KAPITEL 9

Zahlentheoretischer Ausklang

1. Einführung

Auf Fermat (1607-1665) gehen folgende Aussagen über die Darstellbarkeit von Primzahlen zurück[1]:

$$\begin{aligned}
&\text{Es gibt } x,y\in\mathbb{Z} \text{ mit } p=x^2+y^2 &&\iff\quad p=2 \text{ oder } p\equiv 1 \bmod 4,\\
&\text{es gibt } x,y\in\mathbb{Z} \text{ mit } p=x^2+2y^2 &&\iff\quad p=2 \text{ oder } p\equiv 1 \text{ oder } 3 \bmod 8,\\
&\text{es gibt } x,y\in\mathbb{Z} \text{ mit } p=x^2+3y^2 &&\iff\quad p=3 \text{ oder } p\equiv 1 \bmod 3.
\end{aligned}$$

Für die Primzahlen < 100 erhält man folgende Darstellungen:

p	p mod 4	p mod 8	p mod 3	Darstellungen
2	2	2	2	$2=1^2+1^2=0^2+2\cdot 1^2$
3	3	3	0	$3=1^2+2\cdot 1^2=0^2+3\cdot 1^2$
5	1	5	2	$5=2^2+1^2$
7	3	7	1	$7=2^2+3\cdot 1^2$
11	3	3	2	$11=3^2+2\cdot 1^2$
13	1	5	1	$13=3^2+2^2=1^2+3\cdot 2^2$
17	1	1	2	$17=4^2+1^2=3^2+2\cdot 2^2$
19	3	3	1	$19=1^2+2\cdot 3^2=4^2+3\cdot 1^2$
23	3	7	2	
29	1	5	2	$29=5^2+2^2$
31	3	7	1	$31=2^2+3\cdot 3^2$
37	1	5	1	$37=6^2+1^2=5^2+3\cdot 2^2$
41	1	1	2	$41=5^2+4^2=3^2+2\cdot 4^2$
43	3	3	1	$43=5^2+2\cdot 3^2=4^2+3\cdot 3^2$
47	3	7	2	
53	1	5	2	$53=7^2+2^2$
59	3	3	2	$59=3^2+2\cdot 5^2$
61	1	5	1	$61=6^2+5^2=7^2+3\cdot 2^2$
67	3	3	1	$67=7^2+2\cdot 3^2=8^2+3\cdot 1^2$
71	3	7	2	
73	1	1	1	$73=8^2+3^2=1^2+2\cdot 6^2=5^2+3\cdot 4^2$
79	3	7	1	$79=2^2+3\cdot 5^2$
83	3	3	2	$83=9^2+2\cdot 1^2$
89	1	1	2	$89=8^2+5^2=9^2+2\cdot 2^2$
97	1	1	1	$97=9^2+4^2=5^2+2\cdot 6^2=7^2+3\cdot 4^2$

Man kann allgemeiner fragen, wann sich zu gegebenem $d\in\mathbb{N}$ eine Primzahl p in der Form

$$p=x^2+dy^2$$

mit ganzen Zahlen x,y darstellen lässt. (Da es im Fall $p\le d$ nur die Möglichkeit $d=p$ mit $p=0^2+p\cdot 1^2$ gibt, beschränken wir auf $p>d$.) Das folgende Lemma liefert eine notwendige Bedingung:

Datei: alg_zaus.tex. Version vom 5.2.2024

[1]David A. Cox. Primes of the form x^2+ny^2. Second Edition. John Wiley & Sons, 2013. S.8

LEMMA. *Ist $d \in \mathbb{N}$ und p eine Primzahl mit $p > d$, sodass $m, n \in \mathbb{Z}$ existieren mit*

$$p = m^2 + dn^2,$$

so besitzt die Gleichung

$$x^2 \equiv -d \bmod p$$

eine Lösung $x \in \mathbb{Z}$ mit $\mathrm{ggT}(p, x) = 1$.

Beweis: Es ist $n \neq 0$, wegen $p > d$ gilt auch $m \neq 0$. Daraus folgt sofort $\mathrm{ggT}(p, m) = 1$ und $\mathrm{ggT}(p, n) = 1$. Insbesondere ist n invertierbar modulo p, es gibt also ein $v \in \mathbb{Z}$ mit $vn \equiv 1 \bmod p$. Dann gilt modulo p

$$(vm)^2 = v^2(m^2) = v^2(p - dn^2) \equiv -d(vn)^2 \equiv -d \bmod p.$$

Setzt man $x = vm$, so gilt $\mathrm{ggT}(p, x) = 1$ und $x^2 \equiv -d \bmod p$. Dies zeigt die Behauptung. ■

Die notwendige Bedingung [2] im Lemma motiviert nun die Einführung des **Legendre-Symbols**:

2. Das Legendre-Symbol $\left(\frac{a}{p}\right)$

Die Lösbarkeit der Gleichung $x^2 \equiv a \bmod p$ wird durch das sogenannte Legendre-Symbol beschrieben:

DEFINITION. *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann definiert man das* **Legendre-Symbol** $\left(\frac{a}{p}\right)$ *durch*

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } a \not\equiv 0 \bmod p \text{ und ein } x \in \mathbb{Z} \text{ existiert mit } x^2 \equiv a \bmod p, \\ -1, & \text{falls } x^2 \not\equiv a \bmod p \text{ für alle } x \in \mathbb{Z}, \\ 0, & \text{falls } a \equiv 0 \bmod p. \end{cases}$$

Ist $\left(\frac{a}{p}\right) = 1$, so nennt man a einen **quadratischen Rest** *modulo p, d.h. a ist Quadrat modulo p; ist $\left(\frac{a}{p}\right) = -1$, so nennt man a einen* **quadratischen Nichtrest** *modulo p, d.h. a ist kein Quadrat modulo p.*

Bemerkungen:

(1) Die Schreibweise $\left(\frac{a}{p}\right)$ geht auf Legendre zurück.
(2) Vorsicht: Es handelt sich beim Legendre-Symbol nicht um einen Bruch, der in Klammern gesetzt wurde.
(3) Das Legendre-Symbol ist für $p = 2$ nicht definiert.
(4) SAGE berechnet das Legendre-Symbol $\left(\frac{a}{p}\right)$ mit dem Befehl `legendre_symbol(a,p)`.

Beispiele:

(1) $p = 3$: Ist $x \in \mathbb{Z}$, so ist $x \equiv 0 \bmod 3$ oder $x \equiv 1 \bmod 3$ oder $x \equiv 2 \bmod 3$. Aus

$$0^2 \equiv 0 \bmod 3, \quad 1^2 \equiv 1 \bmod 3, \quad 2^2 \equiv 1 \bmod 3$$

sieht man dann

$$\left(\frac{a}{3}\right) = \begin{cases} 0, & \text{falls } a \equiv 0 \bmod 3, \\ 1, & \text{falls } a \equiv 1 \bmod 3, \\ -1, & \text{falls } a \equiv 2 \bmod 3. \end{cases}$$

[2] Am Beispiel $p = 7$, $d = 5$ sieht man, dass die notwendige Bedingung nicht hinreichend ist: Zwar wird $x^2 \equiv -5 \bmod 7$ durch $x = 3$ gelöst, die Gleichung $7 = x^2 + 5y^2$ hat aber keine Lösung in ganzen Zahlen.

(2) $p = 5$. Ist $x \in \mathbb{Z}$, so ist $x \equiv 0 \bmod 5$ oder $x \equiv 1 \bmod 5$ oder $x \equiv 2 \bmod 5$ oder $x \equiv 3 \bmod 5$ oder $x \equiv 4 \bmod 5$. Aus

$$0^2 \equiv 0 \bmod 5, \quad 1^2 \equiv 1 \bmod 5, \quad 2^2 \equiv 4 \bmod 5, \quad 3^2 \equiv 4 \bmod 5, \quad 4^2 \equiv 1 \bmod 5$$

sieht man dann

$$\left(\frac{a}{5}\right) = \begin{cases} 0, & \text{falls } a \equiv 0 \bmod 5, \\ 1, & \text{falls } a \equiv 1, 4 \bmod 5, \\ -1, & \text{falls } a \equiv 2, 3 \bmod 5. \end{cases}$$

(Dabei steht „$a \equiv 1, 4 \bmod 5$“ kurz für „$a \equiv 1$ oder $4 \bmod 5$“, oder noch ausführlicher „$a \equiv 1 \bmod 5$ oder $a \equiv 4 \bmod 5$“.)

(3) $p = 7$. Ist $x \in \mathbb{Z}$, so ist $x \equiv 0, 1, 2, 3, 4, 5, 6 \bmod 7$, was man auch in der Form $x \equiv 0, \pm 1, \pm 2, \pm 3 \bmod 7$ schreiben kann. Aus

$$1^2 \equiv (-1)^2 \equiv 6^2 \equiv 1 \bmod 7, \quad 2^2 \equiv (-2)^2 \equiv 5^2 \equiv 4 \bmod 7, \quad 3^2 \equiv (-3)^2 \equiv 4^2 \equiv 2 \bmod 7$$

folgt dann

$$\left(\frac{a}{7}\right) = \begin{cases} 0, & \text{falls } a \equiv 0 \bmod 7, \\ 1, & \text{falls } a \equiv 1, 2, 4 \bmod 7, \\ -1, & \text{falls } a \equiv 3, 5, 6 \bmod 7. \end{cases}$$

Für eine ungerade Primzahl p ist das Legendre-Symbol also eine Funktion $\mathbb{Z} \xrightarrow{a \mapsto \left(\frac{a}{p}\right)} \{0, 1, -1\}$. Offensichtlich folgt aber aus $a \equiv b \bmod p$ sofort $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, also kann man das Legendre-Symbol auch als Funktion $\mathbb{F}_p \xrightarrow{a \mapsto \left(\frac{a}{p}\right)} \{0, 1, -1\}$ auffassen, wenn wir jetzt $\mathbb{F}_p$ mit $\mathbb{Z}/p\mathbb{Z}$ identifizieren.

Beispiele: Indem man explizit die Menge der Quadrate $\{b^2 : b \in \mathbb{F}_p^*\}$ in $\mathbb{F}_p$ berechnet, kann man leicht Tabellen für das Legendre-Symbol anlegen. Die obigen Beispiele schreiben sich dann in der Form

$$\{b^2 : b \in \mathbb{F}_3^*\} = \{1\}, \quad \{b^2 : b \in \mathbb{F}_5^*\} = \{1, 4\}, \quad \{b^2 : b \in \mathbb{F}_7^*\} = \{1, 2, 4\}.$$

Damit erhält man

$a \in \mathbb{F}_3$	0	1	2
$\left(\frac{a}{3}\right)$	0	1	-1

$a \in \mathbb{F}_5$	0	1	2	3	4
$\left(\frac{a}{5}\right)$	0	1	-1	-1	1

$a \in \mathbb{F}_7$	0	1	2	3	4	5	6
$\left(\frac{a}{7}\right)$	0	1	1	-1	1	-1	-1

Bemerkung: Wird die Gleichung $x^2 \equiv a \bmod p$ von $x = b$ und $x = c$ gelöst, so folgt $c \equiv \pm b \bmod p$, da $\mathbb{F}_p$ ein Körper ist. Damit erhält man sofort folgende Formel:

$$|\{x \in \mathbb{F}_p : x^2 = a\}| = \left(\frac{a}{p}\right) + 1.$$

Wir wissen, dass die multiplikative Gruppe $\mathbb{F}_p^*$ des endlichen Körpers $\mathbb{F}_p$ zyklisch ist. Erzeuger der multiplikativen Gruppe werden Primitivwurzeln (modulo p) genannt. Ist g eine Primitivwurzel modulo p, so gilt also

$$\mathbb{F}_p = \{0, g, g^2, g^3, g^4, \ldots, g^{p-2}, g^{p-1} = 1\}.$$

Für $m, n \in \mathbb{Z}$ gilt genau dann $g^m = g^n$, wenn $m \equiv n \bmod p - 1$ gilt. Aus $1 = g^{p-1} = (g^{\frac{p-1}{2}})^2$ folgt, dass $g^{\frac{p-1}{2}}$ das einzige Element der Ordnung 2 ist, d.h. $g^{\frac{p-1}{2}} = -1$.

LEMMA. *Sei p eine ungerade Primzahl und g eine Primitivwurzel modulo p. Dann gilt für $m \in \mathbb{N}_0$:*

$$g^m \text{ ist Quadrat modulo } p, \text{ d.h. } \left(\frac{g^m}{p}\right) = 1 \quad \Longleftrightarrow \quad m \equiv 0 \bmod 2.$$

Anders ausgedrückt:

$$\left(\frac{g^m}{p}\right) = (-1)^m.$$

Beweis: Ist g^m ein Quadrat, so gibt es ein Element g^n mit $g^m = (g^n)^2$, also nach der Vorbemerkung $m \equiv 2n \bmod p-1$, was sofort $m \equiv 0 \bmod 2$ liefert. Ist umgekehrt $m \equiv 0 \bmod 2$, d.h. $m = 2n$, so ist $g^m = (g^n)^2$ natürlich ein Quadrat, also $\left(\frac{g^m}{p}\right) = 1$. ■

Bemerkung: Aus der Formel ergibt sich unmittelbar, dass es jeweils genau $\frac{p-1}{2}$ Quadrate und Nichtquadrate modulo p gibt, wenn man die 0 herausnimmt:

$$\begin{aligned} \text{Quadrate mod } p: &\quad g^0, g^2, g^4, g^6, \ldots, g^{p-3} \\ \text{Nichtquadrate mod } p: &\quad g^1, g^3, g^5, g^7, \ldots, g^{p-2} \end{aligned}$$

Also:

$$|\{0 \le 1 \le p-1 : \left(\frac{a}{p}\right) = 1\}| = |\{0 \le a \le p-1 : \left(\frac{a}{p}\right) = -1\}| = \frac{p-1}{2}.$$

In Zusammenhang mit dem Legendre-Symbol gibt es einen wichtigen Satz von Euler:

Satz (Euler). *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann gilt:*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

Beweis: Ist $a \equiv 0 \bmod p$, so stimmt die Gleichung offensichtlich. Sei jetzt $a \not\equiv 0 \bmod p$ und g eine Primitivwurzel modulo p. Dann gibt es $m \in \mathbb{N}$ mit $a \equiv g^m \bmod p$ und damit liefern unsere Vorbetrachtungen

$$\left(\frac{a}{p}\right) = \left(\frac{g^m}{p}\right) = (-1)^m \equiv (g^{\frac{p-1}{2}})^m = (g^m)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p,$$

was wir zeigen wollten. ■

Bemerkung: Da man mit der square-and-multiply-Methode schnell potenzieren kann, kann man mit dem Satz von Euler das Legendre-Symbol auch für große Primzahlen schnell berechnen.

Beispiel: Für $p = 1234567891$ findet man

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1, \quad \left(\frac{5}{p}\right) = 1.$$

Mit dem Legendre-Symbol weiß man jetzt, dass die Gleichung $x^2 \equiv 5 \bmod p$ eine Lösung besitzt. Eine andere Frage ist, wie man explizit eine Lösung bestimmen kann.

Im folgenden Satz stellen wir ein paar Eigenschaften des Legendre-Symbols zusammen:

Satz. *Sei p eine ungerade Primzahl. Dann gilt für $a, b \in \mathbb{Z}$:*

(1) $a \equiv b \bmod p \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. *(Das Legendre-Symbol ist also multiplikativ.)*

Beweis:

(1) Dies haben wir schon zuvor angemerkt. Die Eigenschaft folgt unmittelbar aus der Definition.
(2) Mit dem Satz von Euler ergibt sich

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p,$$

und damit

$$p \mid \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Aus

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \in \{-2, -1, 0, 1, 2\} \quad \text{und} \quad p \ge 3$$

folgt sofort die Gleichheit in $\mathbb{Z}$:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

was wir zeigen wollen. ■

Bemerkung: Die Formel $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ kann man für $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = \mathrm{ggT}(b,p) = 1$ auch so interpretieren:

a Quadrat modulo p,	b Quadrat modulo p	$\Rightarrow$	ab Quadrat modulo p,
a kein Quadrat modulo p,	b Quadrat modulo p	$\Rightarrow$	ab kein Quadrat modulo p,
a Quadrat modulo p,	b kein Quadrat modulo p	$\Rightarrow$	ab kein Quadrat modulo p,
a kein Quadrat modulo p,	b kein Quadrat modulo p	$\Rightarrow$	ab Quadrat modulo p.

Die ersten drei Aussagen gelten in jedem Körper, die letzte nicht.

Satz. *Für eine ungerade Primzahl p gilt:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4, \\ -1, & \text{falls } p \equiv -1 \bmod 4. \end{cases}$$

Beweis: Dies ergibt sich sofort aus der Eulerschen Formel. ■

Eine Anwendung des letzten Satzes gibt folgender Satz:

Satz (Zwei-Quadrate-Satz von Fermat). *Eine ungerade Primzahl p ist genau dann Summe zweier Quadrate, d.h. $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$, wenn gilt $p \equiv 1 \bmod 4$.*

Ein Beweis findet sich im nachfolgenden Abschnitt.

Wir wollen jetzt sehen, wann 2 ein Quadrat modulo p ist.

Beispiele: Durch Ausprobieren finden wir: 2 ist kein Quadrat modulo 3, 5, 11, 13, aber

$$3^2 \equiv 2 \bmod 7, \quad 6^2 \equiv 2 \bmod 17, \quad 5^2 \equiv 2 \bmod 23, \ldots$$

Was ist die Gesetzmäßigkeit?

Satz. *Für eine ungerade Primzahl p gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{falls } p \equiv 1, 7 \bmod 8, \\ -1, & \text{falls } p \equiv 3, 5 \bmod 8. \end{cases}$$

Beweis:

(1) Wir brauchen ein ζ in einem Oberkörper von $\mathbb{F}_p$ mit $\mathrm{ord}\,(\zeta) = 8$, was gleichwertig mit $\mathrm{ord}\,(\zeta^4) = 2$, also $\zeta^4 = -1$ ist. Sei $f(x) \in \mathbb{F}_p[x]$ ein irreduzibler normierter Faktor von $x^4 + 1$. Dann ist $K = \mathbb{F}_p[x]/(f)$ ein Oberkörper von $\mathbb{F}_p$. Ist ζ das Bild von x in $\mathbb{F}_p[x]/(f)$, so ist $f(\zeta) = 0$, und damit auch $\zeta^4 + 1 = 0$. Also ist K ein Oberkörper von $\mathbb{F}_p$ der ein Element ζ mit $\mathrm{ord}\,(\zeta) = 8$ enthält.

(2) Sei $\alpha = \zeta + \frac{1}{\zeta}$. Dann gilt

$$\alpha^2 = \zeta^2 + 2 + \frac{1}{\zeta^2} = 2 + \frac{\zeta^4 + 1}{\zeta^2} = 2,$$

und damit

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \left(\alpha^2\right)^{\frac{p-1}{2}} = \alpha^{p-1} = \frac{\alpha^p}{\alpha}.$$

Da Potenzieren mit p additiv in Charakteristik p ist, gilt

$$\alpha^p = \zeta^p + \frac{1}{\zeta^p} = \zeta^{p \bmod 8} + \frac{1}{\zeta^{p \bmod 8}}.$$

Wir unterscheiden jetzt vier Fälle (und verwenden $-\zeta^4 = 1$):

- **Fall** $p \equiv 1 \bmod 8$**:**
$$\alpha^p = \zeta^{p \bmod 8} + \frac{1}{\zeta^{p \bmod 8}} = \zeta + \frac{1}{\zeta} = \alpha.$$
- **Fall** $p \equiv 3 \bmod 8$**:**
$$\alpha^p = \zeta^{p \bmod 8} + \frac{1}{\zeta^{p \bmod 8}} = \zeta^3 + \frac{1}{\zeta^3} = \frac{\zeta^3}{-\zeta^4} + \frac{-\zeta^4}{\zeta^3} = -\left(\zeta + \frac{1}{\zeta}\right) = -\alpha.$$
- **Fall** $p \equiv 5 \bmod 8$**:**
$$\alpha^p = \zeta^{p \bmod 8} + \frac{1}{\zeta^{p \bmod 8}} = \zeta^5 + \frac{1}{\zeta^5} = \zeta^4 \cdot \zeta + \frac{1}{\zeta^4 \cdot \zeta} = -\left(\zeta + \frac{1}{\zeta}\right) = -\alpha.$$
- **Fall** $p \equiv 7 \bmod 8$**:**
$$\alpha^p = \zeta^{p \bmod 8} + \frac{1}{\zeta^{p \bmod 8}} = \zeta^7 + \frac{1}{\zeta^7} = \zeta^{-1} + \zeta = \alpha.$$

Mit $\left(\frac{2}{p}\right) = \frac{\alpha^p}{\alpha}$ erhalten wir daher
$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{für } p \equiv 1, 7 \bmod 8, \\ -1 & \text{für } p \equiv 3, 5 \bmod 8, \end{cases}$$
wie behauptet.

(3) Schreibt man $p = 8k + r$ mit $r \in \{1, 3, 5, 7\}$, so gilt
$$\frac{p^2 - 1}{8} = \frac{64k^2 + 16kr + r^2 - 1}{8} = 8k^2 + 2kr + \frac{r^2 - 1}{8},$$
woraus
$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{r^2-1}{8}}$$
folgt. Nun ist
$$\frac{r^2 - 1}{8} = \begin{cases} 0 & \text{für } r = 1, \\ 1 & \text{für } r = 3, \\ 3 & \text{für } r = 5, \\ 6 & \text{für } r = 7. \end{cases}$$
Daraus ergibt sich zusammen
$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{für } p \equiv 1 \bmod 8, \\ -1 & \text{für } p \equiv 3 \bmod 8, \\ -1 & \text{für } p \equiv 5 \bmod 8, \\ 1 & \text{für } p \equiv 8 \bmod 8. \end{cases}$$
Dies beweist dann auch die Darstellung $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. ■

Sind p und q verschiedene ungerade Primzahlen, so ist natürlich
$$\left(\frac{p}{q}\right) = \pm\left(\frac{q}{p}\right),$$
da das Legendre-Symbol hier nur die Werte ± 1 annehmen kann. Welches Vorzeichen gilt, gibt folgender Satz an, für den Gauß sechs verschiedene Beweise gegeben hat.

Satz (Quadratisches Reziprozitätsgesetz). *Sind p und q verschiedene ungerade Primzahlen, so gilt*
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$
d.h.
$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \textit{falls } p \equiv 1 \bmod 4 \textit{ oder } q \equiv 1 \bmod 4, \\ -\left(\frac{q}{p}\right), & \textit{falls } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Beweis: Zur besseren Unterscheidung schreiben für ℓ statt q.

(1) Wir brauchen einen Oberkörper K von $\mathbb{F}_p$, der ein Element ζ der Ordnung ℓ enthält:

$$\operatorname{ord}(\zeta) = \ell.$$

Dann gilt:

$$i \equiv j \bmod \ell \quad \Longrightarrow \quad \zeta^i = \zeta^j.$$

Daher ist auch ζ^i für $i \in \mathbb{F}_p$ wohldefiniert.

(2) Wir bilden die „Gauß-Summe“:

$$\gamma = \sum_{i \in \mathbb{F}_\ell^*} \left(\frac{i}{\ell}\right) \zeta^i.$$

(3) Die Potenzieren mit p in Charakteristik p additiv ist, erhalten wir:

$$\begin{aligned} \gamma^p &= \left(\sum_{i \in \mathbb{F}_\ell^*} \left(\frac{i}{\ell}\right) \zeta^i\right)^p = \sum_{i \in \mathbb{F}_\ell^*} \left(\frac{i}{\ell}\right)^p \zeta^{ip} = \sum_{i \in \mathbb{F}_\ell^*} \left(\frac{i}{\ell}\right) \zeta^{ip} = \sum_{i \in \mathbb{F}_\ell^*} \left(\frac{ip}{\ell}\right) \left(\frac{p}{\ell}\right) \zeta^{ip} = \\ &\overset{j=ip}{=} \left(\frac{p}{\ell}\right) \sum_{j \in \mathbb{F}_\ell^*} \left(\frac{j}{\ell}\right) \zeta^j = \left(\frac{p}{\ell}\right) \sum_{i \in \mathbb{F}_\ell^*} \left(\frac{i}{\ell}\right) \zeta^i = \left(\frac{p}{\ell}\right) \gamma. \end{aligned}$$

Dabei haben wir benutzt, dass mit i auch ip ganz $\mathbb{F}_\ell^*$ durchläuft.

(4) Wir berechnen nun γ^2:

$$\begin{aligned} \gamma^2 &= \left(\sum_{i \in \mathbb{F}_\ell^*} \left(\frac{i}{\ell}\right) \zeta^i\right) \cdot \left(\sum_{j \in \mathbb{F}_\ell^*} \left(\frac{j}{\ell}\right) \zeta^j\right) = \sum_{i,j \in \mathbb{F}_\ell^*} \left(\frac{ij}{\ell}\right) \zeta^{i+j} \overset{j=ik}{=} \\ &= \sum_{i,k \in \mathbb{F}_\ell^*} \left(\frac{i \cdot ik}{\ell}\right) \zeta^{i+ik} = \sum_{i,k \in \mathbb{F}_\ell^*} \left(\frac{k}{\ell}\right) \zeta^{(1+k)i} = \\ &= \sum_{i \in \mathbb{F}_\ell^*} \left(\frac{-1}{\ell}\right) \zeta^{0 \cdot i} + \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \sum_{i \in \mathbb{F}_\ell^*} \left(\frac{k}{\ell}\right) \zeta^{(1+k)i} = \\ &= \left(\frac{-1}{\ell}\right) \sum_{i \in \mathbb{F}_\ell^*} 1 + \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \left(\frac{k}{\ell}\right) \sum_{i \in \mathbb{F}_\ell^*} (\zeta^{1+k})^i = \\ &= \left(\frac{-1}{\ell}\right) (\ell - 1) + \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \sum_{i=1}^{\ell-1} (\zeta^{1+k})^i = \\ &= \left(\frac{-1}{\ell}\right) (\ell - 1) + \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \left(\frac{k}{\ell}\right) \zeta^{1+k} \sum_{i=0}^{\ell-2} (\zeta^{1+k})^i = \\ &= \left(\frac{-1}{\ell}\right) (\ell - 1) + \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \left(\frac{k}{\ell}\right) \zeta^{1+k} \cdot \frac{(\zeta^{1+k})^{\ell-1} - 1}{\zeta^{1+k} - 1} = \\ &= \left(\frac{-1}{\ell}\right) (\ell - 1) + \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \left(\frac{k}{\ell}\right) \frac{(\zeta^{1+k})^{\ell} - \zeta^{1+k}}{\zeta^{1+k} - 1} = \\ &= \left(\frac{-1}{\ell}\right) (\ell - 1) + \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \left(\frac{k}{\ell}\right) \frac{1 - \zeta^{1+k}}{\zeta^{1+k} - 1} = \\ &= \left(\frac{-1}{\ell}\right) \ell - \left(\frac{-1}{\ell}\right) - \sum_{k \in \mathbb{F}_\ell^* \setminus \{-1\}} \left(\frac{k}{\ell}\right) = \left(\frac{-1}{\ell}\right) \ell - \sum_{k \in \mathbb{F}_\ell^*} \left(\frac{k}{\ell}\right) = \left(\frac{-1}{\ell}\right) \ell. \end{aligned}$$

Im letzten Schritt wurde benutzt, dass es genausoviele Quadrate wie Nichtquadrate modulo ℓ gibt, dass also $\sum_{k \in \mathbb{F}_\ell^*} \left(\frac{k}{\ell}\right) = 0$ gilt.

(5) Wir haben also

$$\gamma^p = \left(\frac{p}{\ell}\right)\gamma \quad \text{und} \quad \gamma^2 = \left(\frac{-1}{\ell}\right)\ell.$$

Damit erhalten wir

$$\begin{aligned}\left(\frac{p}{\ell}\right)\gamma &= \gamma^p = \gamma^{p-1}\cdot\gamma = \left(\gamma^2\right)^{\frac{p-1}{2}}\cdot\gamma = \left(\left(\frac{-1}{\ell}\right)\ell\right)^{\frac{p-1}{2}}\cdot\gamma = \\ &= \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}}\cdot\ell^{\frac{p-1}{2}}\cdot\gamma \overset{\left(\frac{\ell}{p}\right)=\ell^{\frac{p-1}{2}}}{=} \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}}\cdot\left(\frac{\ell}{p}\right)\cdot\gamma.\end{aligned}$$

Wegen $\gamma^2 = \left(\frac{-1}{\ell}\right)\ell$ ist $\gamma \neq 0$. Nach Division der letzten Beziehung durch γ erhalten wir

$$\left(\frac{p}{\ell}\right) = \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}}\cdot\left(\frac{\ell}{p}\right).$$

Setzen wir noch $\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}}$ ein, so erhalten wir schließlich

$$\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2}\cdot\frac{p-1}{2}}\cdot\left(\frac{\ell}{p}\right).$$

Dies war zu zeigen. ■

Beispiele: Wir berechnen Legendre-Symbole unter Verwendung des Reziprozitätsgesetzes und der Formeln für $\left(\frac{-1}{p}\right)$ und $\left(\frac{2}{p}\right)$:

$$\left(\frac{1009}{1033}\right) = \left(\frac{1033}{1009}\right) = \left(\frac{24}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right) = \left(\frac{1009}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Für $p = 10^{10}+19$, $q = 10^{100}+267$ gilt:

$$\begin{aligned}\left(\frac{p}{q}\right) &= -\left(\frac{1066246421}{p}\right) = -\left(\frac{53}{p}\right)\left(\frac{103}{p}\right)\left(\frac{195319}{p}\right) = -\left(\frac{p}{53}\right)\left(\frac{p}{103}\right)\left(\frac{p}{195319}\right) = \\ &= -\left(\frac{34}{53}\right)\left(\frac{85}{103}\right)\left(\frac{57857}{195319}\right) = -\left(\frac{2}{53}\right)\left(\frac{17}{53}\right)\left(\frac{5}{103}\right)\left(\frac{17}{103}\right)\left(\frac{47\cdot 1231}{195319}\right) = \\ &= \left(\frac{2}{17}\right)\left(\frac{3}{5}\right)\left(\frac{1}{17}\right)(-1)\left(\frac{34}{47}\right)(-1)\left(\frac{821}{1231}\right) = -\left(\frac{2}{47}\right)\left(\frac{17}{47}\right)\left(\frac{821}{1231}\right) = \\ &= -\left(\frac{13}{17}\right)\left(\frac{410}{821}\right) = -\left(\frac{-4}{17}\right)\left(\frac{2}{821}\right)\left(\frac{5}{821}\right)\left(\frac{41}{821}\right) = \left(\frac{1}{5}\right)\left(\frac{1}{41}\right) = 1.\end{aligned}$$

(Man sieht hier bereits einen Nachteil dieser Version des Reziprozitätsgesetzes: um es anzuwenden, muss man Primfaktorzerlegung durchführen.)

Eine theoretische Anwendung des Reziprozitätsgesetzes gibt folgender Satz:

Satz (Pepin). *Für $n \geq 1$ ist die Fermat-Zahl $F_n = 2^{2^n}+1$ genau dann prim, wenn gilt*

$$3^{\frac{F_n-1}{2}} = 3^{2^{2^n-1}} \equiv -1 \bmod F_n.$$

Beweis:

- Es gelte $3^{\frac{F_n-1}{2}} \equiv -1 \bmod F_n$. Da $F_n - 1$ eine 2-Potenz ist, hat 3 dann die Ordnung $F_n - 1$ in $(\mathbb{Z}/(F_n))^*$, also ist F_n eine Primzahl.
- Sei nun umgekehrt F_n eine Primzahl. Dann gilt

  $$F_n \equiv 1 \bmod 4 \quad \text{und} \quad F_n = 4^{2^{n-1}}+1 \equiv 1^{2^{n-1}}+1 \equiv 2 \bmod 3$$

  und damit

  $$3^{\frac{F_n-1}{2}} \overset{\text{Euler}}{=} \left(\frac{3}{F_n}\right) \overset{\text{QRG}}{=} \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1 \bmod F_n,$$

  was wir zeigen wollten. ■

Allerdings ist nur von folgenden Fermatzahlen bekannt, dass sie prim sind:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Wir stellen hier die Rechenregeln für das Legendre-Symbol nochmals zusammen:

Rechenregeln für das Legendre-Symbol: Seien p und q ungerade Primzahlen und a, b ganze Zahlen.

(1)

$$a \equiv b \bmod p \quad \Longrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right), \quad \text{also insbesondere} \quad \left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right).$$

(2) (Multiplikativität)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(3) (Satz von Euler)

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

(4) (Quadratisches Reziprozitätsgesetz)

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4, \\ -\left(\frac{p}{q}\right), & \text{falls } p \equiv 3 \bmod 4 \text{ und } q \equiv 3 \bmod 4. \end{cases}$$

(5)

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4, \\ -1, & \text{falls } p \equiv 3 \bmod 4. \end{cases}$$

(6)

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 8 \text{ oder } p \equiv 7 \bmod 8, \\ -1, & \text{falls } p \equiv 3 \bmod 8 \text{ oder } p \equiv 5 \bmod 8. \end{cases}$$

3. Primzahlen als Summe von zwei Quadratzahlen - Der Zwei-Quadrate-Satz von Fermat

Welche Primzahlen p lassen sich als Summe von zwei Quadratzahlen, also in der Form

$$p = x^2 + y^2 \quad \text{mit} \quad x, y \in \mathbb{Z}$$

schreiben? Bei den Primzahlen ≤ 100 sind dies folgende:

$$2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2, \quad 37 = 1^2 + 6^2,$$

$$41 = 4^2 + 5^2, \quad 53 = 2^2 + 7^2, \quad 61 = 5^2 + 6^2, \quad 73 = 3^2 + 8^2, \quad 89 = 5^2 + 8^2, \quad 97 = 4^2 + 9^2.$$

(Aus Symmetriegründen haben wir uns bei der Darstellung $p = x^2 + y^2$ auf $x, y \in \mathbb{N}$ mit $x \leq y$ beschränkt.) Die Primzahl 2 spielt eine Sonderrolle und wird deshalb im Folgenden weggelassen.

LEMMA. *Ist eine ungerade Primzahl p Summe von zwei Quadraten, d.h. $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$, so ist -1 ein Quadrat modulo p, für das Legendre-Symbol gilt also $\left(\frac{-1}{p}\right) = 1$, woraus*

$$p \equiv 1 \bmod 4$$

folgt.

Beweis: Sei $p = x^2 + y^2$. Dann gilt natürlich $\mathrm{ggT}(p, x) = \mathrm{ggT}(p, y) = 1$, insbesondere ist y invertierbar modulo p, es gibt also ein $v \in Z$ mit $vy \equiv 1 \bmod p$. Dann gilt modulo p

$$(vx)^2 = v^2(x^2) = v^2(p - y^2) \equiv -v^2y^2 \equiv -(vy)^2 \equiv -1 \bmod p.$$

Also ist -1 ein Quadrat modulo p, d.h. $\left(\frac{-1}{p}\right) = 1$, was genau für $p \equiv 1 \bmod 4$ der Fall ist. ■

Bemerkung: Wir rechnen im Folgenden auch im euklidischen Ring $\mathbb{Z}[i]$. Da wir kein Repräsentantensystem für die Primelemente ausgezeichnet haben, ist der ggT von zwei Elementen zunächst nur bis auf Assoziiertheit bestimmt, also bis auf Multiplikation mit den Einheiten ± 1 und $\pm i$. Wir verwenden aber trotzdem die Bezeichnung $\mathrm{ggT}(a, b)$, wobei man sich hier $\mathrm{ggT}(a, b)$ als den Rückgabewert des euklidischen Algorithmus vorstellen kann.

Lemma. *Ist p eine Primzahl mit $p \equiv 1 \bmod 4$, so ist $\left(\frac{-1}{p}\right) = 1$, also gibt es ein $w \in \mathbb{Z}$ mit*

$$w^2 \equiv -1 \bmod p.$$

Berechnet man dann in $\mathbb{Z}[i]$ mit dem euklidischen Algorithmus ganze Zahlen $x, y \in \mathbb{Z}$ mit

$$x + iy = \mathrm{ggT}(p, w + i),$$

so gilt

$$p = x^2 + y^2.$$

($x + iy$ ist ein Primelement.)

Beweis: Sei $p \equiv 1 \bmod 4$ und $w \in \mathbb{Z}$ mit $w^2 \equiv -1 \bmod p$. Wir betrachten die Situation im euklidischen Ring $\mathbb{Z}[i]$. Die Kongruenz $w^2 \equiv -1 \bmod p$ können wir auch in der Form $p \mid w^2 + 1$ schreiben, was in $\mathbb{Z}[i]$ zu

$$p \mid (w + i)(w - i)$$

wird. Wegen $\frac{w+i}{p}, \frac{w-i}{p} \notin \mathbb{Z}[i]$ gilt $p \nmid w + i$ und $p \nmid w - i$ gilt, p ist also kein Primelement in $\mathbb{Z}[i]$. Sei π ein Primteiler von p Wegen $\mathrm{N}(p) = p^2$ gilt dann $\mathrm{N}(\pi) = p$. Aus

$$\pi \mid (w + i)(w - i)$$

folgt dann $\pi \mid w + i$ oder $\pi \mid w - i$. Indem wir eventuell π durch $\overline{\pi}$ ersetzen, können wir o.E.

$$\pi \mid w + i$$

annehmen. Dann folgt

$$\pi \mid \mathrm{ggT}(p, w + i).$$

Wegen $p \nmid w + i$ ist $\mathrm{ggT}(p, w + i)$ ein echter Teiler von p, sodass

$$\mathrm{N}(\pi) = \mathrm{N}(\mathrm{ggT}(p, w + i)) = p$$

folgt. Also ist

$$\pi \sim \mathrm{ggT}(p, w + i).$$

Sind $x, y \in \mathbb{Z}$ mit $x + iy = \mathrm{ggT}(p, w + i)$, so folgt

$$x^2 + y^2 = \mathrm{N}(x + iy) = \mathrm{N}(\mathrm{ggT}(p, w + i)) = p,$$

was die Behauptung beweist. ■

Bemerkung: Um das letzte Lemma praktisch umsetzen zu können, d.h. um zu einer Primzahl $p \equiv 1 \bmod 4$ Zahlen $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$ zu finden, braucht man noch ein w mit $w^2 \equiv -1 \bmod p$. Wegen

$$w^2 \equiv -1 \bmod p, \quad w^4 \equiv 1 \bmod p$$

ist w ein Element der Ordnung 4 in $\mathbb{Z}_p^*$. Das folgende Lemma zeigt, wie man solche Elemente leicht finden bestimmen kann.

Lemma. *Sei p eine Primzahl mit $p \equiv 1 \bmod 4$.*

(1) *Für* $a \in \{1, \dots, p-1\}$ *gilt*

$$a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$$

und

$$|\{a \in \{1, \dots, p-1\} : a^{\frac{p-1}{2}} \equiv 1 \bmod p\}| = |\{a \in \{1, \dots, p-1\} : a^{\frac{p-1}{2}} \equiv -1 \bmod p\}| = \frac{p-1}{2}.$$

(2) *Definiert man für* $a \in \{1, \dots, p-1\}$

$$w = a^{\frac{p-1}{4}} \bmod p, \quad \textit{so gilt} \quad w^2 \equiv \begin{cases} 1 \bmod p, & \textit{falls } a^{\frac{p-1}{2}} \equiv 1 \bmod p, \\ -1 \bmod p, & \textit{falls } a^{\frac{p-1}{2}} \equiv -1 \bmod p. \end{cases}$$

Beweis:

(1) Wegen der einfacheren Schreibweise betrachten wir die Situation in $\mathbb{F}_p^*$. Für $x \in \mathbb{F}_p^*$ ist

$$\left(x^{\frac{p-1}{2}}\right)^2 = x^{p-1} = 1, \quad \text{also} \quad x^{\frac{p-1}{2}} = \pm 1.$$

Daher ist

$$\psi : \mathbb{F}_p^* \to \{\pm 1\}, \quad x \mapsto x^{\frac{p-1}{2}}$$

ein Gruppenhomomorphismus. Für eine Primitivwurzel g modulo p gilt $\operatorname{ord}(g) = p-1$, also $\psi(g) \neq 1$, und damit $\psi(g) = -1$. Daher ist ψ surjektiv. Daher sind $\psi^{-1}(1)$ und $\psi^{-1}(-1)$ als Nebenklassen des Kerns gleichmächtig:

$$|\psi^{-1}(1)| = |\psi^{-1}(-1)| = \frac{p-1}{2}.$$

(2) Sei $a \in \{1, \dots, p-1\}$ und $w = a^{\frac{p-1}{4}} \bmod p$.

- Gilt $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, so folgt

$$w^2 \equiv \left(a^{\frac{p-1}{4}}\right)^2 \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

- Gilt $a^{\frac{p-1}{2}} \equiv -1 \bmod p$, so folgt

$$w^2 \equiv \left(a^{\frac{p-1}{4}}\right)^2 \equiv a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

Dies sollte gezeigt werden. ■

Wir fassen die vorangegangenen Lemmas in folgendem Satz zusammen:

Satz (Zwei-Quadrate-Satz - Konstruktive Variante).

- *Eine ungerade Primzahl* p *ist genau dann Summe zweier Quadrate, d.h.* $p = x^2 + y^2$ *mit* $x, y \in \mathbb{Z}$, *wenn gilt* $p \equiv 1 \bmod 4$.
- *Ist* $p \equiv 1 \bmod 4$, *wählt man* $a \in \{1, \dots, p-1\}$ *mit* $a^{\frac{p-1}{2}} \not\equiv 1 \bmod p$ *- es gibt* $\frac{p-1}{2}$ *Zahlen dieser Art -, setzt man* $w = a^{\frac{p-1}{4}} \bmod p$, *berechnet man mit dem euklidischen Algorithmus in* $\mathbb{Z}[i]$ *ganze Zahlen* $x, y \in \mathbb{Z}$ *mit*

$$x + iy = \operatorname{ggT}(p, w + i),$$

so gilt

$$p = x^2 + y^2.$$

Algorithmus zur Bestimmung einer Darstellung $p = x^2 + y^2$ **für Primzahlen** $p \equiv 1 \bmod 4$

Eingabe: Primzahl $p \equiv 1 \bmod 4$

Ausgabe: $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$

```
a ← 2
while a^((p-1)/2) mod p = 1 do
    a ← a + 1
end while
w ← a^((p-1)/4)
x + iy ← ggT(p, w + i) (in Z[i])
```

7: Return (x, y)

Zusammen mit dem früher angegebenen euklidischen Algorithmus für $\mathbb{Z}[i]$, erhalten wir folgendes Python-Programm:

```
# Division mit Rest in Z[i]
def div_rest_Zi(a,b):
  a0,a1=a
  b0,b1=b
  z0,z1,n=a0*b0+a1*b1,a1*b0-a0*b1,b0**2+b1**2
  q0,q1=(2*z0+n)//(2*n),(2*z1+n)//(2*n)
  r0,r1=a0-q0*b0+q1*b1,a1-q0*b1-q1*b0
  return (r0,r1)

# Euklidischer Algorithmus in Z[i]
def ggT_Zi(a,b):
  while b!=(0,0):
    a,b=b,div_rest_Zi(a,b)
  return a

# Fuer eine Primzahl p=1 mod 4 wird (x,y) mit p=x^2+y^2 zurueckgegeben
def zqs(p):
  a=2
  while pow(a,(p-1)//2,p)==1:
    a=a+1
  w=pow(a,(p-1)//4,p)
  return ggT_Zi((p,0),(w,1))
```

Beispiele: Für die ersten 10 Primzahlen $p > 10^{80}$ mit $p \equiv 1 \bmod 4$ haben wir eine Darstellung $p = x^2+y^2$ bestimmt:

$$
\begin{aligned}
10^{80}+129 &= 6863320128014033364225801615663546043615^2 + 72728836660844117116449748390756536773 52^2\\
10^{80}+349 &= 5598295619203883079704562668298907071830^2 + 82860778514326433605200440333100765398 93^2\\
10^{80}+661 &= 2829427409956277815407404976091735852375^2 + 95913680219136680458310001886618832824 94^2\\
10^{80}+913 &= 4300075696249838566013935557056942762588^2 + 90282528213670149796928714588104455007 37^2\\
10^{80}+1089 &= 33^2 + 10000000000000000000000000000000000000000^2\\
10^{80}+1609 &= 2883944973006899899080559827694569355180^2 + 95751167821947859213288723710332779882 03^2\\
10^{80}+1641 &= 5764627814840751428480112463974729710 45^2 + 99833707064079135813110716776093802712 04^2\\
10^{80}+1821 &= 4026923010345952778976255446087805264714^2 + 91533540884610319704919248611681886500 05^2\\
10^{80}+2257 &= 4075672194459977094329271457365111168799^2 + 91317520861719518462455880625592059003 16^2\\
10^{80}+2337 &= 3152550624961861058167567338666289495281^2 + 94900697867324758290393552351747172036 24^2
\end{aligned}
$$

Das folgende Lemma besagt, dass die Darstellung $p = x^2 + y^2$ einer Primzahl $p \equiv 1 \bmod 4$ bis auf die offensichtlichen Symmetrien eindeutig ist.

LEMMA. *Ist p eine Primzahl $p \equiv 1 \bmod$, ist $\pi = a + bi$ ein Primteiler von p in $\mathbb{Z}[i]$, so gilt:*

(1)
$$1 \cdot \pi = a + bi, \quad i \cdot \pi = -b + ai, \quad (-1) \cdot \pi = -a - bi, \quad (-i) \cdot \pi = b - ai$$
und
$$1 \cdot \overline{\pi} = a - bi, \quad i \cdot \overline{\pi} = b + ai, \quad (-1) \cdot \overline{\pi} = -a + bi, \quad (-i) \cdot \overline{\pi} = -b - ai.$$

(2) *Sind $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$, so gilt*
$$(x, y) \in \{(a, b), (a, -b), (-a, b), (-a, -b), (b, a), (b, -a), (-b, a), (-b, -a)\}.$$

Beweis:

(1) Dies rechnet man einfach nach.
(2) Seien $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$. Wegen $\pi \mid (x + yi)(x - yi)$ gibt es dann zwei Möglichkeiten: $\pi \mid x + yi$ oder $\pi \mid x - yi$, also

$$\pi \mid x + yi \quad \text{oder} \quad \overline{\pi} \mid x + yi.$$

Da π, $\overline{\pi}$ und $x + yi$ Norm p haben, folgt

$$x + yi \sim \pi \quad \text{oder} \quad x + yi \sim \overline{\pi},$$

also

$$x + yi = i^a \cdot \pi \text{ oder } x - yi = i^a \cdot \overline{\pi} \text{ für ein } a \in \{0, 1, 2, 3\}.$$

Der Rest folgt mit (1). ■

4. Primelemente in $\mathbb{Z}[\sqrt{d}]$

Das folgende Lemma besagt, dass Primelemente in $\mathbb{Z}[\sqrt{d}]$ eng mit den Primzahlen (aus $\mathbb{Z}$) zusammenhängen:

LEMMA. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$ und $R = \mathbb{Z}[\sqrt{d}]$. Ist π ein Primelement, so gibt es eine Primzahl p mit*

$$\pi \mid p.$$

Dann gilt:

$$\mathrm{N}(\pi) = \pm p \quad \textit{oder} \quad \pi \sim p.$$

Beweis: Sei π ein Primelement in R.

- Dann ist $\mathrm{N}(\pi) \notin \{0, \pm 1\}$, da π weder 0 noch eine Einheit ist. Also gibt es (nicht notwendig verschiedene) Primzahlen $p_1, \ldots, p_r$ mit

  $$\mathrm{N}(\pi) = \pm p_1 \ldots p_r.$$

  Ist $\pi = a + b\sqrt{d}$, so ist $\mathrm{N}(\pi) = (a + b\sqrt{d})(a - b\sqrt{d})$, also gilt $\pi \mid \mathrm{N}(\pi)$, und damit

  $$\pi \mid p_1 \ldots p_r.$$

  Da π ein Primelement sein sollte, gibt es eine Primzahl p_i mit

  $$\pi \mid p_i.$$

  Wir schreiben $p = p_i$ für diese Primzahl:

  $$\pi \mid p.$$

- Wegen $\pi \mid p$ gibt es ein Element $\rho \in R$ mit $p = \pi\rho$. Dann ist $p^2 = \mathrm{N}(\pi)\mathrm{N}(\rho)$. Es folgt $\mathrm{N}(\pi) \in \{\pm p, \pm p^2\}$. Ist $\mathrm{N}(\pi) = \pm p$, so sind wir fertig. Ist $\mathrm{N}(\pi) = \pm p^2$, so gilt $\mathrm{N}(\rho) = \pm 1$; also ist ρ eine Einheit und $\pi \sim p$. ■

LEMMA. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$ und $R = \mathbb{Z}[\sqrt{d}]$. Ist p eine Primzahl und $\pi \in R$ mit $\mathrm{N}(\pi) = \pm p$, so ist π ein Primelement. Schreibt man $\pi = a + b\sqrt{d}$ und $\overline{\pi} = a - b\sqrt{d}$, so ist*

$$p = \pm \pi \cdot \overline{\pi}$$

bis auf Assoziiertheit und Reihenfolge die einzige Zerlegung von p in irreduzible Elemente.

Beweis:

- Es ist

  $$|\mathbb{Z}[\sqrt{d}]/(\pi)| = |\mathrm{N}(\pi)| = p,$$

  also

  $$\mathbb{Z}[\sqrt{d}]/(\pi) \simeq \mathbb{Z}_p = \mathbb{F}_p.$$

  Daher ist (π) ein Primideal, also π ein Primelement.

- Natürlich ist wegen $\mathrm{N}(\overline{\pi}) = \pm p$ auch $\overline{\pi}$ ein Primelement. Ist $p = \alpha\beta$ irgendeine nichttriviale Zerlegung, d.h. $\alpha, \beta \notin R^*$, so gilt $|\mathrm{N}(\alpha)| > 1$, $|\mathrm{N}(\beta)| > 1$, also wegen $p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ dann $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = \pm p$. Aus $\pi \mid p$ folgt $\pi \mid \alpha\beta$, also o.E. $\pi \mid \alpha$. Wegen $\mathrm{N}(\pi) = \pm\mathrm{N}(\alpha)$ sind α und π assoziiert, also $\alpha = \varepsilon\pi$. Dann ist
$$\pm\pi \cdot \overline{\pi} = \varepsilon\pi \cdot \beta,$$
und damit $\beta \sim \overline{\pi}$. Es folgt die Behauptung. ■

Bemerkung: Da wir nachfolgend das Legendre-Symbol $\left(\frac{a}{p}\right)$ benutzen, das nur für ungerade Primzahlen p definiert ist, behandeln für $p = 2$ gesondert. Für $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{N}\}$ gilt: 2 ist kein Primelement in $\mathbb{Z}[\sqrt{d}]$, denn
$$2 \mid \sqrt{d} \cdot \sqrt{d}, \quad \text{aber} \quad 2 \nmid \sqrt{d} \quad \text{im Fall } d \equiv 0 \bmod 2$$
bzw.
$$2 \mid (1+\sqrt{d}) \cdot (1+\sqrt{d}), \quad \text{aber} \quad 2 \nmid 1+\sqrt{d} \quad \text{im Fall } d \equiv 1 \bmod 2.$$

LEMMA. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$ und p eine ungerade Primzahl. Dann gilt:*
$$p \text{ ist Primelement in } \mathbb{Z}[\sqrt{d}] \quad \Longleftrightarrow \quad \left(\frac{d}{p}\right) = -1.$$

Beweis:

- Sei p ein Primelement in $\mathbb{Z}[\sqrt{d}]$. Angenommen, es wäre $\left(\frac{d}{p}\right) \neq -1$. Dann gäbe es ein $a \in \mathbb{Z}$ mit mit $a^2 \equiv d \bmod p$, d.h. es gibt ein $m \in \mathbb{Z}$ mit
$$a^2 - d = mp.$$
In $\mathbb{Z}[\sqrt{d}]$ folgt
$$(a+\sqrt{d})(a-\sqrt{d}) = mp.$$
Da p Primelement sein soll, folgt
$$p \mid a+\sqrt{d} \text{ oder } p \mid a-\sqrt{d}.$$
Dies ist aber nicht der Fall. Also ist die Annahme falsch, d.h. es gilt $\left(\frac{d}{p}\right) = -1$.
- Sei umgekehrt $\left(\frac{d}{p}\right) = -1$. Dann gilt $x^2 \not\equiv d \bmod p$ für alle $x \in \mathbb{Z}$. Sei $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ mit $a + b\sqrt{d} \notin (p)$, d.h. $p \nmid a$ oder $p \nmid b$. Wir zeigen zunächst, dass
$$a^2 - db^2 \not\equiv 0 \bmod p$$
gilt.
  - **Fall $p \mid b$:** Dann gilt $p \nmid a$ und damit $a^2 - db^2 \equiv a^2 \not\equiv 0 \bmod p$.
  - **Fall $p \nmid b$:** Wegen $p \nmid b$ ist b invertierbar modulo p, es gibt also ein $c \in \mathbb{Z}$ mit $bc \equiv 1 \bmod p$. Angenommen, es wäre $a^2 - db^2 \equiv 0 \bmod p$. Dann würde $(ac)^2 \equiv d \bmod p$ folgen, im Widerspruch zur Voraussetzung. Also gilt auch hier $a^2 - db^2 \not\equiv 0 \bmod p$.

  Wir finden dann ein $u \in \mathbb{Z}$ mit
$$u(a^2 - db^2) \equiv 1 \bmod p.$$
Wir schreiben
$$u(a^2 - db^2) = 1 + np \text{ mit } n \in \mathbb{Z}.$$
Es folgt
$$(a + b\sqrt{d}) \cdot u(a - b\sqrt{d}) = 1 + np,$$
also ist $a + b\sqrt{d}$ invertierbar modulo p.
Jedes von 0 verschiedene Element von $\mathbb{Z}[\sqrt{d}]/(p)$ ist also invertierbar, d.h. $\mathbb{Z}[\sqrt{d}]/(p)$ ist ein Körper und damit p ein Primelement in $\mathbb{Z}[\sqrt{d}]$. ■

Wir betrachten nun, was mit ungeraden Primzahlen $p \in \mathbb{Z}$ in $\mathbb{Z}[\sqrt{d}]$ im Fall $\left(\frac{d}{p}\right) = 1$ passiert:

LEMMA. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$ und p eine ungerade Primzahl mit $\left(\frac{d}{p}\right) = 1$. Dann gibt es also ein $w \in \mathbb{Z}$ mit*

$$w^2 \equiv d \bmod p \quad \text{und} \quad \mathrm{ggT}(p, w) = 1.$$

Durch

$$\mathfrak{p}_a = (p, w + \sqrt{d}) \quad \text{und} \quad \mathfrak{p}_b = (p, w - \sqrt{d})$$

werden zwei Ideale in $\mathbb{Z}[\sqrt{d}]$ definiert. Dann gilt:

(1) *p ist kein Primelement in $\mathbb{Z}[\sqrt{d}]$.*
(2) *$\mathfrak{p}_a\mathfrak{p}_b = (p)$ und $\mathfrak{p}_a \neq \mathfrak{p}_b$.*
(3) *$\mathfrak{p}_a$ und $\mathfrak{p}_b$ sind Primideale.*
(4) *Ist π ein Primelement mit $\pi \mid p$, so gilt*

$$\mathfrak{p}_a = (\pi) \quad \text{oder} \quad \mathfrak{p}_b = (\pi)$$

und $\mathrm{N}(\pi) = \pm p$.
(5) *Ist $\mathfrak{p}_a$ ein Hauptideal, d.h. $\mathfrak{p}_a = (\pi)$ für ein $\pi \in \mathbb{Z}[\sqrt{d}]$, so ist π ein Primelement mit $\pi \mid p$. Außerdem ist π ein ggT von p und $w + \sqrt{d}$.*
(6) *Die Gleichung*

$$x^2 - dy^2 = \pm p$$

besitzt genau dann ganzzahlige Lösungen $x, y \in \mathbb{Z}$, wenn $\mathfrak{p}_a$ (und damit auch $\mathfrak{p}_b$) ein Hauptideal ist.

Beweis:

(1) Aus $w^2 \equiv d \bmod p$ folgt $p \mid w^2 - d$, also in $\mathbb{Z}[\sqrt{d}]$

$$p \mid (w + \sqrt{d})(w - \sqrt{d}).$$

Wegen

$$p \nmid w + \sqrt{d} \quad \text{und} \quad p \nmid w - \sqrt{d}$$

ist p kein Primelement in $\mathbb{Z}[\sqrt{d}]$.

(2) Es gilt:

$$\begin{aligned} \mathfrak{p}_a\mathfrak{p}_b &= (p, w + \sqrt{d})(p, w - \sqrt{d}) = (p^2, p(w + \sqrt{d}), p(w - \sqrt{d}), w^2 - d) = \\ &= p \cdot (p, w + \sqrt{d}, w - \sqrt{d}, \frac{w^2 - d}{p}) = p \cdot (p, 2w, w - \sqrt{d}, \frac{w^2 - d}{p}). \end{aligned}$$

Wegen $\mathrm{ggT}(p, w) = 1$ und $p \neq 2$ gibt es $u, v \in \mathbb{Z}$ mit $up + v(2w) = 1$, woraus sofort

$$(p, 2w, w - \sqrt{d}, \frac{w^2 - d}{p}) = (1)$$

folgt. Dies liefert

$$\mathfrak{p}_a\mathfrak{p}_b = (p).$$

Wäre $\mathfrak{p}_a = \mathfrak{p}_b$, so wäre $w - \sqrt{d} \in \mathfrak{p}_a$, und damit auch $2w \in \mathfrak{p}_a$, was wie eben $\mathfrak{p}_a = (1)$ liefern würde. Dann wäre aber $\mathfrak{p}_a\mathfrak{p}_b = (1)$, was nicht der Fall ist. Also gilt

$$\mathfrak{p}_a \neq \mathfrak{p}_b.$$

(3) Warum ist $\mathfrak{p}_a$ ein Primideal? Es ist

$$\mathbb{Z}[\sqrt{d}]/\mathfrak{p}_a = \mathbb{Z}[\sqrt{d}]/(p, w + \sqrt{d}) \simeq \mathbb{Z}[x]/(x^2 - d, p, w + x) = \mathbb{Z}[x]/(p, w + x) \simeq \mathbb{Z}/(p).$$

(4) Sei π ein Primelement mit $\pi \mid p$. Da p kein Primelement ist, folgt $\mathrm{N}(\pi) = \pm p$. Aus $p \mid w^2 - d$ und $\pi \mid p$ folgt

$$\pi \mid w + \sqrt{d} \quad \text{oder} \quad \pi \mid w - \sqrt{d},$$

also

$$\mathfrak{p}_a \subseteq (\pi) \quad \text{oder} \quad \mathfrak{p}_b \subseteq (\pi).$$

Da aber $\mathfrak{p}_a$ und $\mathfrak{p}_b$ maximale Ideale sind - wegen $\mathbb{Z}[\sqrt{d}]/\mathfrak{p}_{a,b} \simeq \mathbb{F}_p$ - gilt

$$\mathfrak{p}_a = (\pi) \quad \text{oder} \quad \mathfrak{p}_b = (\pi),$$

wie behauptet.

(5) Ist $\mathfrak{p}_a = (\pi)$, so ist (π) ein von 0 verschiedenes Primideal, also π ein Primelement. Aus $(\pi) = (p, w + \sqrt{d})$ folgt $\pi \mid p$ und $\pi \mid w + \sqrt{d}$. Ist α irgendein gemeinsamer Teiler von p und $w + \sqrt{d}$, so gilt $\alpha \mid p$ und $\alpha \mid w + \sqrt{d}$, also $p \in (\alpha)$ und $w + \sqrt{d} \in \alpha$, also $\mathfrak{p}_a \subseteq (\alpha)$, also $(\pi) \subseteq (\alpha)$ und damit $\alpha \mid \pi$ liefert. Also ist π ein ggT von p und $w + \sqrt{d}$.

(6) Die folgt sofort aus den vorangegangenen Aussagen. ■

Bemerkung: Ist $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$, so haben wir für ungerade Primzahlen p aus $\mathbb{Z}$ folgendes Verhalten gezeigt:

- **Fall** $\left(\frac{d}{p}\right) = 1$**:** Es gibt zwei verschiedene Primideale $\mathfrak{p}_a, \mathfrak{p}_b$ in $\mathbb{Z}[\sqrt{d}]$ mit
$$(p) = \mathfrak{p}_a \mathfrak{p}_b.$$
- **Fall** $\left(\frac{d}{p}\right) = -1$**:** Die Primzahl p ist auch ein Primelement in $\mathbb{Z}[\sqrt{d}]$. Das Ideal (p) ist also ein Primideal in $\mathbb{Z}[\sqrt{d}]$.

Das quadratische Reziprozitätsgesetz liefert nun, dass das angegebene Verhalten von Primzahlen periodisch modulo $4|d|$ ist:

LEMMA. *Sei $d \in \mathbb{Z} \setminus \{0\}$. Dann gilt für ungerade Primzahlen p, p':*

$$p \equiv p' \bmod 4|d| \quad \Longrightarrow \quad \left(\frac{d}{p}\right) = \left(\frac{d}{p'}\right).$$

Beweis:

- Wir zerlegen
$$d = (-1)^{e_1} \cdot 2^{e_2} \cdot q_1 \dots q_r$$
mit nicht notwendig verschiedenen ungeraden Primzahlen $q_1, \dots, q_r$.
- Für eine ungerade Primzahl p gilt:
$$\left(\frac{d}{p}\right) = \left(\frac{(-1)^{e_1} \cdot 2^{e_2} \cdot q_1 \dots q_r}{p}\right) = \left(\frac{-1}{p}\right)^{e_1} \left(\frac{2}{p}\right)^{e_2} \left(\frac{q_1}{p}\right) \dots \left(\frac{q_r}{p}\right).$$
- Mit den Funktionen
$$\varepsilon(n) = \begin{cases} 0 & \text{für } n \equiv 1 \bmod 4, \\ 1 & \text{für } n \equiv 3 \bmod 4 \end{cases} \quad \text{und} \quad \omega(n) = \begin{cases} 0 & \text{für } n \equiv 1 \text{ oder } 7 \bmod 7, \\ 1 & \text{für } n \equiv 3 \text{ oder } 5 \bmod 8 \end{cases}$$
schreiben sich die Formeln rund um das quadratische Reziprozitätsgesetz wie folgt - q sei eine ungerade Primzahl -
$$\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}, \quad \left(\frac{2}{p}\right) = (-1)^{\omega(p)}, \quad \left(\frac{q}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(q)} \left(\frac{p}{q}\right).$$
- Damit erhalten wir:
$$\begin{aligned} \left(\frac{d}{p}\right) &= (-1)^{\varepsilon(p)e_1} \cdot (-1)^{\omega(p)e_2} \cdot (-1)^{\varepsilon(p)\varepsilon(q_1)} \left(\frac{p}{q_1}\right) \dots (-1)^{\varepsilon(p)\varepsilon(q_r)} \left(\frac{p}{q_r}\right) = \\ &= (-1)^{(e_1+\varepsilon(q_1)+\dots+\varepsilon(q_r))\varepsilon(p)} \cdot (-1)^{e_2\omega(p)} \cdot \left(\frac{p}{q_1}\right) \dots \left(\frac{p}{q_r}\right). \end{aligned}$$
- Sei nun p' eine Primzahl mit $p' \equiv p \bmod 4|d|$.
  - Aus $p' \equiv p \bmod 4$ folgt $\varepsilon(p') = \varepsilon(p)$, und damit
  $$(-1)^{(e_1+\varepsilon(q_1)+\dots+\varepsilon(q_r))\varepsilon(p')} = (-1)^{(e_1+\varepsilon(q_1)+\dots+\varepsilon(q_r))\varepsilon(p)}.$$
  - Aus $p' \equiv p \bmod q_i$ folgt
  $$\left(\frac{p}{q_i}\right) = \left(\frac{p'}{q_i}\right).$$

– Ist $e_2 \geq 1$, so gilt $8 \mid 4|d|$, also $p' \equiv p \bmod 8$. Dann folgt $\omega(p') = \omega(p)$, und damit

$$(-1)^{e_2\omega(p')} = (-1)^{e_2\omega(p)}.$$

Damit folgt insgesamt

$$p \equiv p' \bmod 4|d| \quad \Longrightarrow \quad \left(\frac{d}{p}\right) = \left(\frac{d}{p'}\right),$$

was wir beweisen wollten. ■

Beispiel: Wir wollen für ungerade Primzahlen $p \neq 5$ das Legendre-Symbol $\left(\frac{-5}{p}\right)$ bestimmen. Es ist

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Nun ist

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right) = \left(\frac{-1}{p}\right)\left(\frac{p \bmod 5}{p}\right).$$

$p \bmod 20$	$p \bmod 4$	$\left(\frac{-1}{p}\right)$	$p \bmod 5$	$\left(\frac{p \bmod 5}{5}\right)$	$\left(\frac{-5}{p}\right)$
1	1	1	1	1	1
3	3	-1	3	-1	1
7	3	-1	2	-1	1
9	1	1	4	1	1
11	3	-1	1	1	-1
13	1	1	3	-1	-1
17	1	1	2	-1	-1
19	3	-1	4	1	-1

Wir fassen zusammen:

$$\left(\frac{-5}{p}\right) = \begin{cases} 1 & \text{für } p \equiv 1, 3, 7, 9 \bmod 20, \\ -1 & \text{für } p \equiv 11, 13, 17, 19 \bmod 20. \end{cases}$$

Da $\mathbb{Z}[\sqrt{-5}]$ aber kein Hauptidealring ist, ist $\left(\frac{-5}{p}\right) = 1$ keine hinreichende Bedingung dafür, dass die Gleichung $p = x^2 + 5y^2$ ganzzahlige lösbar ist. Beispielsweise gilt für alle $x, y \in \mathbb{Z}$

$$3 \neq x^2 + 5y^2, \quad 7 \neq x^2 + 5y^2, \quad 23 \neq x^2 + 5y^2, \quad 43 \neq x^2 + 5y^2, \quad 47 \neq x^2 + 5y^2.$$

5. Primfaktorzerlegung in $\mathbb{Z}[i]$ - Natürliche Zahlen als Summe von zwei Quadraten

Da $\mathbb{Z}[i]$ ein Hauptidealring ist, können wir die Ergebnisse des letzten Abschnitts für $\mathbb{Z}[i]$ nochmals übersichtlich formulieren. Dabei benutzen wir auch, dass $\mathbb{Z}[i]^* = \{\pm 1, \pm i\} = \langle i \rangle$ gilt.

Satz (Die Primelemente von $\mathbb{Z}[i]$).

(1) *Für jede ungerade Primzahl $p \equiv 1 \bmod 4$ gibt es $a_p, b_p \in \mathbb{N}$ mit $a_p > b_p$ und $p = a_p^2 + b_p^2$.*
(2) *Die Primelemente von $\mathbb{Z}[i]$ sind (bis auf Assoziiertheit):*
   (a) *$1 + i$ (mit $2 = (-i) \cdot (1 + i)^2$),*
   (b) *$\pi_p = a_p + b_p i$ und $\overline{\pi_p} = a_p - b_p i$ für Primzahlen $p \equiv 1 \bmod 4$,*
   (c) *q für Primzahlen $q \equiv 3 \bmod 4$.*
(3) *Jedes $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ hat eine eindeutige Primfaktorzerlegung*

$$\alpha = u \cdot (1 + i)^b \cdot \prod_{\substack{p \text{ prim} \\ p \equiv 1 \bmod 4}} \pi_p^{c_p} \cdot \overline{\pi_p}^{d_p} \cdot \prod_{\substack{q \text{ prim} \\ q \equiv 3 \bmod 4}} q^{e_q}$$

mit $u \in \{\pm 1, \pm i\}$ und $b, c_p, d_p, e_q \in \mathbb{N}_0$. Dabei gilt für die Norm

$$\mathrm{N}(\alpha) = 2^b \cdot \prod_{p \equiv 1 \bmod 4} p^{c_p + d_p} \cdot \prod_{q \equiv 3 \bmod 4} q^{2e_q}.$$

Beispiele:

(1) Wir faktorisieren 10 in $\mathbb{Z}[i]$:
$$10 = 2 \cdot 5 = (-i) \cdot (1+i)^2 \cdot (2+i) \cdot (2-i).$$
(2) Wir betrachten $\alpha = 123 + 321i \in \mathbb{Z}[i]$. Es ist
$$\alpha = 3 \cdot (41 + 107i) \quad \text{und} \quad \mathrm{N}(41+107i) = 13130 = 2 \cdot 5 \cdot 13 \cdot 101.$$
Nun bilden wir ggTs:
$$\begin{aligned} \mathrm{ggT}(2, 41+107i) &= -1 - i = (-1) \cdot (1+i), \\ \mathrm{ggT}(5, 41+107i) &= 1 + 2i = i \cdot (2-i), \\ \mathrm{ggT}(13, 41+107i) &= 2 + 3i = i \cdot (3-2i), \\ \mathrm{ggT}(101, 41+107i) &= 1 + 10i = i \cdot (10-i). \end{aligned}$$
$1+i$, $2-i$, $3-2i$, $10-i$ sind Primelemente mit Norm 2, 5, 13, 101. Man findet:
$$123 + 321i = i \cdot (1+i) \cdot 3 \cdot (2-i) \cdot (3-2i) \cdot (10-i).$$

Überlegungen: Welche natürlichen Zahlen n lassen sich als Summe von 2 Quadratzahlen, d.h. in der Form
$$n = x^2 + y^2 \text{ mit } x, y \in \mathbb{Z}$$
schreiben? Wegen
$$x^2 + y^2 = (x+yi)(x-yi) = \mathrm{N}(x+yi)$$
ist es mit unseren Vorkenntnissen naheliegend, Kenntnisse über $\mathbb{Z}[i]$ zu benutzen. Um das Zählen etwas zu vereinfachen, betrachten wir
$$\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : n = x^2 + y^2\}.$$
Ein Paar (x,y) können wir dann mit einer Zahl $x + yi \in \mathbb{Z}[i]$ identifizieren. Es gilt:
$$\begin{aligned} \{x+yi \in \mathbb{Z}[i] : n = x^2+y^2\} &= \{\alpha \in \mathbb{Z}[i] : \mathrm{N}(\alpha) = n\} = \\ &= \{i^a \cdot (1+i)^b \cdot \prod_{p \equiv 1 \bmod 4} \pi_p^{c_p} \cdot \overline{\pi_p}^{d_p} \cdot \prod_{q \equiv 3 \bmod 4} q^{e_q} : \\ &\quad a \in \{0,1,2,3\}, b = v_2(n), \\ &\quad c_p + d_p = v_p(n) \text{ für } p \equiv 1 \bmod 4, \\ &\quad 2e_q = v_q(n) \text{ für } q \equiv 3 \bmod 4\}. \end{aligned}$$
Gilt $v_q(n) \equiv 1 \bmod 2$ für eine Primzahl $q \equiv 3 \bmod 4$, so ist
$$\{x+yi \in \mathbb{Z}[i] : n = x^2+y^2\} = \emptyset,$$
d.h. n lässt sich nicht als Summe von 2 Quadraten darstellen.
Gilt $v_q(n) \equiv 0 \bmod 2$ für alle Primzahlen $q \equiv 4 \bmod 4$, so ist
$$\begin{aligned} \{x+yi \in \mathbb{Z}[i] : n = x^2+y^2\} &= \{i^a \cdot (1+i)^{v_2(n)} \cdot \prod_{p \equiv 1 \bmod 4} \pi_p^{c_p} \cdot \overline{\pi_p}^{v_p(n)-c_p} \cdot \prod_{q \equiv 3 \bmod 4} q^{\frac{1}{2}v_q(n)} : \\ &\quad 0 \le a \le 3 \text{ und } 0 \le c_p \le v_p(n)\}. \end{aligned}$$
Insbesondere gilt:
$$|\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : n = x^2+y^2\}| = 4 \prod_{p \equiv 1 \bmod 4} (1 + v_p(n)).$$
Damit haben wir folgenden Satz bewiesen:

Satz. *Für $n \in \mathbb{N}$ gilt:*
- *Existiert eine Primzahl $q \equiv 3 \bmod 4$ mit $v_q(n) \equiv 1 \bmod 2$, so ist*
$$\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : n = x^2+y^2\} = \emptyset.$$
- *Gilt $v_q(n) \equiv 0 \bmod 2$ für alle Primzahlen $q \equiv 3 \bmod 4$, so ist*
$$|\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : n = x^2+y^2\}| = 4 \prod_{p \equiv 1 \bmod 4} (1 + v_p(n)).$$

Beispiele:

n	n	$\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : n = x^2 + y^2\}$
1	1	$\{(0,1),(1,0),(-1,0),(0,-1)\}$
2	2	$\{(-1,1),(1,1),(1,-1),(-1,-1)\}$
3	3	$\emptyset$
4	2^2	$\{(-2,0),(0,2),(0,-2),(2,0)\}$
5	5	$\{(2,-1),(1,2),(2,1),(-1,-2),(-2,-1),(-2,1),(1,-2),(-1,2)\}$
6	$2 \cdot 3$	$\emptyset$
7	7	$\emptyset$
8	2^3	$\{(2,-2),(-2,2),(-2,-2),(2,2)\}$
9	3^2	$\{(0,3),(-3,0),(3,0),(0,-3)\}$
10	$2 \cdot 5$	$\{(-3,-1),(3,-1),(-3,1),(3,1),(-1,-3),(-1,3),(1,-3),(1,3)\}$
11	11	$\emptyset$
12	$2^2 \cdot 3$	$\emptyset$
13	13	$\{(-3,-2),(3,-2),(2,-3),(-2,-3),(2,3),(-2,3),(-3,2),(3,2)\}$
14	$2 \cdot 7$	$\emptyset$
15	$3 \cdot 5$	$\emptyset$
16	2^4	$\{(4,0),(0,-4),(-4,0),(0,4)\}$
17	17	$\{(-4,-1),(1,-4),(-4,1),(-1,4),(1,4),(4,-1),(-1,-4),(4,1)\}$
18	$2 \cdot 3^2$	$\{(-3,3),(-3,-3),(3,3),(3,-3)\}$
19	19	$\emptyset$
20	$2^2 \cdot 5$	$\{(-4,-2),(2,4),(-2,4),(4,2),(-4,2),(2,-4),(4,-2),(-2,-4)\}$
21	$3 \cdot 7$	$\emptyset$
22	$2 \cdot 11$	$\emptyset$
23	23	$\emptyset$
24	$2^3 \cdot 3$	$\emptyset$
25	5^2	$\{(-3,4),(3,4),(4,-3),(4,3),(-5,0),(-4,-3),(-4,3),(5,0),(0,5),(-3,-4),(0,-5),(3,-4)\}$
26	$2 \cdot 13$	$\{(-5,1),(-1,-5),(1,5),(5,-1),(1,-5),(5,1),(-5,-1),(-1,5)\}$
27	3^3	$\emptyset$
28	$2^2 \cdot 7$	$\emptyset$
29	29	$\{(-2,-5),(2,-5),(5,-2),(-2,5),(-5,2),(2,5),(-5,-2),(5,2)\}$
30	$2 \cdot 3 \cdot 5$	$\emptyset$