Låt I vara en icke-tom delmängd av en kommutativ ring R. Vi säger att I är ett *ideal* i R om $a, b \in I, r \in R$ medför att $a + b, ra \in I$.

Mängden är till att börja med icke-tom eftersom att t.ex. 2 är ett jämnt tal och således ligger i mängden. Om vi adderar två jämna tal får vi ett jämnt tal. Om vi multiplicerar ett jämnt tal med ett heltal får vi igen ett jämnt tal.

Lösning till problem 2. Vi noterar först att $7, 4, 3$ är parvis relativt prima vilket innebär att vi får använda Kinesiska restsatsen! Vi ansätter därför en lösning x på följande form:

$$x = 12b_1 + 21b_2 + 28b_3.$$

Om vi sätter in detta i systemet får vi:

$$\begin{cases} 12b_1 + 21b_2 + 28b_3 \equiv 3 \pmod 7 \\ 12b_1 + 21b_2 + 28b_3 \equiv 1 \pmod 4 \\ 12b_1 + 21b_2 + 28b_3 \equiv 2 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} 12b_1 \equiv 3 \pmod 7 \\ 21b_2 \equiv 1 \pmod 4 \\ 28b_3 \equiv 2 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} 5b_1 \equiv 3 \pmod 7 \\ 1b_2 \equiv 1 \pmod 4 \\ 1b_3 \equiv 2 \pmod 3 \end{cases}$$

$$\Leftrightarrow \begin{cases} 3 \cdot 5b_1 \equiv 3 \cdot 3 \pmod 7 \\ b_2 \equiv 1 \pmod 4 \\ b_3 \equiv 2 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} 15b_1 \equiv 9 \pmod 7 \\ b_2 \equiv 1 \pmod 4 \\ b_3 \equiv 2 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} b_1 \equiv 2 \pmod 7 \\ b_2 \equiv 1 \pmod 4 \\ b_3 \equiv 2 \pmod 3 \end{cases}$$

Vi får alltså att

$$x = 12 \cdot 2 + 21 \cdot 1 + 28 \cdot 2 = 101 \equiv 17 \pmod{84}$$

löser systemet. Kinesiska restsatsen ger oss att samtliga lösningar är $x = 17 + 84n$ där $n \in \mathbb{Z}$ (Obs: $84 = 7 \cdot 4 \cdot 3$).

Lösning till problem 3. **a)** Vi vet att om m_1, m_2 är relativt prima så gäller $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$. Då $33 = 3 \cdot 11$ får vi:

$$\varphi(33) = \varphi(3 \cdot 11) = \varphi(3)\varphi(11) = 2 \cdot 10 = 20.$$

b) Vi vet att e, d ska uppfylla $ed \equiv 1 \pmod{\varphi(m)}$. I detta fall ger det oss att d ska uppfylla:

$$3d \equiv 1 \pmod{20}.$$

Vi set att $d = 7$ ger oss

$$3 \cdot 7 = 21 \equiv 1 \pmod{20}.$$

Alltså är $(33, 7)$ motsvarande hemliga nyckel.

c) Låt (m, e) vara en offentlig RSA-nyckel och (m, d) motsvarande hemliga nyckel. Vi vet att för varje heltal a gäller

$$a^{ed} \equiv a \pmod{m}.$$

Alltså får vi från uppgift b) att $ed = 3 \cdot 7 = 21$ och således gäller

$$a^{21} \equiv a \pmod{33}.$$

Alternativt kan vi använda Eulers sats som säger att för varje a som är relativt primt med m gäller

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

Om vi multiplicerar denna ekvation med a på båda sidorna får vi:

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

Eftersom att $\varphi(33) = 20$ så får vi att

$$a^{21} \equiv a \pmod{33}$$

för alla a så att $(a, 33) = 1$.

Lösning till problem 4. Observera att φ är inverterbar (och inversen är en isomorfism), så det räcker att visa att om R är faktoriell implicerar detta att S är faktoriell.

Definitionen av en faktoriell ring är följande:

Definition. Vi säger att en ring R är *faktoriell* om R är ett integritetsområde och varje nollskilt icke-inverterbart element $a \in R$ är en produkt av irreducibla element. Denna produkt är unik upp till ordning av faktorerna samt upp till associering.

Vi får anta att vi vet att R är ett integritetsområde om och endast om S är det. Vi behöver därför endast visa att om R är faktoriell, så kan varje nollskilt icke-inverterbart element i S faktoriseras i irreducibla element. Vi behöver även visa att faktoriseringen är unik upp till ordning och association.

Låt $s \in S$ vara ett godtyckligt nollskilt icke-inverterbart element. Eftersom att φ är surjektiv så finns det ett $r \in R$ så att $\varphi(r) = s$. Eftersom att R är faktoriell så kan vi skriva

$$r = p_1 p_2 \dots p_n$$

där p_i är irreducibel. Men då vet vi att $\varphi(p_i)$ är irreducibel. Eftersom φ är en homomorfism får vi:

$$s = \varphi(r) = \varphi(p_1 p_2 \dots p_n) = \varphi(p_1)\varphi(p_2)\dots\varphi(p_n).$$

Alltså kan s skrivas som en produkt av irreducibla element.

Nu måste vi visa att faktoriseringen är unik upp till ordning och association. Antag att vi har två faktoriseringar:

$$s = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m.$$

Eftersom att φ är en isomofism så finns u_i, $i = 1, \dots, n$ så att $\varphi(u_i) = p_i$ och v_i, $i = 1, \dots, m$ så att $\varphi(v_i) = q_i$. Detta ger oss att

$$\varphi(u_1 u_2 \dots u_n) = \varphi(u_i)\varphi(u_2)\dots\varphi(u_n) = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m = \varphi(v_1)\varphi(v_2)\dots\varphi(v_m) = \varphi(v_1 v_2 \dots v_m).$$

Men φ är bijektiv så detta innebär att

$$u_1 u_2 \dots u_n = v_1 v_2 \dots v_m.$$

Detta är en produkt av irreducibla element i R. Eftersom R är faktoriell så är faktoriseringen unik upp till ordning och association. Det betyder att $n = m$ och vi kan anta att vi ordnat faktorerna så att u_i är associerad med v_i. Alltså finns ett inverterbart element c_i så att $v_i = c_i u_i$. Men detta ger oss att

$$q_i = \varphi(v_i) = \varphi(c_i u_i) = \varphi(c_i)\varphi(u_i) = \varphi(c_i)p_i.$$

Då är c_i är inverterbar så är även $\varphi(c_i)$ det, alltså är q_i associerad med p_i. Detta visar att faktoriseringen är unik upp till ordning och association.

Alltså är S faktoriell om R är det.

Lösning till problem 5. **a)** Låt $\varphi : \mathbb{Z}_{15} \to \mathbb{Z}_5$ ges av $a + 15\mathbb{Z} \mapsto a + 5\mathbb{Z}$. Enligt Problem 1, Inlämningsuppgift 3 så är detta en väldefinierad homomorfism. Denna avbildning är surjektiv så $\mathrm{Im}(\varphi) = \mathbb{Z}_5$.

Vi visar nu att kärnan av denna homomorfism är precis $5\mathbb{Z}_{15}$. Antag att $\varphi(a + 15\mathbb{Z}) = 0$. Det innebär att $a + 5\mathbb{Z} = 0 + 5\mathbb{Z}$, vilket är ekvivalent med att $a \in 5\mathbb{Z}$. Alltså är $a = 5b \in \mathbb{Z}$ och $a + 15\mathbb{Z} = 5b + 15\mathbb{Z} \in 5\mathbb{Z}_{15}$. Nu har vi visat att $\mathrm{Ker}(\varphi) \subseteq 5\mathbb{Z}_{15}$.

Antag istället att $a + 15\mathbb{Z} \in 5\mathbb{Z}_{15}$, då finns det ett $b \in \mathbb{Z}$ så att $a = 5b$. Men detta innebär att $\varphi(a + 15\mathbb{Z}) = \varphi(5b + 15\mathbb{Z}) = 5b + 5\mathbb{Z} = 0$, alltså att $5\mathbb{Z}_{15} \subseteq \mathrm{Ker}(\varphi)$. Detta visar är $\mathrm{Ker}(\varphi) = 5\mathbb{Z}_{15}$.

Noethers första isomorfisats ger oss att

$$\mathbb{Z}_{15}/5\mathbb{Z}_{15} \cong \mathbb{Z}_5.$$

b) Vi vet att för en kommutativ ring gäller det att R/I är en kropp om och endast om $I \subset R$ är ett maximalt ideal. Eftersom $\mathbb{Z}_5$ är en kropp och $\mathbb{Z}_{15}/5\mathbb{Z}_{15} \cong \mathbb{Z}_5$ så är $5\mathbb{Z}_{15}$ ett maximalt ideal.

Lösning till problem 6. **a)** Vi vet att $\mathbb{R}[x]$ är en Euklidisk ring (eftersom $\mathbb{R}$ är en kropp), och alla Euklidiska ringar är huvudidealringar. Detta innebär att alla ideal är huvudideal, dvs på formen $I = \langle p(x) \rangle$ för något reellt polynom $p(x)$.

b) Vi hittar detta $p(x)$ genom att hitta största gemensamma faktor bland polynomen som genererar idealet. Detta är $x + 3$:

$$9 - x^2 = (x + 3)(3 - x), \quad x^2 + x - 6 = (x + 3)(x - 2), \quad 2x + 6 = 2(x + 3).$$

Så varför är $I = \langle x + 3 \rangle$? Jo, vi vet att varje polynom i I är på formen $a(x)(9 - x^2) + b(x)(x^2 + x - 6) + c(x)(2x + 6) = (x + 3)(a(x)(3 - x) + b(x)(x - 3) + c(x)2) \in \langle x + 3 \rangle$. Alltså gäller $I \subseteq \langle x + 3 \rangle$. Nu vill vi visa att $x + 3 \in I$ eftersom att detta implicerar att $\langle x + 3 \rangle \subseteq I$. I detta exempel är det enkelt: låt $c(x) = \frac{1}{2}$ och $a(x) = b(x) = 0$, alla dessa är reella polynom och detta ger oss att $x + 3 \in I$. Alltså gäller $\langle x + 3 \rangle \subseteq I$. Detta ger oss att $I = \langle x + 3 \rangle$.

Vi kan även visa detta mer generellt: Antag att $I = \langle q_1(x), q_2(x), \dots, q_n(x) \rangle$. Låt $p(x)$ vara största gemensamma faktor hos $q_1, q_2, \dots, q_n$. Precis som tidigare ser vi att $I \subseteq \langle p(x) \rangle$. Vi visar sedan att om $r(x)$ är ett nollskilt polynom av minimal grad i I så gäller $I = \langle r(x) \rangle$. Sedan visar vi att $r(x)$ och $p(x)$ är associerade och genererar då samma ideal!

Antag att $r(x)$ är ett nollskilt polynom av minimal grad i I. För ett godtyckligt $a(x) \in I$ har vi:

$$a(x) = b(x)r(x) + c(x)$$

där $c(x) = 0$ eller $\deg(c) < \deg(r)$. Men r hade minimal grad så vi måste ha $c(x) = 0$ och det följer att för varje $a(x) \in I$ gäller $a(x) = b(x)r(x)$. Alltså har vi $I \subseteq \langle r(x) \rangle$. Uppenbarligen gäller $\langle r(x) \rangle \subseteq I$ och vi får $I = \langle r(x) \rangle$.

Eftersom att $\langle r(x) \rangle = I \subseteq \langle p(x) \rangle$ så har vi $r(x) = a(x)p(x)$ för något polynom $a(x)$. Då får vi $\deg(r) = \deg(a) + \deg(p)$ vilket betyder att $\deg(a) = 0$ på grund av minimaliteten hos granden av r. Detta innebär att $a(x)$ är konstant (samt nollskilt) och sådeles inverterbar. Alltså är $r(x)$ och $p(x)$ associerade. Detta innebär att I genereras av $p(x)$, vilket var den största gemensamma faktorn hos de ursprungliga generatorerna.

Lösning till problem 7. Vi börjar med att bryta ut $(315, 225) = 45$:

$$315 + 225i = 45(7 + 5i).$$

Sedan faktoriserar vi den största gemensamma delaren i primtal:

$$45 = 3^2 \cdot 5.$$

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 $3 \equiv 3 \pmod 4$ så är 3 irreducibelt i $\mathbb{Z}[i]$, medan $5 \not\equiv 3 \pmod 4$. Då vet vi dock att 5 kan skrivas som en summa av två kvadrater och vi får därför:

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

Eftersom att både $1 + 2i$ och $1 - 2i$ har normen 5 som är ett primtal så är dessa faktorer irreducibla. Sammanfattningsvis är faktoriseringen av 45 i irreducibla faktorer följande:

$$45 = 3^2(1 + 2i)(1 - 2i).$$

Nu går vi vidare och faktoriserar $7+5i$. Vi börjar med att faktorisera $N(7+5i)$ i irreducibla faktorer:

$$N(7 + 5i) = 7^2 + 5^2 = 49 + 25 = 74 = 2 \cdot 37 = (1 + i)(1 - i)(1 + 6i)(1 - 6i).$$

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 $1 - i$ delar $7 + 5i$:

$$\frac{7 + 5i}{1 - i} = \frac{(7 + 5i)(1 + i)}{(1 - i)(1 + i)} = \frac{(7 - 5) + (7 + 5)i}{2} = \frac{2 + 12i}{2} = 1 + 6i.$$

Vi ser att $1 - i$ delar $7 + 5i$ och att kvoten $1 + 6i$ är irreducibel! Vi har alltså:

$$7 + 5i = (1 - i)(1 + 6i).$$

Sammantaget får vi föjande faktorisering i irreducibla faktorer:

$$315 + 225i = 3^2(1 + 2i)(1 - 2i)(1 - i)(1 + 6i).$$