§ 5 Summen von Quadraten

Jede ganze Zahl hat eine kanonische multiplikative Zerlegung, nämlich als Produkt von Primzahlen.
Additiv gibt es keine kanonische Zerlegung, aber die additive Zahlentheorie ist voll von interessanten Problemen.
Zum Beispiel: Gegeben $\ell \in \mathbb{N}$. Welche $n \in \mathbb{N}$ sind Summen von ℓ Quadraten: $n = x_1^2 + x_2^2 + \dots + x_\ell^2$, alle $x_i \in \mathbb{N}_0$ (0 ist erlaubt).

$\ell = 1$: 1, 4, 9, 16, 25, ...

$\ell = 2$:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
✓	✓		✓	✓			✓	✓	✓			✓							

weiter?

Sehen Sie ein Muster?

„Warum" sind 3, 6, 7, ... keine Summen von zwei Quadraten?
Wie kann man so eine Frage überhaupt angehen?
Andere Frage: Warum haben wir uns so ausführlich mit quadratischen Resten beschäftigt? Ein Quadrat ist auch ein Quadrat modulo p, und diese Quadrate können wir bestimmen und sehen, was sich als Summe von zwei Quadraten modulo p schreiben lässt. Dafür muß p keine Primzahl sein.

Modulo 2: 0 und 1 sind Quadrate, also alle Restklassen.

Modulo 3: 0 und 1 sind Quadrate, 2 nicht, aber jede Restklasse ist Summe von zwei Quadraten, $2 = 1+1$.

Modulo 4: $0^2 = 0$, $1^2 = 1$, $2^2 = 0$, $3^2 = 1$ $\Rightarrow$ 0 und 1 sind Quadrate
$\Rightarrow$ $n \in \mathbb{N}$ Quadratzahl impliziert $n \equiv 0 \pmod 4$ oder $n \equiv 1 \pmod 4$
für $a, b \in \mathbb{N}$ folgt $a^2 + b^2$ kann 0, 1 oder 2 modulo 4 sein, aber $a^2 + b^2 \not\equiv 3 \pmod 4$
$\Rightarrow$ 3, 7, 11, 15, 19, ... können keine Summen von zwei Quadraten sein

Warum sind 6, 12, 18, ... keine Summen von zwei Quadraten?
Das sind Vielfache von 3 und 2.

Aber 9 und 49 sind auch Vielfache ~~a~~ von 3 und 7 und trotzdem Summen von zwei Quadraten. "Schlechte" Primzahlen wie 3 und 7 dürfen also vorkommen. Aber wie oft?

Sei $n = p \cdot q$ mit p prim, $p \equiv 3 \pmod 4$ und $n = a^2 + b^2$.

$p \mid n \Rightarrow p \mid (a^2+b^2) \Rightarrow a^2 \equiv -b^2 \pmod p \Rightarrow -b^2$ ist ein Quadrat mod p

$\Rightarrow \left(\frac{-b^2}{p}\right) = 1$

$= \left(\frac{-1}{p}\right) \underbrace{\left(\frac{b^2}{p}\right)}_{1}$

Korollar 4.3: Für $p \equiv 3 \pmod 4$ ist -1 ein quadratischer Nichtrest

$\Rightarrow \left(\frac{-1}{p}\right) = -1$ Ist das nun ein Widerspruch?

Das Legendre-Symbol ist definiert für Zahlen, die nicht durch p teilbar sind. 0 ist weder ein quadratischer Rest noch ein Nichtrest.

$\Rightarrow p \mid b^2 \Rightarrow p \mid b$

$a^2 \equiv -b^2 \pmod p \Rightarrow p \mid a^2 \Rightarrow p^2 \mid a^2 \Rightarrow p^2 \mid \underbrace{(a^2+b^2)}_{=n}$

Also können 6, 12 und 14 keine Summen von Quadraten sein.

Aus dem Argument kann man noch mehr machen:

$p^2 \mid a^2, b^2$ und $n \Rightarrow \frac{a^2}{p^2} + \frac{b^2}{p^2} = \frac{n}{p^2}$, alle in $\mathbb{N}$. Falls p immer noch als Teiler vorkommt, gilt wieder p^2 muß vorkommen, usw.

$\Rightarrow p$ kommt als Primteiler in n mit einem geraden Exponenten vor.

Überraschung: Diese Bedingung reicht schon aus:

5.1 Theorem: Sei $n \in \mathbb{N}$. Dann sind äquivalent:

(1) Die Gleichung $x^2 + y^2 = n$ hat Lösungen $x, y \in \mathbb{N}_0$.

(2) Jeder Primteiler $p \mid n$ mit $p \equiv 3 \pmod 4$ kommt in n mit geradem Exponenten vor.

Kann das überhaupt stimmen? Auf der vorigen Seite haben wir die Bedingung $n \not\equiv 3 \pmod 4$ hergeleitet. Wie verträgt sich die mit (2)?

Sei $n \equiv 3 \pmod 4$, $n = p_1^{a_1} \cdots p_e^{a_e}$ und zum Beispiel $p_1 \equiv 3 \pmod 4$.
Falls der Exponent a_1 gerade ist: $p_1^2 \equiv 9 \equiv 1 \pmod 4 \Rightarrow p_1^{a_1} \equiv 1 \pmod 4$.
$n \equiv 3 \pmod 4$ geht also nur, wenn mindestens ein a_i ungerade ist, z.B. a_1, nur dann ist $p_1^{a_1} \equiv p_1 \equiv 3 \pmod 4$. Dieser Fall ist durch die Bedingung (2) erfasst.

Wir müssen nur (2) $\Rightarrow$ (1) beweisen.

Beweis von 5.1: Sei $n = p_1^{a_1} \cdots p_e^{a_e}$. Wir wollen die Faktoren $p_i^{a_i}$ oder p_i separat behandeln. Dazu brauchen wir die folgende Aussage (Leonardo von Pisa = Fibonacci, 1202): $x = a^2+b^2$ und $y = c^2+d^2$ beides Summen von zwei Quadraten. Dann ist $x \cdot y$ auch eine Summe von zwei Quadraten.
Denn: $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$ nachprüfen
Sei nun die Bedingung (2) erfüllt für $n = p_1^{a_1} \cdots p_e^{a_e}$. Wir zeigen, daß jedes $p_i^{a_i}$ eine Summe von zwei Quadraten ist.
Falls $p_i = 2$: $p_i = 1+1$. Sei nun p_i ungerade, also $p_i \equiv 3 \pmod 4$ oder $p_i \equiv 1 \pmod 4$.
Falls $p_i \equiv 3 \pmod 4$: a_i gerade wegen (2); $p_i^2 = 0 + p_i^2$ Summe von zwei Quadraten $\Rightarrow p_i^{a_i} = (p_i^2)^{a_i/2}$ auch.
Falls $p_i \equiv 1 \pmod 4$, zeigen wir: dieses $p := p_i$ ist eine Summe von zwei Quadraten. Dafür muss man arbeiten.
Nach Korollar 4.3 ist in diesem Fall -1 ein quadratischer Rest modulo p.
Das bedeutet: $\exists z: z^2 \equiv -1 \pmod p$, d.h. $z^2+1 \equiv 0 \pmod p$, $0 < z < p$
$\Rightarrow \exists m: mp = z^2+1$, mp ist eine Summe von zwei Quadraten. Und $m < p$.
Falls $m = 1$, sind wir fertig. Deshalb zeigen wir: Wenn es $m > 1$ gibt, dann gibt es auch ein r mit $0 < r < m$ und $rp = z^2+1$. Mit Induktion kommen wir zu $m = 1$.
Um r zu finden, ersetzen wir z durch einen Repräsentanten seiner Restklasse in $[-\frac{p}{2}, \frac{p}{2}]$. $\Rightarrow m = \frac{1}{p}(z^2+1) < \frac{1}{p}\left(\frac{1}{4}p^2+1\right) < p$.

$$mp = x^2+y^2,\ m < p \quad \text{(und z.B. } x = z, y = 1\text{, das spielt aber keine Rolle mehr)}$$

Für x und y können wir Repräsentanten modulo m in $[-\frac{1}{2}m, \frac{1}{2}m)$ wählen, $u \equiv x \pmod m$ und $v \equiv y \pmod m$.

Damit ist $u^2+v^2 \equiv x^2+y^2 \pmod{m}$

$$\equiv mp \equiv 0 \pmod{m}$$

$\Rightarrow u^2+v^2 = rm$ für irgendein r. Wir wollen $0<r<m$.

$r=0$ würde bedeuten: $u^2+v^2 = 0 \Rightarrow u=v=0$

Aber $u \equiv x \pmod{m} \Rightarrow m \mid x$ und ebenso $m \mid y \Rightarrow m^2 \mid x^2+y^2 = mp$

$\Rightarrow m \mid p$, aber $m<p$ prim $\Rightarrow$ bleibt nur $m=1 \Rightarrow 0<r$

$r<m$: $u^2+v^2=rm \Rightarrow r = \frac{1}{m}(u^2+v^2) \leq \frac{1}{m}(\frac{1}{4}m^2+\frac{1}{4}m^2) < m$

Aber wir sind noch nicht fertig: $rm = u^2+v^2$, aber wir brauchen, daß rp eine Summe von zwei Quadraten ist. Das ist nochmal eine Rechnung:

$mr = u^2+v^2$, $mp = x^2+y^2 \Rightarrow m^2rp = (u^2+v^2)(x^2+y^2) = (xu+yv)^2+(xv-yu)^2$ Warum?

$u \equiv x \pmod{m}$ und $v \equiv y \pmod{m}$

$\Rightarrow xu+yv \equiv x^2+y^2 \equiv 0 \pmod{m}$

und $xv-yu \equiv xy-yx \equiv 0 \pmod{m}$

$\Rightarrow m^2 \mid (xu+yv)^2$ und $m^2 \mid (xv-yu)^2$, wir dürfen durch m^2 teilen

$\Rightarrow rp = \frac{(xu+yv)^2}{m^2} + \frac{(xv-yu)^2}{m^2}$ ist eine Summe von zwei Quadraten. $\square$

Der schwierige Teil des Beweises war die Zerlegung der Primzahl $4k+1$ in $p=x^2+y^2$. Diese Zerlegung ist sogar eindeutig:

Sei $p = a^2+b^2 = c^2+d^2$. Das bedeutet $a^2 \equiv -b^2 \pmod{p}$ und $c^2 \equiv -d^2 \pmod{p}$.

-1 ist ein quadratischer Rest modulo p (4.3) $\Rightarrow z^2+1 \equiv 0 \pmod{p}$ hat genau zwei Lösungen $z \equiv \pm h \pmod{p}$.

$\Rightarrow a \equiv \pm hb \pmod{p}$ und $c \equiv \pm hd \pmod{p}$

Die Vorzeichen von a, b, c, d spielen für die Eindeutigkeit keine Rolle, deshalb können wir $a \equiv hb \pmod{p}$ und $c \equiv hd \pmod{p}$ annehmen.

Wir rechnen jetzt ähnlich wie im Beweis von 5.1:

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

$ad-bc \equiv hb \cdot d - b \cdot hd \pmod{p}$, also $ad-bc \equiv 0 \pmod{p}$

$ac+bd \equiv hb \cdot hd + bd \equiv h^2bd+bd \pmod{p}$

Aber $h^2 \equiv -1 \pmod{p} \Rightarrow ac+bd \equiv 0 \pmod{p}$

$\Rightarrow p^2 \mid (ac+bd)^2$ und $p^2 \mid (ad-bc)^2$, und natürlich auch $p^2 \mid p^2$.
Daher können wir alles durch p^2 teilen und erhalten

$$1 = \left(\frac{ac+bd}{p}\right)^2 + \left(\frac{ad-bc}{p}\right)^2,$$ Summe von zwei Quadraten.

Aber 1 kann man nur als $1+0$ oder als $0+1$ schreiben

$\Rightarrow ac+bd = 0$ oder $ad-bc=0$

$p = a^2+b^2 \Rightarrow (a,b)=1$, denn ein gemeinsamer Teiler a^2 und b^2 quadratisch teilen, also auch p. Ebenso ist $(c,d)=1$.
Falls $ac+bd=0$: $(a,b)=1 \Rightarrow a \mid d$ und ebenso $d \mid a \Rightarrow a = \pm d,\ b = \pm c$
Falls $ad-bc=0$: $(a,b)=1 \Rightarrow a \mid c$ und ebenso $c \mid a \Rightarrow a = \pm c,\ b = \pm d$
Die Zerlegung von p in eine Summe von zwei Quadraten ist also eindeutig.

5.1 enthält auch die negative Aussage, daß man nicht jedes n als Summe von zwei Quadraten schreiben kann.
Wie sieht es mit drei Quadraten aus?
Auch sie schlecht: 1, 2, –, 6 geht; 7 geht nicht. Das zeigt ein allgemeines Problem: Betrachte x und x^2 modulo 8

x	0	1	2	3	4	5	6	7
x^2	0	1	4	1	0	1	4	1

$\Rightarrow x^2 \equiv 0$ oder 1 oder $4 \pmod 8$ $\forall x$

$\Rightarrow x^2+y^2+z^2 \in \{0,1,2,3,4,5,6\}$ modulo 8, aber niemals 7.
Es gibt noch weitere Bedingungen und eine Charakterisierung der Zahlen, die sich als Summe dreier Quadrate schreiben lassen. Der Beweis ist schwieriger als der von 5.1, weil das Produkt von zwei Zahlen, die Summen von drei Quadraten sind, nicht von dieser Form sein muß. Beispiel: $3 \cdot 5 = 15$.
Also gehen wir gleich zu Summen von vier Quadraten über, und da funktioniert es dann tatsächlich immer.

5.2 Theorem: Jede natürliche Zahl $n \in \mathbb{N}$ ist eine Summe von vier Quadraten. Das bedeutet: für jedes $n \in \mathbb{N}$ hat die Gleichung

$$x^2+y^2+z^2+w^2=n$$

Lösungen $x,y,z,w \in \mathbb{N}_0$.

Beweis: Wir versuchen, die Ideen im Beweis von 5.1 zu recyclen. Zuerst also ein Analogon von Fibonaccis Formel:

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)=(aA+bB+cC+dD)^2+$$
$$+(aB-bA-cD+dC)^2+(aC+bD-cA-dB)^2+(aD-bC+cB-dA)^2$$

Nachrechnen! Wer dazu keine Lust hat: es geht auch intelligenter.
Für Summen zweier Quadrate mit komplexen Zahlen: $|a+bi|^2=a^2+b^2$, $|c+di|^2=c^2+d^2$ ist ein guter Ansatz.
Und für Summen von vier Quadraten kann man Quaternionen verwenden.

Folglich ist unsere eigentliche Aufgabe, Primzahlen als Summen von vier Quadraten zu schreiben. $p=2$ und $p=4k+1$ können wir sogar schon als Summen von zwei Quadraten schreiben. Das Problem sind die Primzahlen der Form $p=4k+3$. Wie im Beweis von 5.1 gehen wir in zwei Schritten vor: Erst schreiben wir ein mp mit $0<m<p$ als Summe von vier Quadraten. Im zweiten Schritt leiten wir daraus die Aussage für p selbst ab.

Behauptung: $\exists m$ und $\exists\, x,y<\frac{p}{2}$: $mp=x^2+y^2+1^2+0^2$ $(p=4k+3$ fest$)$
(Für solch ein m gilt: $m<\frac{1}{p}(x^2+y^2+1)<\frac{1}{p}(\frac{1}{4}p^2+\frac{1}{4}p^2+1)<\frac{p}{2}+1<p$, und natürlich $0<m$.)

x,y können wir immer nichtnegativ wählen und (unabhängig davon) im Intervall $(-\frac{p}{2},\frac{p}{2})$. Es geht nur darum, ob $x^2+1\equiv -y^2 \pmod p$ eine Lösung hat oder nicht.

Beweis der Behauptung, bzw der Existenz einer Lösung von $x^2+1\equiv -y^2 \pmod p$:
Laut 3.1 oder 4.3 ist -1 ein quadratischer Nichtrest modulo $p=4k+3$.
Also ist auch $-y^2$ ein quadratischer Nichtrest modulo $p=4k+3$, und alle quadratischen Nichtreste sehen so aus. warum?

Wir suchen demnach einen quadratischen Nichtrest $N:=-y^2$ von der Form x^2+1, d.h. $N=R+1$, wobei R ein quadratischer Rest ist.

Um so was zu finden, probieren wir einfach durch: 1, 2, 3, usw. 1 ist ein quadratischer Rest, aber irgendwann muß ein Nichtrest N vorkommen, zum ersten Mal, $N-1$ muß also ein Rest R sein. welche Ergebnisse verwenden wir hier

Folglich gibt es eine Lösung und die Behauptung ist gezeigt.

Ein alternativer Beweis verwendet den Satz von Chevalley mit $f(x,y,z) = x^2+y^2+z^2$. Details?

Jetzt kommt der zweite Teil des Beweises. Wir haben ein m gefunden, $0<m<p$, mit $mp = a^2+b^2+c^2+d^2$. Falls $m=1$ sind wir fertig. Falls nicht zeigen wir $\exists r: 0<r<m$ mit derselben Eigenschaft. Das genügt dann.

Wie im Beweis von 5.1 ersetzen wir a, b, c, d durch Repräsentanten modulo m, $A, B, C, D \in (-\frac{m}{2}, \frac{m}{2}]$, $A \equiv a \pmod m$ usw, oder genauer $A = a - r_1 m$ usw

$$\Rightarrow A^2+B^2+C^2+D^2 = (a-r_1m)^2+(b-r_2m)^2+(c-r_3m)^2+(d-r_4m)^2 =$$

$$= \underbrace{a^2+b^2+c^2+d^2}_{mp} - sm \text{ für irgendein } s$$

$\Rightarrow A^2+B^2+C^2+D^2 = mr$ mit $r = p-s$ und natürlich $r \neq 0$ (sonst sind a, b, c, d Vielfache von m und p auch ↯).

Wie in 5.1 zeigen wir jetzt als nächstes: $r<m$.

$r = \frac{1}{m}(A^2+B^2+C^2+D^2)$, $A^2 \leq \frac{1}{4}m^2$, ebenso für $B^2, C^2, D^2 \Rightarrow$

$r \leq \frac{1}{m}\cdot 4 \cdot \frac{1}{4}m^2 = m$. Wir wollen aber $r<m$. Was bedeutet $r=m$?

Das geht nur für $A=B=C=D=\frac{m}{2}$ (also m gerade) und dann ist (wegen $a \equiv A \pmod m$ usw) $mp = a^2+b^2+c^2+d^2$

$$\equiv A^2+B^2+C^2+D^2 \pmod{m^2}$$
$$\equiv m^2 \equiv 0 \pmod{m^2}$$

$\Rightarrow m^2 \mid mp$ ↯

Damit haben wir das Zwischenziel erreicht: $0<r<m$

Jetzt kommen wir zu dem, was wir eigentlich beweisen müssen: rp ist eine Summe von vier Quadraten

Bisher gezeigt: $mp = a^2+b^2+c^2+d^2$ und $mr = A^2+B^2+C^2+D^2$

$\Rightarrow$ $\underbrace{mp\,mr}_{}$ ist auch eine Summe aus vier Quadraten $x^2+y^2+z^2+w^2$

$= m^2pr$, wir wollen m^2 kürzen

x, y, z, w wurden zu Beginn des Beweises explizit angegeben:

$$x = aA+bB+cC+dD \equiv \underbrace{a^2+b^2+c^2+d^2}_{mp} \equiv 0 \pmod m$$

$$y = aB-bA-cD+dC \equiv ab-ba-cd+dc \equiv 0 \pmod m$$

$$z = aC+bD-cA-dB \equiv 0 \pmod m$$

$$w = aD-bC+cB-dA \equiv ad-bc+bc-da = 0 \pmod m$$

$\Rightarrow$ m^2 teilt x^2, y^2, z^2 und w^2 und darf gekürzt werden

$\Rightarrow$ pr ist eine Summe von vier Quadraten. $\square$