

Løsninger til talteori

Opgave 1

For et primtal p lad α_k , α_m og α_n være de størst mulige hele tal så p^{α_k} , p^{α_m} og p^{α_n} går op i henholdsvis k , m og n . Da $m^n \mid n^m$, må $n\alpha_m \leq m\alpha_n$, og tilsvarende da $n^k \mid k^n$ må $k\alpha_n \leq n\alpha_k$. Ved at kombinere de to uligheder får vi $k\alpha_m \leq m\alpha_k$. Da dette gælder for alle primtal, må $m^k \mid k^m$.

Opgave 2

Antag at der findes sådan en tripel, og lad (a, b, c) være den tripel som har mindst mulig a . Da $2a + b > 1$ og $2b + a > 1$, må de begge være 2'er potenser, og dermed må a og b begge være lige. Sæt $a = 2a'$ og $b = 2b'$. Da er $(2a' + b')(2b' + a') = 2^{c-2}$, og da $a', b' \geq 1$, må $c' = c - 2 > 0$. Dermed er (a', b', c') også en tripel som opfylder ligningen, hvilket er i modstrid med at (a, b, c) var valgt så a var mindst mulig. Dermed findes ingen tripler som løser ligningen.

Opgave 3

Antag at $\frac{p}{x} + \frac{q}{y} = n$. Da er $py + qx = nxy$. Af dette ses at x går op i py , og da p er et primtal større end x , må x gå op i y . På tilsvarende vis ses at y går op i x . Dermed er $x = y$.

Opgave 4

Antag at $\sigma(a) > 2a$, og bemærk at hvis d er divisor i a , da er bd divisor i ab . Lad d_1, d_2, \dots, d_m være samtlige positive divisorer i a . Da er $\sigma(ab) \geq bd_1 + bd_2 + \dots + bd_m = b\sigma(a) > 2ab$.

Opgave 5

Lad $x + y = 2^a$ og $xy + 1 = 2^b$. Antag først at $x + y \leq xy + 1$, dvs. at $a \leq b$. Dermed går 2^a op i $xy + 1$ og $-x \equiv y \pmod{2^a}$. Vi har nu $0 \equiv 1 + xy \equiv 1 - x^2 \equiv x^2 - 1 = (x + 1)(x - 1) \pmod{2^a}$. Da $x + 1$ og $x - 1$ ikke begge kan være delelige med 4, må 2^{a-1} gå op i $x + 1$ eller $x - 1$. Dette giver løsningerne $(1, 2^a - 1)$, $(2^a - 1, 1)$, $(2^{a-1} - 1, 2^{a-1} + 1)$, $(2^{a-1} + 1, 2^{a-1} - 1)$.

Til slut antager vi at $x + y > xy + 1$. Dette giver $0 > xy - x - y + 1 = (x - 1)(y - 1)$, hvilket er umuligt da x og y er positive heltal.

Opgave 6

Hvis $n = m$, er $\frac{n^2+m^2}{nm} = 2$, og hvis $n = 1$ og $m > 1$, er $\frac{n^2+m^2}{nm} = \frac{1+m^2}{m}$ ikke et heltal. Antag derfor at $n \neq m$ og $n, m > 1$. Lad p være et primtal som går op i m , og sæt $m = p^s a$ og $n = p^t b$, hvor $s \geq 1$ og $t \geq 0$. Vi kan uden tab af generalitet antage at $s \geq t$. Da

$$\frac{m^2 + n^2}{mn} = \frac{p^{2s}a^2 + p^{2t}b^2}{p^{s+t}ab} = \frac{p^{2(s-t)}a^2 + b^2}{p^{s-t}ab},$$

må $s = t$ hvis brøken skal være et heltal. Da p var et tilfældigt primtal, må $m = n$.

Dermed er den eneste mulige heltallige værdi af $\frac{m^2+n^2}{mn}$ tallet 2.

Opgave 7

Da d er en ægte divisor i $n!$, findes et helt tal s , $1 < s < n!$, så $ds = n!$. Lad p være det mindste primtal som går op i s . Da er $(p - 1, s) = 1$, og da $(p - 1)$ går op i $n!$, må $p - 1$ også gå op i d . Sæt $f = \frac{d}{p-1}$. Da vil f oplagt gå op i $n!$, og $f + d = \frac{d+d(p-1)}{p-1} = \frac{pd}{p-1} = pf$. Vi ved at f går op i d , og p går op i s , og dermed også at $f + d = pf$ går op i $ds = n!$.

Opgave 8

Der findes hele tal a og b så $(n, m) = an + bm$. Dermed er

$$\frac{(n, m)}{n} \binom{n}{m} = \frac{an + bm}{n} \binom{n}{m} = a \binom{n}{m} + b \binom{n-1}{m-1},$$

hvilket er et helt tal.

Opgave 9

Der gælder at $f(m) = 2m - 1$. Vi viser først at $f(m) \geq 2m - 1$, derefter at $f(p) \leq 2p - 1$ for et primtal p , og til sidst at hvis $f(u) = 2u - 1$ og $f(v) = 2v - 1$, da er $f(uv) \leq 2uv - 1$, da dette samlet beviser påstanden.

Mængden som indeholder $m - 1$ nuller og $m - 1$ et-taller, indeholder ikke en delmængde med m elementer hvis sum er delelig med m . Dermed er $f(m) \geq 2m - 1$.

Lad p være et primtal, og lad $x_1, x_2, \dots, x_{2p-1}$ være $2p - 1$ vilkårlige hele tal. Vi kan uden tab af generalitet antage at $0 \leq x_i \leq p - 1$ da vi kun er interesseret i deres rest modulo p . Vi kan yderligere antage at $x_1 \leq x_2 \leq x_3 \leq \dots \leq x_{2p-1}$. For $1 \leq i \leq p - 1$, sæt $y_i = x_{p+i} - x_i$, dvs. at $0 \leq y_i \leq p - 1$. Hvis $y_i = 0$ for et eller andet i , da er $x_{i+1} = x_{i+2} = \dots = x_{i+p}$, og dermed har vi p tal hvis sum er delelig med p .

Vi betragter nu tilfældet hvor $y_i > 0$ for alle $i = 1, 2, \dots, p - 1$. Sæt $s = x_1 + x_2 + \dots + x_p$. Hvis vi udskifter x_i med x_{i+p} , vokser summen med y_i . Vi ønsker derfor at finde en delmængde af $\{y_1, y_2, \dots, y_{p-1}\}$ hvis sum er $-s \pmod{p}$, for da kan vi opnå at en sum af p af x 'erne er delelig med p . Lad A_k , $k = 1, 2, \dots, p - 1$, være mængden af hele tal $i \in \{0, 1, 2, \dots, p - 1\}$ for hvilke der findes en delmængde af $\{y_1, y_2, \dots, y_k\}$ hvis sum har rest i ved division med p . Summen af den tomme mængde sættes til 0. Vi ønsker at vise at A_{p-1} indeholder samtlige rester, for da indeholder den også $-s$. Antag at der findes et $j \in \{1, 2, \dots, p - 2\}$ så $A_j = A_{j+1}$. Da $y_{j+1} \in A_{j+1} = A_j$, må $2y_{j+1} = y_{j+1} + y_{j+1} \in A_{j+1} = A_j$, og yderligere $3y_{j+1} = 2y_{j+1} + y_{j+1} \in A_{j+1} = A_j$, osv. Da $(p, y_{j+1}) = 1$, opnår vi på denne måde samtlige rester af p , dvs. at $A_j = \{0, 1, 2, \dots, p - 1\}$. Hvis der ikke findes et j så $A_j = A_{j+1}$, da må A_{j+1} indeholde mindst et element mere end A_j for alle j , og da $A_1 = \{0, y_1\}$ indeholder to elementer, må A_{p-1} indeholde mindst p elementer og dermed samtlige rester. Vi har nu vist at der findes en delmængde af $\{y_1, y_2, \dots, y_k\}$ hvis sum har rest $-s$ modulo p , og dermed en delmængde med p elementer af $\{x_1, x_2, \dots, x_{2p-1}\}$ hvis sum er delelig med p . Vi har nu vist at $f(p) \leq 2p - 1$.

Antag nu at $f(u) = 2u - 1$ og $f(v) = 2v - 1$. Vi betragter nu en delmængde med $2uv - 1$ hele tal. Hver gang vi vælger $2u - 1$ af tallene, findes der ifølge antagelsen en delmængde med u tal hvis sum er delelig med u . Når vi har gjort dette $2v - 2$ gange, er der stadig $2u - 1$ tal tilbage, dvs. vi kan vælge en delmængde af disse tal bestående af u tal hvis sum er delelig med u . Vi har på denne måde ud af de $2uv - 1$ hele tal opnået $2v - 1$ disjunkte delmængder, hver med u elementer og en sum der er delelig med u . Summen af den første delmængde vi vælger, kalder vi $s_1 = a_1u$, summen af den anden $s_2 = a_2u$, osv. Ud fra antagelsen ved vi at vi blandt $a_1, a_2, \dots, a_{2v-1}$ kan vælge v tal hvis sum er delelig med v . Vi kan uden tab af generalitet antage at det netop er a_1, a_2, \dots, a_v . Nu ved vi, at hvis vi tager alle elementerne i de første v delmængder med u elementer som vi valgte fra den store mængde med $2uv - 1$ elementer, da er summen af disse uv elementer $u(a_1 + a_2 + \dots + a_v)$ hvilket er deleligt med uv . Vi har dermed vist at $f(uv) \leq 2uv - 1$. Samlet har vi vist at $f(m) = 2m - 1$.

Opgave 10

Sæt $m = p_1 p_2 \dots p_n$. Det er velkendt at $2^u + 1$ går op i $2^m + 1$ hvis u går op i m . Hvis a og b er ulige og indbyrdes primiske, er

$$(2^a + 1, 2^b + 1) | (2^{2a} - 1, 2^{2b} - 1) = 2^{(2a, 2b)} - 1 = 2^2 - 1 = 3,$$

og da a og b er ulige, må $(2^a + 1, 2^b + 1) = 3$. Samlet har vi at hvis u og v er ulige og indbyrdes primiske, og hvis begge går op i m , da vil $\frac{(2^u+1)(2^v+1)}{3}$ gå op i $2^m + 1$.

Vi viser nu ved induktion efter n at $2^m + 1$ har mindst 4^n forskellige divisorer. For $n = 1$ ved vi at $3 | 2^m + 1$, samt at $\frac{2^m+1}{3} > 3$, og dermed er $1, 3, \frac{2^m+1}{3}, 2^m + 1$ fire forskellige divisorer i $2^m + 1$. Antag nu at for $m = p_1 p_2 \dots p_n$ har $2^m + 1$ mindst 4^n divisorer. Vi betragter nu $m' = p_1 p_2 \dots p_n p_{n+1}$. Fra før ved vi at $k = (2^m + 1) \frac{2^{p_{n+1}} + 1}{3}$ går op i $2^{m'} + 1$, og da $2^m + 1$ har mindst 4^n divisorer, må k have mindst $2 \cdot 4^n$ divisorer. Vi mangler nu blot at vise at $2^{m'} + 1$ har mindst dobbelt så mange divisorer som k , og til dette får vi brug for følgende ulighed:

$$k^2 = \frac{(2^{m+p_{n+1}} + 2^m + 2^{p_{n+1}} + 1)^2}{9} < \frac{(2 \cdot 2^{m+p_{n+1}} + 1)^2}{9} =$$

$$\frac{4 \cdot 2^{2(m+p_{n+1})} + 4 \cdot 2^{m+p_{n+1}} + 1}{9} < 2^{2(m+p_{n+1})} + 1 < 2^{mp_{n+1}} + 1 = 2^{m'} + 1.$$

Undervejs har vi benyttet at $2(m + p_{n+1}) < mp_{n+1}$, da $m, p_{n+1} \geq 5$. Ifølge uligheden er $l = \frac{2^{m'}+1}{k} > k$, og dvs. at for hver divisor a i k , har vi yderligere en divisor la i $2^{m'} + 1$. Dermed er antal divisorer i $2^{m'} + 1$ mindst $2 \cdot 2 \cdot 4^n = 4^{n+1}$, og induktionen er fuldført.