Explorativ övning 13

RESTARITMETIKER*

Restaritmetiker påminner om heltalsaritmetiken, men i stället för att addera eller multiplicera vanliga heltal adderar man och multiplicerar rester vid division med ett fixt heltal n. Rester adderas och multipliceras så att summan och produkten också är rester. Dessa operationer kallas addition och multiplikation modulo n. Det är ett exempel på nya "talsystem" som lyder samma räknelagar som de vanliga heltalen. Restaritmetiker förekommer mycket ofta i vardagliga situationer även om man inte alltid är medveten om deras närvaro – veckodagar återkommer modulo 7, och tiden räknas ofta modulo 24 (eller 12). Restaritmetiker ger en möjlighet att lösa många relativt enkla och intressanta problem som gäller delbarhetsegenskaper hos heltalen.

Vi följer avsnitt 13 i kompendiet "Talsystem och restaritmetiker". Läs också avsnitt 3.4 (3.5) i Vretblads bok.

Övning A

Denna övning handlar om aritmetiker modulo 7 och modulo 31.

1. Den 1 maj var en fredag. Med ledning av detta, beräkna vilken veckodag den 24 maj är. Förklara hur du resonerar.
2. Maj har 31 dagar. Beräkna vilken veckodag den 8 juni är (den 1 maj var en fredag).
3. Låt oss numrera veckodagarna så att söndag har nummer 0, måndag nummer 1, tisdag nummer 2 osv. Om den 1 i månaden infaller på en måndag så kan man bestämma veckodagen i denna månad genom att dela datumet med 7 – resten säger vilken veckodag man har (t ex infaller den 24 på en onsdag ty 24 lämnar resten 3 vid division med 7). Föreslå en metod för att bestämma veckodagen i en månad som börjar på en torsdag dvs vad skall man göra med dagens datum för att resten vid division med 7 skall ge veckodagen.
4. Konstruera en "kalender" för resten av året genom att för varje månad ange ett tal som skall adderas till dagens datum så att resten av datumet modulo 7 ger veckodagen.

*__MAL200, ht 99__

Övning B

1. Bestäm sista siffran i talen
   (a) 2^{1999}, (b) 13^{20}, (c) $7^{7^{7^7}}$.

2. Bestäm resten vid division av
   (a) 3^{100} med 7, (b) 2^{1000} med 3,5,11,13, (c) 99^{99} med 13.
   Ledning. Visa först att $99^2 \equiv -1 \pmod{13}$.

Övning C

1. (a) P. Fermat påstod att talen $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, ...$ är primtal. Det är verkligen sant då $n = 0, 1, 2, 3, 4$. Visa det! (en miniräknare kan vara till hjälp).
   (b) Hundra år senare visade L. Euler att $641|F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$. Visa det genom att räkna i $\mathbb{Z}_{641}$ och utnyttja följande likheter: $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$.

2. (a) För 2500 år sedan påstod kinesiska matematiker att om ett heltal $n > 1$ är en delare till $2^n - 2$ så måste n vara ett primtal. Detta påstående är sant då $n < 341$ men $341|2^{341} - 2$ trots att 341 inte är ett primtal. Visa det!
   Ledning. $341 = 11 \cdot 31$ och $2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$.
   Anmärkning. P. Fermat kände till den kinesiska hypotesen och han visste att hans tal $F_n = 2^{2^n} + 1$ hade egenskapen
   $$F_n|2^{F_n} - 2.$$
   Det var grunden för hans påstående att F_n var primtal.
   (b) Visa att $F_n|2^{F_n} - 2$.

Övning D

1. (a) Beräkna summorna
   $1^3 + 2^3$ modulo 3,
   $1^3 + 2^3 + 3^3 + 4^3$ modulo 5,
   $1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3$ modulo 7.
   Ser du ett mönster? Vad kan man säga om summan
   $1^3 + 2^3 + ... + 100^3$ modulo 101?
   Ledning. Räkna i $\mathbb{Z}_{101}$.
   (b) Kan du ställa upp en förmodan angående summan
   $1^3 + 2^3 + ... + (n-1)^3$
   modulo n? Bevisa ditt påstående!

2. Visa att $m|1^k + 2^k + ... + (m-1)^k$ då k och m är positiva udda heltal.

Övning E

1. Beräkna inverser a^{-1} till alla $a \in \mathbb{Z}_7$, $a \neq 0$. Beräkna också $\sum a^{-1}$, $a \in \mathbb{Z}_7$, $a \neq 0$.
2. Låt p vara ett udda primtal. Visa att om
$$1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{a}{b},$$
där a, b är heltal så gäller $p|a$.

   Ledning. Utnyttja att $\mathbb{Z}_p$ är en kropp.

Övning F

1. Visa att om $x^2 + y^2 = z^2$, där x, y, z är heltal så finns det bland dessa tal ett som är delbart med 3, ett delbart med 4 och ett delbart med 5 ($3^2 + 4^2 = 5^2$ är "den minsta" Pythagoreiska triangeln).

   Ledning. Det kan vara till hjälp att först lösa Vretblad 3.20 och 3.21 (316 och 317).
2. Visa att om $x^3 + y^3 = z^3$, där x, y, z är heltal så är minst ett av dessa tal delbart med 7.

   Ledning. Arbeta med rester modulo 7. Visa att $x^3 \equiv \pm 1 \pmod 7$ om $7 \nmid x$.

Övning G

Fermats lilla sats säger att att $p|a^p - a$ då p är ett primtal och a är ett godtyckligt heltal. Utnyttja denna sats i följande uppgifter:

1. Visa att $6|n^3 - n$ då n är ett heltal.
2. Visa att $30|n^5 - n$ då n är ett heltal.
3. Visa att $42|n^7 - n$ då n är ett heltal.

Övning H

1. Bestäm det minsta positiva heltalet n som lämnar resterna 1,2,3,4,5 vid division med respektive 2,3,4,5,6.
2. Bestäm alla n sådana att $4|n$, $9|n+1$, $25|n+2$.

Följande övningar i Vretblads bok rekommenderas: **3.15 (312), 3.18 (315), 3.23 (319), 3.29 – 3.31 (323 – 325).**