ÖVNING 8 - DISKRET MATEMATIK 030409

HANNES REIJNER

observation. Vi börjar med en observation. Om man vill ta reda på inversen till något inverterbart r tillhörande $\mathbf{Z}_m$ och m är stort använder man sig med fördel av euklides algoritm. Vi har ju att om x är inversen till r så gäller att $rx \equiv 1 \mod m$ och alltså att $rx - 1 = km$ för något heltal k. Det följer att $rx - km = 1$ och vi kan med hjälp av euklides algoritm bestämma att x och k. Vi behöver bara x vilket ju är inversen till r

13.3.7 Visa att ekvationen $x = x^{-1}$ i $\mathbf{Z}_p$ medför att $x^2 - 1 = 0$ och drag slutsatsen att 1 och -1 är de enda elementen i $\mathbf{Z}_p$ som är sina egna inverser.

lösning. Ekvationen $x = x^{-1}$ i $\mathbf{Z}_p$ är ekvivalent med att $x \equiv x^{-1} \mod p$. Antag att $x \equiv x^{-1} \mod p$. Vi multiplicerar med x och får då att $x^2 \equiv xx^{-1} \mod p$ vilket ger oss att $x^2 - 1 \equiv 0 \mod p$. Att $x^2 - 1 \equiv 0 \mod p$ är ekvivalent med att $p \mid (x^2 - 1) = (x - 1)(x + 1)$ vilket medför att $p \mid (x - 1)$ eller att $p \mid (x + 1)$ (tänk eller se sats 8.6.1 i nya boken eller 1.8.1 i gamla boken). Att $p \mid (x - 1)$ är ekvivalent med att $x \equiv 1 \mod p$ vilket i sin tur är ekvivalent med att $x = 1$ i $\mathbf{Z}_p$. Vi har på samma sätt att $p \mid (x + 1)$ är ekvivalent med att $x = -1$ i $\mathbf{Z}_p$. Vi har därmed att om $x = x^{-1}$, det vill säga x är lika med sin egen invers i $\mathbf{Z}_p$ så är $x = \pm 1$.

kommentar. Detta tal kan lösas ännu enklare om man vet att $\mathbf{Z}_p$ inte innehåller några noll-delare (förutom 0). Med det menas att det inte existerar något några noll-skilda element x och y sådana att $xy = 0$ i $\mathbf{Z}_p$. Exempel på nolldelare är 2 och 4 i $\mathbf{Z}_8$ eftersom $2 \cdot 4 = 0$. Vi lämnar beviset som en övning (ledtråd: alla noll-skillda element i $\mathbf{Z}_p$ har inverser). Eftersom $x^2 - 1 = (x - 1)(x + 1) = 0$ och $\mathbf{Z}_p$ saknar nolldelare så måste vi ha att $x - 1 = 0$ eller att $x + 1 = 0$ vilket är ekvivalent med att $x = \pm 1$ i $\mathbf{Z}_p$. Detta gäller inte i $\mathbf{Z}_8$ där ekvationen $x^2 - 1 = 0$ har 4 lösningar, nämligen $x = 1, 3, 5$ eller 7, men så är ju 8 heller inte ett primtal.

13.3.8 Visa att $(p-1)! \equiv -1 \mod p$ genom att studera de noll-skillda elementen i $\mathbf{Z}_p$. (Detta kallas Wilsons sats.)

lösning. Vi börjar med att observera att alla noll-skillda element i $\mathbf{Z}_p$ har en unik invers. Eftersom elementen $(p-2), (p-3), \ldots, 2$ inte är sina egna inverser (se 13.6.7) kommer vi därmed få att $(p-2)(p-3)\cdots 2 \equiv 1 \mod p$ (Vi har ju att inversen till $(p-k)$ varken är $(p-k)$,0, 1 eller -1 och därmed något annat element i produkten). Det följer därmed att $(p-1)! \equiv (p-1)(p-2)\cdots 2\cdot 1 \equiv (p-1)\cdot 1\cdot 1 \equiv (p-1) \equiv -1 \mod p$.

kommentar: Lösningar till ekvationer av typen $x^2 = r$ i $\mathbf{Z}_p$ kommer alltid i par. Antag exempelvis att $s^2 = r$ vi har då att $(-s)^2 = (-1)^2 s^2 = s^2 = r$ och alltså att även $-s$ är en lösning.

13.6.1 (Endast (i), testa (ii) själv!) Bestäm alla tänkbara lösningar till $5x \equiv 1 \mod 11$.

lösning. Detta är precis detsamma som att bestämma inversen till 5 i $\mathbf{Z}_{11}$. Vi observerar att 11 är ett primtal och att 5 därmed har en invers i $\mathbf{Z}_{11}$. Vi bestämmer nu inversen till 5 på förljande enkla sätt: Vi vet att 0 är kongruent med 0, 11, 22, 33, 44 osv modulo 11 och vi ser därmed att 1 är kongruent med 1, 12, 23, 34, 45, 56 osv modulo 11 Vi studerar nu 5:ans multiplikationstabell och ser att $5*9 = 45$ som ju är kongruent med 1 modulo 11. Vi har därmed att 9 är invers till 5. Vidare har vi att en invers alltid är unik, det vill säga det kan bara finnas en invers. Jag visar: antag att det finns två inverser r och s till x. Alltså så att $rx = 1$ och $sx = 1$. Vi multiplicerar uttrycket $rx = 1$ med s och får $srx = s$. Detta är ekvivalent med att $rsx = s$ och eftersom $sx = 1$ att $r = s$. Vi har alltså att en invers är unik. Vi har därmed att den enda lösningen ges av $x \equiv 9 \mod 11$.

E-mail address: hannes@math.kth.se
URL: www.math.kth.se/~hannes