

TALTEORI

Wilson's 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 se på divisorer eller benytte Wilson's sætning eller Euler-Fermats sætning.

1 Primfaktoropløsning

Ifølge aritmetikkens fundamentalsætning kan ethvert naturligt tal større end 1 primfaktoropløses på entydig måde, og dette er grundlaget for hele talteorien.

1.1 Sætning

Et naturligt tal n større end 1 med primfaktoropløsning

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

har $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m)$ forskellige divisorer.

BEVIS. Enhver divisor i n er på formen

$$p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m},$$

hvor $\beta_i \in \{0, 1, \dots, \alpha_i\}$. Dermed har n i alt $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m)$ forskellige divisorer.

1.2 Eksempel

Denne sætning medfører eksempelvis at samtlige tal med netop p divisorer hvor p er et primtal, netop er alle $(p-1)$ 'te potenser af primtal.

1.3 Opgave

Et naturligt tal n , som højst er 500, har den egenskab at når man vælger et tal m tilfældigt blandt tallene $1, 2, 3, \dots, 499, 500$, så er sandsynligheden $\frac{1}{100}$ for at m går op i n . Bestem den største mulige værdi af n . (Georg Mohr-Konkurrencen 2006)

1.4 Opgave

Lad n være produktet af samtlige tal mindre end en million med præcis 9 divisorer. Vis at n er et kvadrattal.

2 Divisorer

I mange typer opgaver kan det betale sig at se på hvilke mulige divisorer et udtryk kan have eller finde største fælles divisor for to udtryk.

2.1 Eksempel

I dette eksempel vil vi vise at hvis a, b, c og d er naturlige tal således at $ab = cd$, da er $a^n + b^n + c^n + d^n$ et sammensat tal for alle naturlige tal n . Når vi skal vise at $a^n + b^n + c^n + d^n$ er sammensat, skal vi gerne kunne faktorisere udtrykket, og derfor ønsker vi at se på hvilke fælles faktorer a, b, c og d har. Da $ab = cd$, kan vi se at en primdivisor i a også er divisor i c eller d . Dette udnytter vi til at indse at der findes naturlige tal r, s, u og v så $a = ru$, $b = sv$, $c = rs$ og $d = uv$. Nu har vi klarlagt sammenhængen mellem de fire tal og kan derfor faktorisere:

$$a^n + b^n + c^n + d^n = r^n u^n + s^n v^n + r^n s^n + u^n v^n = (r^n + v^n)(s^n + u^n).$$

Da begge faktorer er større end 1 for alle naturlige tal n , er $a^n + b^n + c^n + d^n$ et sammensat tal.

2.2 Opgave

Om tre naturlige tal a, b og c gælder at a er ulige, og at a, b og c ikke har en fælles divisor større end 1. Desuden er

$$\frac{2}{a} + \frac{1}{b} = \frac{1}{c}.$$

Bevis at abc er et kvadrattal.

2.3 Største fælles divisor

Den største fælles divisor og regnereglerne for den kan fx benyttes til at vise at brøken $\frac{n^2+n-1}{n^2+2n}$ er uforkortelig for alle naturlige tal n , da dette er ensbetydende med at største fælles divisor mellem tæller og nævner er 1. Der gælder som bekendt følgende regneregler for den største fælles divisor

$$\gcd(a, b) = \gcd(a, b - ma), m \in \mathbb{Z}.$$

Dermed er

$$\begin{aligned} \gcd(n^2 + n - 1, n^2 + 2n) &= \gcd(n^2 + n - 1, n^2 + 2n - (n^2 + n - 1)) = \gcd(n^2 + n - 1, n + 1) = \\ &= \gcd(n^2 + n - 1 - n(n + 1), n + 1) = \gcd(-1, n + 1) = 1. \end{aligned}$$

2.4 Opgave

Vis at brøken

$$\frac{n^3 + 2n}{n^4 + 3n^2 + 1}$$

er uforkortelig for alle hele tal n .

2.5 Opgave

Lad $a_n = n^2 + 500$ og $g(n) = \gcd(a_n, a_{n+1})$. Vis at g er en begrænset funktion, og bestem den største værdi af g .

2.6 Eksempel

Nu skal vi se et eksempel på hvordan man også i forbindelse med at bestemme største fælles divisor kan benytte moduloregning.

Lad x, m og n være naturlige tal, hvor m er ulige, og $x > 1$.

Vi vil nu bestemme $\gcd(a^m - 1, a^n + 1)$.

Sæt $\gcd(a^m - 1, a^n + 1) = d$. I stedet for at forsøge at reducere dette udtryk regner vi a^{nm} modulo d på to forskellige måder da det kan give os informationer om d .

$$a^{nm} = (a^m)^n \equiv 1^n \equiv 1 \pmod{d}.$$

Desuden er

$$a^{nm} = (a^n)^m \equiv (-1)^m \equiv -1 \pmod{d}.$$

Dermed er $d = 2$ når a er ulige, og $d = 1$ når a er lige.

2.7 Opgave

Bestem samtlige naturlige tal $n, m > 2$ for hvilke $2^n - 1$ går op i $2^m + 1$.

3 Potenser af heltal som divisorer

Når divisorerne er potenser af heltal, kan man udnytte dette.

3.1 Eksempel

I dette eksempel skal vi se på hvordan man udnytter at en potens af et helt tal er divisor i et produkt. Hvis vi ser på ligningen

$$x(x + 1) = y^n,$$

kan vi se at hvis findes er en heltallig løsning, da må både x og $x + 1$ være n 'te potenser af et helt tal da to på hinanden følgende hele tal ikke har nogen fælles divisorer. Men da må $1 = x + 1 - x = b^n - a^n$ hvilket ikke kan lade sig gøre når $n > 1$.

Vi udnytter altså her at to på hinanden følgende tal ikke har nogen fælles divisorer, til at indse at ligningen ikke har nogen heltallige løsninger. I det hele taget kan man udnytte at fælles divisorer for n og $n + a$ også er divisorer i a .

3.2 Opgave

Vis at ligningen

$$x^3 + 3 = 4y(y + 1)$$

ikke har nogen heltallige løsninger.

3.3 Opgave

For hvilke naturlige tal m og n , hvor m er ulige, er $m^n + 1$ et kvadrattal?

3.4 Opgave

Vis at der ikke findes naturlige tal x, y og $n, n > 1$, for hvilke

$$x(x+1)(x+2) = y^n.$$

Bemærkning

Generelt gælder at k på hinanden følgende tal, $k > 1$, aldrig er en n 'te potens af et helt tal, når $n > 1$.

3.5 Opgave

Bestem alle naturlige tal n for hvilke $n2^{n-1} + 1$ er et kvadrattal.

3.6 Opgave

Bestem alle par x og y af hele tal for hvilke

$$1 + 2^x + 2^{2x+1} = y^2.$$

(IMO 2006)

4 Wilson's sætning

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

4.1 Wilson's sætning

For ethvert primtal p gælder

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

4.2 Eksempel

Wilson's 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 Wilson's 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 $4m + 3$.

4.3 Opgave

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

4.4 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?

5 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.

5.1 Euler-Fermat

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

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

5.2 Fermats lille sætning

Fermats lille sætning er et specialtilfælde af Euler-Fermat:

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

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

5.3 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 $6^{162} = 6^2(6^{20})^8 \equiv 6^2 \equiv 11 \pmod{25}$.

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

5.5 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

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

5.6 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.

5.7 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 .

5.8 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 $\phi(n)$.

5.9 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 .

5.10 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.

5.11 Opgave

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

6 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.

6.1 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 sæt 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.

6.2 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 .

6.3 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.

6.4 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.

6.5 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.

6.6 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 skuffeprincippet mindst to par så $ax' + y'$ 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

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

6.7 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.

6.8 Opgave

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

7 Løsniner

Opgave 1.3 Hvis sandsynligheden er $\frac{1}{100}$ for at et tilfældigt valgt tal m blandt tallene $1, 2, 3, \dots, 499, 500$ går op i n , må n have præcis 5 divisorer. Et tal med primfaktoropløsning $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i}$ har $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_i)$ divisorer, dvs. $n = p^4$ for et primtal p . Det største mulige n med den ønskede egenskab er derfor $n = 3^4 = 81$, da $5^4 > 500$.

Opgave 1.4 Tal med netop 3^2 divisorer må ifølge sætning 1.1 være på formen p^8 eller $p^2 q^2$ hvor p og q er primtal. Et sådant tal er derfor altid et kvadrattal, og produktet af sådanne tal er derfor også et kvadrattal.

Opgave 2.2 Af ligningen ses at $2bc + ac = ba$. Da a er ulige, må $a|bc$, $b|ac$ og $c|ab$. Dermed findes naturlige tal u, v og w , så $au = bc$, $bv = ac$ og $cw = ab$. Af dette får vi

$$a^2 = vw, \quad b^2 = uw, \quad c^2 = uv. \quad **)$$

Vi vil nu vise at $\gcd(u, v) = \gcd(u, w) = \gcd(v, w) = 1$. Lad p være en primdivisor i u . Af **) ses nu at p også er primdivisor i b og c , og dermed ikke i a da a, b og c ikke har nogen fælles divisorer. Da $a^2 = vw$, går p heller ikke op i v og w . På denne måde ses at $\gcd(u, v) = \gcd(u, w) = \gcd(v, w) = 1$.

Vi har nu at $a^2 = uv$ og $\gcd(u, v) = 1$. Dermed må u og v være kvadrattal. Tilsvarende ses at w er et kvadrattal. Da $abc = uvw$, må abc være et kvadrattal.

Opgave 2.4 Brøken er uforkortelig når største fælles divisor for nævner og tæller er 1.

$$\gcd(n^4 + 3n^2 + 1, n^3 + 2n) = \gcd(n^2 + 1, n^3 + 2n) = \gcd(n^2 + 1, n) = \gcd(1, n) = 1.$$

Opgave 2.5 Først finder vi et udtryk for $g(n)$ der viser at g er begrænset.

$$g(n) = \gcd(n^2 + 500, n^2 + 2n + 1 + 500) = \gcd(n^2 + 500, 2n + 1).$$

Da $2n + 1$ er ulige, ændrer det ikke ved den største fælles divisor at gange det første tal med 2. Derfor får vi at

$$\begin{aligned} g(n) &= \gcd(2n^2 + 1000, 2n + 1) = \gcd(1000 - n, 2n + 1) = \\ &= \gcd(2000 - 2n, 2n + 1) = \gcd(2001, 2n + 1). \end{aligned}$$

Heraf ses at g altid er divisor i 2001, og da $g(1000) = 2001$ er det også den maksimale værdi for g .

Opgave 6.7 Sæt $m = dn + r$, $0 \leq r < n$. Da er

$$2^m + 1 = 2^{dn+r} + 1 = (2^n)^d 2^r + 1 \equiv 1^d 2^r + 1 \equiv 2^r + 1 \pmod{2^n - 1}.$$

Da $n > r$, er der ingen naturlige tal $m, n > 2$ som opfylder betingelserne.

Opgave 3.2 Ved omrokering får vi

$$x^3 = 4y^2 + 4y - 3 = (2y + 1)^2 - 4 = (2y - 1)(2y + 3).$$

Da $\gcd(2y - 1, 2y + 3) = \gcd(2y - 1, 4) = 1$, er både $2y - 1$ og $2y + 3$ kubiktal, men der findes ikke to kubiktal hvis forskel er 4. Dermed har ligningen ingen heltallige løsninger.

Opgave 3.3 Hvis $m^n + 1$ er et kvadrattal, findes et naturligt tal x så

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

Da m er ulige, er x lige, dvs. at $\gcd(x - 1, x + 1) = 1$. Dermed findes to naturlige tal a og b således at $x - 1 = a^n$ og $x + 1 = b^n$. Men da er $2 = (x + 1) - (x - 1) = b^n - a^n$, hvilket giver at $n = 1$.

Tallet $m^n + 1$ er dermed et kvadrattal, når $n = 1$ og $m = (2k - 1)^2 - 1$ for alle $k \in \mathbb{N}$.

Opgave 3.4 Antag at der findes en løsning, og sæt $w = x + 1$. Da er

$$y^n = (w - 1)w(w + 1) = w(w^2 - 1).$$

Da $\gcd(w, w^2 - 1) = 1$, findes naturlige tal a og b således at $w = a^n$ og $w^2 - 1 = b^n$. Dermed er $1 = w^2 - (w^2 - 1) = (a^2)^n - b^n$, hvilket er en modstrid da $n > 1$.

Opgave 3.5 Ved at tjekke $n = 1, 2, 3, 4, 5, 6$ indses at blandt disse opfylder kun $n = 5$ det ønskede.

Vi viser indirekte at der ikke er flere n der opfylder betingelsen.

Antag at $n > 6$, og at $m^2 = n2^{n-1} + 1$. Da er

$$(m + 1)(m - 1) = n2^{n-1},$$

dvs. at $2^{n-2} | m + 1 \vee 2^{n-2} | m - 1$. Dermed er $m \geq 2^{n-2} - 1$, og

$$m^2 \geq (2^{n-2} - 1)^2 > 2^{2n-5} \geq n2^{n-1} + 1 = m^2,$$

da $2^{n-4} > n$ når $n > 6$. Men dette er en modstrid.

Opgave 3.6 Det er indlysende at der ikke er nogle løsninger for $x < 0$, og for $x = 0$ er der to løsninger $(0, 2)$ og $(0, -2)$.

Antag at $x > 0$. Hvis (x, y) er en løsning, da er også $(x, -y)$ en løsning, og derfor kan vi antage at også $y > 0$. Vi omskriver nu ligningen til

$$2^x(1 + 2^{x+1}) = (y - 1)(y + 1),$$

hvilket viser at y er ulige. Da netop en af faktorerne $y - 1$ og $y + 1$ er delelig med 4, får vi at $x > 2$, samt at en af faktorerne er delelig med 2^{x-1} .

Sæt nu

$$y = 2^{x-1}m + \epsilon, \text{ hvor } m \text{ er ulige, og } \epsilon = \pm 1.$$

Når vi indsætter dette i ligningen, får vi

$$2^x(1 + 2^{x+1}) = (2^{x-1}m + \epsilon)^2 - 1 = 2^{2x-2}m^2 + 2^x m \epsilon,$$

eller ækvivalent

$$1 + 2^{x+1} = 2^{x-2}m^2 + m\epsilon.$$

Derfor er

$$1 - \epsilon m = 2^{x-2}(m^2 - 8).$$

Hvis $\epsilon = 1$, må $m^2 - 8 \leq 0$, hvilket giver $m = 1$. Dermed er $1 - 1 = 2^{x-2}(1 - 8)$ hvilket er umuligt.

Hvis $\epsilon = -1$, må

$$1 + m = 2^{x-2}(m^2 - 8) \geq 2(m^2 - 8),$$

dvs. at $2m^2 - m - 17 \leq 0$. Dette giver at $m = 1$ eller $m = 3$. Det er igen nemt at se at $m = 1$ ikke er en løsning. Hvis $m = 3$, får vi at $x = 4$, dvs. at $y = 23$, og disse værdier opfylder den oprindelige ligning.

Dermed er samtlige løsninger $(0, 2)$, $(0, -2)$, $(4, 23)$ og $(4, -23)$.

Opgave 4.3 Hvis p er et primtal, gælder ifølge Wilson's 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 4.4 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 Wilson's 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 5.7 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 5.8 Ifølge Sætning 5.5 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 5.9 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 5.10 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 5.11 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 5.5 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 6.4 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 6.2, må p_i gå op i både a og b , dvs. at n går op i a og b hvilket er en modstrid.

Opgave 6.5 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 6.2 må 2 gå op i p . Dette er en modstrid, og dermed er antagelsen forkert.

Opgave 6.7 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 6.8

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:

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

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 6.2 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.