UPPSALA UNIVERSITET
Matematiska institutionen
Johan Björklund

Prov i matematik
Ma kandidat, lärare, fristående
Algebra II, 5 p
2008–08–18

Tillåtna hjälpmedel: Skrivdon, passare och linjal. Lösningarna skall åtföljas av förklarande text. Varje uppgift ger maximalt 5 poäng. Om inget annat anges så antags alla ringar vara kommutativa ringar med egenskapen att $1 \neq 0$.
Skrivtid: *08.00–13.00.*

1. Ordna följande fyra påståenden i en följd så att det första påståendet implicerar det andra, det andra implicerar det tredje osv. R antags vara en ring (ej nödvändigtvis kommutativ eller med $0 \neq 1$). Inga bevis krävs.

- R är en kropp.
- R är kommutativ.
- R är ett integritetsområde.
- R är euklidisk.

2. **a)** Ge ett exempel på en ickekommutativ ring.

b) Det är givet att en ring R är isomorf till en ring R'. Om R är ett integritetsområde, kan man dra slutsatsen att R' är ett integritetsområde? Bevis eller motexempel.

c) Formulera Noethers första isomorfisats.

d) Visa att $\mathbb{Z}_2$ är isomorf med $\mathbb{Z}_4/\langle 2 \rangle$ med hjälp av Noethers första isomorfisats.

3. Faktorisera 318 i irreducibla faktorer i $\mathbb{Z}[i]$.

4. **a)** Formulera Eulers sats (bevis ej nödvändigt).

b) Använd satsen för att förenkla $2135^{3312} \pmod{12}$

5. Hitta alla heltalslösningar till ekvationssystemet

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv (728)^{13} \pmod{13} \end{cases}$$

6. Givet två stora primtal p, q (som är relativt prima) och en publik krypteringsnyckel e så att $(e, (p-1)(q-1)) = 1$, beskriv hur du konstruerar en privat dekrypteringsnyckel d samt hur ett meddelande a krypteras respektive dekrypteras med RSA-algoritmen.

Vänd blad!

7. **a)** Antag att R uppfyller definitionen för att vara en ring, vilka ytterligare krav skall den uppfylla för att vara en kropp av karaktäristik 0?

b) Ge ett exempel på en kropp med karaktäristik 0 och ett exempel på en kropp av karaktäristik 5.

c) Antag att $I \subset R$ är ett maximalideal och R är en ring. Visa att R/I är en kropp.

8. Låt p vara ett primtal sådant att $p = a^2 + b^2$ där a, b är heltal sådana att $a > b > 0$. Visa att om $p = c^2 + d^2$ där c, d är heltal så att $c > d > 0$ så är $c = a$, $d = b$ dvs vi har någon form av "unik kvadratupdelning" för primtal.
Tips: Prova att faktorisera p i någon lämplig ring.