

TALTEORI

Wilsons sætning og Euler-Fermats sætning.

Disse noter forudsætter et grundlæggende kendskab til talteori som man kan få i Marianne Terps og Peter Trosborgs noter om talteori.

Noterne vil primært introducere forskellige opgaveteknikker hvor man skal benytte Wilsons sætning eller Euler-Fermats sætning.

1 Wilsons sætning

I Marianne Terps og Peter Trosborgs noter om talteori er Wilsons sætning bevist så her refererer vi den blot.

1.1 Wilsons sætning

For ethvert primtal p gælder

$$(p-1)! \equiv -1 \pmod{p}.$$

1.2 Eksempel

Wilsons sætning kan bl.a. benyttes til at vise at hvis p er et primtal som har rest 1 ved division med 4, da er -1 kvadratisk rest modulo p , dvs. at ligningen $x^2 \equiv -1 \pmod{p}$ har en løsning.

Lad nemlig p være et primtal på formen $p = 4m + 1$. Ifølge Wilsons sætning gælder

$$-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdot \dots \cdot 2m \cdot (-2m) \cdot \dots \cdot (-2) \cdot (-1) \equiv ((2m)!)^2 \pmod{p}.$$

Dvs. at $((2m)!)^2 \equiv -1 \pmod{p}$, og dermed ses at -1 er kvadratisk rest modulo p . Senere skal vi se at -1 ikke er kvadratisk rest modulo primtal på formen $4m + 3$.

1.3 Opgave

Bestem samtlige naturlige tal n for hvilke n går op i $(n-1)! + 1$.

1.4 Opgave

Er det muligt at dele en mængde bestående af ti på hinanden følgende naturlige tal i to disjunkte delmængder, som samlet indeholder alle ti tal, således at produktet af elementerne i hver af de to delmængder bliver det samme tal?

2 Euler-Fermats sætning

I talteori opgaver hvor der indgår potenser, kan det være en hjælp at kende Euler-Fermats sætning. Sætningen er bevist i Marianne Terps og Peter Trosborgs noter om talteori så her refererer vi den blot.

2.1 Euler-Fermat

Lad n være et naturligt tal, og a et helt tal således at $(a, n) = 1$. Da gælder

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

2.2 Fermats lille sætning

Fermats lille sætning er et specialtilfælde af Euler-Fermat:

Før et primtal p og et helt tal a hvor $(p, a) = 1$, gælder

$$a^{p-1} \equiv 1 \pmod{p}.$$

2.3 Eksempel

Euler-Fermats sætning kan bl.a. benyttes til at reducere potensen hvis man fx ønsker at udregne $6^{162} \pmod{25}$. Da $\phi(25) = \phi(5^2) = (5-1)5 = 20$, er $6^{162} = 6^2(6^{20})^8 \equiv 6^2 \equiv 11 \pmod{25}$.

2.4 Inverse elementer

Hvis a og n er to indbyrdes primiske hele tal, da kan Euler-Fermats sætning benyttes til at konstruere en invers til $a \pmod{n}$. En invers til a er et helt tal a^{-1} som opfylder $a \cdot a^{-1} \equiv 1 \pmod{n}$. Ifølge Euler-Fermats sætning er $a^{\phi(n)-1}$ en invers til a da $a^{\phi(n)} \equiv 1 \pmod{n}$.

2.5 Sætning

Lad $(a, n) = 1$, og antag at $a^m \equiv 1 \pmod{n}$. Da gælder at

$$a^{(\phi(n), m)} \equiv 1 \pmod{n}.$$

BEVIS: Den største fælles divisor af to tal kan altid skrives som en linearkombination af tallene, dvs. der findes hele tal s og t så $(\phi(n), m) = s\phi(n) + tm$. Dermed er

$$a^{(\phi(n), m)} = a^{s\phi(n) + tm} = (a^{\phi(n)})^s (a^m)^t \equiv 1 \pmod{n}.$$

2.6 Eksempel

Findes der et helt tal n hvis cifre er lutter 1-taller således at n er delelig med 1999? Ja, det kan man benytte Euler-Fermats sætning til at vise. Da 1999 er et primtal, er $\phi(1999) = 1998$. Der gælder nu at

$$10^{1998} \equiv 1 \pmod{1999}.$$

Dermed går 1999 op i $10^{1998} - 1 = 9 \cdot \underbrace{1111111 \dots 111}_{1998}$, og da $(1999, 9) = 1$, må 1999 gå op

i $\underbrace{1111111 \dots 111}_{1998}$.

Opgaven kan faktisk også løses alene ved brug af skuffeprincippet og simple overvejelser om rester.

2.7 Opgave

Vis at hvis m er et naturligt tal der ikke er delelig med 2, 3 eller 5, da findes et helt tal n hvis cifre er lutter 1-taller således at n er delelig med m .

2.8 Opgave

Lad a og n være to indbyrdes primiske hele tal. Vis at hvis m er det mindste naturlige tal så

$$a^m \equiv 1 \pmod{n},$$

da er m divisor i $\phi(n)$.

2.9 Opgave

Lad m være et ulige naturligt tal, og betragt følgen $a_0 = m$ og $a_n = 2a_{n-1} + 1$ for $n \in \mathbb{N}$.
Vis at der findes uendeligt mange tal i følgen som er delelige med m .

2.10 Opgave

Antag at $n, k \geq 2$ er to naturlige tal.

Vis at da er mindst et af tallene $p = n + k^n$ og $q = nk^{(k^n-1)} + 1$ ikke et primtal.

2.11 Opgave

Bestem alle naturlige tal n , således at $3^n + 1$ er delelig med n^2 . (Baltic Way 2006)

3 Primtal på formen $p = 4m + 3$

Primtal af formen $p = 4m + 1$ og primtal af formen $p = 4m + 3$ har forskellige egenskaber, og her vil vi se på et par af disse.

3.1 Sætning

Der gælder at -1 er kvadratisk rest modulo primtal på formen $p = 4m + 1$, mens -1 ikke er kvadratisk rest modulo primtal på formen $p = 4m + 3$.

BEVIS: Vi har tidligere set at -1 er kvadratisk rest modulo primtal p på formen $p = 4m + 1$. Antag nu at der findes et helt tal x så $x^2 \equiv -1 \pmod{p}$, hvor $p = 4m + 3$. Dette giver at

$$x^{4m+2} = (x^2)^{2m+1} \equiv (-1)^{2m+1} \equiv -1 \pmod{p},$$

men ifølge Euler-Fermat er $x^{4m+2} \equiv 1 \pmod{p}$, hvilket er en modstrid.

3.2 Sætning

Lad p være et primtal på formen $p = 4m + 3$. Hvis p går op i summen af to kvadrattal $a^2 + b^2$, da går p op i både a og b .

BEVIS: Antag at $a^2 + b^2 \equiv 0 \pmod{p}$, og at a ikke er delelig med p . Da findes en invers a^{-1} til a modulo p , og dermed har vi

$$a^2(a^{-1})^2 + b^2(a^{-1})^2 \equiv 0 \pmod{p}.$$

Dette giver

$$1 + (ba^{-1})^2 \equiv 0 \pmod{p},$$

hvilket er en modstrid da -1 ikke er kvadratisk rest modulo p . Derfor må p gå op i a og dermed også i b .

3.3 Korollar

Et specialtilfælde af sætningen er at et primtal p på formen $p = 4m + 3$ ikke kan skrives som sum af to kvadrattal. Primtal på formen $p = 4m + 1$ kan derimod altid skrives som sum af to kvadrattal, og det skal vi se nærmere på om lidt.

3.4 Opgave

Om et helt tal n oplyses at n er kvadrattal, og at samtlige primfaktorer i n er på formen $4m + 3$. (At et tal er kvadrattal betyder at alle primtal i primfaktoropløsningen indgår i 1. potens.)

Vis at n ikke kan skrives som sum af to kvadrattal.

3.5 Opgave

Vis at $n^2 + 3$ ikke er et kubiktal for noget naturligt tal n . (Vink: Udnyt ovenstående teori samt at $m^3 + 1 = (m + 1)(m^2 - m + 1)$.)

For at bevise at primtal på formen $p = 4m + 1$ kan skrives som sum af to kvadrater, har vi brug for følgende sætning.

3.6 Thues sætning

Lad n være et helt tal større end 1, og lad k være det mindste hele tal så $k > \sqrt{n}$, dvs. at $k - 1 \leq \sqrt{n}$.

Antag at a er et tal som er primisk med n . Da findes hele tal x og y , $x, y \in \{1, 2, \dots, k-1\}$, så

$$ay \equiv x \pmod{n} \text{ eller } ay \equiv -x \pmod{n}.$$

BEVIS.

Betragt alle tal på formen $ay' + x'$ hvor $x', y' \in \{0, 1, 2, \dots, k-1\}$. Da der er $k^2 > n$ par x', y' , findes ifølge skuffeprikket mindst to par så $ay' + x'$ har samme rest modulo n . Der findes altså $x_1, x_2, y_1, y_2 \in \{0, 1, 2, \dots, k-1\}$, så $a(y_1 - y_2) \equiv x_2 - x_1 \pmod{n}$, hvor $x_1 \neq x_2$ eller $y_1 \neq y_2$.

Antag at $x_1 = x_2$. Da vil n gå op i $a(y_1 - y_2)$, og da $(a, n) = 1$ vil n gå op i $y_1 - y_2$, dvs. $y_1 = y_2$ da $y_1, y_2 \in \{0, 1, 2, \dots, k-1\}$. Hvis vi antager at $y_1 = y_2$, får vi tilsvarende at $x_1 = x_2$. Dermed er

$$0 < |x_1 - x_2|, |y_1 - y_2| \leq k - 1.$$

Sæt nu $y = |y_1 - y_2|$ og $x = |x_1 - x_2|$. Da er

$$ay \equiv x \pmod{n} \text{ eller } ay \equiv -x \pmod{n}.$$

3.7 Opgave

Lad p være et primtal på formen $p = 4m + 1$. Udnyt Thues sætning samt at -1 er kvadratisk rest modulo p , til at vise at p kan skrives som sum af to kvadrater.

3.8 Opgave

Hvilke positive hele tal n kan skrives som sum af to kvadrater? (Bemærk at nul også regnes for et kvadrat)

4 Løsninger

Opgave 1.3 Hvis p er et primtal, gælder ifølge Wilsons sætning at $(p-1)! \equiv -1 \pmod{p}$, dvs. p går op i $(p-1)! + 1$.

Hvis n ikke er et primtal, findes et primtal p som går op i n , hvor $p < n$. Da p går op i $(n-1)!$, kan p og dermed heller ikke n gå op i $(n-1)! + 1$.

Opgave 1.4 Vi viser indirekte at svaret er nej. Antag at mængden $S = \{n, n+1, \dots, n+9\}$ kan deles i to disjunkte mængder S_1 og S_2 således at produkterne π_1 og π_2 af henholdsvis elementerne i S_1 og S_2 er ens. Blandt ti på hinanden følgende tal kan højst et være deleligt med 11, men hvis et af tallene var deleligt med 11, ville de to produkter ikke være ens. Tallene i S repræsenterer således restklasserne $1, 2, \dots, 10$ modulo 11. Ifølge Wilsons sætning gælder nu at

$$\pi_1^2 = \pi_1 \pi_2 \equiv (11-1)! \equiv -1 \pmod{11}.$$

Men der er ingen rester modulo 11 der opfylder ligningen $x^2 \equiv -1 \pmod{11}$, hvilket er en modstrid. Dermed er antagelsen forkert.

Opgave 2.7 Da $(m, 10) = 1$, gælder ifølge Euler-Fermat at

$$10^{\phi(m)} \equiv 1 \pmod{m}.$$

Dermed går m op i $10^{\phi(m)} - 1 = 3^2 \cdot \underbrace{1111111 \dots 111}_{\phi(m)}$, og da $(m, 3) = 1$, må m gå op i $\underbrace{1111111 \dots 111}_{\phi(m)}$.

Opgave 2.8 Ifølge Sætning 2.5 ved vi at hvis $a^m \equiv 1 \pmod{n}$, da er $a^{(m, \phi(n))} \equiv 1 \pmod{n}$. Hvis m er det mindste naturlige tal som opfylder $a^m \equiv 1 \pmod{n}$, må $(m, \phi(n)) = m$. Dermed er m divisor i $\phi(n)$.

Opgave 2.9 Bemærk først at

$$a_n + 1 = 2(a_{n-1} + 1) = 2^2(a_{n-2} + 1) = \dots = 2^n(a_0 + 1) = 2^n m + 2^n.$$

Dermed er $a_n = 2^n m + 2^n - 1$. Da $\gcd(m, 2) = 1$, er $2^{\phi(m)} \equiv 1 \pmod{m}$.

For $n = k\phi(m)$ er

$$a_n = 2^n m + 2^n - 1 \equiv (2^{\phi(m)})^k - 1 \equiv 1 - 1 = 0 \pmod{m}.$$

Dermed er der uendelige mange tal i følgen som er delelige med m .

Opgave 2.10 Hvis p ikke er et primtal, er vi færdige. Antag derfor at p er et primtal. Da $(p, k) = 1$, gælder ifølge Euler-Fermats sætning at

$$q = nk^{(k^n-1)} + 1 = (p - k^n)k^{p-n-1} + 1 \equiv -k^{p-1} + 1 \equiv 0 \pmod{p}.$$

Da $k, n \geq 2$, er $q = nk^{(k^n-1)} + 1 > n + k^n = p$. Heraf følger at q ikke er et primtal.

Opgave 2.11 Hvis n er lige, er $3^n + 1 \equiv 1 + 1 = 2 \pmod{4}$, og dermed er $3^n + 1$ ikke delelig med n .

Antag nu at n er ulige, og at $3^n + 1$ er delelig med n^2 . Det er klart at $n = 1$ opfylder

betingelsen, så vi antager yderligere at $n > 1$. Lad p være den mindste primdivisor i n . Ifølge antagelsen går p op i $3^{2n} - 1 = (3^n + 1)(3^n - 1)$, og ifølge Euler-Fermat går p op i $3^{p-1} - 1$. Fra Sætning 2.5 ved vi nu at p går op i $3^{(2n, p-1)} - 1 = 3^2 - 1 = 8$, hvilket er en modstrid. (Bemærk at $(2n, p-1) = 2$ da p er den mindste primdivisor i n). Dermed er $n = 1$ den eneste løsning.

Opgave 3.4 Antag at $a^2 + b^2 = n$, og lad $n = p_1 p_2 \dots p_s$. Da er $a^2 + b^2 \equiv 0 \pmod{p_i}$ for alle $i = 1, 2, \dots, s$. Ifølge Sætning 3.2, må p_i gå op i både a og b , dvs. at n går op i a og b hvilket er en modstrid.

Opgave 3.5 Antag at $n^2 + 3 = m^3$. Hvis man betragter ligningen modulo 8, ser man ved at gennemgå de mulige restklasser for n og m at n må være lige samt at m har rest 3 modulo 4. Ifølge antagelsen er

$$n^2 + 2^2 = m^3 + 1 = (m + 1)(m^2 - m + 1).$$

Desuden er $m^2 - m + 1 \equiv 3^3 - 3 + 1 \equiv 3 \pmod{4}$, dvs. at der findes en primdivisor p i $m^2 - m + 1$ som har rest 3 modulo 4. Dermed er $n^2 + 2^2 \equiv 0 \pmod{p}$, og ifølge Sætning 3.2 må p gå op i 2. Dette er en modstrid, og dermed er antagelsen forkert.

Opgave 3.7 Vi ved at der findes et helt tal z så $z^2 + 1 \equiv 0 \pmod{p}$. Da $(z, p) = 1$, findes ifølge Thues sætning hele tal x og y , $0 < x, y < \sqrt{p}$, så

$$zy \equiv x \pmod{p} \text{ eller } zy \equiv -x \pmod{p}.$$

Da $z^2 + 1 \equiv 0 \pmod{p}$, må $(yz)^2 + y^2 \equiv 0 \pmod{p}$, og dermed

$$x^2 + y^2 \equiv 0 \pmod{p}.$$

Da $0 < x^2 + y^2 < 2p$, må $x^2 + y^2 = p$.

Opgave 3.8

De tal der kan skrives som sum af to kvadrater, er netop tal med primfaktoropløsning

$$n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s},$$

hvor $p_i \equiv 1 \pmod{4}$, $q_j \equiv 3 \pmod{4}$, og hvor β_1, \dots, β_s er lige.

Først bemærker vi at hvis to tal kan skrives som sum af to kvadrater, da kan deres produkt også skrives som sum af to kvadrater:

$$(a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (ac + bd)^2 + (ad - bc)^2.$$

Da 2, alle primtal på formen $4m + 1$ samt alle kvadrater kan skrives som sum af to kvadrater, kan alle tal på ovenstående form dermed skrives som sum af to kvadrater.

Antag at $n = a^2 + b^2$, og at primfaktoropløsningen for n indeholder et primtal q hvor $q \equiv 3 \pmod{4}$. Da q går op i en sum af to kvadrater, vil q ifølge sætning 3.2 gå op i både a og b . Dermed vil q^2 gå op i $a^2 + b^2 = n$. Vi reducerer nu n, a^2 og b^2 med q^2 og får $a_1^2 + b_1^2 = n_1$. Hvis n_1 er delelig med q , kan vi gentage proceduren en gang til og se at q^2 vil gå op i n_1 . På denne måde indses at q indgår i primfaktoropløsningen for n i en lige potens.