1 Darstellung natürlicher Zahlen als Summe zweier Quadrate

1.1 Hilfssatz: Für Primzahlen $p = 4m + 1$ hat die Gleichung $s^2 = -1$ im $\mathbb{F}_p$ zwei Lösungen, für $p = 2$ gibt es genau eine solche Lösung, während es für $p = 4m + 3$ keine Lösung gibt.

Beweis: Für $p = 2$ ist $s = 1$ die einzige Lösung. Für ungerades p betrachten wir die Äquivalenzrelation auf $\mathbb{F}_p^*$, die durch die Äquivalenzklassen $[x] = \{x; -x; x^{-1}; -x^{-1}\}$ gegeben ist. Wir betrachten nun die Fälle, in denen die Äquivalenzklassen nicht vier Elemente haben:

1. Möglichkeit: $x = -x$.
Wegen $x = -x$ ist dann $2x = x + (-x) = 0 \overset{p\neq 2}{\Rightarrow} x = 0$, was kein Element aus $\mathbb{F}_p^*$ ist, also kann dieser Fall nicht auftreten.

2. Möglichkeit: $x = x^{-1}$.
Wegen $x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow x = 1 \vee x = p - 1$ erhalten wir in diesem Fall mit $\{1; p - 1\}$ eine Äquivalenzklasse der Größe 2, die auf alle Fälle auftritt.

3. Möglichkeit: $x = -x^{-1}$.
Hier ist $x = -x^{-1} \Leftrightarrow x^2 = -1$. Diese Gleichung ist entweder unlösbar oder besitzt die Lösungen x_0 und $p - x_0$, die mit der gleichen Begründung wie oben garantiert verschieden sind. In diesem Fall ist die Äquivalenzklasse $\{x_0; p - x_0\}$.

Damit haben wir $\mathbb{F}_p^*$ in Äquivalenzklassen der Größe 4 und ein oder zwei Äquivalenzklassen der Größe 2 partitioniert. Da $\mathbb{F}_p^*$ gerade $p - 1$ Elemente hat, gibt es im Fall $p = 4m + 3$ (also $p - 1 = 4m + 2$) nur eine zweielementige Äquivalenzklasse, nämlich $\{1; p - 1\}$, womit oben die dritte Möglichkeit nicht eintreten kann und damit $s^2 = -1$ keine Lösung hat. Ist $p - 1 = 4m = 4(m - 1) + 2 + 2$, so gibt es zwei Äquivalenzklassen der Größe 2, also tritt die dritte Möglichkeit ein, und x_0 und $p - x_0$ sind gerade die zwei verschiedenen Lösungen von $s^2 = -1$.

1.2 Satz: Jede Primzahl der Form $p = 4m+1$ ist Summe zweier Quadratzahlen, das heißt, es existieren $x, y \in \mathbb{N}_0$ mit $p = x^2 + y^2$.

Beweis 1: Sei s eine Lösung von $s^2 \equiv -1 \bmod p$, die nach **1.1** existiert. Betrachte die Paare $(x'; y') \in \{0; \ldots ; [\sqrt{p}]\}^2 =: D$, von denen es $([\sqrt{p}] + 1)^2$ gibt. Wegen $[x] + 1 > x$ mit $x = \sqrt{p}$ sehen wir, daß $|D| > p$ gilt. Damit kann $f : D \to \mathbb{F}_p$, $(x'; y') \mapsto x' - sy'$ nicht injektiv sein, womit es zwei verschiedene Paare $(x'; y')$ und $(x''; y'')$ gibt mit $x' - sy' \equiv x'' - sy'' \bmod p \Leftrightarrow x' - x'' \equiv s(y' - y'') \bmod p$. Jetzt definieren wir $x := |x' - x''|$ und $y := |y' - y''|$. Aus der obigen Gleichung folgt nun $x \equiv \pm sy \bmod p$ und weiter $x^2 \equiv s^2y^2 \equiv -y^2 \bmod p$, was $x^2 + y^2 \equiv 0 \bmod p$ impliziert. Da $(x'; y')$ und $(x''; y'')$ verschieden waren, können nicht sowohl x als auch y Null sein, also ist $x^2 + y^2 > 0$. Wegen $x, y \in \{0; \ldots ; [\sqrt{p}]\}$ und damit $x^2, y^2 \leqslant [\sqrt{p}]^2 < p$ erhalten wir zuletzt $x^2 + y^2 < 2p$ womit für $x^2 + y^2$ nur noch der Wert p übrigbleibt.

Beweis 2: Wir untersuchen die Menge $S := \{(x; y; z) \in \mathbb{Z}^3 \mid 4xy + z^2 = p, x \geqslant 1, y \geqslant 1\}$. Da z^2 immer nichtnegativ ist, muß für $(x; y; z) \in S$ gelten: $4xy \leqslant p \Leftrightarrow xy \leqslant \frac{p}{4}$, was wegen $x, y \geqslant 1$ nur für $x, y \leqslant \frac{p}{4}$ erfüllbar ist. Für gegebene x, y ist z bis auf das Vorzeichen eindeutig bestimmt, also ist S endlich. Im Folgenden untersuchen wir außer S noch zwei Teilmengen von S, nämlich $T := \{(x; y; z) \in S \mid z > 0\}$ und $U := \{(x; y; z) \in S \mid x - y + z > 0\}$.

1. Schritt: Wir betrachten $f : S \to S$, $(x; y; z) \mapsto (y; x; -z)$ mit $f \circ f = \mathrm{id}$, also ist f insbesondere bijektiv. In S existiert kein Fixpunkt von f, denn dann wäre $z = -z \Rightarrow z = 0$ und damit

$4xy = p$, was wegen p Primzahl unmöglich ist. Weiterhin ist das Bild eines Elementes aus T ein Element aus $S \setminus T$ und umgekehrt. Da für $(x; y; z) \in S$ mit $x - y + z = 0$ gelten würde: $p = 4xy + z^2 = 4xy + (x - y)^2 = 4xy + x^2 - 2xy + y^2 = x^2 + 2xy + y^2 = (x + y)^2$, kann es keine solchen Elemente in S geben, also werden die Elemente aus U durch f auf Elemente von $S \setminus U$ abgebildet, da $x - y$ und z durch f negiert werden.
Damit haben wir gezeigt: $f : T \leftrightarrow T^C$ und $f : U \leftrightarrow U^C$, wobei die Komplementbildung in der Grundmenge S aufgefaßt sei. Damit folgt $f : T \setminus U = T \cap U^C \leftrightarrow T^C \cap U = U \setminus T$ und damit $|U| = |U \cap T| + |U \setminus T| = |U \cap T| + |T \setminus U| = |T|$.

2. Schritt: Nun betrachten wir $g : U \to U$, $(x; y; z) \mapsto (x-y+z; y; 2y-z)$ und zeigen zunächst, daß dies wirklich eine Abbildung von U nach U definiert: Ist $(x; y; z) \in U$, so ist $x-y+z > 0$, $y > 0$ und $4(x-y+z)y+(2y-z)^2 = 4xy-4y^2+4yz+4y^2-4yz+z^2 = 4xy+z^2 = p$, also ist $g(x; y; z) \in S$ und wegen $(x - y + z) - y + (2y - z) = x > 0$ ist sogar $g(x; y; z) \in U$. Weiterhin ist $g(g(x; y; z)) = g(x-y+z; y; 2y-z) = (x-y+z-y+2y-z; y; 2y-(2y-z)) = (x; y; z)$ also $g \circ g = \mathrm{id}$.
Zuletzt untersuchen wir g auf Fixpunkte: $(x; y; z) = g(x; y; z) \Leftrightarrow (x; y; z) = (x - y + z; y; 2y - z) \Leftrightarrow y = z$. Unter dieser Bedingung ist $p = 4xy + y^2 = (4x + y)y$, womit wegen p Primzahl $y = 1 = z$ sein muß, was aber zu $p = 4xy + z^2 \Leftrightarrow x = \frac{p-z^2}{4y} = \frac{p-1}{4}$ führt und damit den einzigen Fixpunkt eindeutig charakterisiert.
Wir sehen nun, daß durch die Mengen $\{(x; y; z); g(x; y; z)\}$ für $(x; y; z) \in U$ eine Partitionierung von U gegeben ist, die aus zweielementigen Mengen und genau einer einelementigen Menge besteht, womit $|U|$ ungerade ist.

3. Schritt: Als dritte Abbildung untersuchen wir $h : T \to T$, $(x; y; z) \mapsto (y; x; z)$ mit $h \circ h = \mathrm{id}$. Wegen $|T| = |U|$ ungerade muß h einen Fixpunkt haben, also gibt es in T einen Punkt mit $x = y$. Für diesen Punkt gilt nun $p = 4xy + z^2 = 4x^2 + z^2 = (2x)^2 + z^2$.

1.3 Satz: Eine natürliche Zahl n ist genau dann Summe zweier Quadratzahlen, wenn die Primfaktoren $p = 4m + 3$ von n mit geradem Exponenten auftreten.

Beweis: Im Folgenden nennen wir eine Zahl *darstellbar*, wenn sie Summe zweier Quadrate ist.
„$\Rightarrow$“: $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$ und Primzahlen der Form $p = 4m + 1$ sind darstellbar (**1.2**). Wegen $(x^2 + y^2)(a^2 + b^2) = x^2a^2 + y^2b^2 + x^2b^2 + y^2a^2 = (x^2a^2 + 2xayb + y^2b^2) + (x^2b^2 - 2xbya + y^2a^2) = (xa + yb)^2 + (xb - ya)^2$ ist auch das Produkt darstellbarer Zahlen darstellbar und nach $(x^2+y^2)z^2 = (xz)^2+(yz)^2$ sind auch quadratische Vielfache darstellbarer Zahlen darstellbar, womit die Zahlen n mit obiger Primfaktorzerlegung darstellbar sind.
„$\Leftarrow$“: Sei $n = x^2 + y^2$ darstellbar. Für einen Primteiler $p = 4m + 3$ von n nehmen wir $x \not\equiv 0 \bmod p$ an. Dann könnten wir ein x' finden mit $xx' \equiv 1 \bmod p$. Dann würde gelten: $x^2 + y^2 \equiv 0 \bmod p \Rightarrow 1 + x'^2y^2 = 1 + (x'y)^2 \equiv 0 \bmod p \Rightarrow (x'y)^2 \equiv -1 \bmod p$, was nach **1.1** nicht möglich ist, also muß p ein Teiler von x (und analogerweise auch von y) sein. Damit folgt $p^2|n$ und $\frac{n}{p^2} = (\frac{x}{p})^2 + (\frac{y}{p})^2$ ist darstellbar, also gilt entweder $p \nmid \frac{n}{p^2}$ oder $p^2|\frac{n}{p^2}$. Rekursiv erhalten wir, daß p in der Primfaktorzerlegung von n mit geradem Exponenten auftauchen muß.

2 Der Vier-Quadrate-Satz

2.1 Hilfssatz: Sei p eine Primzahl. Dann gibt es genau $[\frac{p}{2}] + 1$ Quadratzahlen in $\mathbb{F}_p$.

Beweis: Sowohl 0 als auch 1 sind Quadrate, also stimmt die Formel für $p = 2$. Sei im Folgenden p ungerade, also insbesondere x und $-x$ verschieden für $x \in \mathbb{F}_p^*$. Betrachte die Äquivalenzklassen

$\{x;-x\}$, von denen es eine einelementige ($\{0\}$) und $\frac{p-1}{2}$ zweielementige gibt. Alle Elemente einer Äquivalenzklasse haben gleiche Quadrate, während die Quadrate zweier Elemente aus verschiedenen Äquivalenzklassen verschieden sind: $s^2 = 0$ hat nur eine Lösung $s = 0$, während $s^2 = a$ für $a \in \mathbb{F}_p^*$ nach dem Fundamentalsatz der Algebra höchstens zwei Lösungen hat, die aber dann auf jeden Fall in einer Äquivalenzklasse $\{x;-x\}$ vorkommen. Insgesamt gibt es also $1 + \frac{p-1}{2} = 1 + [\frac{p}{2}]$ verschiedene Quadrate in $\mathbb{F}_p$.

2.2 Hilfssatz: Für alle Primzahlen p gibt es eine Lösung der Gleichung $x^2 + y^2 = -1$ im $\mathbb{F}_p$.

Beweis: Es gibt $[\frac{p}{2}] + 1$ verschiedene Quadrate in $\mathbb{F}_p$ und ebensoviele verschiedene Zahlen der Form $-(1+y^2)$. Diese beiden Mengen sind zu groß um disjunkt zu sein, da $\mathbb{F}_p$ nur p Elemente hat, und somit müssen x, y existieren mit $x^2 = -(1 + y^2) \Leftrightarrow x^2 + y^2 = -1$.

2.3 Hilfssatz: Sind zwei Zahlen als Summe von vier Quadraten darstellbar, so besitzt auch ihr Produkt eine solche Darstellung.

Beweis: $(a^2+b^2+c^2+d^2)(u^2+v^2+w^2+x^2) = (au+bv+cw+dx)^2 + (av-bu+cx-dw)^2 + (aw-cu+dv-bx)^2 + (ax-du+cw-dv)^2$.

2.4 Satz: Jede Primzahl p ist Summe von vier Quadratzahlen.

Beweis: Wir bestimmen im Folgenden die kleinste natürliche Zahl m, für die mp Summe von vier Quadraten ist.
Nach **2.2** existieren Zahlen s, t mit $s^2 + t^2 \equiv -1 \bmod p$. Dann ist $0 = 1 + (-1) \equiv 0^2 + 1^2 + s^2 + t^2 \bmod p$, wobei wir $s, t < \frac{p}{2}$ annehmen können, da entweder s oder $p - s$ kleiner als $\frac{p}{2}$ ist (analog für t). Damit folgt $0^2 + 1^2 + s^2 + t^2 < 1 + 2\frac{p^2}{4} < p^2$, also ist $1 \leqslant m < p$.
Sei nun $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Wegen der Minimalität von m muß $\operatorname{ggT}(x_1; x_2; x_3; x_4) = 1$ sein. Ist m gerade, so sind entweder alle Zahlen gerade oder alle ungerade oder zwei gerade und zwei ungerade (o. B. d. A. seien dies x_3 und x_4). In allen Fällen sind $x_1 + x_2$, $x_1 - x_2$, $x_3 + x_4$ und $x_3 - x_4$ gerade und deshalb ist

$$\frac{1}{2}mp = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

Summe von vier Quadraten, was im Widerspruch zur Minimalität von m steht, also ist m ungerade.
Sei nun angenommen, daß $m \geqslant 3$ ungerade ist. Dann finden wir Zahlen y_i mit $y_i \equiv x_i \bmod m$ und $-\frac{m}{2} < y_i < \frac{m}{2}$ und es gilt $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \bmod m$ wegen $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \bmod m$. Da nicht alle x_i durch m teilbar sein können (sonst wäre ihr größter gemeinsamer Teiler nicht 1), ist $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2$, und diese Summe ist echt kleiner als $4(\frac{m}{2})^2 = m^2$. Damit existiert ein natürliches $n < m$ mit $y_1^2 + y_2^2 + y_3^2 + y_4^2 = mn$. Man erhält durch Multiplikation: $m^2np = (x_1^2 + x_2^2 + x_3^2 + x_4)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$, und nach **2.3** existieren Zahlen z_i mit $z_1^2 + z_2^2 + z_3^2 + z_4^2 = m^2np$, wobei aus der Darstellung in **2.3** folgt, daß $z_i \equiv 0 \bmod m$ gilt. Daher ist $np = (\frac{z_1}{m})^2 + (\frac{z_2}{m})^2 + (\frac{z_3}{m})^2 + (\frac{z_4}{m})^2$ Summe von vier Quadratzahlen, was wegen $n < m$ im Widerspruch zur Minimalität von m steht. Damit verbleibt nur noch die Möglichkeit $m = 1$, was die Behauptung liefert.

2.5 Folgerung: (Vier-Quadrate-Satz)
Jede natürliche Zahl ist als Summe von vier Quadratzahlen darstellbar.