Matematiska Institutionen
KTH

Lösning till lappskrivning nummer 3B till kursen Diskret matematik, moment B, för D2 och F, SF1631 och SF1630, den 23 april 2008, kl 08.15-08.40.

1. Visa att polynomet $x^3 + 3x + 4$ inte är irreducibelt i ringen $Z_5[x]$.

LÖSNING: Om polynomet går att faktorisera måste en av faktorerna ha grad ett och därmed, enligt faktorsatsen, kommer polynomet att ha minst ett nollställe. Vi finner, efter lite sökande, att -1, dvs elementet 4 i kroppen Z_5, är ett nollställe eftersom

$$(-1)^3 + 3(-1) + 4 = -1 - 3 + 4 = 0.$$

Enligt faktorsatsen gäller nu att

$$x^3 + 3x + 4 = (x - 4)p(x),$$

för något polynom $p(x)$ vilket visar att det givna polynomet ïnte är irreducibelt.

2. Bestäm ett irreducibelt andragradspolynom i polynomringen $Z_{19}[x]$, (vilket är möjligt att göra utan alltför mycket trial and error sökande). En motivering krävs också varför polynomet i fråga är irreducibelt.

LÖSNING: Vi undersöker först om det finns något polynom av typen

$$x^2 - a,$$

som är irreducibelt i den givna polynomringen. Ett sådant polynom är irrducibelt, då det är av grad 2, om och endast om polynomet saknar nollställe, dvs det finns inget element $\alpha \in Z_{19}$ sådant att $\alpha^2 = a$. Vi beräknar nu kvadraterna på samtliga element i ringen Z_{19}.

$$0^2 = 0,\ \ 1^2 = (-1)^2 = 18^2 = 1,\ \ 2^2 = (-2)^2 = 17^2 = 4,\ \ 3^2 = (-3)^2 = 16^2 = 9,$$

$$4^2 = (-4)^2 = 15^2 = 16,\ \ 5^2 = (-5)^2 = 14^2 = 6,\ \ 6^2 = (-6)^2 = 13^2 = 17,$$

$$7^2 = (-7)^2 = 12^2 = 11,\ \ 8^2 = (-8)^2 = 11^2 = 7,\ \ 9^2 = (-9)^2 = 10^2 = 5.$$

Vi ser att elementet 2 inte dök upp bland de ”jämna” kvadraterna i ringen Z_{19}. Således saknas nollställen till polynomet

$$x^2 - 2.$$

SVAR: Polynomet $x^2 - 2$ är irreducibelt i polynomringen $Z19[x]$.

Alternativ lösning: Vi använder att multiplikativa gruppen till en kropp är cyklisk, dvs och i detta fall, att det finns ett element $g \in Z_{19}$ sådant att

$$Z_{19} \setminus \{0\} =< g >= \{g, g^2, g^3, \ldots, g^{18} = 1\}.$$

De jämna kvadraterna i ringen är då elementen i mängden

$$\mathcal{Q} = \{(g^i)^2 \mid i = 1, 2, \ldots, 18\} = \{g^2, g^4, g^6, \ldots, g^{18} = 1\}.$$

Elementet g^9 är ingen jämn kvadrat. Vi visar nu att g^9 är lika med elementet -1 (oberoende av val av generator g för den multiplikativa gruppen): Eftersom $(g^9)^2 = 1$ så måste g^9 vara en av lösningarna till ekvationen $x^2 = 1$. Då $g^{18} = 1$ och $g^{18} \neq g^9$ så måste g^9 vara lika med den andra lösningen till ekvationen $x^2 = 1$ som ju är -1.

Vår slutsats är alltså att -1 inte är en jämn kvadrat och alltså att ekvationen $x^2 + 1$ saknar nollställe och därmed faktorer av grad ett. Ett ej irreducibelt polynom av grad två måste ha faktorer av grad ett och därmed minst ett nollställe. Alltså är $x^2 + 1$ irreducibelt i $Z_{19}[x]$.