Supplementära övningar

1. Visa att Euclids algoritm slutar efter högst $2(1+[\log_2 a])$ steg, där $a < b$. Dvs, visa att $r_k = 0$ för något $k \leq 2(1+[\log_2 a])$.

2. Ge ett exempel av ett pseudoprimtal som inte är ett primtal. Visa att villkoret $\phi(n) \mid n-1$ är tillräckligt men inte nödvändigt för n att vara ett pseudoprimtal.

3. Bevisa en sats som karakteriserar precist de $n > 0$ så att ekvationen $x^2 + y^2 = n$ har en lösning $(x, y) \in \mathbf{Z}^2$.

4. Den ändliga kroppen av ordning q betecknas $\mathbf{F}_q$. Låt $N(q,n)$ beteckna antalet 'monic' irreducibla polynom $p(x) \in \mathbf{F}_q[x]$ av grad n. I denna övning, bevisar vi en formel för $N(q,n)$.

(i) Visa att ett irreducibelt polynom $f(x) \in \mathbf{F}_q[x]$ är en faktor av $x^{q^n} - x$ omm $\deg(f) \mid n$. (Ledning : Betrakta kroppen $\mathbf{F}_q[x]/(f(x))$).

(ii) Visa att $x^{q^n} - x = \prod f_i(x)$ där produkten 'runs over' alla monic irreducibla polynom vars grader delar n.

(iii) Deducera att

$$q^n = \sum_{d|n} dN(q,d).$$

(iv) Deducera att

$$N(q,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

5. Visa att, för $\mathrm{Re}(s) > 2$,

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}.$$

6. Låt A vara en ändlig abelsk grupp. Sätt

$$\hat{A} = \{\chi : A \to \mathbf{C}^{\times} \text{ så att } \chi \text{ är en grupp hom. (dvs en karaktär)}\}.$$

(i) Visa att om $\chi_1, \chi_2 \in A^*$, så också är $\chi_1 \circ \chi_2$ som ges av

$$(\chi_1 \circ \chi_2)(x) := \chi_1(x)\chi_2(x).$$

(ii) Visa att $(\hat{A}, \circ)$ är en ändlig abelsk grupp.
(iii) Visa att $A \cong \hat{A}$ som abstrakta grupper.

Obs ! Gruppen A^* kallas för *dual* gruppen till A.

7. Låt p vara ett udda primtal. Visa att det finns ett positivt $n < 1 + \sqrt{p}$ så att $\left(\frac{n}{p}\right) = -1$.

8 (generaliserar nr. 6). (i) Ange alla KONTINUERLIGA grupp-homomorfismer

$$\chi : \mathbf{R} \to \mathbf{C}^{\times}.$$

(ii) Visa då att gruppen $\hat{\mathbf{R}}$ av sådana avbildningar (den så kallad *karaktär gruppen*) är isomorfisk med $\mathbf{R}$ på ett naturligt sätt.

9. Definiera $\Lambda : \mathbf{N} \to \mathbf{R}$ genom

$$\Lambda(n) = \begin{cases} p, & \text{om } n \text{ är en potens av primtalet p,} \\ 0, & \qquad \text{om } n \text{ inte är en primpotens.} \end{cases}$$

(i) Bevisa att

$$\sum_{m|n} \Lambda(m) = \log n.$$

(ii) Hence, or otherwise, bevisa att, för $\mathrm{Re}(s) > 1$,

$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_1^{\infty} \psi(x) x^{-s-1}\, dx,$$

där

$$\psi(x) \stackrel{\text{def}}{=} \sum_{n \leq x} \Lambda(n).$$

***10.** Låt $z \in \mathbf{C}$ med $\mathrm{Im}(z) > 0$. Låt $k > 0$ vara ett heltal. Definiera den så kallade *Eisenstein serien* $E(z,s;k)$ genom

$$E(z,s;k) := \sum_{\mathbf{Z}^2 \ni (m,n) \neq (0,0)} \frac{1}{(mz+n)^k |mz+n|^{2s}}.$$

Bevisa att $E(z,s;k)$ konvergerar absolut omm $k + \mathrm{Re}(2s) > 2$.

11. Bevisa att L-funktionen $L(E,s)$ av en elliptisk kurva E över $\mathbf{Q}$ (se lösningarna till inlämningsuppgift nr. 1 för definitionen) konvergerar och definierar en analytisk funktion om $\mathrm{Re}(s) > 3/2$.

12. (i) Visa att, om $d \equiv 0$ eller $1 \pmod 4$, då är

$$H(d) = \sum_{t^2 | d} h\left(\frac{d}{t^2}\right).$$

(ii) VIsa att $d \in \mathbf{Z}$ är en fundamental diskriminant omm

$$\begin{cases} d \text{ kvadratfri}, & \text{om } d \equiv 1 \pmod 4, \\ d/4 \text{ kvadratfri och } \equiv 2 \text{ eller } 3 \pmod 4, & \text{om } d \equiv 0 \pmod 4). \end{cases}$$

13. Ange precist vilka diskriminanter $d < 0$ av positiv definita binära kvadratiska former har egenskapen att alla former av diskriminant d har samma antal automorfismer.

14. Låt $d > 0$. Visa att d är en perfekt kvadrat omm kongruensen $x^2 \equiv d \pmod q$ har en lösning för varje primtal q.

(Ledning : Dirichlets sats).

15. Visa att idealen $< 2, 1+\sqrt{-5} >$ i $\mathbf{Z}[\sqrt{-5}]$ är inte principal.

***16.** (i) Bevisa att en ändligt genererad torsionfri abelsk grupp är fri.
(ii) Bevisa att en ändligt genererad abelsk grupp är en direkt summa $T \oplus F$, där T är en ändlig delgrupp och F är fri.
(iii) Deducera att varje ändligt genererad abelsk grupp har en unik decomposition som en direkt summa av cyckliska delgrupper, var en av antingen prim potens eller oändlig ordning.

(Obs : Detta generaliserar den fundamentala satsen om ändliga abelska grupper).

(iv) Ge ett exempel av en torsionfri abelsk grupp som inte är fri.

17 (i) Ge ett exempel av en strängt växande följd av prima ideal av längd n i polynom ringen $\mathbf{C}[x_1, ..., x_n]$

(glöm inte att bevisa att idealen i din kedja ÄR prima !).

(ii) Ge ett exempel, med bevis, av en ring som inte är Noetersk.

(iii) Ge ett exempel av ett ideal i polynom ringen $\mathbf{C}[x, y]$ som inte kan skrivas som en produkt av prima ideal (jämför med huvudsatsen om Dedekind domäner).

18. En ring R kallas för *lokal* om R har ett unikt maximalt ideal.

(i) För vilka n är $\mathbf{Z}/n\mathbf{Z}$ en lokal ring ?

(ii) Låt p vara ett primtal. Låt $\mathbf{Z}_p$ beteckna mängden av alla serier

$$a_0 + a_1 p + a_2 p^2 + \cdots, \qquad \text{där } 0 \leq a_i < p \text{ för alla } i.$$

Hur skulle du definiera addition och multiplikation av element i $\mathbf{Z}_p$ så att den utgör en kommutativ ring med enhet ?

Visa att $\mathbf{Z}_p$ blir då en lokal ring, och ange det unika maximala idealet.

Obs : $\mathbf{Z}_p$ kallas för ringen av *p-adiska heltal.*

19 (a) Låt A vara en godtycklig ring med enhet. För varje ideal $\mathbf{a}$ av A, definiera

$$r(\mathbf{a}) := \{x \in A : x^n \in \mathbf{a} \text{ för något } n > 0\}.$$

Visa att $r(\mathbf{a})$ är ett ideal i A och att det är precist snittet av alla prima ideal i A som innehåler $\mathbf{a}$[1].

(b) Låt Spec(A) vara mängden av alla prima ideal i A. För varje delmängd E till A definiera

$$V(E) := \{\mathbf{p} \in \text{ Spec}(A) : E \subseteq \mathbf{p}\}.$$

[1] Idealet $r(\mathbf{a})$ kallas för *nilradical* av $\mathbf{a}$. I fallet $\mathbf{a} = \{0\}$ då kallas det för *nilradical av A*.

Visa att

(i) Om $\mathbf{a}$ är idealet som genereras av E, då är $V(E) = V(\mathbf{a}) = V(r(\mathbf{a}))$.
(ii) $V(\{0\}) = \mathrm{Spec}(A)$ och $V(\{1\}) = \phi$.
(iii) Om $(E_\lambda)_{\lambda \in \Lambda}$ är en familj av delmängder till A, då är

$$V\left(\bigcup_{\lambda \in \Lambda} E_\lambda\right) = \bigcap_{\lambda \in \Lambda} V(E_\lambda).$$

(iv) För två ideal $\mathbf{a}$ och $\mathbf{b}$,

$$V(\mathbf{a} \cap \mathbf{b}) = V(\mathbf{ab}) = V(\mathbf{a}) \cup V(\mathbf{b}).$$

OBS : Denna övning visar att mängderna $V(E)$ kan betraktas som de slutna mängderna i någon topologi på $\mathrm{Spec}(A)$. Denna topologi kallas för *Zariski topologin*, och är viktig i algebraisk geometri.

***** betecknar en övning som jag betraktar svårare !