Algebra II: Provtenta + Lösningar

1. Låt $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ vara Eulers φ-funktion. Bestäm alla $n \in \mathbb{N}$ med $\varphi(n) = 32$.

   Lösning: Vi har $32 = 2^5$. Det innebär att talet n har bara udda enkla primdelare $p = 2^m + 1$, dvs. $17, 5, 3$ och möjligtivs $p = 2$ (pga. $\varphi(2n) = \varphi(n)$ för udda $n \in \mathbb{N}$.)

   (a) Om $n = 17n_0$, delar 17 inte n_0 och $\varphi(n_0) = 2$, dvs. $n_0 = 3, 6, 4$. Således får vi $n = 51, 102, 68$.

   (b) Om $n = 5n_0$ med 5 som största primdelare, delar 5 inte n_0 och $\varphi(n_0) = 8$. Om n_0 är delbart med 3, har vi möjligheten $n_0 = 3 \cdot 8 = 24$ och annars $n_0 = 16$. M.a.o. vi får $n = 120, 80$.

   (c) Om $n = 3n_0$ med 3 som största primdelare, delar 3 inte n_0 och $\varphi(n_0) = 16$, således $n_0 = 32$, dvs $n = 96$.

   (d) Till sist är bara $n = 64$ kvar.

2. Hitta en primitiv rot för enhetsgruppen $\mathbb{Z}_{49}^*$.

   Lösning: $\overline{2} \in \mathbb{Z}_7$ har ordning 3, men $\overline{3} \in \mathbb{Z}_7$ har ordning 6. Ordningen till restklassen $\overline{3} \in \mathbb{Z}_{49}$ är därför delbart med 6 och en delare till $42 = |\mathbb{Z}_{49}^*|$. Men $\overline{3}^6 = -\overline{6} \neq 1$. Så $\text{ord}(\overline{3}) = 42$, dvs. $\overline{3}$ är en primitiv rot.

3. Given den offentliga nyckeln $(91, 53)$ avkoda $\overline{41} \in \mathbb{Z}_{91}$.

   Lösning: Avkodningen funkar så här:

   $$\mathbb{Z}_{91} \longrightarrow \mathbb{Z}_{91}, b \mapsto b^d,$$

   där $53d \equiv 1 \mod (72)$ pga. $\varphi(91) = 72$. Euklidiska algoritmen ger $d = 53$ som den minsta exponenten. Så vi måste beräkna

   $$\overline{41}^{53} \in \mathbb{Z}_{91} \cong \mathbb{Z}_7 \times \mathbb{Z}_{13}.$$

   Kinesiska isomorfimen fungerar så här

$\cdot\mathbb{Z}_{91}$	$\mathbb{Z}_7 \times \mathbb{Z}_{13}$
$\overline{78}$	$(\overline{1}, \overline{0})$
$\overline{14}$	$(\overline{0}, \overline{1})$
$\overline{41}$	$(-\overline{1}, \overline{2})$
$\overline{41}^{53}$	$(-\overline{1}, \overline{2}^5)$
$\overline{41}^{53}$	$(-\overline{1}, \overline{6})$
$\overline{6}$	$(-\overline{1}, \overline{6})$

   ,

så avkodningen ger $\overline{6}$. Vi har utnyttjad att $\overline{2}^{12} = \overline{1} \in \mathbb{Z}_{13}$ och således

$$\overline{2}^{53} = \overline{2}^{5} = \overline{6}.$$

4. Ange alla idempotenta och alla nilpotenta element i restklassringen $\mathbb{Z}_{693}$.

   Lösning: Vi har

   $$\mathbb{Z}_{693} \cong \mathbb{Z}_7 \times \mathbb{Z}_9 \times \mathbb{Z}_{11}.$$

   De idempotenta elementen $\neq 0, 1$ resp. de nilpotenta elementen $\neq 0$ finns listade i vänstra kolonnen till tabellen:

$\mathbb{Z}_{693}$	$\mathbb{Z}_7 \times \mathbb{Z}_9 \times \mathbb{Z}_{11}$
$\overline{99}$	$(\overline{1}, \overline{0}, \overline{0})$
$\overline{154}$	$(\overline{0}, \overline{1}, \overline{0})$
$-\overline{252}$	$(\overline{0}, \overline{0}, \overline{1})$
$\overline{253}$	$(\overline{1}, \overline{1}, \overline{0})$
$-\overline{153}$	$(\overline{1}, \overline{0}, \overline{1})$
$-\overline{98}$	$(\overline{0}, \overline{1}, \overline{1})$
$-\overline{231}$	$(\overline{0}, \overline{3}, \overline{0})$
$\overline{231}$	$(\overline{0}, \overline{6}, \overline{0})$

   ,

5. För vilka primtal p har polynomet $f := X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}_p[X]$ ett nollställe i $\mathbb{Z}_p$? Kan det då faktoriseras som produkt av linjära polynom? Gör det ifall $p = 11$.

   Lösning: Vi har $(X - 1)f = X^5 - 1$.

   (a) Om $p \neq 5$, gäller $f(\overline{1}) \neq 0$ och således är rötterna till f restklasserna av ordning 5. Sådana finns om $|\mathbb{Z}_p^*| = p - 1$ är delbart med 5, dvs. omm $p = 5k + 1$. Ta en primitiv rot $a \in \mathbb{Z}_p^*$. Sedan är $a^k, a^{2k}, a^{3k}, a^{4k}$ elementen av ordning 5 och

   $$f = \prod_{\nu=1}^{4} (X - a^{\nu k}).$$

   För $p = 11 = 5 \cdot 2 + 1$ kan vi ta $a = \overline{2}$, och får

   $$f = (X - 4)(X - 5)(X + 2)(X - 3).$$

(b) Om $p = 5$, gäller $X^5 - 1 = (X - 1)^5$ och således $f = (X - 1)^4$.

6. Visa: Ett ändligt integritetsområde R är en kropp!

   Lösning: Vi måste visa, att varje ekement $a \neq 0$ är inverterbart. Abildningen $\mu_a : R \longrightarrow R, x \mapsto ax$, är injektiv, eftersom R är ett integritetsområde. Men en injektiv självavbildning av en ändlig mängd är också surjektiv - så finns det ett element $b \in R$ med $ab = \mu_a(b) = 1$. Eftersom R är kommutativ följer $a \in R^*$.

7. Faktorisera det Gaußiska heltalet $70+i$ som produkt av Gaußiska primtal!

   Lösning: Vi har
   $$|70 + i|^2 = 4901 = 13^2 \cdot 29$$
   och således
   $$70 + i = (3 \pm 2i)^2 \cdot (5 \pm 2i).$$
   Vi har $(70 + i)(3 + 2i)/13 = (208 + 143i)/13 = 16 + 11i$ samt $(16 + 11i)(3 + 2i)/13 = (26 + 65i)/13 = 2 + 5i$, alltså
   $$70 + i = i(3 - 2i)^2(5 - 2i).$$

8. Är ringen $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ ett principalidealområde? Bevis eller motbevis!

   Svar: Den är inte ett PID: I ett PID är reducibla element prim. Men $2 \in A_{-5}$ är

   (a) irreducibelt: Om $2 = ab$ med icke-enheter $a, b \in A_{-5}$, så har vi $4 = N(2) = N(a)N(b)$ och således $N(a) = 2 = N(b)$. Men $2 = N(x + i\sqrt{5}y) = x^2 + 5y^2$ är inte möjligt med $x, y \in \mathbb{Z}$.

   (b) men inte prim: 2 delar produkten $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6$, men inte någon av faktorerna.