Løsningsforslag til midtsemesterprøve i MA1301-Tallteori høsten 2005

Her vil vi også presentere tankegangen bak svarene på flervalgsdelen.

Oppgave 1

a) Definisjon av største felles divisor: Den største felles divisoren $d = gcd(a, b)$ til to tall a og b er definert ved de to kravene i) $d|a$ og $d|b$ (d er en felles divisor) og ii) hvis $c|a$ og $c|b$, så er $c \leq d$.

b) Kriterium for at en lineær diofantisk likning skal ha løsning: En lineær diofantisk likning $ax + by = c$ har løsning hvis og bare hvis $gcd(a, b)|c$.

Et brev skal frankeres med 32 kroner, og du har frimerker av valør 7,50 og 9,50.

c) Diofantisk likning som viser problemet, og løsning av denne: Her er ikke $7,50$ og $9,50$ heltall, men det kan vi fikse ved å regne i hele femtiøringer. Ligningen sier da

$$19x + 15y = 64$$

som betyr at vi skal frankere med verdi 64 femtiøringer, og har frimerker med verdi 19 femtiøringer og 15 femtiøringer (vi kunne også regnet med hele ører).

Euklids algoritme for 19 og 15 gir

$$\begin{aligned}19 &= 1.15 + 4\\15 &= 3.4 + 3\\4 &= 1.3 + 1\\3 &= 3.1 + 0\end{aligned}$$

Dermed er $gcd(15, 19) = 1$, og $1|64$, så vi har løsninger. Vi finner en av løsningnene ved å gå baklengs gjennom regnestykkene i Euklids algoritme, og så gange med $64 = 64/1$:

$$1 = 4 - 3 = 4 - (15 - 3.4) = 4.4 - 15 = 4(19 - 15) - 15 = 4.19 - 5.15$$

Dermed er $64 = 19.256 - 320.15$, så en spesiell løsning er $x_0 = 256, y_0 = -320$ og den generelle løsningen er

$$x = x_0 + \frac{b}{d}t = 256 + 15t, y = y_0 - \frac{a}{d}t = -320 - 19t$$

der t er et vilkårlig heltall.

d) Løsning av frimerkeproblemet: Siden antallet frimerker alltid må være positivt, må vi løse likningen fra c) sammen med de to ulikhetene $x \geq 0$ og $y \geq 0$:

$$\begin{array}{lll} 0 \le x = 256 + 15t, & 15t \ge -256, & t \ge -256/15 \text{ mellom -17 og -18} \\ 0 \le y = -320 - 19t, & 19t \le -320, & t \le -320/19 \text{ mellom -16 og -17} \end{array}$$

Dermed er den eneste muligheten $t = -17$, vi får da $x = 256 - 15.17 = 1$, $y = -320 + 19.17 = 3$.

Konklusjon: vi trenger 3 frimerker av valør 7,50 og ett frimerke av valør 9,50 for å frankere et brev med 32 kroners porto.

Oppgave 2

Definisjon av primtall: Et primtall er et heltall større enn 1, som bare kan deles på seg selv og på 1.

Bevis for at det finnes uendelig mange primtall: Anta det motsatte, nemlig at det bare finnes endelig mange. Vi ønsker å komme fram til en selvmotsigelse, det vil vise resultatet.

Siden det er antatt at det bare finnes endelig mange primtall, kan vi liste dem opp som $p_1, p_2, \cdots, p_n$. Se på tallet som er 1 mer enn produktet av dette tallet, og faktoriser det (OK ved aritmetikkens fundamentalteorem):

$$N = p_1 p_2 \cdots p_n + 1 = q_1 q_2 \cdots q_r$$

Her er altså q-ene primtall. Se på q_1. Siden dette er et primtall, og $p_1, \cdots, p_n$ er listen av alle primtall, må $q_1 = p_j$ for en av p-ene. Men da har vi

$$q_1 | N \text{ og } q_1 | p_1 \cdots p_j \cdots p_n, \text{ så } q_1 | (N - p_1 \cdots p_n) = 1$$

Dette er en selvmotsigelse, for intet primtall kan dele 1. Dermed er det umulig at det bare finnes endelig mange primtall, så det må nødvendigvis finnes uendelig mange.

Nå kommer vi til flervalgsdelen:

Oppgave 3

a) $\binom{5}{3} = \frac{5.4}{2.1} = \frac{20}{2} = 10$, $\binom{10}{7} = \frac{10.9.8}{3.2.1} = 10.3.4 = 120$.

b) $\binom{n}{1} = n$?
$\binom{n}{1} = \frac{n}{1} = n$, så dette er sant.

$\binom{n}{2} = n(n+1)$?
$\binom{n}{2} = \frac{n(n-1)}{2.1} = \frac{n(n-1)}{2}$, som ikke er lik $n(n+1)$, så denne påstanden er gal (f.eks. for $n = 2$ er $\binom{2}{2} = 1$, mens $2(2+1) = 6 \neq 1$).

$\binom{n}{k} = \binom{n}{n-k}$?
$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}$, så denne påstanden er sann.

$\binom{n}{k} = -\binom{n}{n-k}$?
Siden den forrige påstanden var sann, kan ikke denne være det (f.eks. for $n = 2, k = 1$ er $\binom{2}{1} = 1 \neq -1 = -\binom{2}{1}$).

$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$?

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!}$$

Vi setter dette på felles brøkstrek; da må vi gange med $n - k + 1$ oppe og nede i første ledd, og med k i annet:

$$\frac{n!}{k!(n-k)!}\frac{n-k+1}{n-k+1}+\frac{n!}{(k-1)!(n-k+1)!}\frac{k}{k} = \frac{(n-k+1)n! + kn!}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}$$

Påstanden er derfor sann.

$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k-1}$?
Siden den forrige var sann, må denne være gal. For eksempel er $\binom{2}{1} + \binom{2}{0} = 2 + 1 = 3 \neq 1 = \binom{3}{0}$.

Oppgave 4

a) Euklids algoritme på 17 og 3 gir

$$17 = 5.3 + 2,\ \ 3 = 1.2 + 1,\ \ 3 = 3.1 + 0$$

Dermed er $gcd(17, 3) = 1$.
Euklids algoritme på 2883 og 219 gir

$$2883 = 13.219 + 36,\ \ 219 = 6.36 + 3,\ \ 36 = 12.3 + 0$$

så $gcd(2883, 219) = 3$.
Euklids algoritme på 89 og 55:

$$\begin{aligned}
&89 = 1.55 + 34\\
&55 = 1.34 + 21\\
&34 = 1.21 + 13\\
&21 = 1.13 + 8\\
&13 = 1.8 + 5\\
&8 = 1.5 + 3\\
&5 = 1.3 + 2\\
&3 = 1.2 + 1\\
&2 = 2.1 + 0
\end{aligned}$$

så $gcd(89, 55) = 1$.

b) Likningen $18x + 42y = c$ har løsning hvis og bare hvis $gcd(18, 42)|c$. Så vi regner først ut denne, med Euklids algoritme:

$$42 = 2.18 + 6, \ \ 18 = 3.6 + 0$$

Så kriteriet er at likningen kan løses hvis og bare hvis $6|c$. Det er sant for $6, 30 = 5.6$ og $-78 = -13.6$, men ikke for $1, 2, 3$.

Oppgave 5

Det finnes uendelig mange primtall på formen $4n + 3$?
Det finnes uendelig mange primtall på formen $4n + 3$. Dette beviste vi på forelesning (der vi fulgte boken); det er også et spesialtilfelle av Dirichlets teorem, som sier at det finnes uendelig mange primtall på formen $an + b$ hvis og bare hvis $gcd(a, b) = 1$. Så denne påstanden er sann.

Det finnes uendelig mange primtall på formen $3n + 6$?
Det finnes ikke uendelig mange primtall på formen $3n + 6$. Det følger av Dirichlets teorem som over, eller vi kan direkte observere at alle disse tallene kan deles på 3. Så denne påstanden er ikke sann.

Det finnes heltall a og b slik at $\sqrt{3} = \frac{a}{b}$?
Det finnes ikke heltall a og b slik at $\sqrt{3} = \frac{a}{b}$. For om det var mulig, kunne vi anta at a og b er relativt primiske (forkort eventuelle felles divisorer i brøken); dermed finnes det heltall x og y slik at $ax + by = 1$. Men da ville vi hatt

$$\sqrt{3} = \sqrt{3}(ax + by) = (\sqrt{3}a)x + (\sqrt{3}b)y = 3bx + ay$$

som ville bety at $\sqrt{3}$ er et heltall, som er umulig! Dermed er påstanden gal.

Jon Eivind Vatne