UPPSALA UNIVERSITET
Matematiska institutionen
Original av Isac Hedén,
Reviderad av Elin Persson Westin,
elin.persson.westin@math.uu.se

Övningsuppgifter
Algebra II
VT2022

Nedan finns ett antal uppgifter som behandlar det vi pratat om på föreläsningarna. Känn inte att du behöver räkna alla uppgifter, utan fokusera på de ***rekommenderade uppgifterna*** *vilka är markerade med* ***fet stil****.*

Lektion 1 - Talteori, kongruenser och Kinesiska restsatsen

1. Bestäm det största icke-negativa heltalet n för vilket

   (a) $2^n|360$ (b) $3^n|360$ (c) $5^n|360$ (d) $7^n|360$.

2. Låt n vara ett heltal. Visa att $15|n \Leftrightarrow (3|n$ och $5|n)$

3. Bestäm med hjälpa av Euklides algoritm största gemensamma delaren till

   (a) 512 och 299 (b) 1079 och 611.

4. Visa att produkten av

   (a) två konsekutiva heltal är delbar med 2
   (b) tre konsekutiva heltal är delbar med 6
   (c) fyra konsekutiva heltal är delbar med 24.

5. Bestäm primfaktoriseringen av

   (a) 360 (b) 271 (c) 2981 (d) 10^{20} (e) 10!.

6. Bestäm den största potensen av 15 som delar 60!.

7. Ett primtal (skrivet som decimaltal) har alla siffror lika med 1. Visa att antalet ettor är ett primtal.

8. Visa att inget kvadrattal är av formen $4n + 2$ eller $4n + 3$.

9. Visa att varje positivt heltal på formen $4k + 3$ har en primfaktor av samma form.

10. Visa att det finns oändligt många primtal som har formen $4k + 3$.

11. Visa att decimalutvecklingen av ett rationellt tal förr eller senare blir periodisk.

12. Visa att om $a \equiv b \pmod{p}$ för varje primtal p, så är $a = b$.

13. Ge enkla kriterier för att ett heltal n ska vara delbart med

(a) 2 (b) 3 (c) 4 (d) 5 (e) 6 (f) 8 (g) 9 (h) 11.

14. Visa att talet
$$S_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$
inte är ett heltal för något $n > 1$.

15. Visa att n är en heltalskvadrat om och endast om varje exponent a_i är jämn i den kanoniska primfaktoriseringen $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$.

16. Vilka tal n, där $1 \leq n \leq 20$, är kongruenta med 45 modulo

(a) 9 (b) 10 (c) 11 (d) 30 (e) 40 (f) 50.

17. För vilka tal $m \geq 2$ gäller

(a) $20 \equiv 13 \pmod{m}$ (b) $20 \equiv -13 \pmod{m}$ (c) $25 \equiv 13 \pmod{m}$.

18. Visa att kongruensen $x^2 \equiv x \pmod{m}$ endast har lösningarna $x \equiv 0$ och $x \equiv 1 \pmod{m}$, om m är

(a) ett primtal (b) en primtalspotens.

19. För vilka $n \geq 2$ gäller

(a) $1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 \equiv 0 \pmod{n}$
(b) $1^3 + 2^3 + 3^3 + \ldots + (n-1)^3 \equiv 0 \pmod{n}$?

20. Bestäm slutsiffran i

(a) 3^{60} (b) 2^{60} (c) 57^{57}.

21. Bestäm de två sista sifforna i

(a) 3^{60} (b) 2^{60} (c) 57^{57}.

22. Hur många nollor slutar 169! på?

23. Sätt $S_n = 1 + 2 + 3 + \ldots + (n-1)$ för $n \geq 2$.

(a) Visa att $S_n \equiv 0 \pmod{n}$, om n är udda.

(b) Bestäm huvudresten av S_n modulo n om n är jämnt, dvs. bestäm den minsta icke-negativa resten då S_n divideras med n.

24. Visa att det för varje $k \geq 1$ finns k konsekutiva heltal, som vart och ett är delbart med en heltalskvadrat > 1.

25. Bestäm lösningarna till följande system av kongruenser
$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{7} \\ x \equiv 7 \pmod{12} \end{cases}$$

26. Bestäm lösningarna till följande system av kongruenser

(a) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 5 \pmod{7} \\ x \equiv 7 \pmod{15} \end{cases}$ (b) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 5 \pmod{7} \\ x \equiv 8 \pmod{15} \end{cases}$ (c) $\begin{cases} 2x \equiv 3 \pmod{9} \\ 4x \equiv 6 \pmod{10} \\ 6x \equiv 9 \pmod{11} \end{cases}$

Lektion 2 - Eulers och Fermats satser, RSA

27. Bestäm $\varphi(n)$ för $n = 1, 2, 3, \ldots, 10$.

28. Skriv upp ett

(a) fullständigt (b) reducerat

restklassystem modulo 20.

29. Låt $\mathcal{R}(m) = \{s_1, s_2, \ldots, s_{\varphi(m)}\}$ beteckna ett reducerat restklassystem modulo m. Visa att om $(a, m) = 1$, så är även $\{as_1, as_2, \ldots, as_{\varphi(m)}\}$ ett reducerat restklassystem modulo m.

30. Lös kongruensen $7x \equiv 11 \pmod{20}$ med hjälp av Eulers sats.
Ledning: Beräkna $\varphi(20)$. Multiplicera båda leden med 7^7.

31. För vilka n är $\varphi(n)$ udda?

32. Visa att för varje $x \geq 1$ har x och x^5 samma slutsiffra (i decimalsystemet).

33. Vilka positiva heltal n satisfierar $\varphi(2n) = \varphi(n)$?

34. Bestäm alla naturliga tal n för vilka $\varphi(n) = 24$.

35. Visa att om $a \equiv b \pmod{m}$, så är $\text{sgd}(a, m) = \text{sgd}(b, m)$.

36. Låt $a_1, a_2, \ldots, a_k$ vara ett

(a) fullständigt (b) reducerat

restklassystem modulo n. Bestäm huvudresten av $a_1 + a_2 + \ldots + a_k$ modulo n.

37. Låt p vara ett primtal. Visa att om $a^p \equiv b^p \pmod{p}$, så är $a^p \equiv b^p \pmod{p^2}$.

38. Hur många av talen a, $1 \leq a \leq 100$, satisfierar villkoret

(a) $\text{sgd}(a, 100) = 1$ (b) $\text{sgd}(a, 100) > 1$ (c) $\text{sgd}(a, 100) = 2$?

39. Hur många av talen a, $1 \leq a \leq n$, satisfierar $\text{sgd}(a, n) = d$, där d är en positiv delare till n?

40. Visa att för $n > 1$ är $\sum a = \frac{1}{2}n \cdot \varphi(n)$, där summationen utsträcks över alla a sådana att $1 \leq a \leq n$ och $\text{sgd}(a, n) = 1$.

41. Låt p vara ett primtal.

(a) Visa med hjälp av Fermats sats att $(a + b)^p \equiv a^p + b^p \pmod{p}$.
(b) Visa att $(a + b)^p \equiv a^p + b^p \pmod{p}$ utan att använda Fermats sats.
(c) Visa att $a^p \equiv a \pmod{p}$, dvs. Fermats sats, med hjälp av (b).

42. Vilka positiva tal n satisfierar

(a) $\varphi(n) = \frac{1}{3}n$ (b) $\varphi(n) = \frac{2}{7}n$?

43. Vilket är det minsta

(a) positiva tal n (b) positiva jämna tal n,

för vilket $\varphi(x) = n$ saknar lösning x?

44. Visa att för givet n har ekvationen $\varphi(x) = n$ endast ändligt många lösningar.

45. Visa att talen $a, 2a, 3a, \ldots, na$ bildar ett fullständigt restklassystem modulo n om $\text{sgd}(a, n) = 1$.

46. En pojke har ett antal kulor som är mindre än 100. När han delar dem i tre högar med lika många kulor i varje blir det en kula över, när han delar dem i fyra högar blir det två kulor över, och när han delar dem i fem högar blir det tre kulor över. Hur många kulor har han?

47. Beräkna

    (a) $\varphi(100)$ (b) $\varphi(10!)$

48. Välj i detta lilla testexempel för RSA-algoritmen $p = 11$ och $q = 13$ så att $m = pq = 143$. Välj vidare krypteringsnyckeln $e = 77$

    (a) Beräkna dekrypteringsnyckeln d.

    (b) Kryptera talet 50 och verifiera att det återfås vid dekryptering.

49. Skriv upp en till $20x^3 + 15x^2 + 12x + 4 \equiv 0 \pmod{m}$ ekvivalent polynomkongruens genom att reducera koefficienterna, om m är lika med

    (a) 2 (b) 3 (c) 4 (d) 5 (e) 11.

50. Skriv upp en till $x^9 + 2x^7 + 3x^4 + 4x^2 + 5x + 6 \equiv 0 \pmod{p}$ ekvivalent polynomkongruens genom att reducera graden och även koefficienterna, om p är lika med

    (a) 2 (b) 3 (c) 5.

51. Visa att alla heltal x satisfierar $x^{42} + 40x^2 \equiv 0 \pmod{41}$.

Lektion 3 - Ringar och olika egenskaper

52. Beräkna följande produkter i den angivna ringen.

(a) $20 \cdot (-8)$ i $\mathbb{Z}_{26}$ (b) $(2,3) \cdot (3,5)$ i $\mathbb{Z}_5 \times \mathbb{Z}_9$.

53. Avgör för var och en av följande mängder tillsammans med de angivna additions- och multiplikationsreglerna om de utgör en ring eller inte. Om de inte utgör en ring, varför inte? Om de utgör en ring, är den kommutativ? är den en kropp? är den ett integritetsområde?

(a) $\mathbb{Z}^+$, de positiva heltalen, med de vanliga operationerna.

(b) $\mathbb{Z} \times \mathbb{Z}$, med de komponentvisa operationerna.

(c) $\{a + b\sqrt{2} \mid \ a, b \in \mathbb{Z}\}$ med de vanliga operationerna.

(d) $\{a + b\sqrt{2} \mid \ a, b \in \mathbb{Q}\}$ med de vanliga operationerna.

(e) Mängden av rent imaginära komplexa tal $\{ri \mid r \in \mathbb{R}\}$ med de vanliga operationerna.

54. Är följande ring ett integritetsområde?

$$\mathbb{Z}_5[i] = \{a + bi \mid a, b \in \mathbb{Z}_5 \text{ och } i^2 = -1\}$$

55. Ringen $M_3(\mathbb{R})$ består av 3×3-matriser med reella koefficienter. Ta en titt på följande lösningsförslag till ekvationen $X^2 = I$ i $M_3(\mathbb{R})$, där I betecknar enhetsmatrisen i $M_3(\mathbb{R})$, dvs. matrisen med 1:or på diagonalen och 0:or på de andra platserna. $X^2 = I$ medför $X^2 - I = 0$, så $(X + I)(X - I) = 0$. Alltså gäller endera $X = I$ eller $X = -I$. Är lösningen korrekt? Om den inte är det, berätta vad som gick snett och ge exempel på någon annan matris X sådan att $X^2 = I$.

56. Hitta alla lösningar till ekvationen $x^2 + x - 6 = 0$ i $\mathbb{Z}_{14}$ genom att först faktorisera polynomet. Jämför med föregående uppgift.

57. Ett element a i en ring R kallas för idempotent om $a^2 = a$.

(a) Visa att mängden av idempotenta element i en kommutativ ring är multiplikativt sluten.

(b) Hitta alla idempotenta element i ringen $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

(c) Vad kan vi säga om ett idempotent element i ett integritetsområde?

58. Visa att matrisen

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$$

är en nolldelare i $M_2(\mathbb{Z})$.

59. I vilka av ringarna $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_{20}$ och $\mathbb{Z}_{15}$ medför likheten $2x = 2y$ att $x = y$?

60. Bestäm inverserna till $2, 3$, och 6 i $\mathbb{Z}_7$.

61. Låt R vara en kommutativ ring. Visa att mängden $U(R)$ av inverterbara element är multiplikativt sluten.

62. Låt S vara delmängden $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ av $\mathbb{R}$. Visa att S är ett integritetsområde. Är S en kropp?

63. Låt S vara delmängden $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ av $\mathbb{R}$. Visa att S är en kropp.

64. Låt S vara delmängden $\{a + b\sqrt{6} \mid a, b \in \mathbb{Q}\}$ av $\mathbb{R}$. Är S en kropp?

65. Låt $\mathbb{Z}_3[i] = \{a+bi \mid a, b \in \mathbb{Z}_3 \text{ och } i^2 = -1\}$. Addition och multiplikation i den här mängden utförs som om elementen vore polynom i variablen i, varpå man ersätter i^2 med -1, och reducerar koefficienterna modulo 3. Visa att $\mathbb{Z}_3[i]$ är en kropp. Vad är den multiplikativa inversen till $2 + i$? Lös ekvationen $(2 + i)x = 1 + 2i$ i $\mathbb{Z}_3[i]$.

66. Vilka inverterbara element finns det i följande ringar?

(a) $\mathbb{Z}$ (b) $\mathbb{Z} \times \mathbb{Z}$ (c) $\mathbb{Q}$ (d) $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ (e) $\mathbb{Z}_4$.

67. Bestäm inverserna till $3, 23, 24$, och 32 i $\mathbb{Z}_{47}$.

Lektion 4 - Bråkkroppar, karakteristik och olika typer av element

68. Beräkna bråkkroppen av följande ringar i de fall denna existerar. Om bråkkroppen inte existerar, förklara varför.

(a) $\mathbb{Z}$ (b) $\mathbb{Z} \times \mathbb{Z}$ (c) $\mathbb{Z}_3$ (d) $\mathbb{R}$ (e) $\mathbb{Z}_{57}$ (f) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

69. Beräkna bråkkroppen av följande ringar i de fall denna existerar. Om bråkkroppen inte existerar, förklara varför.

(a) $\mathbb{R} \times \mathbb{R}$ (b) $\mathbb{Z}[i]$ (c) $\mathbb{Q}[i]$ (d) $\mathbb{Z}_3[i]$ (e) $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$

(f) $\{\frac{a + b\sqrt{-3}}{2} \mid a, b \in \mathbb{Z},$ där både a och b är båda jämna eller båda udda$\}$

70. Bestäm karaktäristiken för följande ringar.

(a) $\mathbb{Z}_3 \times \mathbb{Z}_3$ (b) $\mathbb{Z}_3 \times \mathbb{Z}_4$ (c) $\mathbb{Z}_6 \times \mathbb{Z}_{15}$.

71. Låt R vara en kommutativ ring, med karaktäristik 3. Beräkna och förenkla $(a + b)^9$, för $a, b \in R$.

72. Är följande påståenden sanna eller falska?

(a) Varje kropp är ett integritetsområde.

(b) Varje kropp som har karaktäristik 0 innehåller oändligt många element.

(c) Den kartesiska produkten av två integritetsområden är ett integritetsområde.

(d) En nolldelare i en kommutativ ring kan inte ha någon multiplikativ invers.

(e) $\mathbb{Z}$ är en delkropp till $\mathbb{Q}$.

73. Visa att karaktäristiken för en kropp måste vara endera ett primtal eller 0.

74. Låt D vara ett integritetsområde av karaktäristik p, där p är ett primtal. Visa att följande gäller för alla $a, b \in D$, och $n \in \mathbb{N}$

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Kan du generalisera detta resultat, så att det blir giltigt även för fler termer? Vad blir $(a + b + c)^{p^n}$? $(a_1 + \ldots + a_k)^{p^n}$?.

75. Visa att i ringen

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

så är 5 ett primelement, men 7 är inte ett primelement.

76. Vilka är de irreducibla elementen i $\mathbb{R}[x]$?

Lektion 5 - Faktoriella ringar och polynomringar

77. Antag att R är en faktoriell ring. Låt a, b, c vara element i R. Visa att följande är sant:

(a) Om $c|ab$ och $\text{sgd}(a, c) = 1$, då gäller $c|b$.
(b) Om $a|c$, $b|c$ och $\text{sgd}(a, b) = 1$, då gäller $ab|c$.
(c) Om $\text{sgd}(a, c) = 1 = \text{sgd}(b, c)$, så gäller $\text{sgd}(ab, c) = 1$.
(d) Om $c|a$ och $c|b$, då gäller $c \cdot \text{sgd}(a/c, b/c) = \text{sgd}(a, b)$.
(e) Om m, n är positiva heltal då är $\text{sgd}(a, b) = 1$ om och endast om $\text{sgd}(a^m, b^n) = 1$.
(f) $\text{sgd}(a, b)\text{mgm}(a, b)$ är associerad med ab.
(g) $\text{sgd}(a, b, c) = \text{sgd}(a, \text{sgd}(b, c))$ och $\text{mgm}(a, b, c) = \text{mgm}(a, \text{mgm}(b, c))$.

78. Har polynomekvationen $x^2 + x + 4 = 0$ någon lösning i $\mathbb{Z}_5$? Samma fråga för $\mathbb{Z}_7$.

79. Hitta alla nollställen till följande polynom i $\mathbb{Z}_7[x]$, och faktorisera dem så långt som möjligt.

(a) $x^2 + x + 2$ (b) $x^2 + 2x + 4$ (c) $x^2 + x + 3$ (d) $x^6 - 1$.

80. Låt F vara en kropp. Vilka är de inverterbara elementen i polynomringen $F[x]$?

81. Hitta alla nollställen till $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44} \in \mathbb{Z}_5[x]$.

82. Ge exempel på ett inverterbart polynom i $\mathbb{Z}_4[x]$ av grad > 0.

83. Är $x^3 + 2x + 3$ irreducibelt i $\mathbb{Z}_5[x]$? Faktorisera det i irreducibla faktorer annars.

84. Hitta alla irreducibla polynom i $\mathbb{Z}_3[x]$ av grad

(a) 2 (b) 3.

85. Låt p vara ett primtal. Visa att $x^p + a \in \mathbb{Z}_p[x]$ inte är irreducibelt för något $a \in \mathbb{Z}_p$.

86. Visa att följande polynom är irreducibla i $\mathbb{Q}[x]$

(a) $x^3 + 9$ (b) $x^3 + 9x^2 + 24x + 19$.

87. Låt R vara ett integritetsområde. Vilka är de inverterbara elementen i $R[x]$?

88. Hitta polynom $q(x)$ och $r(x)$ enligt divisionsalgoritmen sådana att $f(x) = g(x)q(x) + r(x)$ där $r(x)$ antingen är nollpolynomet eller ett polynom av grad mindre än g:s grad.

(a) $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ och $g(x) = x^2 + 2x - 3$ i $\mathbb{Z}_7[x]$
(b) $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ och $g(x) = 3x^2 + 2x - 3$ i $\mathbb{Z}_7[x]$
(c) $f(x) = x^5 - 3x^4 + 3x - 5$ och $g(x) = 3x + 2$ i $\mathbb{Z}_{11}[x]$
(d) $f(x) = x^4 + 5x^3 - 3x^2$ och $g(x) = 5x^2 - x + 2$ i $\mathbb{Z}_{11}[x]$

89. Skriv polynomet $x^4 + 4$ som en produkt av linjära polynom i $\mathbb{Z}_5[x]$.

90. Skriv polynomet $2x^3 + 3x^2 - 7x - 5$ som en produkt av linjära polynom i $\mathbb{Z}_{11}[x]$.

91. Visa att polynomet x^2+8x-2 är irreducibelt sett som ett element i $\mathbb{Q}[x]$. Är det irreducibelt även sett som ett element i $\mathbb{R}[x]$? $\mathbb{C}[x]$?

92. Vilka av följande påståenden är sanna respektive falska?

(a) $x - 2$ är irreducibelt över $\mathbb{Q}$ (dvs. sett som element i $\mathbb{Q}[x]$).

(b) $3x - 6$ är irreducibelt över $\mathbb{Q}$.

(c) $x^2 - 3$ är irreducibelt över $\mathbb{Q}$.

(d) Om K är en kropp, så är de inverterbara elementen i $K[x]$ precis de nollskilda elementen i K.

(e) Ett polynom $f(x) \in K[x]$ av grad n kan högst ha n nollställen om K är en kropp.

(f) Varje förstagradspolynom i $K[x]$ har minst ett nollställe i kroppen K.

(g) Varje polynom i $K[x]$ kan ha högst ändligt många nollställen i K om K är en kropp.

Lektion 6 - Homomorfismer och isomorfismer samt Kinesiska restsatsen som ringisomorfi

93. Låt R, S och T vara tre ringar, och låt $f : R \longrightarrow S$ respektive $g : S \longrightarrow T$ vara ringhomomorfismer. Visa att sammansättningen $g \circ f$ är en ringhomomorfism från R till T.

94. Låt R vara ringen av 2×2-matriser på formen

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Visa att funktionen

$$a + ib \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

är en isomorfism från $\mathbb{C}$ till R.

95. Är funktionen $f : \mathbb{Z}_9 \longrightarrow \mathbb{Z}_{12}, x \mapsto 4x$ väldefinierad? Är en ringhomomorfism?

96. Visa att om $f : R \to S$ är en ringhomomorfism så avbildas inverterbara element på inverterbara element.

97. Visa att om $f : R \to S$ är en monomorfism så avbildas nolldelare på nolldelare.

98. Visa att om $f : R \to S$ är en isomorfism så är a irreducibelt om och endast om $f(a)$ är irreducibelt.

99. Visa att om $f : R \to S$ är en isomorfism så är a ett primelement om och endast om $f(a)$ är ett primelement.

100. Finns det någon ringhomomorfism $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_{10}$? Använd att f bestäms entydigt av $f(1)$.

101. Visa att om R och S är två isomorfa ringar så gäller följande:

(a) R är kommutativ om och endast om S är kommutativ.

(b) R är ett integritetsområde om och endast om S är ett integritetsområde.

(c) R är en kropp om och endast om S är en kropp.

(d) R är en faktoriell ring om och endast om S är en faktoriell ring.

102. Låt R vara en ring av karaktäristik p, där p är ett primtal. Visa att $\varphi_p : R \longrightarrow R, a \mapsto a^p$ är en homomorfism (den kallas för Frobeniushomomorfismen).

103. Låt R vara en ring och $a \in R$. Visa att $R[x] \longrightarrow R[x],\ f(x) \mapsto f(x + a)$ är en isomorfism.

104. Låt R vara en ring. Visa att ett polynom $p \in R[x]$ har en rot $a \in R$ om och endast om $p(x) = (x - a) \cdot h(x)$ för något $h(x) \in R[x]$.

105. Låt K vara en kropp. Visa att $K[x] \cong K[x^2]$.

106. Vilka av följande ringar är isomorfa?

(a) $\mathbb{Z}_{45}$ och $\mathbb{Z}_5 \times \mathbb{Z}_9$.

(b) $\mathbb{Z}_{30}$ och $\mathbb{Z}_3 \times \mathbb{Z}_{10}$.

(c) $\mathbb{Z}_{24}$ och $\mathbb{Z}_7 \times \mathbb{Z}_3$.

(d) $\mathbb{Z}_{45}$ och $\mathbb{Z}_{15} \times \mathbb{Z}_3$.

107. Skriv följande ringar på formen $\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$ där k_i är så stor som möjligt.

(a) $\mathbb{Z}_{245}$ (b) $\mathbb{Z}_{75} \times \mathbb{Z}_{14}$ (c) $\mathbb{Z}_{150} \times \mathbb{Z}_{25}$ (d) $\mathbb{Z}_{99} \times \mathbb{Z}_{18} \times \mathbb{Z}_{12}$ (e) $\mathbb{Z}_{27} \times \mathbb{Z}_{25}$

108. Låt $m, n \in \mathbb{N}$ vara två naturliga tal som är relativt prima. Visa att $\mathbb{Z}_{mn}$ är isomorf med $\mathbb{Z}_m \times \mathbb{Z}_n$.

Lektion 7 - Ideal

109. Låt X vara en icke-tom delmängd av en kommutativ ring R. Visa att

$$A = \{a \in R \mid xa = 0 \text{ för alla } x \in X\}$$

är ett ideal i R.

110. Låt R vara en ring och $a \in R$. Visa att

$$\{na + xa \mid n \in \mathbb{Z}, x \in R\}$$

är ett ideal i R som innehåller a.

111. Låt R och S vara två ringar, och $f : R \longrightarrow S$ en homomorfism. Låt I vara ett ideal i S. Visa att den inversa bilden $f^{-1}(I)$ av I är ett ideal i R. Eller med andra ord: Visa att delmängden

$$\{x \in R \mid f(x) \in I\}$$

i R är ett ideal.

112. Låt R och S vara två ringar, och $f : R \longrightarrow S$ en surjektiv homomorfism. Låt I vara ett ideal i R. Visa att bilden av I är ett ideal i S. Med andra ord: Visa att delmängden

$$\{y \in S \mid y = f(x) \text{ för något } x \in I\}$$

är ett ideal i S.

113. Låt R vara en ring, och S en delring av R. Låt I vara ett ideal i R. Visa att

$$S + I = \{x + a \mid x \in S, a \in I\}$$

är en delring av R och att

$$I \cap S$$

är ett ideal i S.

114. Låt $\varphi : A \longrightarrow B$ vara en ringhomomorfism, och låt $\mathfrak{p} \subset B$ vara ett primideal. Visa att $\varphi^{-1}(\mathfrak{p}) \subset A$ är ett primideal.

115. Låt $\varphi : A \longrightarrow B$ vara en ringhomomorfism; vi definierar $\ker(\varphi)$ som $\{a \in A \mid \varphi(a) = 0\}$. Visa att $\ker(\varphi)$ är ett ideal, samt att φ är injektiv om och endast om $\ker(\varphi) = \{0\}$.

116. Vilka av följande påståenden är sanna?

(a) $\mathbb{Q}$ är ett ideal i $\mathbb{R}$.

(b) En ringhomomorfism $\varphi : R \longrightarrow S$ avbildar ideal på ideal.

(c) Låt R vara en ring och I ett ideal i R. Då är I en delring av R.

(d) Låt R vara en ring. Varje delring av R är ett ideal i R.

(e) Ett ideal I i en ring R är ett äkta ideal om och endast om $1 \notin I$.

117. Låt R vara en ring. Hitta ett nödvändigt och tillräckligt villkor för att unionen av två ideal I och I' ska vara ett ideal.

118. Låt K vara en kropp och R en nollskild ring. Visa att varje homomorfism $\varphi : K \longrightarrow R$ är injektiv.

119. Visa att om $\{I_\gamma\}_{\gamma\in\Gamma}$ är en familj av ideal i en ring R, så är deras snitt

$$\bigcap_{\gamma\in\Gamma} I_\gamma$$

också ett ideal i R.

120. Hitta alla primideal och maximala ideal i

(a) $\mathbb{Z}_6$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_2 \times \mathbb{Z}_2$

(d) $\mathbb{Z}_2 \times \mathbb{Z}_4$

121. Låt K vara en kropp. Visa att idealet $\langle p(x)\rangle \subset K[x]$ är ett maximalt ideal om och endast om $p(x)$ är irreducibelt.

122. Vilka av följande påståenden är sanna?

(a) Varje primideal i varje ring är ett maximalt ideal.

(b) Varje maximalt ideal i varje ring är ett primideal.

(c) Varje kropp med karakteristik 0 har en delkropp som är isomorf med $\mathbb{Q}$

(d) Låt K vara en kropp. Eftersom K inte har några nolldelare måste varje ideal i $K[x]$ vara ett primideal.

(e) Låt K vara en kropp. Varje ideal i $K[x]$ är ett huvudideal, dvs. är på formen $\{ak \mid k \in K\}$ för något $a \in K$.

(f) Låt K vara en kropp. Varje huvudideal i $K[x]$ är ett maximalt ideal.

123. Hitta ett maximalt ideal i $\mathbb{Z} \times \mathbb{Z}$.

124. Hitta ett primideal i $\mathbb{Z} \times \mathbb{Z}$ som inte är ett maximalideal.

125. Hitta ett icke-trivialt äkta ideal i $\mathbb{Z} \times \mathbb{Z}$ som inte är ett primideal.

126. Visa att idealet $\langle 3x, 2\rangle$ inte är ett huvudideal i ringen $\mathbb{Z}[x]$.

127. Vilka av följande mängder är ideal i $\mathbb{Z}[X]$?

(a) $\{f \in \mathbb{Z}[X] \mid f(3) = 0\}$

(b) $\{f \in \mathbb{Z}[X] \mid f$ har ingen linjär term, dvs. koefficienten för X är $0\}$

(c) $\{f \in \mathbb{Z}[X] \mid$ Summan av f:s koefficienter är delbar med $3\}$

(d) $\{f \in \mathbb{Z}[X] \mid f(0)$ är delbart med $2\}$

(e) $\{f \in \mathbb{Z}[X] \mid \deg(f) = 7\}$

(f) $\{f \in \mathbb{Z}[X] \mid \deg(f) \geq 7\}$

Lektion 8 - Kvotringar

128. Visa att om K är en kropp, och $I \subset K$ ett äkta ideal, så är $K/I \simeq K$.

129. Låt $\varphi : A \longrightarrow B$ vara en ringhomomorfism, och $I \subset A$ resp. $J \subset B$ två ideal. Visa att om $\varphi(I) \subset J$ så definierar φ en ringhomomorfism

$$\begin{array}{rcl} \overline{\varphi} : A/I & \longrightarrow & B/J \\ \overline{a} & \mapsto & \overline{\varphi(a)}. \end{array}$$

130. Låt R vara en ring, och $I \subset R$ ett ideal. Låt $\pi : R \longrightarrow R/I$ beteckna den naturliga kvotprojektionen, som avbildar $r \in R$ på $\overline{r} \in R/I$. Visa att π inducerar en 1:1-korrespondens mellan idealen i R som innehåller I, och idealen i R/I.

131. Låt R vara en ring, låt $I \subset R$ ett ideal, och låt π beteckna den naturliga kvotprojektionen $R \longrightarrow R/I$. Låt J vara ett ideal i R som innehåller I, och låt slutligen $J/I = \pi(J)$, dvs. J/I är bilden av J under kvotprojektionen. Eftersom π är surjektiv, vet vi att J/I är ett ideal i R/I, och vi kan därför bilda kvotringen $(R/I)/(J/I)$. Noethers andra isomorfisats säger att

$$(R/I)/(J/I) \simeq R/J,$$

visa detta. Tips: använd Noethers första isomorfisats.

132. Visa med ett exempel att om R är en ring med nolldelare, och $I \subset R$ ett ideal, så kan det ändå hända att R/I är ett integritetsområde.

133. Visa med ett exempel att om R är ett integritetsområde, och $I \subset R$ ett ideal, så kan R/I vara en kropp.

134. Visa med ett exempel att om R är ett integritetsområde, och $I \subset R$ ett ideal, så kan R/I ha nolldelare.

135. Hitta alla $c \in \mathbb{Z}_3$ sådana att

(a) $\mathbb{Z}_3[x]/\langle x^2 + c\rangle$ är en kropp.
(b) $\mathbb{Z}_3[x]/\langle x^3 + x^2 + c\rangle$ är en kropp.
(a) $\mathbb{Z}_3[x]/\langle x^3 + cx^2 + 1\rangle$ är en kropp.

136. Hitta alla $c \in \mathbb{Z}_5$ sådana att $\mathbb{Z}_5[x]/\langle x^2 + x + c\rangle$ är en kropp.

137. Är $\mathbb{Q}[x]/\langle x^2 - 5x + 6\rangle$ en kropp? Varför?

138. Är $\mathbb{Q}[x]/\langle x^2 - 6x + 6\rangle$ en kropp? Varför?

139. Låt $I \subset \mathbb{Z} \times \mathbb{Z}$ vara idealet

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ och } y \text{ är jämna}\}.$$

Hitta de olika elementen i $(\mathbb{Z} \times \mathbb{Z})/I$, och skriv upp en additions- respektive multiplikationstabell.

140. Visa att $\mathbb{Q}[X]/\langle X^2 + 1\rangle \simeq \mathbb{Q}[i]$, där $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}, i^2 = -1\}$.

141. Visa att $\mathbb{Q}[X]/\langle X^2 - 2\rangle \simeq \mathbb{Q}[\sqrt{2}]$, där $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

142. Låt K vara en kropp. Visa att $K[x, y]/\langle x^2 - y^3\rangle \simeq K[T^2, T^3]$.

Lektion 9 - Euklidiska ringar och Gaussiska heltal

143. Skriv följande Gaussiska heltal som produkt av irreducibla element i $\mathbb{Z}[i]$

(a) $3 + 9i$

(b) $70 + i$

(c) $4 + 3i$

(d) $201 + 43i$

(e) $99 + i$.

144. Visa att $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ är en Euklidisk ring.

145. Vilka är de olika elementen i ringen $\mathbb{Z}[i]/\langle 2 + i\rangle$? Skriv upp en additions- respektive multiplikationstabell för den ringen.

146. (Löst exempel) Skriv $z = 390 + 210i$ som produkt av primelement i $\mathbb{Z}[i]$.

Vi börjar med att bryta ut den största gemensamma faktorn till 390 och 210: $\text{sgd}(390, 210) = 30 = 2{\cdot}3{\cdot}5$. I $\mathbb{Z}[i]$ har vi $2 = (1+i)(1-i)$. Primfaktorn 3 är kongruent med 3 modulo 4 och är därför en primfaktor även i $\mathbb{Z}[i]$. 5, slutligen, är kongruent med 1 modulo 4 och kan därför skrivas som summan av två kvadrater: $5 = 1^2 + 2^2$, så vi får $5 = (2 + i)(2 - i)$. Av estetsika skäl kan man vilja byta ut $1-i$ mot $-i(1+i)$, då får man $30 = -3i(1+i)^2(2+i)(2-i)$.

Sedan återstår att faktorisera $z/30 = 13+7i$. Vi har $N(13+7i) = 13^2+7^2 = 218 = 2\cdot 109$. Faktorn 109 är kongruent med 1 modulo 4, så vi kan skriva den som summan av två heltalskvadrater: $109 = 10^2 + 3^2$. Alltså är $13 + 7i$ delbart med antingen $10 + 3i$ eller $10 - 3i$; vi avgör genom prövning.

$$\frac{13 + 7i}{10 + 3i} = \frac{(13 + 7i)(10 - 3i)}{109} = \frac{151 + 31i}{109} \notin \mathbb{Z}[i],$$

alltså måste $13 + 7i$ vara delbart med $10 - 3i$, och mycket riktigt har vi

$$\frac{13 + 7i}{10 - 3i} = 1 + i.$$

Eftersom både $10 - 3i$ och $1 + i$ är primelement, blir den slutliga faktoriseringen

$$\begin{aligned} 390 + 210i &= -3i(1 + i)^2(2 + i)(2 - i)(10 - 3i)(1 + i) \\ &= -3i(1 + i)^3(2 + i)(2 - i)(10 - 3i). \end{aligned}$$

Övriga uppgifter

I avsnittet om euklidiska ringar, för att senare kunna karaktärisera primelementen i $\mathbb{Z}[i]$, visade vi att ett udda primtal $p \in \mathbb{N}$ kan skrivas som summan av två heltalskvadrater om och endast om $p \equiv 1 \pmod 4$. Under bevisets gång använde vi att $\mathbb{Z}_p^*$ är cyklisk för varje primtal p, dvs. att det finns ett element $a \in \mathbb{Z}_p^*$ sådant att $\mathbb{Z}_p^* = \{1, a, a^2, \ldots, a^{p-2}\}$ ($\mathbb{Z}_p^*$ betecknar de inverterbara elementen i $\mathbb{Z}_p$). Detta är ett specialfall av ett mer generellt resultat som naturligast formuleras i termer från gruppteori, nämligen: "Varje ändlig delgrupp av den multiplikativa enhetsgruppen till en kropp är cyklisk". Den som fortsätter läsa algebra efter den här kursen kommer med största sannolikhet att stöta på den satsen i senare kurser, exempelvis Galoisteori.

Eftersom vi för närvarande inte har tillgång till någon gruppteori blir beviset för att $\mathbb{Z}_p^*$ är cyklisk lite längre än vad det annars skulle ha blivit, men inget av stegen är särskilt svårt. Det kan också vara värt att nämna att det här beviset har ganska låg prioritet; om ni är nyfikna och tycker att de verkar roliga är det förstås bra att göra de fyra uppgifterna nedan, men den som hoppar över uppgifterna går inte miste om något väsentligt.

147. Om $a \in \mathbb{Z}_p^*$, skriver vi $\operatorname{ord}(a)$ för a:s *ordning*, dvs. $\operatorname{ord}(a)$ är det minsta positiva heltal k sådant att $a^k = 1$. Vi låter ω vara den minsta gemensamma multipeln av alla $\operatorname{ord}(a)$, där $a \in \mathbb{Z}_p^*$, dvs.
$$\omega = \operatorname{mgm}(\operatorname{ord}(a) \mid a \in \mathbb{Z}_p^*)$$
   (a) Visa att $\omega \leq p - 1$.
   Ledning: Använd Fermats lilla sats och divisionsalgoritmen.
   (b) Visa att $\omega \geq p - 1$.
   Ledning: Använd att $X^\omega - 1 \in \mathbb{Z}_p[X]$ högst har ω stycken olika nollställen, samt att varje $a \in \mathbb{Z}_p^*$ är ett nollställe.

   Det följer att $\omega = p - 1$.

148. Visa att om a och b i $\mathbb{Z}_p^*$ har ordning r respektive s, där r och s är relativt prima, så har ab ordning rs.

149. Visa att mängden $\{\operatorname{ord}(a) \mid a \in \mathbb{Z}_p^*\} \subset \mathbb{N}$ är sluten under mgm", dvs. att om $\operatorname{ord}(a) = r$ och $\operatorname{ord}(b) = s$ för två element $a, b \in \mathbb{Z}_p^*$ så finns det ett element i $\mathbb{Z}_p^*$ av ordning m där $m = \operatorname{mgm}(r, s)$.
   Ledning: Om $a \in \mathbb{Z}_p^*$ har ordning r och r' är en delare till r, så har $a^{r/r'}$ ordning r'.

150. Visa att $\mathbb{Z}_p^*$ är cyklisk.
   Ledning: Att säga att $\mathbb{Z}_p^*$ är cyklisk är detsamma som att säga att det finns ett element av ordning $p - 1$. Visa med hjälp av uppgift 1 och 3 att det finns ett sådant element (i själva verket finns det $\varphi(p - 1)$ stycken, där φ betecknar Eulers φ-funktion; detta är enkelt att visa med gruppteori).