Her ere de to mellemste Determinanter lige store og hæve hinanden, og det ses, at den nødvendige og tilstrækkelige Betingelse for, at Ligningen bliver homogen i $\frac{df}{dx}, \frac{df}{dy}, \frac{df}{dz}$ er, at den første Determinant er $= 0$. Den tilhørende partielle Differentialligning af første Orden bliver

$$\begin{vmatrix} A & F & E & p \\ F & B & D & q \\ E & D & C & -1 \\ p & q & -1 & 0 \end{vmatrix} = 0.$$

TALTHEORETISKE UNDERSØGELSER.

(AF A. S. BANG).

(Fortsat, se S. 80).

9. Da man for $a > 1$ har

$$F_{p^n}(a) = (a^{p^{n-1}})^{p-1} + (a^{p^{n-1}})^{p-2} + \ldots a^{p^{n-1}} + 1 > p,$$

vil $F_{p^n}(a)$ indeholde mindst en Primfaktor af Formen $\alpha p^n + 1$. Her kan n være 1, naar undtages $p = 2$.

For at bevise, at $F_t(a)$ indeholder mindst en Primfaktor af Formen $\alpha t + 1$, maa man vise, at $F_t(a) > p_1$, idet $p_1 = \alpha p_2 p_3 \ldots p_n + 1$.

Først kan det vises, at $F_t(a)$ eller $F_{p_1 p_2 \ldots p_n}(b)$ er større end 1. Var dette ikke Tilfældet, havde man $F_{p_1 p_2 \ldots p_n}(b) = 1$, hvoraf følger

$$(b^{p_1 p_2 \ldots p_n} - 1)(b^{p_1 p_2 \ldots p_{n-2}} - 1)(b^{p_1 p_2 \ldots p_{n-3} p_{n-1}} - 1) \ldots =$$
$$(b^{p_1 p_2 \ldots p_{n-1}} - 1)(b^{p_1 p_2 \ldots p_{n-2} p_n} - 1) \ldots$$

Udføres Multiplikationen og lægges 1 til paa begge Sider af Lighedstegnet, ville Leddene paa den ene Side ende med $\pm b$, paa den anden Side med $\pm b^{p_n}$, idet p_n er det mindste af Primtallene. Efter Division med b vil da det ene Udtryk være $\equiv 0$, medens det andet $\equiv \pm 1$ for Modulus b, hvilket er umuligt, saa at $F_t(a) > 1$.

Saafremt $F_t(a)$ ikke er delelig med p_1, som er den største af Primfaktorerne i t, maa altsaa $F_t(a)$ indeholde mindst en Primfaktor af Formen $\alpha t + 1$.

Er derimod $p_1 = \alpha . p_2 p_3 \dots p_n + 1$, og tilfredsstiller den den i 8 stillede Betingelse, er p_1 Faktor i $F_t(a) = F_{p_1 p_2 \dots p_n}(b)$, saa at man for at bevise, at $F_t(a)$ indeholder mindst en Primfaktor af Formen $\alpha t + 1$, skal bevise, at $F_{p_1 p_2 \dots p_n}(b) > p_1$, naar $p_1 = \alpha p_2 p_3 \dots p_n + 1$.

Nu er $F_{p_1}(b) = b^{p_1 - 1} + b^{p_1 - 2} + \dots b + 1$, saa at

$$b^{p_1} > F_{p_1}(b) > b^{p_1 - 1}, \text{ hvoraf}$$

$$b^{p_1 p_2 - p_1 + 1} > F_{p_1 p_2}(b) = \frac{F_{p_1}(b^{p_2})}{F_p(b)} > b^{p_1 p_2 - p_1 - p_2} \text{ og}$$

$$b^{p_1 p_2 p_3 - p_1 p_2 - p_1 p_3 + p_1 + p_2 + p_3} > F_{p_1 p_2 p_3}(b) > b^{p_1 p_2 p_3 - p_1 p_2 - p_1 p_3 - p_2 p_3 + p_1 - 1}.$$

Det sidste Udtryk kan skrives

$$b^{p_1 (p_2 - 1)(p_3 - 1) + p_2 + p_3} > F_{p_1 p_2 p_3}(b) > b^{p_1 (p_2 - 1)(p_3 - 1) - p_1 p_2 - 1},$$

hvorpaa man faar

$$b^{p_1 (p_2 - 1)(p_3 - 1)(p_4 - 1) + p_2 p_3 + p_2 p_4 + p_3 p_4 + 1} > F_{p_1 p_2 p_3 p_4}(b) > b^{p_1 (p_2 - 1)(p_3 - 1)(p_4 - 1) - p_2 p_3 p_4 - p_2 - p_3 - p_4}.$$

Fortsættes saaledes, faar man

$$b^{p_1 (p_2 - 1) \dots (p_n - 1) + S_2} > F_{p_1 p_2 \dots p_n}(b) > b^{p_1 (p_2 - 1) \dots (p_n - 1) - S_1},$$

hvor $S_1 = p_2 . p_3 \dots p_n \left(1 + \frac{1}{p_2 p_3} + \frac{1}{p_2 p_4} + \dots \frac{1}{p_2 p_3 p_4 p_5} + \dots\right)$

og $\quad S_2 = p_2 . p_3 \dots p_n \left(\frac{1}{p_2} + \frac{1}{p_3} + \dots \frac{1}{p_2 p_3 p_4} + \dots\right)$,

hvilket kan bevises exakt ved Induktion.

Var nu $F_t(a) = p_1$, maatte man have

$$p_1 > b^{p_1 (p_2 - 1) \dots (p_n - 1) - S_1}$$

eller $\quad p_1 - 1 \geqq b^{p_1 (p_2 - 1) \dots (p_n - 1) - S_1}$,

hvilket er umuligt, da man kan bevise, at

$$b^{p_1 (p_2 - 1) \dots (p_n - 1)} > (p_1 - 1) b^{2 S_1}.$$

Af Værdierne for S_1 og S_2 følger

$$S_1 + S_2 = (p_2 + 1)(p_3 + 1) \dots (p_n + 1)$$

og $\quad S_1 - S_2 = (p_2 - 1)(p_3 - 1) \dots (p_n - 1)$,

altsaa $\quad 2 S_1 = (p_2 + 1)(p_3 + 1) \dots + (p_2 - 1)(p_3 - 1) \dots$, hvilket tilligemed Indsættelse af Værdien af p_1 giver, at man skal have Uligheden

$$b^{\alpha p_2 p_3 \ldots p_n (p_2-1)\ldots(p_n-1)} > \alpha p_2 p_3 \ldots p_n b^{(p_2+1)(p_3+1)\ldots(p_n+1)}.$$

Vi antage, for at bevise, at denne Ulighed finder Sted, først at alle Primtallene ere ulige.

Da er $p_2 > 2$, hvoraf følger, da $b > 1$,

$$b^{p_2(p_2-1)} > p_2\, b^{p_2+1},$$

og da $x^\alpha \geqq \alpha x$, faar man heraf

$$b^{\alpha p_2(p_2-1)} > \alpha p_2 b^{p_2+1},$$

hvilket giver

$$b^{\alpha p_2 p_3 (p_2-1)(p_3-1)} > p_3\,(\alpha p_2 b^{p_2+1})^{p_3+1} >$$
$$\alpha p_2 p_3 b^{(p_2+1)(p_3+1)} \text{ o. s. v.;}$$

saa at man ikke kan have $F_{p_1 p_2 \ldots p_n}(b) = p_1$, naar alle Primtallene ere ulige.

Indeholdes tillige Faktoren 2, kan man, idet man undtager Tilfældet $t = 6$, paavise, at

$$b^{2\alpha p_2 p_3 \ldots p_n (p_2-1)\ldots(p_n-1)} >$$
$$2\alpha p_2 p_3 \ldots p_n\, b^{3\cdot(p_2+1)(p_3+1)\ldots(p_n+1)}.$$

Der vil da blandt $p_2, p_3 \ldots p_n$ findes mindst et p_2, som er lig eller større end 5, og da i saa Tilfælde

$$b^{2p_2(p_2-1)} > 2p_2\, b^{3(p_2+1)},$$

idet nemlig

$$b^{2p_2(p_2-1)-3(p_2+1)} = b^{(2p_2+1)(p_2-3)} > 2p_2, \text{ da } p_2 > 3,$$

faar man heraf

$$b^{2\alpha p_2(p_2-1)} > 2\alpha p_2 b^{3(p_2+1)}$$

og som før

$$b^{2\alpha p_2 p_3 (p_2-1)(p_3-1)} > 2\alpha p_2 p_3 b^{3(p_2+1)(p_3+1)} \text{ o. s. v.,}$$

hvorved er bevist, at $F_{2p_1 p_2 \ldots p_n}(b) > p_1$.

Tilbage haves Tilfældet $F_6(b)$, i hvilket Tilfælde $t = 2^n \cdot 3^m$. Naar $F_6(b)$ ikke indeholder nogen Primfaktor af Formen $6\alpha + 1$, er $F_6(b) = b^2 - b + 1 = 3$, altsaa $b = 2$, og da

$$b = a^{2^{n-1}\cdot 3^{m-1}}, \text{ bliver } n = 1,\ m = 1 \text{ og } a = 2.$$

Heraf følger, at naar t indeholder 2 eller flere Primfaktorer, vil $F_t(a)$, naar undtages $F_6(2)$, indeholde mindst en Primfaktor af Formen $\alpha t + 1$.

I Forbindelse med det foregaaende, giver dette, at naar $a > 1$ og $t > 2$ og man undtager $F_6(2)$, vil $F_t(a)$ indeholde mindst en Primfaktor af Formen $\alpha t + 1$.

Da endvidere $F_t(a)$ er en Faktor i $a^t - 1$, og

$a^2 - 1 = (a - 1)(a + 1)$ kun kan være en Potens af 2, naar saavel $a - 1$ som $a + 1$ ere det, hvilket giver $a = 3$, samt

$2^6 - 1$ er delelig med 7, faar man heraf, at

$a^t - 1$, naar a og t ere større end 1, samt man undtager $3^2 - 1$, indeholder mindst en Primfaktor af Formen $\alpha t + 1$.

10. Sætningerne kunne udvides, idet

$a^m - b^m$ og $a^n - b^n$ have største fælles Faktor $a^s - b^s$, naar s er st. f. F. for m og n, samt a primisk med b.

Saaledes vil $b^{\varphi(t)} \cdot F_t\left(\frac{a}{b}\right)$ foruden Primfaktorer af Formen $\alpha t + 1$ kun kunne indeholde p_1, naar p_1 gaar op i t og $p_1 - 1$ er delelig med de øvrige af t's Primfaktorer.

11. Ved Hjælp af Sætningen i 9 kan man bevise, at i en Differensrække, hvis første Led er 1, findes der uendelig mange Primtal.

At der altid findes Primtal, følger af, at $a^t - 1$, idet Differensen er t, vil indeholde mindst et Primtal af Formen $\alpha t + 1$.

Var nu Rækken af Primtal i Differensrækken endelig, bestaaende af Primtallene $p_1, p_2 \ldots p_n$, fik man, at Tallet $(p_1 . p_2 \ldots p_n)^t - 1$ maatte indeholde mindst et Primtal, forskjelligt fra $p_1, p_2 \cdots p_n$ hørende til Differensrækken, saa at Antagelsen er fejl og Rækken indeholder uendelig mange Primtal.

Det er saaledes lykkedes, elementært at bevise et specielt Tilfælde af den almindelige, af Lejeune-Dirichlet beviste Sætning:

I en Differensrække, hvis første Led og Differens ere primiske, findes uendelig mange Primtal, en Sætning, som tidligere kun er bevist ved Hjælp af Integralregning.

12. Borttages de Primtal, som give Resten 1 for Divisor t, vil der være uendelig mange tilbage.

Var Rækken endelig, bestaaende af Primtallene $p_1, p_2 \ldots p_n$, skulde $t . p_1 . p_2 \ldots p_n + \alpha$, hvor α er mindre end og primisk med t, dog ikke 1, bestaa af lutter Primfaktorer, som give Resten 1 for Divisor t, hvilket er umuligt, da Produktet af Primfaktorerne i saa Fald maatte give Resten 1 for Divisor t, medens det giver Resten α.

Specielt faar man heraf, at Primtallene af hver af Formerne $3\alpha - 1$, $4\alpha - 1$ og $6\alpha - 1$ gaa i det Uendelige.

(Primtallene af Formen $3\alpha - 1$ ere paa Primtallet 2 nær de samme som Primtallene af Formen $6\alpha - 1$).

Borttages de Primtal, som give en af Resterne ± 1 for Divisor t, vil der være uendelig mange tilbage.

Beviset herfor er som før, kun maa α ikke være 0 eller ± 1, af hvilken Grund Sætningen ikke kan anvendes paa de før nævnte specielle Tilfælde, da der ikke var Primtal, som gav andre Rester end ± 1.

13. Idet t gaar op i $a^n - 1$ og man borttager de Primtal, som give en af Resterne $1, a, a^2 \ldots a^{n-1}$ for Divisor t, vil der være uendelig mange tilbage.

Var Rækken endelig, bestaaende af $p_1, p_2 \ldots p_n$, fik man, at $t . p_1 p_2 \ldots p_n + \alpha$, hvor α er mindre end og primisk med t samt forskjellig fra $1, a, a^2 \ldots a^{n-1}$, skulde bestaa af lutter Primfaktorer, som give en af Resterne $1, a, a^2 \ldots a^{n-1}$ for Divisor t, men Produktet af saadanne Tal giver en Rest, som er en Potens af a, altsaa da $a^n \equiv 1$, en af Resterne $1, a, a^2 \ldots a^{n-1}$, hvilket er umuligt, da det giver Resten α.

Specielt faar man, at der findes uendelig mange Primtal, som give en af Resterne 3 eller 7 for Divisor 8.

Gaar t op i $a^n + 1$ og man borttager de Primtal, som give en af Resterne $\pm 1, \pm a, \pm a^2 \ldots \pm a^{n-1}$ for Divisor t, vil der være uendelig mange tilbage.

Beviset er som før, kun maa α ikke være

$$\pm 1, \pm a, \pm a^2 \ldots \pm a^{n-1}.$$

14. Det er bekjendt, at en Kongruens af n'te Grad

$$x^n + a_1\ x^{n-1} + a_2\ x^{n-2} + \ldots + a_n \equiv 0\ (mod\ p)$$

højst har n Rødder.

Saafremt den har Rødderne $\alpha_1,\ \alpha_2 \ldots \alpha_n$, kan man bevise, at

$$\begin{aligned} \alpha_1 + \alpha_2 + \ldots \alpha_n &\equiv - a_1 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots \alpha_{n-1}\,\alpha_n &\equiv a_2 \\ \alpha_1\alpha_2\alpha_3 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n &\equiv - a_3 \\ &\vdots \\ \alpha_1\alpha_2\alpha_3 \ldots \alpha_n &\equiv + (-1)^n a_n. \end{aligned}$$

Sætter man nemlig venstre Side identisk lig med

$$(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) + f(x) \equiv 0\ (mod\ p),$$

maa $f(x)$ højst være af Graden $n - 1$, men den tilfredsstilles af de n Rødder $\alpha_1,\ \alpha_2 \ldots \alpha_n$, og maa følgelig være identisk $\equiv 0$, det vil sige, dens Koefficienter maa alle være delelige med p, hvoraf Sætningen følger, da Koefficienterne til samme Led i begge Kongruenser maa være lige store.

Vi skulle nu give nogle Anvendelser af denne Sætning.

Er p et Primtal, vil Kongruensen $x^{p-1} - 1 \equiv 0\ (mod\ p)$ i Følge Fermats Sætning have de $p - 1$ Rødder $1, 2, 3 \ldots p - 1$, hvoraf følger de bekjendte Sætninger, at

Summen af Produkterne af n og n af de første $p - 1$ Tal, naar $n < p - 1$, er delelig med p, og at

Produktet af de første $p - 1$ Tal er kongruent med $- 1$ for Modulus p (Wilsons Sætning).

Er $2n + 1$ et Primtal, ville Tallene $1^2,\ 2^2,\ 3^2 \ldots n^2$ give forskjellige Rester for Divisor $2n + 1$, hvoraf følger, at Kongruensen $x^n - 1 \equiv 0\ (mod\ 2n + 1)$ har Rødderne $1^2,\ 2^2 \ldots n^2$. Heraf kan man udlede Sætningerne:

Summen af Produkterne af r og r af de første n Kvadrattal, naar $r < n$, vil være delelig med $2n + 1$, samt

Produktet af de første n Kvadrattal vil være kongruent med ± 1, eftersom n lige eller ulige, for Modulus $2n + 1$. (Opgave 480 her i Tidsskriftet).

15. Den nævnte Sætning skal endvidere benyttes til Under-

søgelse af de Tal, som for Primtallet p høre til Exponenten n, det vil sige, for hvilke den n'te Potens er den laveste, hvortil de skulle opløftes for at give Resten 1 for Divisor p.

For at der overhovedet skal gives Tal, som gjøre $x^n \equiv 1$, maa n være en Divisor i $p-1$.

Ere nu n's Divisorer $n, n', n'' \ldots$, da er

$$x^n - 1 = F_n(x) \,.\, F_{n'}(x) \,.\, F_{n''}(x) \ldots,$$

hvoraf følger, da ethvert Tal, som tilfredsstiller Kongruensen $F_{n^r}(x) \equiv 0$ tillige tilfredsstiller $x^{n^r} - 1 \equiv 0$, at de Tal, som høre til Exponenten n, maa være Rødder i $F_n(x) \equiv 0$, saa at der højst findes $\varphi(n)$ Rødder.

At der netop findes $\varphi(n)$ Rødder, følger af, at idet Divisorerne i $p-1$, ere $1, \alpha, \beta \ldots p-1$, da er

$$\varphi(1) + \varphi(\alpha) + \varphi(\beta) + \ldots \varphi(p-1) = p-1,$$

saa at, hvis der fandtes mindre end $\varphi(n)$ Rødder, da maatte $x^{p-1} - 1 \equiv 0$ have mindre end $p-1$ Rødder.

Da $F_n(x)$ ender med Leddet $+1$, idet Tæller og Nævner i Udtrykket for $F_n(x)$ begge ende paa plus eller minus 1, og Tallene $< p$ hørende til Exponenten n, ere Rødder i $F_n(x) \equiv 0$, er Produktet af de $\varphi(n)$ Rødder, som for Primtallet p høre til Exponenten n, kongruent med ± 1, eftersom $\varphi(n)$ ulige eller lige. Et specielt Tilfælde, nemlig for $n = p-1$, er den bekjendte Sætning:

Produktet af de $\varphi(p-1)$ primitive Rødder til Primtallet p, er for $p > 3$ kongruent med -1, for $p = 3$ kongruent med $+1$.

Gauss har desuden angivet Sætningen:

Summen af de primitive Rødder er kongruent med 0, naar $p-1$ er delelig med et Kvadrat, med ± 1 naar $p-1$ er Produktet af et lige eller ulige Antal Primfaktorer.

Denne gjælder mere almindelig for Tallene, hørende til Exponenten n, for hvilket Tilfælde den ogsaa her skal bevises. Da

$$F_n(x) = F_{p_1 p_2 \ldots p_n}\left(x^{p_1^{a_1-1} \,.\, p_2^{a_2-1} \ldots p_n^{a_n-1}}\right),$$
$$\text{idet } n = p_1^{a_1} \,.\, p_2^{a_2} \ldots p_n^{a_n},$$

vil $F_n(x)$ kun indeholde Potenser af x, hvis Exponenter ere delelige med $p_1^{\alpha_1-1} . p_2^{\alpha_2-1} \dots p_n^{\alpha_n-1}$, hvoraf følger, at naar kun en af Exponenterne $\alpha_1, \alpha_2 \dots \alpha_n$ er større end 1, vil Koefficienten til Leddet $x^{\varphi(n)-1}$ i $F_n(x)$ være Nul, og da Summen af Tallene hørende til Exponenten n er kongruent med denne Koefficient med modsat Fortegn, vil Summen være kongruent med 0.

Ere $\alpha_1, \alpha_2 \dots \alpha_n$ alle 1, faar man

$$F_n(x) = \frac{(x^{p_1 p_2 \dots p_n} - 1)\,(x^{p_1 p_2 \dots p_{n-2}} - 1)\dots}{(x^{p_1 p_2 \dots p_{n-1}} - 1)\dots}.$$

Er nu n lige, bliver ved Udførelse af Multiplikationen i Tælleren og i Nævneren

$$F_n(x) = \frac{x^\alpha - x^{\alpha-1} - \dots}{x^\beta - x^{\beta - p_n} - \dots},$$

idet p_n er det mindste af Primtallene, saa at man faar, da $\alpha - \beta = \varphi(n)$,

$$F_n(x) = x^{\varphi(n)} - x^{\varphi(n)-1} + \dots,$$

saa at Summen af Rødderne er kongruent med $+1$. n ulige giver $F_n(x) = \dfrac{x^\alpha - x^{\alpha-p_n} - \dots}{x^\beta - x^{\beta-1} - \dots}$, hvoraf

$$F_n(x) = x^{\varphi(n)} + x^{\varphi(n)-1} + \dots,$$

saa at Summen af Rødderne er kongruent med -1.

LØSNING AF OPGAVERNE 321 OG 537.

321. De n Ligninger

$$\begin{aligned}
&ax_1x_2 + bx_1 + cx_2 + d = 0,\\
&ax_2x_3 + bx_2 + cx_3 + d = 0,\\
&ax_3x_4 + bx_3 + cx_4 + d = 0,\\
&\dots\dots\dots\dots\dots\dots\\
&ax_rx_{r+1} + bx_r + cx_{r+1} + d = 0,\\
&\dots\dots\dots\dots\dots\dots\\
&ax_{n-1}x_n + bx_{n-1} + cx_n + d = 0,\\
&ax_nx_1 + bx_n + cx_1 + d = 0,
\end{aligned}$$