Fermats sats om summor av två kvadrater

Gustav Hammarhjelm

Våren 2020

1 Introduktion

Målet med denna text är att med hjälp av Minkowskis sats bevisa följande klassiska resultat från talteorin:

Sats 1.1 (Fermats sats om summor av två kvadrater)**.** *Varje primtal p på formen $4k+1$ kan skrivas som en summa av två kvadrater.*

Satsen säger alltså att för varje primtal p som är 1 större än en multipel av 4 finns det heltal a, b så att $p = a^2 + b^2$. Exempelvis är primtalet 17 på denna form och $17 = 1^2 + 4^2$. Detsamma gäller för $61 = 4 \cdot 15 + 1$, eftersom $61 = 5^2 + 6^2$.

Som så många andra resultat som tillskrivs Fermat så gav han inget bevis för detta påstående, utan det bevisades först av Euler på 1700-talet. Det mest välkända exemplet när det gick till på detta sätt är fallet med Fermats stora sats: Fermat hävdade på 1600-talet att han hade ett briljant bevis för att ekvationen $x^n+y^n = z^n$ inte har några lösningar i positiva heltal om $n > 2$. Han skrev inte ner detta bevis, utan påståendet bevisades av Andrew Wiles först på 1990-talet. Man är numera övertygad om att Fermat inte hade ett bevis, möjligen trodde han sig ha ett bevis, vilket i själva verket var ofullständigt. Det ska dock nämnas att Fermat faktiskt skrev ner ett vackert bevis i specialfallet $n = 4$ som finns bevarat för eftervärlden. Fermat bevisade alltså att ekvationen $x^4 + y^4 = z^4$ inte har några lösningar bland de positiva heltalen.

Texten är tänkt att bygga upp all den talteori som behövs från grunden. I övrigt bör man känna till gitter och konvexa mängder; detta kan man läsa om Uppsala matematiska cirkels kompendium från år 2020 till exempel.

Vi inleder med några grundläggande begrepp och resultat från talteorin i Avsnitt 2. Därefter introduceras moduloräkning i Avsnitt 3. I Avsnitt 4 används moduloräkning för att visa några resultat som används i beviset av Sats 1.1, men som också är intressanta i sig. Därefter kommer en påminnelse om Minkowskis sats och beviset av Fermats sats slutförs. I Avsnitt 5 betraktar vi moduloräkning från ett mer algebraiskt perspektiv och ser ett annat bevis av en av de viktiga ingredienserna i beviset av Sats 1.1. Texten avslutas med en problemsamling.

2 Delbarhet och aritmetikens fundamentalsats

I detta avsnitt definierar vi grundläggande talteoretiska begrepp, samt bevisar aritmetikens fundamentalsats, som visar att varje heltal kan skrivas som en produkt av primtal på endast ett sätt.

Definition 2.1. Vi säger att ett heltal a *delar* ett heltal b om det finns ett heltal k så att $ak = b$. Om a delar b skriver vi $a \mid b$. Andra sätt att läsa ut $a \mid b$ är "a är en faktor i b" eller "b är delbart med a".

Observera att $a \mid 0$ för varje heltal a eftersom $0 = 0 \cdot a$ och att $1 \mid a$ för varje heltal a.

Definition 2.2. Ett positivt heltal p är ett *primtal* om de enda positiva heltalsfaktorerna till p är 1 och p. Med andra ord, p är ett primtal om det för varje heltal $k > 0$ gäller att $k \mid p$ medför att $k \in \{1, p\}$.

Definition 2.3. Det största positiva heltalet d som delar två heltal a, b kallas den *största gemensamma delaren* av a och b. Talen a, b kallas *relativt prima* om den största gemensamma delaren av a och b är 1.

Observera att om a är ett heltal skilt från $0, 1, -1$ så är 0 och a inte relativt prima. Ett annat användbart faktum är att om p är ett primtal och a är ett heltal som inte är delbart med p så är a och p relativt prima. Vi visar nu ett användbart faktum om relativt prima tal.

Sats 2.4. *Om m, n är relativt prima tal så finns heltal x, y så att $mx + ny = 1$.*

Bevis. Studera mängden $M = \{ma + nb \mid a, b \in \mathbb{Z}\}$. Den måste innehålla ett positivt element (exempelvis m eller $-m$) och måste därför innehålla ett minsta positivt tal $d = mx + ny$. Vi hävdar att d är den största gemensamma delaren till m och n, d.v.s. 1. Vi måste därmed visa att d delar både m och m. Vi kan dividera m med d med rest, d.v.s. vi kan skriva $m = q_m d + r_m$ där q_m är ett heltal (kvoten) och r_m ett heltal med $0 \leq r_m < d$ (resten). Vi ser att $r_0 = m - q_m d = m - q_m(mx + ny) = m(1 - q_m x) + ny \in M$. Det följer att $r_0 = 0$, eftersom $r_0 < d$, och d var det minsta positiva elementet i M. Alltså $d \mid m$ eftersom resten då vi dividerade m med d visade sig vara 0. På samma sätt visar man att $d \mid n$. Vi antog att m, n var relativt prima och då $d \mid m$ och $d \mid n$ måste det gälla att $d = 1$. Slutsatsen blir att $1 \in M$, så det finns heltal x, y så att $mx + ny = 1$. □

Med hjälp av Sats 2.4 får vi följande mycket viktiga resultat, som säger att om ett primtal delar en produkt så måste primtalet dela någon av faktorerna.

Sats 2.5. *Om p är ett primtal och $p \mid ab$ så gäller $p \mid a$ eller $p \mid b$.*

Bevis. Antag att $p \mid ab$ men $p \nmid a$. Vi visar att $p \mid b$. Eftersom $p \nmid a$ vet vi att a, p är relativt prima, så enligt Sats 2.4 finns heltal x, y så att $px + ay = 1$, eller $ay = 1 - px$. Enligt antagandet $p \mid ab$ så finns det ett heltal k så att $ab = pk$. Om vi multiplicerar detta med y så får vi $ayb = yab = ypk$. Detta ger att $(1 - px)b = ypk$ eller $b = pxb + pyk = p(xb + yk)$ så $p \mid b$. □

Genom upprepad användning av denna sats får man att om ett primtal delar en produkt av tal, måste primtalet dela någon av faktorerna. I symboler: om p är ett primtal och $p \mid a_1 a_2 \cdots a_n$ så gäller $p \mid a_i$ för något $1 \leq i \leq n$.

Nu är vi redo att bevisa aritmetikens fundamentalsats, som säger att varje heltal kan skrivas som en produkt av primtal. Med andra ord utgör primtalen heltalens byggstenar eller "atomer".

Sats 2.6 (Aritmetikens fundamentalsats)**.** *Varje positivt heltal n kan skrivas som en produkt av positiva primtal på endast ett sätt om vi bortser från ordningen på primtalsfaktorerna.*

Bevis. Om $n = 1$ så är n en "tom produkt" av primtal, så det är okej. Om $n > 1$ så är n antingen ett primtal eller ett sammansatt tal. I det första fallet är vi klara, annars kan vi skriva $n = ab$ där $n > a, b > 1$. Vi fortsätter på samma sätt att dela upp a, b om möjligt. Eftersom faktorerna hela tiden blir mindre och mindre kommer denna process till slut inte kunna fortskrida och vi har hittat ett sätt att skriva n som en produkt av primtal.

Vi ska nu visa att framställningen av n som en produkt av primtal är entydig, så när som på ordningen av faktorerna. Antag därför att vi har två framställningar av n som en produkt av primtal, dels $n = p_1 p_2 \cdots p_s$ och dels $n = q_1 q_2 \cdots q_r$. Vårt mål är att visa att $r = s$ och att varje p_i är lika med något q_j. Antag för en motsägelse att dessa faktoriseringar är olika. Vi kan då välja n som det *minsta* positiva heltalet som har två olika primtalsfaktoriseringar. Vi har att $p_1 \mid n = q_1 q_2 \cdots q_r$, så enligt Sats 2.5 har vi $p_1 \mid q_i$ för något $1 \leq i \leq r$. Eftersom p_1 och q_i är primtal så måste $p_1 = q_i$. Alltså gäller

$$p_2 \cdots p_s = \frac{n}{p_1} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_r.$$

Så $\frac{n}{p_1} < n$ är ett heltal med två *olika* primtalsfaktoriseringar (för om dessa hade varit samma, så hade även faktoriseringarna $n = p_1 p_2 \cdots p_s$ och $n = q_1 q_2 \cdots q_r$ av n varit det). Alltså har vi hittat ett positivt tal mindre än n som har två olika primtalsfaktoriseringar, vilket är en motsägelse, då vi antog att n var det minsta positiva talet med denna egenskap. □

3 Moduloräkning

I detta avsnitt introduceras moduloräkning, eller så kallad restklassaritmetik, d.v.s. räkning med rester.

Definition 3.1. Låt n vara ett positivt heltal och a, b vara heltal. Vi skriver $a \equiv b \pmod{n}$ om $n \mid a - b$ d.v.s. om n delar differensen mellan a och b. Ekvivalent, så gäller $a \equiv b \pmod{n}$ om $a - b = kn$ för något heltal k. Vi utläser $a \equiv b \pmod{n}$ som "a är kongruent b modulo n".

Om a är kongruent b modulo n så lämnar a och b samma rest vid division med n, så ett annat sätt att uttrycka $a \equiv b \pmod{n}$ är att säga att a och b *tillhör samma restklass* modulo n.

När vi säger *reducera* ett heltal a modulo n menar vi att vi beräknar *resten* av a vid division med n. Vi kan alltid skriva $a = qn + r$ där q är ett heltal, *kvoten*, och r ett heltal, *resten*, som uppfyller $0 \leq r < n$. Per definition gäller $a \equiv r \pmod{n}$ och r är *reduktionen* av a modulo n.

Exempel. Reduktionen av 36 modulo 7 är 1 eftersom $36 = 5 \cdot 7 + 1$. Eftersom $7 \mid 35 = 36 - 1$ så gäller $36 \equiv 1 \pmod{7}$.

I följande sats sammanfattar vi några viktiga räkneregler för moduloräkning, d.v.s. räkneregler för addition och multiplikation av restklasser. Vissa delar av beviset lämnas som övningar i slutet av kapitlet.

Sats 3.2. *Låt a, b, c, d, n vara heltal, $n > 0$.*

(i) *Om $a \equiv b \pmod{n}$ så $b \equiv a \pmod{n}$.*

(ii) *Om* $a \equiv b \pmod{n}$ *och* $c \equiv d \pmod{n}$ *så gäller* $(a+b) \equiv (c+d) \pmod{n}$.

(iii) *Om* $a \equiv b \pmod{n}$ *och* $c \equiv d \pmod{n}$ *så gäller* $ac \equiv bd \pmod{n}$.

(iv) *Om* $a \equiv b \pmod{n}$ *så gäller* $ca \equiv cb \pmod{n}$.

(v) *Om* $ca \equiv cb \pmod{n}$ *och* c *och* n *är relativt prima så gäller* $a \equiv b \pmod{n}$.

Bevis. (i) Övning.

(ii) Övning.

(iii) Vi vet att $n \mid a-b$ och $n \mid c-d$ och vill visa att $n \mid ac-bd$. Så $a-b = k_1 n$ och $c-d = k_2 n$ för några heltal k_1, k_2. Därmed gäller också $a = b+k_1 n$, $c = d+k_2 n$. Multiplikation ger $ac = (b+k_1 n)(d+k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2)n$ så $n \mid ac-bd$.

(iv) Övning.

(v) Enligt Sats 2.4 finns heltal x, y så att $nx+cy = 1$ eftersom n och c är relativt prima. Med andra ord har vi att $cy \equiv 1 \pmod{n}$. Om vi multiplicerar $ca \equiv cb \pmod{n}$ med y får vi, enligt (iv) att $yca \equiv ycb \pmod{n}$ och eftersom $yc \equiv 1 \pmod{n}$ så följer det att $a \equiv b \pmod{n}$.

□

Övning 1. Bevisa punkterna (i), (ii) och (iv) i Sats 3.2.

Punkt (v) i satsen ovan säger att vi (under vissa förutsättningar) kan ”stryka” faktorer vid moduloräkning. Jämför med ekvationslösning, då vi kan stryka c i $ca = cb$ och få $a = b$ så länge $c \neq 0$.

Exempel. Moduloräkning är ett kraftfullt verktyg för att beräkna rester vid division av stora tal. Till exempel kan vi beräkna resten då 2^{100} divideras med 13 på följande sätt. Per definition är denna rest det heltal x så att $0 \leq x < 13$ och $2^{100} \equiv x \pmod{13}$. Exempelvis vet vi att $2^4 = 16 \equiv 3 \pmod{13}$ eftersom $16-3$ är delbart med 13. Vi vet också att $2^2 = 4 \equiv 4 \pmod{13}$ eftersom $13 \mid 4-4 = 0$ (kom ihåg att 0 är delbart med vilket tal som helst). Enligt Sats 3.2 (iii) så gäller

$$16 \cdot 4 \equiv 3 \cdot 4 \pmod{13},$$

alltså $16 \cdot 4 = 2^4 \cdot 2^2 = 2^6 \equiv 3 \cdot 4 = 12 \equiv -1 \pmod{13}$. Detta ger

$$2^{12} = 2^6 \cdot 2^6 \equiv (-1)(-1) = 1 \pmod{13}, \tag{1}$$

d.v.s. 2^{12} lämnar resten 1 vid division med 13. Låt oss kontrollera detta: $2^{10} = 1024$ så $2^{12} = 4 \cdot 1024 = 4096$ och $4096 = 13 \cdot 315 + 1$ eller $13 \mid 2^{12} - 1$.

Nu kan vi enkelt beräkna resten då 2^{100} divideras med 13: Vi vet att $100 = 8 \cdot 12 + 4$ så

$$2^{100} = (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 = 16 \equiv 3 \pmod{13}$$

enligt (1), alltså är den sökta resten $x = 3$. Notera här att $2^{12} \equiv 1 \pmod{13}$. Detta är ett specialfall av ”Lilla Fermat” (eller Fermats lilla sats) som du kan bevisa i Problem 3.

4 Wilsons sats och bevis av Sats 1.1

En viktig ingrediens i beviset av Sats 1.1 är det faktum att om p är ett primtal på formen $4k+1$ så finns det ett heltal m så att $p \mid m^2+1$. För att hitta ett sådant tal kan man använda Wilsons sats, som vi nu bevisar.

Sats 4.1 (En del av Wilsons sats)**.** *Om p är ett primtal så gäller* $(p-1)! \equiv -1 \pmod{p}$.

Bevis. Om $p = 2$ är satsen uppenbarligen sann, varför vi kan anta att p är ett udda primtal. Per definition är $(p-1)!$ produkten av talen $1, 2, \ldots, p-1$. Vi visar först att vart och ett av talen $2, \ldots, p-2$ kan paras ihop med ett annat tal så att deras produkt är kongruent 1 modulo p. Observera att $2, \ldots, p-2$ är ett jämnt antal tal eftersom p är udda.

Så tag ett tal $m \in \{2, \ldots, p-2\}$. Eftersom m och p är relativt prima så finns det heltal x och y så att $mx + py = 1$, d.v.s. $mx \equiv 1 \pmod{p}$. Vi modifierar x genom att addera multipler av p så att $x \in \{0, 1, \ldots, p-1\}$. Eftersom $mx \equiv 1 \pmod{p}$ kan x inte vara 0. Eftersom $m \in \{2, \ldots, p-2\}$ och $mx \equiv 1 \pmod{p}$ kan inte x vara 1 eller $p-1$. Alltså gäller $x \in \{2, \ldots, p-2\}$. Vi visar nu att $m \neq x$.

Antag för en motsägelse att $m = x$. Då gäller $mx = m^2 \equiv 1 \pmod{p}$. Alltså gäller $p \mid m^2 - 1 = (m+1)(m-1)$. Eftersom p är ett primtal så gäller $p \mid m+1$ eller $p \mid m-1$ enligt Sats 2.5. Eftersom $m \in \{2, \ldots, p-2\} \subset \{1, \ldots, p-1\}$ så ser vi att $p \mid m+1$ medför att $m = p-1$, vilket är omöjligt, och att $p \mid m-1$ medför att $m = 1$, vilket också är omöjligt. Alltså måste det gälla att $m \neq x$.

Slutsatsen blir att vi kan dela in $2, \ldots, p-2$ i par av olika tal vars produkt är kongruent 1 mod p. Talen $2, \ldots, p-2$ är ett jämnt antal, alltså är produkten av alla dessa tal kongruent 1 modulo p. Talet $(p-1)!$ är produkten av alla dessa tal och talen 1 och $p-1$. Det sista talet är kongruent -1 modulo p, alltså är $(p-1)!$ kongruent -1 modulo p, vilket var vad vi ville visa. □

Övning 2. Kontrollera Wilsons sats för primtalen 3 och 7.

Wilsons sats i sin helhet säger att ett positivt heltal n är ett primtal om och endast om $(n-1)! \equiv -1 \pmod{n}$. I Sats 4.1 visade vi ena halvan av detta påstående, d.v.s. att om p är ett primtal så gäller $(p-1)! \equiv -1 \pmod{p}$. För att visa satsen i sin helhet behöver vi visa att om $(n-1)! \equiv -1 \pmod{n}$ gäller så är n ett primtal. Detta kan du göra i Problem 1 nedan.

Vi vet ju att ekvationen $x^2 = -1$ saknar lösningar bland de reella talen. I nästa sats visar vi att ekvationen $x^2 = -1$ i vissa fall har lösningar modulo p. I dessa fall använder vi Sats 4.1 för atthitta en lösning.

Sats 4.2. *Om p är ett primtal kongruent 1 modulo 4 så finns ett heltal x som löser ekvationen $x^2 \equiv -1 \pmod{p}$, d.v.s. "-1 är en kvadrat modulo p".*

Bevis. Eftersom $p \equiv 1 \pmod{4}$ är p udda och $\frac{p-1}{2}$ är ett jämnt heltal. Vi visar nu att $x = \left(\frac{p-1}{2}\right)!$ löser ekvationen $x^2 \equiv -1 \pmod{p}$.

Enligt Sats 4.1 vet vi att $(p-1)! \equiv -1 \pmod{p}$. Vi tittar närmare på detta faktum:

$$\begin{aligned}
-1 \equiv (p-1)! &= 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1) \\
&\equiv \left(\frac{p-1}{2}\right)!\left(\frac{-p+1}{2}\right)\cdots(-2)(-1) = \left(\frac{p-1}{2}\right)!(-1)(-2)\cdots\left(-\frac{p-1}{2}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)! \pmod{p} = x^2 \pmod{p}.
\end{aligned}$$

Vid övergången från första till andra raden i beräkningarna ovan subtraherade vi p från var och en av faktorerna $\frac{p+1}{2}, \ldots, p-2, p-1$, vilket inte förändrar uttrycket modulo p. Mellan andra och tredje raden bröt vi ut en faktor -1 från var och en av faktorerna $-1, -2, \ldots, -\frac{p-1}{2}$, vilket ger en produkt av totalt $\frac{p-1}{2}$ minustecken. När vi sedan erinrar oss att $\frac{p-1}{2}$ är jämnt enligt antagandet får vi den sista likheten och beviset är klart. □

Övning 3. Kontrollera att $x = \left(\frac{p-1}{2}\right)!$ löser ekvationen $x^2 \equiv -1 \pmod{p}$ då $p = 13$ (observera att $p \equiv 1 \pmod{4}$).

Innan vi bevisar Sats 1.1 påminner vi om Minkowskis sats.

Sats 4.3 (Minkowski, 1889)**.** *Låt $\mathcal{L} \subset \mathbb{R}^d$ vara ett gitter med en fundamentaldomän av volym V. Låt $D \subset \mathbb{R}^d$ vara en konvex, symmetrisk mängd vars volym är större än $2^d V$. Då innehåller D en nollskild gitterpunkt ur $\mathcal{L}$.*

Vi är nu redo för följande häpnadsväckande bevis av Fermats sats. Det är magiskt hur gitter kommer till undsättning i lösningen av ett rent talteoretiskt problem!

Bevis av Sats 1.1. Enligt Sats 4.2 kan vi hitta ett heltal m så att p är en faktor i m^2+1. Låt $\boldsymbol{v}_1 = \boldsymbol{e}_1 + m\boldsymbol{e}_2$ och $\boldsymbol{v}_2 = p\boldsymbol{e}_2$ (kom ihåg att $\boldsymbol{e}_1 = \begin{pmatrix}1\\0\end{pmatrix}$ och $\boldsymbol{e}_2 = \begin{pmatrix}0\\1\end{pmatrix}$) och låt $\mathcal{L}$ vara gittret i $\mathbb{R}^2$ som spänns upp av $\boldsymbol{v}_1$ och $\boldsymbol{v}_2$, d.v.s.

$$\mathcal{L} = \{n_1\boldsymbol{v}_1 + n_2\boldsymbol{v}_2 \mid n_1, n_2 \in \mathbb{Z}\}.$$

(Vektorerna $\boldsymbol{v}_1$ och $\boldsymbol{v}_2$ är uppenbarligen inte parallella och utgör därmed en bas till planet). Observera att $\mathcal{L} \subset \mathbb{Z}^2$. Vi tar nu ett element i $\mathcal{L}$ och räknar ut dess längd i kvadrat:

$$\begin{aligned}
\|n_1\boldsymbol{v}_1 + n_2\boldsymbol{v}_2\|^2 &= \|n_1\boldsymbol{e}_1 + (n_1m + n_2p)\boldsymbol{e}_2\|^2 = \left\|\begin{pmatrix} n_1 \\ n_1m + n_2p\end{pmatrix}\right\|^2 \\
&= n_1^2 + (n_1m + n_2p)^2 = n_1^2(1+m^2) + 2n_1n_2mp + n_2^2p^2.
\end{aligned}$$

Notera att en sådan kvadrerad längd är ett heltal som kan skrivas som en summa av två kvadrater, och att detta tal är delbart med p eftersom m^2+1 är delbart med p.

Arean av en fundamentaldomän till $\mathcal{L}$ är lika med arean av parallellogrammet som spänns upp av vektorerna $\boldsymbol{v}_1$ och $\boldsymbol{v}_2$, d.v.s. p. Låt $D = \{\boldsymbol{x} \in \mathbb{R}^2 \mid \|\boldsymbol{x}\| < \sqrt{2p}\}$, d.v.s. D består av alla punkter i planet vars längd är *mindre* än $\sqrt{2p}$. Notera att D är symmetrisk och konvex. Låt $A = 2\pi p$ vara arean av D. Eftersom[1] $\pi > 2$ gäller $A = 2\pi p > 4p$, så enligt Minkowskis sats, Sats 4.3, innehåller D en nollskild vektor $w = m_1\boldsymbol{v}_1 + m_2\boldsymbol{v}_2$ från

[1]Hitta ett bra argument för detta utifrån någon lämplig definition av π och ett för att $\pi > 3$. "Bra argument" = bättre än "miniräknaren säger att $\pi = 3.14\ldots$".

$\mathcal{L}$. Observera att $w \in D$, så $0 < \|\boldsymbol{w}\|^2 < (\sqrt{2p})^2 = 2p$. Vi visade ju tidigare att $\|\boldsymbol{w}\|^2$ är ett heltal som är delbart med p. Det enda heltalet mellan 0 och $2p$ som är delbart med p är p självt, därför måste $\|\boldsymbol{w}\|^2 = p$. Alltså kan p skrivas som en summa av två kvadrater, vilket var vad vi ville visa! □

En intressant Youtube-video av Mathologer om ett annat bevis av Fermats sats om summor av två kvadrater hittar du här:

`https://www.youtube.com/watch?v=DjI1NICfjOk`.

Minkowskis sats kan även användas för att bevisa följande fascinerande resultat (vi hoppar dock över beviset i detta kompendium, satsen brukar bevisas i kursen Elementär talteori).

Sats 4.4 (Lagrange, 1770)**.** *Varje positivt heltal kan uttryckas som en summa av fyra kvadrater av heltal.*

Satsen säger alltså att för varje heltal $n > 0$ finns det heltal x_1, x_2, x_3, x_4 så att $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. För vissa tal räcker det med färre kvadrater, men då väljer vi bara några x_i som 0. Exempelvis gäller ju $2 = 1^2 + 1^2 + 0^2 + 0^2$. Att det inte räcker med ett mindre antal kvadrater för att representera varje heltal visar $n = 7$. Vi kan skriva $7 = 2^2 + 1^2 + 1^2 + 1^2$, men det finns inget sätt att skriva 7 som en summa av en, två eller tre kvadrater. Däremot finns ett annat resultat som säger att varje heltal som inte är på formen $n = 4^a(8b + 7)$ för några heltal $a, b > 0$ kan uttryckas som en summa av tre kvadrater. Minkowskis sats har även viktiga tillämpningar inom algebraisk talteori.

5 Lite algebra och ett annat bevis av Sats 4.2

Vi studerar här moduloräkning ifrån ett mer algebraiskt perspektiv och använder detta för ett "elegant" bevis av Sats 4.2. Vi ska närmare studera *restklassringar*.

Låt $n > 0$ vara ett heltal. Mängden $\mathbb{Z}$ av heltal delas in i *restklasser*, där en restklass består av mängden av de tal som ger samma rest vid division med n. Per definition tillhör a och b samma restklass om $a \equiv b \pmod{n}$. Det finns n möjliga rester r, med $0 \leq r < n$, nämligen $0, 1, \ldots, n-1$. Vart och ett av dessa tal r ger en restklass som vi betecknar $\overline{r}$. Notera att $\overline{r}$ är en mängd! Om $n = 5$ och $r = 3$ så gäller exempelvis

$$\overline{3} = \{5k + 3 \mid k \in \mathbb{Z}\},$$

vilket är mängden av de heltal som lämnar resten 3 vid division med 5. Notera exempelvis att $\overline{-2} = \overline{3} = \overline{8}$, mer allmänt gäller $\overline{a} = \overline{b}$ om och endast om $a \equiv b \pmod{5}$.

Notera att om $a \equiv b \pmod{n}$ och $c \equiv d \pmod{n}$ så gäller, enligt Sats 3.2, både $(a + c) \equiv (b + d) \pmod{n}$ och $ac \equiv bd \pmod{n}$. Detta säger oss följande: Om a och b, samt c och d tillhör samma restklass, så tillhör $a + c$ och $b + d$ samma restklass, och dessutom tillhör ac och bd samma restklass. Från detta kan vi definiera *addition* och *multiplikation* av restklasser modulo n, nämligen:

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}. \tag{2}$$

Detta gör mängden av restklasser modulo n till en *ring* som vi betecknar $\mathbb{Z}_n$. Som mängd gäller $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ så denna ring har precis n element (ett element för varje möjlig rest vid division med n). Vi ska nu definiera vad en ring är.

En ring är en mängd utrustad med två operationer, *addition* och *multiplikation*, som uppfyller vissa regler eller *axiom*. Det klassiska exemplet på en ring är mängden $\mathbb{Z}$ av heltal och axiomen för ringar är tänkt att kräva de regler vi är vana vid från addition och multiplikation av heltal.

Mer exakt, så är definitionen av en ring följande.

Definition 5.1. En (kommutativ) ring R är en mängd utrustad med två operationer, $+$ och $\cdot$ som tar två element $a, b \in R$ och ger nya element $a + b, a \cdot b \in R$ (produkten $a \cdot b$ skrivs ofta ab). För alla $a, b, c \in R$ ska följande gälla:

- (Associativitet för addition) $(a + b) + c = a + (b + c)$,
- (Kommutativitet för addition) $a + b = b + a$,
- (Associativitet för multiplikation) $(ab)c = a(bc)$,
- (Kommutativitet för multiplikation)[2] $ab = ba$.
- (Distributiva lagarna) $a(b + c) = ab + ac$ och $(a + b)c = ac + bc$.

Dessutom ska det finnas två speciella (olika) element, 0 och 1, sådana att:

- (Neutralt element för addition) $0 + a = a = a + 0$ för alla $a \in R$,
- (Existens av additiva inverser) för varje $a \in R$ finns ett element $-a$ så att $a+(-a) = 0$,
- (Neutralt element för addition) $1 \cdot a = a = a \cdot 1$ för alla $a \in R$.

Om vi dessutom lägger till axiomet

- (Existens av multiplikativa inverser) För varje $a \in R$, $a \neq 0$, finns ett element a^{-1} så att $aa^{-1} = 1 = a^{-1}a$

kallas ringen R för en *kropp*. Vi använder boktstaven K för att beteckna en kropp.

Notera att en ring alltid har minst två skilda element $0, 1$. Alltså räknas $\mathbb{Z}_1$ inte som en ring, för den har bara ett element.

Man kan alltså säga att en ring är en struktur där vi kan utföra addition, subtraktion och multiplikation enligt "de vanliga reglerna" (d.v.s. det fungerar som för heltalen). I en kropp kan vi dessutom utföra division. Exempel på kroppar är $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$. Vi ska nu se att restklassringarna $\mathbb{Z}_n$ faktiskt är ringar och att de i vissa fall dessutom är kroppar.

Kom ihåg att om $n > 0$ är ett heltal, så definierar vi addition och multiplikation av restklasser i $\mathbb{Z}_n$ enligt (2). Med dessa definitioner verifieras axiomen i Definition 5.1 lätt, så $\mathbb{Z}_n$ är en ring. Vi ska nu bevisa följande sats:

Sats 5.2. *Ringen $\mathbb{Z}_n$ är en kropp om och endast om $n > 1$ är ett primtal.*

[2]Egentligen krävs inte detta axiom för en ring, en ring som uppfyller detta kallas för en *kommutativ* ring, men vi kommer hålla oss till sådana ringar.

Bevis. Antag att n inte är ett primtal, och skriv $n = ab$ där a, b är två positiva heltal större än 1. Då gäller $\overline{a}\overline{b} = \overline{n} = \overline{0}$. Detta leder till att $\overline{a}$ inte kan ha en invers $\overline{a}^{-1}$, för i så fall så skulle $\overline{a}^{-1}\overline{a} = 1$ men om vi multiplicerar med $\overline{b}$ från vänster så får vi $\overline{b} = \overline{0}$, vilket är en motsägelse (ty detta säger att b är delbart med n, vilket är omöjligt).

Om $n = p$ är ett primtal, så kan vi visa att varje $\overline{a} \neq \overline{0}$ har en invers. Eftersom a och p är relativt prima finns det enligt Sats 2.4 heltal b, c så att $ab + pc = 1$ eller $ab = 1 - pc$. Vi ser att $\overline{a}\overline{b} = \overline{ab} = \overline{1 - pc} = \overline{1}$, så $\overline{a}$ har en invers, alltså är $\mathbb{Z}_p$ en kropp. □

Sats 5.3. *Om K är en ändlig kropp (d.v.s. antalet element $|K|$ i K är ändligt) så gäller*

$$a^{|K|-1} = 1$$

för alla $a \in K$, $a \neq 0$.

Bevis. Tag ett element $a \in K$ som inte är 0. Låt m_a vara funktionen som definieras av $m_a(x) = ax$, d.v.s. m_a är vänstermultiplikation med x. Då gäller att bilden av $K \setminus \{0\}$ är $K \setminus \{0\}$, alltså,

$$\{m_a(x) \mid x \in K \setminus \{0\}\} = K \setminus \{0\}.$$

Detta är sant ty om $b \in K \setminus \{0\}$ så $m_a(a^{-1}b) = a(a^{-1}b) = (aa^{-1}) = 1 \cdot b = b$. Dessutom, om $m_a(x) = b$ så gäller $ax = b$ eller $x = a^{-1}b$. Därför gäller

$$\prod_{x \in K\setminus\{0\}} x = \prod_{x \in K\setminus\{0\}} \mu_a(x) = \prod_{x \in K\setminus\{0\}} ax = a^{|K|-1} \prod_{x \in K\setminus\{0\}} x.$$

Om vi sätter $y = \prod_{x \in K\setminus\{0\}} x$ gäller alltså $y = a^{|K|-1}y$ och därför $a^{|K|-1} = 1$. □

För $K = \mathbb{Z}_p$ ger Sats 5.3 att $\overline{a}^{p-1} = 1$ för alla $a \neq 0$.

Definition 5.4. Låt K vara en kropp. Då är $K[x]$ *polynomringen* med koefficienter i K, d.v.s. mängden av alla polynom på formen

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

där $a_0, a_1, \ldots, a_n = \sum_{k=0}^{n} a_kx^k \in K$ och $n \geq 0$ är ett heltal.

Polynom i $K[x]$ kan adderas; om $f(x) = \sum_{k=0}^{n} a_kx^k$ och $g(x) = \sum_{k=0}^{n} b_kx^k$ så är $h(x) = f(x)+g(x) = \sum_{k=0}^{n}(a_k+b_k)x^k$. Polynom kan även multipliceras enligt följande: två *monom*, d.v.s. polynom med endast en term multipliceras såhär $(ax^m)(bx^n) = (ab)x^{n+m}$. Vi multiplicerar ett godtyckligt polynom $f(x) = \sum_{k=0}^{n} a_kx^k$ med ett monom på det uppenbara sättet, nämligen $(ax^m)f(x) = \sum_{k=0}^{n}(ax^m)(a_kx^k) = \sum_{k=0}^{n}(aa_k)x^{k+m}$, d.v.s. varje term i $f(x)$, som är ett monom, multipliceras med ax^m. Slutligen definierar vi $f(x)g(x)$ som $\sum_{k=0}^{n}(a_kx^k)g(x)$, om $f(x) = \sum_{k=0}^{n} a_kx^k$. Vi tar det som ett faktum att $K[x]$ är en kommutativ ring med dessa operationer.

Om $f(x) = \sum_{k=0}^{n} a_kx^k$, med $a_0, a_n \neq 0$ så kallas n för *graden* av f och betecknas $\deg f(x)$. Om $f(x) = 0$, d.v.s. alla koefficienter i $f(x)$ är 0, så bestämmer vi oss för att f:s grad är $-\infty$. Anledningen till denna bestämmelse är att vi får följande resultat: Om $f(x), g(x) \in K[x]$ är polynom, så gäller

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

Vi visar nu att ett polynom i $K[x]$ av grad n maximalt kan ha n olika nollställen i K.

Sats 5.5. *Låt K vara en kropp. Ett polynom $p(x) \in K[x]$ av grad n har maximalt n nollställen i K.*

Bevis. Vi visar detta med hjälp av induktion. För $n = 1$ är påståendet sant, varje polynom av grad 1 har precis ett nollställe. Låt nu $p(x)$ vara ett polynom av grad $n > 1$ och antag att varje polynom av grad högst $n - 1$ har maximalt $n - 1$ nollställen (detta är induktionsantagandet). Antag att $p(x) = \sum_{k=0}^{n} a_k x^k$ har ett nollställe $b \in K$. Då gäller

$$p(x) = p(x) - p(a) = \sum_{k=0}^{n} a_k x^k - \sum_{k=0}^{n} a_k a^k = \sum_{k=1}^{n} a_k (x^k - a^k).$$

Det gäller att $x - a$ är en faktor i $x^k - a^k$ för varje $k \geq 1$ (se Övning 4) och därmed kan vi skriva $p(x) = (x - a)q(x)$, där $q(x)$ är ett polynom av grad $n - 1$. Enligt induktionsantagandet har $q(x)$ maximalt $n - 1$ nollställen och alltså har $p(x)$ maximalt n nollställen, och satsen följer enligt induktionsprincipen. □

Övning 4. Visa att för varje $k \geq 1$ finns det ett polynom $p(x)$ så att $x^k - a^k = (x - a)p(x)$.

Sats 5.6. *Låt p vara ett primtal. Om d är en faktor i $p - 1$ så har $x^d - 1$ exakt d olika nollställen i $\mathbb{Z}_p$.*

Bevis. Enligt Sats 5.3 så är varje nollskilt element i $\mathbb{Z}_p$ ett nollställe till $x^{p-1} - 1$, så detta polynom har exakt $p - 1$ olika nollställen (notera att detta är det högsta möjliga antalet enligt Sats 5.5). Skriv $p - 1 = dq$ för något positivt heltal q. Alltså, om $y = x^d$ så gäller $x^{p-1} - 1 = y^q - 1 = (y - 1)(y^{q-1} + y^{q-2} + \ldots + y + 1) = (x^d - 1)g(x)$, där $g(x)$ är ett polynom av grad $d(q - 1)$. Vi vet att $x^d - 1$ kan ha maximalt d nollställen och att $g(x)$ kan ha maximalt $d(q - 1)$ nollställen. Om $x^d - 1$ skulle ha färre än d nollställen, skulle produkten $x^{p-1} - 1 = (x^d - 1)g(x)$ ha färre än $d + d(q - 1) = dq = p - 1$ nollställen, vilket är en motsägelse då vi visste att $x^{p-1} - 1$ hade exakt $p - 1$ olika nollställen. □

Definition 5.7. Låt R vara en ring med etta 1. Ett element $r \in R$ har *ändlig ordning* om det finns ett heltal $n > 0$ så att $r^n = 1$. Om r har ändlig ordning så finns ett minsta heltal $n \geq 1$ så att $r^n = 1$, vi kallar detta för *ordningen* av r och betecknar detta tal med $\text{ord}(r)$.

Exempel. Låt p vara ett primtal och $K = \mathbb{Z}_p$. Om $a \in K \setminus \{0\}$ så gäller enligt Sats 5.3 $a^{p-1} = 1$, så varje nollskilt element i K har ändlig ordning, och denna ordning är mindre än eller lika med $p - 1$.

Hjälpsats 5.8. *Låt R vara en ring. Antag att a, b är två element med ändlig ordning m respektive n. Om m, n är relativt prima tal så gäller* $\text{ord}(ab) = mn$.

Bevis. Eftersom R är kommutativ så gäller $(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1$ så ab har ändlig ordning mindre än eller lika med mn. Låt $\text{ord}(ab) = r \leq mn$. Om mn inte vore delbar med r så skulle det finnas heltal k och $0 < r' < r$ så att $mn = kr + r'$ och det följer att $(ab)^{r'}$, vilket är en motsägelse, då r var det minsta talet som uppfyller $(ab)^r = 1$. Alltså är mn delbar med r och därmed kan vi skriva $r = m'n'$ där $m' \mid m$ och $n' \mid n$. Skriv $d = \frac{m}{m'}$. Vi ser att

$$((ab)^{m'n'})^d = (ab)^{mn'} = b^{mn'}$$

eftersom $m'd = m$ och $a^m = 1$. Då ordningen av b är n så får vi, precis som ovan, att $n \mid mn'$. Eftersom n och m är relativt prima, så måste $n \mid n'$ och alltså är $n = n'$. På samma sätt visas att $m = m'$. □

Definition 5.9. Låt p vara ett primtal. Ett element $a \in \mathbb{Z}_p$ kallas för en *primitiv rot* om $\text{ord}(a) = p - 1$.

Primitiva rötter är användbara av följande anledning: I $\mathbb{Z}_p$ finns det $p-1$ nollskilda element. Om vi har en primitiv rot a så gäller att $a, a^2, \ldots, a^{p-2}, a^{p-1}$ är $p-1$ stycken olika element, alltså kan varje nollskilt element skrivas som en potens av den primitiva roten!

Sats 5.10. *Varje kropp $\mathbb{Z}_p$ har en primitiv rot.*

Bevis. Låt $p - 1 = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ vara primtalsfaktoriseringen av $p-1$ (alla k_i är positiva heltal). Enligt Sats 5.6 har $x^{p_i^{k_i}} - 1$ exakt $p_i^{k_i}$ olika nollställen i $\mathbb{Z}_p$ och polynomet $x^{p_i^{k_i-1}} - 1$ har exakt $p_i^{k_i-1}$ olika nollställen i $\mathbb{Z}_p$. Det finns alltså $x^{p_i^{k_i}} - 1 - x^{p_i^{k_i-1}} - 1 > 0$ element i $\mathbb{Z}_p$ som är nollställen till $x^{p_i^{k_i}} - 1$ men inte till $x^{p_i^{k_i-1}} - 1$. Detta är de element i $\mathbb{Z}_p$ av ordning $p_i^{k_i}$. Låt, för varje $1 \leq i \leq n$, a_i vara ett element av ordning $p_i^{k_i}$. Enligt Hjälpsats 5.8 så har $a = a_1 a_2 \cdots a_n$ ordning $p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n} = p - 1$, och är alltså en primitiv rot enligt Definition 5.7. □

Nu är vi redo för ett alternativt bevis av Sats 4.2.

Sats 5.11. *Låt $p \neq 2$ vara ett primtal. Ekvationen $x^2 = \overline{-1}$ är lösbar i kroppen $\mathbb{Z}_p$ om och endast om $p \equiv 1 \pmod 4$.*

Notera att ekvationen $x^2 = \overline{-1}$ är lösbar i $\mathbb{Z}_p$ om och endast om det finns heltal m så att $p \mid m^2 + 1$.

Bevis. Antag att $p \equiv 1 \pmod 4$, alltså $p = 4k + 1$ för något positivt heltal k. Låt a vara en primitiv rot i $\mathbb{Z}_p$. Låt $i = a^{\frac{p-1}{4}}$. Då gäller att $(i^2)^2 = \overline{1}$, d.v.s. i^2 är ett nollställe till $x^2 - \overline{1}$. Detta polynom har nollställena $\overline{\pm 1}$ i $\mathbb{Z}_p$ och kan, enligt Sats 5.5, inte ha andra nollställen. Alltså är i^2 lika med något av elementen $\overline{\pm 1}$. Det kan inte vara lika med 1 för då vore ordningen av a mindre än eller lika med $\frac{p-1}{2}$.

Antag att $p \equiv 3 \pmod 4$, d.v.s. $p = 4k + 3$ för något positivt heltal k. Antag att det finns $i \in \mathbb{Z}_p$ så att $i^2 = \overline{-1}$. Vi visar att detta leder till en motsägelse. Å ena sidan gäller, enligt Sats 5.3, $i^{p-1} = \overline{1}$. Å andra sidan gäller

$$i^{p-1} = i^{4k+2} = (i^4)^k i^2 = \overline{1}^k \overline{-1} = \overline{-1}$$

eftersom $i^4 = \overline{-1}^2 = \overline{1}$. □

Problem

Problem 1. Visa den andra delen av Wilsons sats, d.v.s. att om $(n-1)! \equiv -1 \pmod n$ så är n ett primtal, på följande vis: Antag att n *inte* är ett primtal och visa att $(n-1)! \equiv -1 \pmod n$ *inte* gäller.

Problem 2. Välj ett heltal $n > 1$ och ett tal $1 < m < n$ så att m och n är relativt prima. Kontrollera att om talen $m, 2m, 3m, \ldots, (n-1)m$ reduceras modulo n så får vi talen $1, 2, 3, \ldots, n-1$ (i någon ordning). Försök bevisa att detta alltid är fallet då n är ett primtal.

Problem 3. Bevisa Fermats lilla sats: Visa att om $a > 0$ inte är delbar med primtalet p så gäller $a^{p-1} \equiv 1 \pmod p$.

Ledtråd. Problem 2 och Wilsons sats.

Problem 4. Beräkna resten när 2^{100} divideras med 17.

Problem 5. Visa att om p är ett primtal kongruent 3 modulo 4 så är -1 *inte* en kvadrat modulo p.

Problem 6. Visa att om p är ett primtal kongruent 3 modulo 4 och om $p \mid a^2 + b^2$ så gäller $p \mid a$ och $p \mid b$.

Problem 7. Visa att om p är ett primtal kongruent 3 modulo 4 så kan p ej skrivas som en summa av två kvadrater.

Problem 8. Visa att om två positiva heltal skrivas som en summa av två kvadrater så kan deras produkt också skrivas som en summa av två kvadrater.

Problem 9. Skriv ett program i valfritt språk som kollar om ett givet tal n kan skrivas som en summa av två kvadrater. Om detta är möjligt, ska programmet hitta alla möjligheter att uttrycka n som en summa av två kvadrater av icke-negativa heltal, med den minsta kvadraten först.

Exempelvis, om $n = 25$, ska programmet ge svaren $25 = 0^2 + 5^2$, $25 = 3^2 + 4^2$ och om $n = 31$ ska programmet säga att det inte är möjligt att uttrycka n som en summa av två kvadrater (eftersom 31 är ett primtal 3 modulo 4).

Lösningsförslag

Problem 1. Antag först att n är sammansatt av två relativt prima tal, d.v.s. $n = ab$ där $1 < a, b < n$ och a, b är relativt prima. Vi kan anta att $a < b$. Då gäller

$$(n-1)! = 1 \cdot 2 \cdots a \cdots b \cdots (n-1)$$

och alltså är $(n-1)!$ delbar med $n = ab$ så $(n-1)! \equiv 0 \pmod{n}$.

Antag nu att n inte är ett primtal, men att n inte kan skrivas som en produkt av två relativt prima tal $n = ab$. Då måste $n = p^k$ för något primtal p och heltal $k \geq 2$, d.v.s. n måste vara en primtalspotens. Vi ser då att

$$(n-1)! = 1 \cdot 2 \cdots p \cdots p^2 \cdots p^{k-1} \cdots (n-1)$$

så $(n-1)!$ är delbar med $p \cdot p^{k-1} = p^k = n$ så återigen gäller $(n-1)! \equiv 0 \pmod{n}$.

Problem 2. Exempel: $n = 7$ och $m = 3$. Vi får $\{m, 2m, \ldots, 6m\} = \{3, 6, 9, 12, 15, 18\}$. Om vi reducerar dessa tal modulo 7 får vi $3, 6, 2, 5, 1, 4$ som är talen $1, 2, 3, 4, 5, 6$ i en annan ordning.

Ytterligare ett: $n = 9$ och $m = 4$. Vi får $\{m, 2m, \ldots, 8m\} = \{4, 8, 12, 16, 20, 24, 28, 32\}$, och reducerat $4, 8, 3, 7, 2, 6, 1, 5$.

Om $n = p$ är ett primtal, så får vi talen $m, 2m, \ldots, (p-1)m$. När vi reducerar något av dessa tal modulo p så får vi något av talen $1, 2, \ldots, p-1$. Vi kan inte få 0 eftersom m inte är delbart med p. Då talen $m, 2m, \ldots, (p-1)m$ är lika många som talen $1, 2, \ldots, p-1$ räcker det med att visa att inget par av tal från $m, 2m, \ldots, (p-1)m$ är lika modulo p. Om så vore fallet, skulle det finnas $1 \leq i < j < p$ så att $mj \equiv mi \pmod{p}$ d.v.s. $p \mid m(j-i)$. Eftersom $p \nmid m$ så måste $p \mid j - i$, vilket är omöjligt, då $1 \leq j - i < p$.

Alternativt kan vi använda Sats 3.2, delen om när man kan "stryka" faktorer. Om $mj \equiv mi \pmod{p}$ så får vi $j \equiv i \pmod{p}$, vilket inte går om $1 \leq i < j < p$.

Problem 3. Börja med talen $1, 2, \ldots, p-1$ och multiplicera dessa med a för att få talen $a, 2a, \ldots, (p-1)a$. Reducerar vi dessa tal modulo p får vi enligt Problem 2 $1, 2, \ldots, p-1$ i någon ordning. Alltså förekommer alla restklasser (utom 0) bland $a, 2a, \ldots, (p-1)a$. Detta innebär att $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Antingen ger nu Wilsons sats att $a^{p-1} \equiv 1 \pmod{p}$ eller så resonerar vi som följer: Vi får att $p \mid (p-1)!(a^{p-1}-1)$. Eftersom $p \nmid (p-1)!$ så måste $p \mid a^{p-1} - 1$ d.v.s. $a^{p-1} \equiv 1 \pmod{p}$ per definition.

Problem 4. Vi söker $0 \leq x < 17$ i $2^{100} \equiv x \pmod{17}$. Enligt "Lilla Fermat", Problem 3, så har vi $2^{16} \equiv 1 \pmod{17}$. Eftersom $100 = 6 \cdot 16 + 4$ så $2^{100} = (2^{16})^6 \cdot 2^4 \equiv 1^6 \cdot 2^4 = 16 \pmod{17}$.

Problem 5. Om -1 vore en kvadrat modulo p så skulle ekvationen $x^2 \equiv -1 \pmod{p}$ ha en lösning. Å ena sidan får vi, enligt Lilla Fermat $x^{p-1} \equiv 1 \pmod{p}$. Å andra sidan får vi

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

p.g.a. $x^2 \equiv -1 \pmod{p}$, $x^4 \equiv 1 \pmod{p}$ och $p = 4k + 3$ för något heltal $k \geq 0$. Detta är en motsägelse.

Problem 6. Antag att p inte delar både a och b. Vi kan då anta att $p \nmid a$. Då finns det heltal x och y så att $px + ay = 1$, d.v.s. $ay \equiv 1 \pmod{p}$. Vi vet att $p \mid a^2 + b^2$ d.v.s. $a^2 + b^2 \equiv 0 \pmod{p}$ eller $b^2 \equiv -a^2 \pmod{p}$. Multiplikation med y^2 ger att $(by)^2 \equiv -1 \pmod{p}$. Detta motsäger Problem 5. Alltså måste p dela både a och b.

Problem 7. Antag att $p = a^2 + b^2$. Enligt föregående problem gäller $p \mid a$ och $p \mid b$. Då gäller $p^2 \mid a^2$ och $p^2 \mid b^2$ och därför gäller $p^2 \mid a^2 + b^2 = p$, motsägelse.

Problem 8. Denna lösning använder komplexa tal: Om $m = a^2 + b^2$ och $n = c^2 + d^2$ så är $m = |z|^2$ och $n = |w|^2$ där $z = a + bi$ och $w = c + di$. Det gäller nu att $mn = |zw|^2$ så m, n kan skrivas som en summa av två kvadrater.