Matematiska Institutionen
KTH

Lösning till lappskrivning nummer 6B till kursen Diskret matematik för D2 och F, SF1631 och SF1630, den 11 maj 2010, kl 15.15-15.40.

Namn:

Resultat:

Bonuspoäng till tentan från denna lappskrivning är antalet godkanda uppgifter nedan.

OBS Lösningarna skall motiveras väl och skrivas på detta pappers fram- och baksida. Inga hjälpmedel är tillåtna.

1. Betrakta den kropp F_{25} med 25 element, som man får genom att som element ta elementen i mängden

$$\{a_0 + a_1 x \mid a_0, a_1 \in Z_5 \} ,$$

och räkna som om $x^2 + 2 = 0$. Bestäm inversen till elementet $x + 3$ i denna kropp F_{25}.

Lösning: Vi beräknar inversen genom att först genomfïa Euklides algoritm i syfte att hitta en lösning till den "diofantiska" ekvationen $q(x)(x + 3) + p(x)(x^2 + 2) = 1$.

$$x^2 + 2 \quad = \quad (x - 3)(x + 3) + 1 ,$$

så $(x - 3)(x + 3) - (x^2 + 2) = 4$. Vi multiplicerar nu denna likhet med inversen till 4 i kroppen Z_5, dvs med elementet 4 (ty $4 \cdot 4 \equiv 1 \pmod 5$). Alltså gäller i polynomringen $Z_5[x]$ att

$$4(x - 3)(x + 3) - 4(x^2 + 2) = 1 .$$

Inversen till det givna elementet är således $4(x - 3)$ dvs $4x + 3$, eftersom vi betraktar $x^2 + 2$ som varandes lika med noll.

2. Betrakta den kropp F_{27} med 27 element som består av elementen

$$\{a_0 + a_1 x + a_2 x^2 \mid a_0, a_1, a_2 \in Z_3 \} ,$$

och där man räknar som om $x^3 + 2x + 2 = 0$. Bestäm samtliga lösningar till ekvationen $z^4 = 1$ i kroppen F_{27}.

Lösning: Den multiplikativa gruppen $(F_{27} \setminus \{0\}, \cdot)$ är cyklisk och består av 26 element, dvs

$$(F_{27} \setminus \{0\}, \cdot) =< \alpha >= \{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{26} = 1\} .$$

Enligt känd sats från teorin för grupper gäller att om ett gruppelement g satisfierar g^4 så är g:s ordning en delare till 4. Vidare vet vi att i den givna gruppen med 26 element så är ordningen av varje element en delare till talet 26. Så enda möjligheten för ett element g att lösa den givna ekvationen är att ordningen av g är 1 eller 2, dvs en lösning till ekvationen $w^2 = 1$. Varje lösning till denna ekvation löser ju också $z^4 = 1$ (eftersom $1^2 = 1$). För en given kropp finns högst två lösningar till en ekvation av grad två. Och i detta fall har vi ju 1 och -1 som lösningar. Så

SVAR: Elementen 1 och -1, dvs 1 och 4.