3. Quadratische Zahlkörper

Ein quadratischer Zahlkörper K ist ein algebraischer Zahlkörper vom Grad 2.

Ein solcher Körper lässt sich stets schreiben als $K = \mathbb{Q}(\sqrt{d})$, wobei $d \in \mathbb{Z} \setminus \{0, 1\}$ eine quadratfreie ganze Zahl ist.

Der Zahlkörper $\mathbb{Q}(\sqrt{d})$ heißt *reell-quadratisch*, falls $d > 1$ (dann gilt $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$) und *imaginär-quadratisch*, falls $d < 0$ (dann hat man eine natürliche Einbettung $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$).

Man hat in $K = \mathbb{Q}(\sqrt{d})$ eine Konjugations-Abbildung

$$\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}), \quad \sigma(x + y\sqrt{d}) := x - y\sqrt{d}.$$

σ ist ein Körper-Automorphismus von K, der zusammen mit der Identität die Galoisgruppe von K über $\mathbb{Q}$ bildet. Im Falle eines imaginär-quadratischen Zahlkörpers ist σ die übliche komplexe Konjugation.

Mithilfe von σ kann man die Spur und Norm $\mathrm{Tr}, \mathrm{N} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ definieren. Für $\xi = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ ist

$$\begin{aligned} \mathrm{Tr}(\xi) &:= \xi + \sigma(\xi) = 2x \\ \mathrm{N}(\xi) &:= \xi \cdot \sigma(\xi) = x^2 - dy^2. \end{aligned}$$

Die Spur ist eine $\mathbb{Q}$-lineare Abbildung, d.h.

$$\mathrm{Tr}(\alpha\xi + \beta\eta) = \alpha\mathrm{Tr}(\xi) + \beta\mathrm{Tr}(\eta) \quad \text{für alle } \xi, \eta \in K \text{ und } \alpha, \beta \in \mathbb{Q}.$$

Die Norm ist multiplikativ, d.h.

$$\mathrm{N}(\xi\eta) = \mathrm{N}(\xi)\mathrm{N}(\eta) \qquad \text{und} \qquad \mathrm{N}(\xi) = 0 \Leftrightarrow \xi = 0.$$

Für einen imaginär-quadratischen Zahlkörper ist die Norm eines Elementes $z \in \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ das Quadrat des üblichen Absolut-Betrages, d.h. $\mathrm{N}(z) = |z|^2$. Für reell-quadratische Zahlkörper kann die Norm eines Elementes auch negativ sein.

3.1. Satz. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper mit $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Ein Element $\xi \in K$ ist genau dann ganz-algebraisch, wenn $\mathrm{Tr}(\xi) \in \mathbb{Z}$ und $\mathrm{N}(\xi) \in \mathbb{Z}$.*

Beweis. a) Sei $\xi \in K$ ganz-algebraisch. Dann genügt ξ einer Gleichung $f(\xi) = 0$ mit einem normierten Polynom $f(X) \in \mathbb{Z}[X]$. Anwendung des Automorphismus σ auf die Gleichung liefert $f(\sigma(\xi)) = 0$. Also ist auch $\sigma(\xi)$ ganz-algebraisch. Daraus folgt, dass $\mathrm{Tr}(\xi) = \xi + \sigma(\xi)$ und $\mathrm{N}(\xi) = \xi\sigma(\xi)$ ganz-algebraisch sind. Da aber $\mathrm{Tr}(\xi), \mathrm{N}(\xi) \in \mathbb{Q}$, gilt nach Satz 2.16 sogar $\mathrm{Tr}(\xi), \mathrm{N}(\xi) \in \mathbb{Z}$.

b) Sei umgekehrt vorausgesetzt, dass $t := \mathrm{Tr}(\xi) = \xi + \sigma(\xi) \in \mathbb{Z}$ und $c := \mathrm{N}(\xi) = \xi\sigma(\xi) \in \mathbb{Z}$. Dann sind ξ und $\sigma(\xi)$ Nullstellen des Polynoms

$$(X - \xi)(X - \sigma(\xi)) = X^2 - tX + c \ \in \ \mathbb{Z}[X],$$

also ξ ganz-algebraisch.

3.2. Satz. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper ($d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei) und $R := \mathfrak{O}_K$ sein Ganzheitsring.*

a) *Falls $d \equiv 2 \bmod 4$ oder $d \equiv 3 \bmod 4$, gilt*

$$R = \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}.$$

b) *Falls $d \equiv 1 \bmod 4$, gilt*

$$R = \mathbb{Z}\Big[\frac{1 + \sqrt{d}}{2}\Big] = \Big\{x + y\frac{1 + \sqrt{d}}{2} : x, y \in \mathbb{Z}\Big\}.$$

Bemerkung. Der Fall $d \equiv 1 \bmod 4$ lässt sich auch so schreiben

$$R = \mathbb{Z}\Big[\frac{1 + \sqrt{d}}{2}\Big] = \Big\{\frac{x + y\sqrt{d}}{2} : x, y \in \mathbb{Z},\ x \equiv y \bmod 2\Big\}.$$

Beweis. a) Dass alle Elemente $x + y\sqrt{d}$ mit $x, y \in \mathbb{Z}$ ganz sind, ist klar.

Sei umgekehrt ein Element $\xi = x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$ gegeben, das ganz ist. Wir müssen zeigen, dass dann $x, y \in \mathbb{Z}$. Es ist

$$\mathrm{Tr}(\xi) = 2x \in \mathbb{Z} \quad \text{und} \quad \mathrm{N}(\xi) = x^2 - dy^2 \in \mathbb{Z}.$$

Aus $2x \in \mathbb{Z}$ folgt entweder (i) $x \in \mathbb{Z}$, oder (ii) $x \in \frac{1}{2} + \mathbb{Z}$ (d.h. x ist halbganz).

Im ersten Fall folgt $dy^2 \in \mathbb{Z}$. Angenommen y sei nicht ganz. Dann ist $y = m/n$ mit teilerfremden ganzen Zahlen m, n und $n \geqslant 2$. Da dy^2 ganz ist, würde folgen $n^2 \mid d$. Dies ist ein Widerspruch dazu, dass d quadratfrei ist. Also muss y ganz sein.

Im zweiten Fall ist $x = t/2$ mit einer ungeraden ganzen Zahl t. Aus der Normbedingung folgt dann $t^2 - d(2y)^2 \in 4\mathbb{Z}$. Daraus folgt zunächst (wie im ersten Fall), dass $2y =: z \in \mathbb{Z}$ und weiter $4 \mid t^2 - dz^2$. Dies ist unmöglich für $d \equiv 2 \bmod 4$, aber auch für $d \equiv 3 \bmod 4$, wie man durch Betrachtung modulo 8 erkennt. Der zweite Fall kann also nicht auftreten.

b) Das Element $\omega := \frac{1}{2}(1 + \sqrt{d})$ ist ganz, denn $\mathrm{Tr}(\omega) = 1$ und $\mathrm{N}(\omega) = (1 - d)/4 \in \mathbb{Z}$. Daraus folgt, dass alle Elemente der Gestalt $x + y\frac{1+\sqrt{d}}{2}$ mit $x, y \in \mathbb{Z}$ ganz sind.

Sei umgekehrt ein Element $\xi = x + y\frac{1+\sqrt{d}}{2}$ mit $x, y \in \mathbb{Q}$ gegeben, das ganz ist. Es ist zu zeigen, dass dann $x, y \in \mathbb{Z}$. Man berechnet

$$\mathrm{N}(\xi) = (x + \tfrac{y}{2})^2 - d(\tfrac{y}{2})^2 = \tfrac{1}{4}\left((2x + y)^2 - dy^2\right)$$

Da $\mathrm{Tr}(\xi) = 2x + y =: t \in \mathbb{Z}$, folgt $t^2 - dy^2 \in 4\mathbb{Z}$. Daraus ergibt sich wie oben $y \in \mathbb{Z}$ und wegen $d \equiv 1 \bmod 4$ auch $t \equiv y \bmod 2$, also $t - y = 2x \in 2\mathbb{Z}$, d.h. $x \in \mathbb{Z}$, q.e.d.

Beispiele. Wir geben einige typische Beispiele.

1) Der Ganzheitsring von $\mathbb{Q}(\sqrt{2})$ ist $\mathbb{Z}[\sqrt{2}]$.

2) Der Ganzheitsring von $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ ist $\mathbb{Z}[i]$. Man nennt

$$\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}$$

den Ring der ganzen Gauß'schen Zahlen.

3) Der Ganzheitsring von $\mathbb{Q}(\sqrt{-3})$ ist (da $-3 \equiv 1 \bmod 4$)

$$\mathbb{Z}[\tfrac{1+i\sqrt{3}}{2}] = \mathbb{Z}[\tfrac{-1+i\sqrt{3}}{2}] = \mathbb{Z}[\rho],$$

wobei $\rho := \frac{-1+i\sqrt{3}}{2} = e^{2\pi i/3}$ eine primitive dritte Einheitswurzel in $\mathbb{C}$ ist.

Bemerkung. Satz 3.2 sagt insbesondere: Der Ganzheitsring des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$, $(d \neq 0, 1$ quadratfrei), ist ein freier $\mathbb{Z}$-Modul vom Rang 2. Eine Basis bilden die Elemente 1, ω, wobei

$$\omega := \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2, 3 \bmod 4, \\ \frac{1}{2}(1 + \sqrt{d}), & \text{falls } d \equiv 1 \bmod 4. \end{cases}$$

3.3. Definition (Diskriminante). Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper und ω_1, ω_2 eine Basis von K über $\mathbb{Q}$. Dann ist die Diskriminante dieser Basis definiert als

$$\mathrm{discr}(\omega_1, \omega_2) := \det \begin{pmatrix} \omega_1 & \sigma(\omega_1) \\ \omega_2 & \sigma(\omega_2) \end{pmatrix}^2.$$

Da die Diskriminante offensichtlich invariant gegenüber der Konjugation σ ist, gilt $\mathrm{discr}(\omega_1, \omega_2) \in \mathbb{Q}$. Ist ω_1', ω_2' eine weitere Basis von K über $\mathbb{Q}$, so gibt es eine invertierbare 2×2-Matrix (c_{ij}) mit Koeffizienten aus $\mathbb{Q}$, so dass

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Es folgt

$$\mathrm{discr}(\omega_1', \omega_2') = \det(c_{ij})^2 \mathrm{discr}(\omega_1, \omega_2).$$

Setzen wir jetzt speziell voraus, dass die von ω_1', ω_2' und ω_1, ω_2 aufgespannten $\mathbb{Z}$-Moduln gleich sind, d.h.

$$\Lambda := \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2' = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,$$

so ist die Übergangs-Matrix $(c_{ij}) \in M(2 \times 2, \mathbb{Z})$ invertierbar über dem Ring $\mathbb{Z}$, d.h. die Determinante gleich ± 1. Daraus folgt

$$\mathrm{discr}(\omega_1', \omega_2') = \mathrm{discr}(\omega_1, \omega_2) =: \mathrm{discr}(\Lambda),$$

die Diskriminante hängt also nur von dem $\mathbb{Z}$-Modul Λ ab. Insbesondere ist daher die Diskriminante $\mathrm{discr}(\mathfrak{O}_K)$ der Maximalordnung von K wohldefiniert. Diese wird auch als Diskriminante des Körpers K bezeichnet, $\mathrm{discr}(K) := \mathrm{discr}(\mathfrak{O}_K)$.

3.4. Satz. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper ($d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei). Dann gilt für die Diskriminante von K*

$$\mathrm{discr}(K) = \mathrm{discr}(\mathfrak{O}_K) = \begin{cases} 4d, & \text{falls } d \equiv 2, 3 \bmod 4, \\ d, & \text{falls } d \equiv 1 \bmod 4. \end{cases}$$

Beweis. a) Im Fall $d \equiv 2, 3 \bmod 4$ ist $1, \sqrt{d}$ eine $\mathbb{Z}$-Basis von $\mathfrak{O}_K$, also

$$\mathrm{discr}(K) = \det \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}^2 = (-4\sqrt{d})^2 = 4d.$$

b) Falls $d \equiv 1 \bmod 4$, ist $1, \frac{1}{2}(1 + \sqrt{d})$ eine $\mathbb{Z}$-Basis von $\mathfrak{O}_K$, also

$$\mathrm{discr}(K) = \det \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = (-\sqrt{d})^2 = d.$$

Für die Teibarkeitslehre in einem Integritätsbereich R spielen die Einheiten, d.h. die invertierbaren Elemente von R eine wichtige Rolle.

3.5. Satz. *Sei R der Ring der ganzen Zahlen in einem quadratischen Zahlkörper. Ein Element $\xi \in R$ ist genau dann Einheit in R, wenn $\mathrm{N}(\xi) = \pm 1$.*

Beweis. Die Bedingung ist notwendig. Denn gilt $\xi\eta = 1$ in R, so folgt $\mathrm{N}(\xi)\mathrm{N}(\eta) = 1$ in $\mathbb{Z}$, also $\mathrm{N}(\xi) = \pm 1$. Umgekehrt folgt aus $\mathrm{N}(\xi) = \pm 1$, dass $\xi^{-1} = \mathrm{N}(\xi)\sigma(\xi) \in R$, q.e.d.

Für imaginär-quadratische Zahlkörper ist es leicht, eine vollständige Übersicht über die Einheiten zu bekommen.

3.6. Satz. *Sei $d < 0$ eine quadratfreie ganze Zahl und R der Ganzheitsring des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$.*

a) *Falls $d = -1$, also $R = \mathbb{Z}[i]$, besteht die Gruppe R^* der Einheiten genau aus den vierten Einheitswurzeln in $\mathbb{C}$, d.h.*

$$R^* = \{1, i, -1, -i\}.$$

b) *Falls $d = -3$, also $R = \mathbb{Z}[\rho]$, ($\rho = \frac{-1+i\sqrt{3}}{2}$), besteht R^* genau aus den sechsten Einheitswurzeln in $\mathbb{C}$, d.h.*

$$R^* = \{\pm 1, \pm\rho, \pm\rho^2\}.$$

c) *In allen anderen Fällen gilt $R^* = \{1, -1\}$.*

Beweis. Für $\xi = x + iy\sqrt{|d|} \in \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ ist $\mathrm{N}(\xi) = x^2 + |d|y^2$ gleich dem Quadrat des gewöhnlichen Betrags der komplexen Zahl ξ, woraus folgt, dass alle Einheiten auf dem Einheitskreis der komplexen Ebene liegen. Die Fälle a) und b) sind leicht direkt nachzuprüfen.

c) In den übrigen Fällen ist $d = -2$ oder $d \leqslant -5$. Für den Imaginärteil eines Elementes $\xi \in \mathbb{Q}(\sqrt{d})$ gilt dann $\mathsf{Im}(\xi) = 0$ oder $|\mathsf{Im}(\xi)| > 1$. Im zweiten Fall ist $|\xi| > 1$, also ξ keine Einheit. Eine Einheit ξ ist daher notwendig reell, also $\xi = \pm 1$.

In reell-quadratischen Zahlkörpern ist die Situation nicht so einfach. Z.B. ist im Ring $\mathbb{Z}[\sqrt{2}]$ die Zahl $u := 1 + \sqrt{2}$ eine Einheit (mit $u^{-1} = -1 + \sqrt{2}$). Da die Einheiten eine Gruppe bilden, sind auch $u_n := u^n$ für alle $n \in \mathbb{Z}$ Einheiten in $\mathbb{Z}[\sqrt{2}]$. Es gibt also unendlich viele Einheiten. Wir werden auf dieses Problem in später noch zurückkommen.

3.7. Ein Beispiel für Nicht-Faktorialität. Der Ganzheitsring eines quadratischen Zahlkörpers ist im Allgemeinen nicht faktoriell. Betrachten wir etwa den Körper $K = \mathbb{Q}(\sqrt{-5})$. Sein Ganzheitsring ist $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$. Das Element $6 \in \mathbb{Z}[\sqrt{-5}]$ besitzt zwei wesentlich verschiedene Zerlegungen in irreduzible Elemente:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Dass die Elemente 2, 3, $z := 1 + \sqrt{-5}$ und $\overline{z} = 1 - \sqrt{-5}$ irreduzibel sind, sieht man so: Wäre 2 reduzibel, etwa $2 = \xi\eta$ mit Nicht-Einheiten $\xi, \eta \in \mathbb{Z}[\sqrt{-5}]$, so wäre $4 = \mathrm{N}(2) = \mathrm{N}(\xi)\mathrm{N}(\eta)$, also $\mathrm{N}(\xi) = 2$. Es gibt aber in $\mathbb{Z}[\sqrt{-5}]$ kein Element der Norm 2, denn die Gleichung $x^2 + 5y^2 = 2$ ist ganzzahlig unlösbar. Ebenso gibt es in $\mathbb{Z}[\sqrt{-5}]$ kein Element der Norm 3, was zeigt, dass 3 irreduzibel ist. Da $N(z) = 6$, müsste bei einer nicht-trivialen Zerlegung $z = z_1 z_2$ einer der Faktoren die Norm 2 haben. Da dies unmöglich ist, ist z irreduzibel, ebenso $\overline{z}$. Aus Normgründen ist z weder zu 2 noch zu 3 assoziiert, ebenso $\bar{z}$. Also handelt es sich tatsächlich um zwei wesentlich verschiedene Zerlegungen der Zahl 6 im Ring $\mathbb{Z}[\sqrt{-5}]$. Das Beispiel zeigt auch, dass

2 kein Primelement in $\mathbb{Z}[\sqrt{-5}]$ ist, denn 2 ist ein Teiler des Produkts $z\overline{z}$, ohne einen Faktor zu teilen. Aus demselben Grund ist 3 kein Primelement in $\mathbb{Z}[\sqrt{-5}]$.

3.8. Legendre-Symbol. Wir erinnern an einige Begriffe und Tatsachen aus der Theorie der quadratischen Reste. Sei p eine ungerade Primzahl. Eine Zahl $a \in \mathbb{Z}$ mit $p \nmid a$ heißt quadratischer Rest modulo p, wenn die Kongruenz $x^2 \equiv a \bmod p$ lösbar ist, andernfalls heißt a quadratischer Nichtrest. Damit definiert man das *Legendre-Symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } a \text{ quadratischer Rest modulo } p, \\ -1, & \text{falls } a \text{ quadratischer Nichtrest modulo } p. \end{cases}$$

Da $(\frac{a}{p})$ nur von der Restklasse $a \bmod p$ abhängt, kann man das Legendre-Symbol auch als Funktion

$$\left(\frac{-}{p}\right) : \mathbb{F}_p^* \to \{\pm 1\}, \qquad a \mapsto \left(\frac{a}{p}\right)$$

auffassen, die auf den Quadraten den Wert 1 und auf den Nicht-Quadraten den Wert -1 annimmt. Da die Quadrierungs-Abbildung

$$\mathrm{sq} : \mathbb{F}_p^* \to \mathbb{F}_p^*, \quad x \mapsto \mathrm{sq}(x) = x^2,$$

den Kern $\{\pm 1\}$ hat, ist die Menge der Quadrate $\mathrm{sq}(\mathbb{F}_p^*) \subset \mathbb{F}_p^*$ eine Untergruppe vom Index 2, hat also $\frac{p-1}{2}$ Elemente. Es gilt das Kriterium von Euler

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

woraus die Rechenregel $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ folgt. Für das Legendre-Symbol gilt das berühmte Quadratische Reziprozitätsgesetz von Gauß: Sind $p \neq q$ ungerade Primzahlen, so folgt

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

Außerdem gelten die beiden Ergänzungssätze

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{und} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

3.9. Hilfssatz. *Sei $K = \mathbb{Q}(\sqrt{d})$, ($d \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei), ein quadratischer Zahlkörper und $\mathfrak{O}_K$ sein Ganzheitsring.*

a) *Sei p eine ungerade Primzahl mit $(\frac{d}{p}) = -1$. Ist dann $\xi \in \mathfrak{O}_K$ ein Element mit $p \mid \mathrm{N}(\xi)$, so folgt $p \mid \xi$.*

b) *Sei $d \equiv 5 \bmod 8$. Ist dann $\xi \in \mathfrak{O}_K$ ein Element mit $2 \mid \mathrm{N}(\xi)$, so folgt $2 \mid \xi$.*

Beweis. a) Wir unterscheiden zwei Fälle:

(i) $d \equiv 2, 3 \bmod 4$. Dann ist

$$\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}.$$

Sei $\xi = x + y\sqrt{d}$ ein beliebiges Element aus $\mathfrak{O}_K$. Es ist $\mathrm{N}(\xi) = x^2 - dy^2$. Aus $p \mid \mathrm{N}(\xi)$ folgt daher

$$x^2 \equiv dy^2 \bmod p.$$

Wäre $y \not\equiv 0 \bmod p$, würde daraus folgen, dass d ein Quadrat modulo p ist. Dies ist aber nach Voraussetzung ausgeschlossen. Daher gilt $y \equiv 0 \bmod p$, und daraus folgt auch $x \equiv 0 \bmod p$, d.h. $p \mid x$ und $p \mid y$, also $p \mid \xi$, q.e.d.

(ii) $d \equiv 1 \bmod 4$. Dann ist

$$\mathfrak{O}_K = \mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] = \{x + y\tfrac{1+\sqrt{d}}{2} : x, y \in \mathbb{Z}\}.$$

Sei $\xi = x + y\frac{1+\sqrt{d}}{2}$ ein beliebiges Element. Dann gilt

$$\mathrm{N}(\xi) = \mathrm{N}(x + \tfrac{y}{2} + \tfrac{y}{2}\sqrt{d}) = (x + \tfrac{y}{2})^2 - d(\tfrac{y}{2})^2 = \frac{(2x+y)^2 - dy^2}{4}.$$

Aus $p \mid \mathrm{N}(\xi)$ folgt daher

$$(2x + y)^2 \equiv dy^2 \bmod p.$$

Wäre $y \not\equiv 0 \bmod p$, würde daraus folgen, dass d ein Quadrat modulo p ist. Dies ist aber nach Voraussetzung ausgeschlossen. Daher gilt $y \equiv 0 \bmod p$, und daraus folgt $2x + y \equiv 0 \bmod p$, und weiter (da 2 invertierbar modulo p), dass $x \equiv 0 \bmod p$, d.h. $p \mid x$ und $p \mid y$, also $p \mid \xi$, q.e.d.

b) Wie im Fall a)(ii) gilt $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Für $\xi = x + y\frac{1+\sqrt{d}}{2}$ folgt aus $2 \mid \mathrm{N}(\xi)$, dass $8 \mid 4\mathrm{N}(\xi)$, d.h.

$$(2x + y)^2 \equiv dy^2 \bmod 8.$$

Wäre y ungerade, also $y^2 \equiv 1 \bmod 8$, würde daraus folgen, dass d ein Quadrat mod 8 ist. Dies ist aber wegen $d \equiv 5 \bmod 8$ nicht der Fall. Also ist y gerade, $y = 2y_1$ mit $y_1 \in \mathbb{Z}$. Setzt man dies in die obige Kongruenz ein und kürzt durch 4, erhält man

$$(x + y_1)^2 \equiv y_1^2 \bmod 2 \quad \Rightarrow \quad x + y_1 \equiv y_1 \bmod 2 \quad \Rightarrow \quad x \equiv 0 \bmod 2.$$

Also ist auch x gerade und daher $2 \mid \xi$, q.e.d.

Der nächste Satz gibt für einen quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ Auskunft über die Primideale des Ganzheitsrings $\mathfrak{O}_K$ sowie über die Struktur der Abbildung $\mathrm{Specm}(\mathfrak{O}_K) \to \mathrm{Specm}(\mathbb{Z})$.

3.10. Satz. *Sei $K := \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper ($d \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei) mit Diskriminante*

$$D = \begin{cases} 4d, & \text{falls } d \equiv 2,3 \bmod 4, \\ d, & \text{falls } d \equiv 1 \bmod 4 \end{cases}$$

und $\mathfrak{O}_K$ sein Ganzheitsring. Für eine Primzahl $p \in \mathbb{Z}$ zeigt das von p in $\mathfrak{O}_K$ erzeugte Hauptideal $(p) = p\,\mathfrak{O}_K$ folgendes Zerlegungs-Verhalten:

1. Fall: *Sei p eine ungerade Primzahl.*

(i) *Falls $p \mid D$, gibt es genau ein Primideal $\mathfrak{P} \subset \mathfrak{O}_K$ mit $p \in \mathfrak{P}$, nämlich $\mathfrak{P} = (p, \sqrt{d})$. Es gilt*

$$(p) = \mathfrak{P}^2 \quad \text{und} \quad \mathfrak{O}_K/\mathfrak{P} \cong \mathbb{F}_p.$$

(ii) *Falls $\left(\frac{D}{p}\right) = 1$, gibt es genau zwei Primideale $\mathfrak{P}_1, \mathfrak{P}_2 \subset \mathfrak{O}_K$ mit $p \in \mathfrak{P}_i$, nämlich $\mathfrak{P}_{1/2} = (p, x \pm \sqrt{d})$, wobei $x \in \mathbb{Z}$ eine Lösung der Kongruenz $x^2 \equiv d \bmod p$ ist. Es gilt*

$$(p) = \mathfrak{P}_1\mathfrak{P}_2 \quad \text{und} \quad \mathfrak{O}_K/\mathfrak{P}_i \cong \mathbb{F}_p.$$

(iii) *Falls $\left(\frac{D}{p}\right) = -1$, ist (p) selbst Primideal, d.h. p ein Primelement in $\mathfrak{O}_K$ und es gilt*

$$\mathfrak{O}_K/(p) \cong \mathbb{F}_{p^2}.$$

2. Fall: *Sei $p = 2$.*

(i) *Falls $2 \mid D$, also $D = 4d$ mit $d \equiv 2,3 \bmod 4$, gibt es genau ein Primideal $\mathfrak{P} \subset \mathfrak{O}_K$ mit $2 \in \mathfrak{P}$, nämlich $\mathfrak{P} = (2, d + \sqrt{d})$. Es gilt*

$$(2) = \mathfrak{P}^2 \quad \text{und} \quad \mathfrak{O}_K/\mathfrak{P} \cong \mathbb{F}_2.$$

Falls $2 \nmid D$, ist $D = d \equiv 1 \bmod 4$, also tritt einer der beiden folgenden Fälle ein.

(ii) *Falls $d \equiv 1 \bmod 8$, gibt es genau zwei Primideale $\mathfrak{P}_1, \mathfrak{P}_2 \subset \mathfrak{O}_K$ mit $2 \in \mathfrak{P}_i$, nämlich $\mathfrak{P}_{1/2} = (2, \frac{1}{2}(1 \pm \sqrt{d}))$. Es gilt*

$$(2) = \mathfrak{P}_1\mathfrak{P}_2 \quad \text{und} \quad \mathfrak{O}_K/\mathfrak{P}_i \cong \mathbb{F}_2.$$

(iii) *Falls* $d \equiv 5 \bmod 8$, *ist* (2) *selbst Primideal, also* 2 *ein Primelement in* $\mathfrak{O}_K$ *und es gilt*

$$\mathfrak{O}_K/(2) \cong \mathbb{F}_4.$$

Zum *Beweis* von Satz 3.10 verwenden wir zwei Hilfsaussagen:

(A) Für jede Primzahl $p \in \mathbb{Z}$ besteht der Restklassenring $\mathfrak{O}_K/(p)$ aus p^2 Elementen. Ist $\mathfrak{q} \subset \mathfrak{O}_K$ irgend ein Ideal mit $(p) \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{O}_K$, so ist $\mathfrak{q}$ ein Primideal mit $\mathfrak{O}_K/\mathfrak{q} \cong \mathbb{F}_p$.

Beweis von (A). Als additive Gruppe ist $\mathfrak{O}_K \cong \mathbb{Z} \times \mathbb{Z}$, also ist $\mathfrak{O}_K/(p) \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ eine Gruppe mit p^2 Elementen. Man hat eine natürliche surjektive Abbildung $\phi : \mathfrak{O}_K/(p) \to \mathfrak{O}_K/\mathfrak{q}$. Der Kern von ϕ hat als nicht-triviale Untergruppe von $\mathfrak{O}_K/(p)$ dann p Elemente. Daraus folgt, dass $\mathfrak{O}_K/\mathfrak{q}$ ebenfalls p Elemente hat. Daher ist $\mathfrak{q}$ ein maximales Ideal in $\mathfrak{O}_K$, also prim, und $\mathfrak{O}_K/\mathfrak{q} \cong \mathbb{F}_p$.

(B) Sind $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ Ideale eines Rings R und $\mathfrak{p} \subset R$ ein Primideal mit $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{p}$, so folgt $\mathfrak{a}_i \subset \mathfrak{p}$ für wenigstens ein $i \in \{1, 2\}$.

Beweis von (B). Angenommen $\mathfrak{a}_1 \not\subset \mathfrak{p}$. Dann gibt es ein Element $a_1 \in \mathfrak{a}_1 \setminus \mathfrak{p}$. Für ein beliebiges $x \in \mathfrak{a}_2$ ist dann $a_1 x \in \mathfrak{a}_1\mathfrak{a}_2$, also $a_1 x \in \mathfrak{p}$. Da $a_1 \notin \mathfrak{p}$, folgt $x \in \mathfrak{p}$, also insgesamt $\mathfrak{a}_2 \subset \mathfrak{p}$, q.e.d.

Beweis von Satz 3.10

Fall 1(i). Für das Ideal $\mathfrak{P} := (p, \sqrt{d})$ (von dem wir noch nicht annehmen, dass es prim ist) gilt $(p) \subsetneqq \mathfrak{P}$, da offensichtlich $\sqrt{d} \notin (p)$. Es ist

$$\mathfrak{P}^2 = (p, \sqrt{d})(p, \sqrt{d}) = (p^2, p\sqrt{d}, d) = p \cdot (p, \sqrt{d}, d/p).$$

(Man beachte, dass nach Voraussetzung $d/p \in \mathbb{Z}$). Nun sind p und d/p in $\mathbb{Z}$ teilerfremd (da $p^2 \nmid d$), woraus folgt $(p, \sqrt{d}, d/p) = (1)$, also $\mathfrak{P}^2 = (p)$. Daraus folgt auch $\mathfrak{P} \neq \mathfrak{O}_K$, also ist $\mathfrak{P}$ nach (A) ein Primideal mit $\mathfrak{O}_K/\mathfrak{P} \cong \mathbb{F}_p$. Dass $\mathfrak{P}$ das einzige Primideal von $\mathfrak{O}_K$ mit $p \in \mathfrak{P}$ ist, sieht man so: Wäre $\mathfrak{P}'$ ein weiteres Primideal mit dieser Eigenschaft, hätte man $\mathfrak{P}^2 = (p) \subset \mathfrak{P}'$, woraus mit (B) folgt, dass $\mathfrak{P} \subset \mathfrak{P}'$, wobei sogar Gleichheit gelten muss, da $\mathfrak{P}$ ein maximales Ideal ist.

Fall 1(ii). Für die beiden Ideale $\mathfrak{P}_{1/2} := (p, x \pm \sqrt{d})$ gilt $(p) \subsetneqq \mathfrak{P}_i$, da offensichtlich $x \pm \sqrt{d} \notin (p)$. Es ist

$$\begin{aligned}\mathfrak{P}_1\mathfrak{P}_2 &= (p, x + \sqrt{d})(p, x - \sqrt{d}) = (p^2, p(x-\sqrt{d}), p(x+\sqrt{d}), x^2 - d) \\ &= p \cdot (p, x-\sqrt{d}, x+\sqrt{d}, (x^2 - d)/p).\end{aligned}$$

(Man beachte, dass nach Definition von x gilt $p \mid x^2 - d$).

Behauptung. $\mathfrak{a} := (p, x-\sqrt{d}, x+\sqrt{d}, (x^2-d)/p) = (1)$.

Dies folgt daraus, dass $2x \in \mathfrak{a}$ und die Zahlen p und $2x$ in $\mathbb{Z}$ teilerfremd sind.
Aus $\mathfrak{a} = (1)$ folgt jetzt $\mathfrak{P}_1\mathfrak{P}_2 = (p)$. Weiter folgt $\mathfrak{P}_i \neq \mathfrak{O}_K$ sowie $\mathfrak{P}_1 \neq \mathfrak{P}_2$, denn andernfalls ergäbe sich $2x \in \mathfrak{P}_1$, also wäre wegen $(p, 2x) = (1)$ doch $\mathfrak{P}_1 = \mathfrak{O}_K$.
Die Aussage (A) impliziert nun $\mathfrak{O}_K/\mathfrak{P}_i \cong \mathbb{F}_p$ und aus (B) folgt, dass $\mathfrak{P}_{1/2}$ die einzigen Primideale von $\mathfrak{O}_K$ mit $p \in \mathfrak{P}_i$ sind.

Fall 1(iii). Es ist zu zeigen: Teilt p ein Produkt $\xi\eta$ zweier Elemente $\xi, \eta \in \mathfrak{O}_K$, so teilt p mindestens einen Faktor. Aus $p \mid \xi\eta$ folgt aber $\mathrm{N}(p) \mid \mathrm{N}(\xi)\mathrm{N}(\eta)$ im Ring $\mathbb{Z}$. Da $\mathrm{N}(p) = p^2$, muss $\mathrm{N}(\xi)$ oder $\mathrm{N}(\eta)$ durch p teilbar sein, etwa $p \mid \mathrm{N}(\xi)$. Nach Hilfssatz 3.9 folgt daraus $p \mid \xi$. Die Isomorphie $\mathfrak{O}_K/(p) \cong \mathbb{F}_{p^2}$ folgt aus (A).

Fall 2(i). Wir unterscheiden die Fälle $d \equiv 2 \bmod 4$ und $d \equiv 3 \bmod 4$.

Falls $d \equiv 2 \bmod 4$, gilt $\mathfrak{P} = (2, d + \sqrt{d}) = (2, \sqrt{d})$.
Falls $d \equiv 3 \bmod 4$, gilt $\mathfrak{P} = (2, d + \sqrt{d}) = (2, 1 + \sqrt{d}) = (2, -1 + \sqrt{d})$.
Im folgenden beschränken wir uns auf den (etwas komplizierteren Fall) $d \equiv 3 \bmod 4$. Es gilt $(2) \subsetneqq \mathfrak{P}$, da $1 + \sqrt{2} \notin (2)$. Es gilt

$$\begin{aligned}\mathfrak{P}^2 = (2, 1 + \sqrt{d})(2, -1 + \sqrt{d}) &= (4, 2 + 2\sqrt{d}, -1 + d) \\ &= 2 \cdot (2, 1 + \sqrt{d}, (d-1)/2).\end{aligned}$$

Wegen $d \equiv 3 \bmod 4$ ist $(d-1)/2 =: t \in \mathbb{Z}$ eine ungerade Zahl, woraus folgt

$$(2, 1 + \sqrt{d}, (d-1)/2) = (1),$$

also $\mathfrak{P}^2 = (2)$. Daraus folgt $\mathfrak{P} \neq \mathfrak{O}_K$, also mit (A), dass $\mathfrak{O}_K/\mathfrak{P} \cong \mathbb{F}_2$. Aus (B) folgt, dass $\mathfrak{P}$ das einzige Primideal von $\mathfrak{O}_K$ mit $2 \in \mathfrak{P}$ ist.

Die Fälle 2(ii) und 2(iii) werden ganz analog den Fällen 1(ii) und 1(iii) bewiesen. Die Ausführung sei dem Leser überlassen.

Bemerkung. Es gibt also für eine Primzahl $p \in \mathbb{Z}$ (gerade oder ungerade) drei verschiedene Verhaltensmuster der Zerlegung in einem quadratischen Zahlkörper der Diskriminante D:

(i) $(p) = \mathfrak{P}^2$ ist das Quadrat eines Primideals in $\mathfrak{O}_K$. Man nennt dann p *verzweigt*. Dieser Fall tritt genau dann ein, wenn $p \mid D$ (unabhängig davon, ob p gerade oder ungerade ist).

(ii) $(p) = \mathfrak{P}_1\mathfrak{P}_2$ ist das Produkt von zwei verschiedenen Primidealen von $\mathfrak{O}_K$. Man sagt denn, p *spaltet* in $\mathfrak{O}_K$. Dieser Fall tritt genau dann ein, wenn D ein Quadrat modulo p ist (falls p ungerade) bzw. $D \equiv 1 \bmod 8$, falls $p = 2$. Die letzte Bedingung bedeutet, dass D ein Quadrat modulo 8 ist

(iii) (p) ist ein Primideal in $\mathfrak{O}_K$, d.h. p bleibt auch in $\mathfrak{O}_K$ prim. Man nennt dann die Primzahl p *träge*. Dieser Fall tritt genau dann ein, wenn D kein Quadrat modulo p ist (falls p ungerade) bzw. $D \equiv 5 \bmod 8$, falls $p = 2$. Die letzte Bedingung bedeutet, dass D kein Quadrat modulo 8 ist.

Es gibt also nur endlich viele verzweigte Primzahlen. Die übrigen Primzahlen p spalten oder sind träge in $\mathfrak{O}_K$. Der nächste Satz zeigt, dass dies nur von der Restklasse von p modulo D abhängt und dass es asymptotisch gleich viele Primzahlen jeder Sorte gibt.

3.11. Satz. *Sei K ein quadratischer Zahlkörper mit Diskriminante D. Dann gibt es einen surjektiven Gruppen-Homomorphismus*

$$\chi_D : (\mathbb{Z}/D)^* \to \{\pm 1\},$$

so dass gilt: Eine ungerade Primzahl p mit $p \nmid D$ spaltet bzw. ist träge in $\mathfrak{O}_K$, je nachdem $\chi_D(p) = 1$ oder $\chi_D(p) = -1$.

Bemerkung. Der Kern von χ_D ist dann eine Untergruppe vom Index 2 in $(\mathbb{Z}/D)^*$. Da die Anzahl der Elemente von $(\mathbb{Z}/D)^*$ gleich $\varphi(D)$ (Eulersche Phi-Funktion) ist, gibt es je $s := \frac{\varphi(D)}{2}$ zu D teilerfremde Zahlen $a_1, \ldots, a_s$ und $b_1, \ldots, b_s$, (die paarweise modulo D verschieden sind), so dass alle Primzahlen mit $p \equiv a_i \bmod D$ spalten und alle Primzahlen mit $p \equiv b_j \bmod D$ träge sind. Nach dem Satz von Dirichlet über Primzahlen in arithmetischen Progressionen gibt es zu jeder zu D teilerfremden Zahl a unendlich viele Primzahlen mit $p \equiv a \bmod D$ und zwar mit einer von a unabhängigen asymptotisch sog. *Dirichlet-Dichte* $\frac{1}{\varphi(D)}$, die wir aber hier nicht näher definieren.

Beweis. Nach Satz 3.10 ist nur zu zeigen: Es gibt einen Gruppen-Homomorphismus $\chi_D : (\mathbb{Z}/D)^* \to \{\pm 1\}$, so dass

$$\chi_D(p) = \Big(\frac{D}{p}\Big) \quad \text{für alle ungeraden Primzahlen } p \text{ mit } p \nmid D.$$

Zur Konstruktion von χ_D benutzen wir das quadratische Reziprozitätsgesetz. Sei

$$D = (-1)^\alpha 2^\beta q_1 q_2 \cdots q_m, \qquad \alpha \in \{0,1\}, \quad \beta \in \{0,2,3\},$$

die Primfaktorzerlegung der Diskriminante (q_j ungerade Primzahlen). Dann ist

$$\Big(\frac{D}{p}\Big) = \Big(\frac{-1}{p}\Big)^\alpha \Big(\frac{2}{p}\Big)^\beta \prod_{j=1}^m \Big(\frac{q_j}{p}\Big).$$

Wir definieren zwei Gruppen-Homomorphismen (Charaktere)

$$\chi_4 : (\mathbb{Z}/4)^* \to \{\pm 1\}, \qquad \chi_8 : (\mathbb{Z}/8)^* \to \{\pm 1\}$$

durch $\chi_4(a) := (-1)^{(a-1)/2}$ und $\chi_8(a) := (-1)^{(a^2-1)/8}$. Man kann χ_4 und χ_8 auch als Funktionen, die auf allen ungeraden ganzen Zahlen definiert sind, auffassen. Damit gilt

$$\Big(\frac{-1}{p}\Big) = \chi_4(p), \qquad \Big(\frac{2}{p}\Big) = \chi_8(p)$$

und nach dem quadratischen Reziprozitätsgesetz

$$\begin{aligned}\Big(\frac{q_j}{p}\Big) &= \Big(\frac{p}{q_j}\Big), && \text{falls } q_j \equiv 1 \bmod 4,\\ \Big(\frac{q_j}{p}\Big) &= \chi_4(p)\Big(\frac{p}{q_j}\Big), && \text{falls } q_j \equiv 3 \bmod 4.\end{aligned}$$

Ist γ die Anzahl der Primfaktoren $q_j \equiv 3 \bmod 4$ von D, so gilt deshalb

$$\Big(\frac{D}{p}\Big) = \chi_4(p)^{\alpha+\gamma}\chi_8(p)^{\beta}\prod_{j=1}^{m}\Big(\frac{p}{q_j}\Big).$$

Wir unterscheiden jetzt drei Fälle:

a) $D \equiv 1 \bmod 4$. Dann ist $\beta = 0$ und $\alpha + \gamma$ gerade. Dann defineren wir

$$\chi_D(a) := \prod_{j=1}^{m}\Big(\frac{a}{q_j}\Big), \qquad |D| = q_1 q_2 \cdots q_m$$

Offensichtlich hängt $\chi_D(a)$ nur von der Restklasse $a \bmod D$ ab und es gilt $\chi_D(p) = (\frac{D}{p})$ für alle ungeraden Primzahlen, die kein Teiler von D sind.

b) $D = 4d$ mit $d \equiv 3 \bmod 4$. Dann ist $\beta = 2$ und $\alpha + \gamma$ ungerade. Dann defineren wir

$$\chi_D(a) := \chi_4(a)\prod_{j=1}^{m}\Big(\frac{a}{q_j}\Big), \qquad |d| = q_1 q_2 \cdots q_m$$

Offensichtlich hängt $\chi_D(a)$ nur von der Restklasse $a \bmod 4d$ ab und es gilt $\chi_D(p) = (\frac{D}{p})$ für alle ungeraden Primzahlen, die kein Teiler von D sind.

Speziell für Diskriminante $D = -4$ (d.h. für den Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen) ergibt sich $\chi_{-4} = \chi_4$.

c) $D = 4d$ mit $d \equiv 2 \bmod 4$. Dann gilt $8 \mid D$, also $\beta = 3$. Die Parität von $\alpha + \gamma$ hängt von der Restklasse $(d/2) \bmod 4$, d.h. von der Restklasse $d \bmod 8$ ab. Wir setzen

$$\delta := \begin{cases} 0, & \text{falls } d \equiv 2 \bmod 8,\\ 1, & \text{falls } d \equiv 6 \bmod 8.\end{cases}$$

Dann gilt $\alpha + \gamma \equiv \delta \bmod 2$. Wir können jetzt defineren

$$\chi_D(a) := \chi_4(a)^\delta \chi_8(a) \prod_{j=1}^{m} \Big(\frac{a}{q_j}\Big), \qquad |d| = 2q_1 q_2 \cdots q_m$$

$\chi_D(a)$ hängt nur von der Restklasse $a \bmod D$ ab und es gilt $\chi_D(p) = (\frac{D}{p})$ für alle ungeraden Primzahlen, die kein Teiler von D sind.

Im Fall der Diskriminante $D = 8$, d.h. für den Zahlring $\mathbb{Z}[\sqrt{2}]$ ist $\delta = 0$ und $m = 0$, also stimmt χ_D mit dem schon früher definierten χ_8 überein. Für $D = -8$ (Zahlring $\mathbb{Z}[\sqrt{-2}]$) ergibt sich $\chi_{-8} = \chi_4\chi_8$.

3.12. Beispiel. Wir wollen den Fall des Zahlkörpers $\mathbb{Q}(\sqrt{-5})$ und seines Ganzheitsrings $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$ näher ansehen. Seine Diskriminante ist $D = -20$ und nach Satz 3.11 gilt

$$\chi_{-20}(a) = \chi_4(a)\Big(\frac{a}{5}\Big).$$

Die zu 20 teilerfremden Restklassen sind $1, 3, 7, 9, 11, 13, 17, 19$ und man berechnet

a	1	3	7	9	11	13	17	19
$\chi_{-20}(a)$	1	1	1	1	-1	-1	-1	-1

Damit erhält man eine Liste von spaltenden Primzahlen in $\mathbb{Z}[\sqrt{-5}]$

$$\begin{aligned}
p \equiv 1 \bmod 20 &: \quad 41, 61, 101, 181, 241, 281, 401, 421, 461, \ldots \\
p \equiv 3 \bmod 20 &: \quad 3, 23, 43, 83, 103, 163, 223, 263, 283, 383, 443, 463, \ldots \\
p \equiv 7 \bmod 20 &: \quad 7, 47, 67, 107, 127, 167, 227, 307, 347, 367, 467, 487, \ldots \\
p \equiv 9 \bmod 20 &: \quad 29, 89, 109, 149, 229, 269, 349, 389, 409, 449, \ldots
\end{aligned}$$

und von trägen Primzahlen in $\mathbb{Z}[\sqrt{-5}]$

$$\begin{aligned}
p \equiv 11 \bmod 20 &: \quad 11, 31, 71, 131, 151, 191, 211, 251, 271, 311, 331, 431, 491, \ldots \\
p \equiv 13 \bmod 20 &: \quad 13, 53, 73, 113, 173, 193, 233, 293, 313, 353, 373, 433, \ldots \\
p \equiv 17 \bmod 20 &: \quad 17, 37, 97, 137, 157, 197, 257, 277, 317, 337, 397, 457, \ldots \\
p \equiv 19 \bmod 20 &: \quad 19, 59, 79, 139, 179, 199, 239, 359, 379, 419, 439, 479, 499, \ldots
\end{aligned}$$