Matematik Chalmers

Tentamen i tmv200 Diskret matematik IT den 17 december 2004, kl. 8.30-12.30

Hjälpmedel: Inga hjälpmedel

Telefonvakt: Elin Götmark, tel. 0739-779268

1. (8p) Hur många sjusiffriga tal där alla siffror är 1, 2 eller 3 finns det
   (a) totalt?
   (b) som innehåller exakt tre tvåor?
   (c) som saknar treor?
   (d) som innehåller minst fem ettor?

2. (6p) Visa att det för alla udda positiva heltal n gäller att
$$1+3+5+7+\ldots+n=(\frac{n+1}{2})^2.$$

3. (6p) Ge fullständig lösning till den diofantiska ekvationen
$$23x+17y=11.$$

4. (6p) Följden $f_1, f_2, f_3, \ldots$ är given av att $f_1=1$ och att det för $n \geq 2$ gäller att $f_n=\sqrt{1+f_{n-1}^2}$. Visa att det för alla n gäller att $f_n=\sqrt{n}$.

5. (6p) Lina har en stor släkt, så för att göra julklappsinköpen enklare ger hon alla varsin marsipangris. Om hon hon köper marsipangrisar av en enkel sort för 29 kronor styck kan alla de närmaste släktingarna plus kusinerna på mammas sida få varsin och Lina får 3 kronor över. Om hon istället satsar på en finare sorts grisar för 40 kronor styck räcker pengarna till för att de närmaste släktingarna plus kusinerna på pappas sida ska få varsin. Det blir då 8 kronor över. Lina har mindre än 1000 kronor. Hur mycket pengar har hon? Hur många fler är kusinerna på mammas sida än kusinerna på pappas sida?

6. (6p) Låt n vara ett positivt heltal större än 1. Vad är $\Phi(n)$ (dvs hur är Eulers funktion definierad)? Förklara varför $\Phi(n)=n-1$ om n är ett primtal. Visa också att om p och q är två olika primtal och $n=pq$ så är $\Phi(n)=\Phi(p)\Phi(q)$.

7. (6p) Låt f_n vara antalet följder av längd n av talen 1, 2 och 3 sådana att det ingenstans står en etta omedelbart före en tvåa. Finn en rekursiv formel för följden $f_1, f_2, f_3, \ldots$.

8. (6p) En generalisering av Eulers sats: Låt p och q vara två olika primtal och låt $n=pq$. Visa att det för alla heltal a gäller att
$$a^{1+\Phi(n)} \equiv a \bmod n.$$

/Johan Jonasson

Lösningar

1. På var och en av talens sju positioner kan vilken som helst av de tre siffrorna stå. Detta ger tre valmöjligheter per position, så enligt multiplikationsprincipen finns det totalt 3^7 tal av sökt slag. Del (c) löses på samma sätt och svaret är 2^7 då man ju uteslutit treorna från alla val.

   För del (b): Positionerna där det står ettor kan väljas på $\binom{7}{3}$ sätt. Givet varje sådant val kan de övriga två positionerna fyllas på 2^4 sätt. Svaret är alltså $2^4\binom{7}{3}$. Del (d): Svaret är $2^2\binom{7}{5} + 2\binom{7}{6} + \binom{7}{7}$ där de tre termerna i tur och ordning ger antalet tal med exakt 5, exakt 6, respektive exakt 7 ettor.

2. Formeln är uppenbart sann då $n = 1$ så antag att formeln gäller då $n = m$ där m är ett givet udda heltal. Om vi kan visa att formeln då måste gälla även för $n = m + 2$ så följer formelns allmänna giltighet av induktionsprincipen. Men enligt antagandet gäller

$$1 + 2 + \ldots + m + (m + 2) = (\frac{m+1}{2})^2 + m + 2 = \frac{m^2 + 2m + 1 + 4m + 8}{4}$$

$$= \frac{m^2 + 6m + 9}{4} = (\frac{m+3}{2})^2$$

   som önskat.

3. Talen 23 och 17 är relativt prima, så en bra start är att först lösa ekvationen $23x + 17y = 1$. En lösning till denna är $x = 3, y = -4$. En lösning till den ursprungliga ekvationen är alltså $x = 33, y = -44$ och den allmänna lösningen blir $(x, y) = (33 - 17n, -44 + 23n)$, $n \in \mathbf{Z}$.

4. $f_1 = 1 = \sqrt{1}$ så om vi under antagandet $f_n = \sqrt{n}$ för ett givet n kan visa att $f_{n+1} = \sqrt{n+1}$ följer det önskade resultatet av induktionsprincipen. Men detta är rättframt:

$$f_{n+1} = \sqrt{1 + f_n^2} = \sqrt{1 + \sqrt{n}^2} = \sqrt{n+1}.$$

5. Låt x vara det belopp som Lisa äger. Enligt uppgift gäller

$$\begin{cases} x \equiv 3 \bmod 29 \\ x \equiv 8 \bmod 40 \end{cases}$$

   Enligt den andra raden gäller att $x = 8 + 40k$ för något heltal k. Insättning i den första raden ger att $8 + 40k \equiv 3$ mod 29, dvs $11k \equiv 24$ mod 29, dvs $k \equiv 8 \cdot 24$ som ger $k \equiv 18$ mod 29, dvs $k = 18 + 29m$. Vi får då $x = 8 + 40(18 + 29m) = 728 + 1160m$. Lina hade alltså 728 kronor. Kusinerna på mammas sida är $725/29 = 25$ till antalet och på pappas sida $720/40 = 18$, så på mammas sida var kusinerna 7 stycken fler.

6. $\Phi(n)$ är det antalet hetal, a, i mängden $\{1, 2, \ldots, n\}$ sådana att $sgd(a, n) = 1$. Om n är ett primtal är alla tal i den givna mängden utom talet n trivialt relativt

prima n, varav $\Phi(n) = n - 1$ följer. Om $n = pq$ är alla talen i $\{1, 2, \ldots, pq - 1\}$ relativt prima n utom talen $p, 2p, 3p, \ldots, (q-1)p$ och $q, 2q, \ldots, (p-1)q$. Alla dessa är olika ty om $ip = jq$ gäller att $p|jq$ varför $p|j$ och något sådant j finns inte med i uppräkningen nyss. Vi får $\Phi(pq) = pq - 1$ minus antalet tal i de två uppräkningarna tillsammans, dvs $pq - 1 - (q-1) - (p-1) = (p-1)(q-1)$.

7. Uppenbarligen är $f_1 = 3$. För att bilda en rekursiv formel, antag att vi känner till f_{n-1} för ett givet n. Av varje godkänd följd av längd $n-1$ kan man bilda en följd av längd n genom att sätta en av siffrorna 1, 2 eller 3 omedelbart före följden. På detta sätt kan man bilda $3f_{n-1}$ olika följder. Nu är inte all dessa godkända, nämligen de följder som man får genom att ta en längd-$n-1$-följd som börjar med en tvåa och sätta en etta framför. Antalet sådana är f_{n-2} ty med en tvåa i början bildar man en godkänd följd genom att sätta vilken godkänd följd som helst efter denna tvåa. Den korrekta rekursiva formeln blir alltså

$$f_n - 3f_{n-1} - f_{n-2}$$

med startvärdet $f_1 = 3$.

8. Om a och pq är relativt prima följer det önskade resultatet disrekt av Eulers sats, så vi kan fritt anta att a är en multipel av antingen p eller q, säg p. Med andra ord kan vi anta att $a = kp$ är k är ett heltal sådant att $1 \leq k \leq q - 1$. Då får vi vid räkning modulo $n = pq$:

$$a^{1+\Phi(n)} = kp(kp)^{\Phi(p)\Phi(q)} = kp \cdot k^{\Phi(n)} \cdot (p^{\Phi(q)})^{\Phi(p)} \equiv kp \cdot (1 + mq)^{\Phi(p)}$$

där den sista likheten följer av Eulers sats använd två gånger, då ju p och q är relativt prima. Talet m är ett heltal. Enligt binomialsatsen gäller

$$(1 + mq)^{\Phi(p)} = 1 + \sum_{k=1}^{\Phi(p)} \binom{\Phi(p)}{k} (mq)^k.$$

Multiplicera detta med pk och se att produkten blir kp plus ett antal termar som alla innehåller en faktor pq, dvs produketn är kongruent med $kp = a$ modulo pq som önskat.