Läsanvisning till Discrete matematics av Norman Biggs - 5B1118 Diskret matematik

Mats Boij

11 november 2001

6 Modulär aritmetik

Det sjätte kapitlet behandlar *modulär aritmetik* som är ett sätt att räkna med *restklasser* av heltal istället för med vanliga heltal. För ett givet heltal n finns precis n olika rester vid division med n och tal som ger samma rest bildar en restklass. Det finns allstå n restklasser modulo n.

Rekommenderade uppgifter

	lättare	svårare
6.1	3	
6.2	3	4
6.3	4,5	
5.6	1,4,5,7	

Dessutom rekommenderas uppgifter från *Kryptografi och primalitet*.

6.1 Kongruenser

Heltal som ger samma rest vid division med n kallas *kongruenta modulo* n och vi skriver $a \equiv b \pmod{n}$ om a är kongruent med b modulo n. Alla heltal som ger samma rest vid division med n bildar en *restklass* modulo n.

Poängen med det här avsnittet är att Sats 6.1 visar att vi kan räkna med restklasser precis som med vanliga heltal. När vi skall lägga ihop eller multiplicera restklasser tar vi bara ett tal ur varje, lägger ihop eller multiplicerar dessa representanter och tar den restklass som resultatet ligger i.

Exemplet visar att vi kan ta reda på resten av ett heltal vid division med 9 genom att ta siffersumman i den decimala framställningen. Om siffersumman fortfarande är större än 10 tar vi siffersumman av siffersumman, och så vidare. Til slut får vi ett tal som är mindre än 10 och det är resten av det ursprungliga talet vid division med 9.

Samma princip gäller vid division med $b - 1$ om talen är skrivna i basen b.

Översättningar

congruence *kongruens*
modulo *modulo*

6.2 $\mathbf{Z}_n$ och dess aritmetik

Här bildas $\mathbf{Z}_n$ - *heltalen modulo* n - som mängden av restklasser modulo n. Enligt det som bevisades i föregående avsnitt kan vi nu införa addition och multiplikation på $\mathbf{Z}_n$ och Sats 6.2 visar att de sex första axiomen för heltalen också gäller för heltalen modulo n. Däremot kan man kontrollera att de resterande axiomen för heltalen inte längre går igenom för $\mathbf{Z}_n$ i allmänhet.

Översättningar

integers modulo n *heltalen modulo n*

6.3 Inverterbara element i $\mathbf{Z}_m$

Ett element a i $\mathbf{Z}_n$ är *inverterbart* om det har en *multiplikativ invers*, dvs ett element b så att $ab = 1$. Bland heltalen finns det bara två inverterbara element, 1 och -1, men bland heltalen modulo n visar det sig att det finns $\phi(n)$ inverterbara element, nämligen alla restklasser av tal som saknar gemensamma delare med n. Om n är ett primtal finns det bara en restklass som innehåller tal som har gemensamma delare med n, nämligen klassen som innehåller 0. Därför är alla element utom nollan inverterbar i $\mathbf{Z}_p$, för primtal p. Detta är vad som sägs i sats 6.3.1.

Sats 6.3.2 är *Eulers sats* som säger att $a^{\phi}(n) \equiv 1 \pmod{n}$ om a och n är relativt prima.

Med hjälp av Eulers sats kan man lätt bevisa Fermats lilla sats, att om p är ett primtal så gäller att $a^{p-1} \equiv 1 \pmod{p}$ om p inte delar a. Det följer också att $a^p \equiv a \pmod{p}$ för alla a.

Översättningar

invertible *inverterbar*
inverse *invers*
Euler's Theorem *Eulers sats*
Fermat's Theorem *Fermats lilla sats*