Summen von Quadraten Prüfungsmusterlösung und Punkteschema

Dem Punkteschema unterliegen drei Grundprinzipien.

- Eine vollständige Lösung gibt volle Punktzahl.
- Für eine im Wesentlichen vollständige Lösung können vereinzelt Punkte abgezogen werden für kleine Lücken im Beweis.
- Für unvollständige Lösungen werden Punkte vergeben für sinnvolle Teilresultate.

Wir bemerken, dass es keine im Wesentlichen vollständige Lösung mit grossen Lücken im Beweis gibt. In diesem Fall wird die Antwort als unvollständige Lösung bewertet und Teilpunkte für Teilresultate vergeben.

Ferner stellen wir klar, dass die Punkte, welche vergeben werden, nicht notwendigerweise additiv sind. Manchmal sind sie superadditiv und manchmal subadditiv. Das Punkteschema für die jeweilige Aufgabe drückt dies genauers aus.

Enthält die Antwort einer Aufgabe verschiede Lösungsansätze, welche verschiedener Punkteschemen unterliegen, so wird die maximale Punktzahl über alle Lösungsansätze vergeben.

Aufgabe 1: Seien $a, b \in \mathbb{Z}$ ungerade ganze Zahlen. Sei ferner $c \in \mathbb{Z}$ ein grösster gemeinsamer Teiler von a und b. Ist c notwendigerweise auch ein grösster gemeinsamer Teiler von $2a$ und $27a + 8b$?

[4 Punkte]

Lösung 1:

Sei c ein grösster gemeinsamer Teiler von a, b. Aufgrund der Linearität der Teilerbarkeit folgt, dass $c \mid 2a$ und $c \mid 27a + 8b$ also ist c ein gemeinsamer Teiler von $2a$ und $27a + 8b$.

Umgekehrt sei d ein gemeinsamer Teiler von $2a$ und $27a + 8b$. Nun ist 2 kein Teiler von $27a + 8b$, da $27a + 8b \equiv a \not\equiv 0 \mod (2)$. Es folgt $2 \nmid d$ und da 2 prim ist, sind sogar 2 und d teilerfremd. Aus dem und $d \mid 2a$ folgern wir, dass $d \mid a$. Ferner gilt dann $d \mid 27a + 8b - 27a = 8b$ und dann $d \mid b$, da d und $8 = 2^3$ teilerfremd sind. Das heisst d ist auch ein gemeinsamer Teiler von a und b. Insbesondere gilt $d \mid c$, da c ein grösster gemeinsamer Teiler ist von a und b.

Daraus folgern wir, dass c auch ein grösster gemeinsamer Teiler ist von $2a$ und $27a + 8b$.

Lösung 2:

Wie vorhin zeigt man, dass c ein gemeinsamer Teiler ist von $2a$ und $27a+8b$. Sei d nun ein gemeinsamer Teiler von $2a$ und $27a + 8b$. Dann findet man $d \mid 2(27a + 8b) - 27(2a) = 16b$ und $d \mid 2a \mid 16a$. Nach dem Satz von Bézout können wir $c = xa + yb$ schreiben für ganze Zahlen $x, y \in \mathbb{Z}$. Es folgt, dass $d \mid x(16a) + y(16b) = 16c$. Es gilt also noch zu zeigen, dass d und $16 = 2^4$, beziehungsweise d und 2, teilerfremd sind, denn dann würde $d \mid c$ folgen. Für dies kann man wie vorhin argumentieren.

Punkteschema :

Das Punkteschema ist in zwei Teile aufgeteilt:

(A1) $c \mid 2a$ und $c \mid 27a + 8b$, **[1 Punkt]**

(A2) Jeder gemeinsame Teiler von $2a$ und $27a + 8b$ teilt c. **[3 Punkte]**

Im Punkt **(A2)** lassen sich maximal zwei Teilpunkte erzielen, indem man folgendes zeigt:

(a) Jeder gemeinsame Teiler von $2a$ und $27a+8b$ ist ungerade, bzw. $27a+8b$ ist ungerade, [**1 Punkt**]

(b) Jeder gemeinsame Teiler von $2a$ und $27a+8b$ teilt $2^\alpha c$ für ein $\alpha \in \mathbb{N}_0$, [**1 Punkt**]

(c) Jeder gemeinsame Teiler von $2a$ und $27a+8b$ teilt a. [**1 Punkt**]

Aufgabe 2: Seien $\alpha, \beta \in \mathbb{Z}[i]$ zwei Gauss'sche Zahlen.

(a) Nehme an es gibt eine natürliche Zahl $n \in \mathbb{N}$ mit $n > 1$, sodass $n \mid N(\alpha)$ und $n \mid N(\beta)$. Gibt es dann zwingend eine Gauss'sche Zahl γ, welche keine Einheit ist und ein gemeinsamer Teiler von α und β ist?

[1 Punkt]

Lösung:
Die zwei Gauss'schen Zahlen $1+2i$ und $1-2i$ haben beide Norm gleich 5. Jedoch sind sie zwei prime/irreduzible Gauss'sche Zahlen, welche sich nicht durch eine Einheit unterscheiden. Falls man die Klassifikation der primen Gauss'schen Zahlen nicht verwenden will, kann man auch wiefolgt argumentieren. $1+2i$ und $1-2i$ unterscheiden sich nicht durch Multiplikation mit einer Einheit, denn $(1+2i)\cdot\{\pm 1, \pm i\} = \{\pm(1+2i), \pm(-2+i)\} \not\ni (1-2i)$. Falls nun γ ein grösster gemeinsamer Teiler von $1+2i$ und $1-2i$ ist, so gilt $N(\gamma) \mid N(1+2i) = 5$. Es folgt, dass $N(\gamma) = 1, 5$. Im ersten Fall sind $1+2i$ und $1-2i$ teilerfremd und zweiten Fall würden $1+2i$ und $1-2i$ sich durch Multiplikation mit einer Einheit unterscheiden. Letzteres ist aber ein Widerspruch.

Punkteschema :
Für eine vollständige Lösung benötigt es:

(B1) Ein korrekt begründetes Gegenbeispiel. [**1 Punkt**]

(b) Bestimmen Sie alle natürlichen Primzahlen $p \in \mathbb{N}$, sodass folgendes gilt: Aus $p \mid N(\alpha)$ und $p \mid N(\beta)$ folgt, dass α und β nicht teilerfremd sind.

[3 Punkte]

Lösung 1:
Wir benützen die Klassifikation der primen/irreduziblen Gauss'schen Zahlen. Wie im Teil (a) finden wir ein Gegenbeispiel für Primzahlen $p \equiv 1 \mod (4)$, denn in diesem Falle gibt es zwei prime Gauss'sche Zahlen α, β mit Norm gleich p, welche sich nicht Multiplikation mit einer Einheit unterscheiden. Das heisst sie sind also teilerfremd.

Wir behaupten nun, dass die Aussage in (b) für alle anderen Primzahlen gelten. Wir dürfen α, β in ihre (Gauss'sche) Primfaktoren zerlegen, e.g. $\alpha = \alpha_1 \cdots \alpha_r$. Wir bemerken, dass $r \geq 1$ gilt, da α keine Einheit sein kann, denn sonst gälte $p \mid N(\alpha) = 1$ - ein Widerspruch. Da nun p eine Primzahl ist und $N(\alpha_i)$ ganz sind, folgt aus $p \mid N(\alpha) = N(\alpha_1)\cdots N(\alpha_r)$, dass α einen primen Faktor α_i besitzt, dessen Norm durch p teilerbar ist. Analoges gilt für β. Falls nun γ ein gemeinsamer Teiler ist von α_i und β_j, welcher keine Einheit ist, dann ist γ auch ein gemeinsamer Teiler von α und β, da $\alpha_i \mid \alpha$ und $\beta_j \mid \beta$. Das heisst, dass ohne Beeinschränkung der Allgemeinheit dürfen wir annehmen, dass α und β prime/irreduzible Gauss'sche Zahlen sind. Für $p \not\equiv 1 \mod (4)$ gibt es aber bis auf Multiplikation mit einer Einheit aber genau eine prime Gauss'sche Zahl, dessen Norm durch p teilbar ist. Es folgt, dass α und β bis auf Multiplikation mit einer Einheit, die selbe prime Gauss'sche Zahl sind und folglich gilt $\alpha \mid \alpha$ und $\alpha \mid \beta$ und α ist keine Einheit, da α prim ist.

Lösung 2:
Alternativ kann man auch wiefolgt argumentieren. Falls $p \equiv 3 \mod (4)$, so ist p eine prime Gauss'sche Zahl. Wir möchten nun zeigen, dass aus $p \mid N(\alpha)$ sogar $p \mid \alpha$ folgt. Da $N(\alpha) = \alpha\overline{\alpha}$ gilt und p prim ist, gilt $p \mid \alpha$ oder $p \mid \overline{\alpha}$. Im ersten Fall sind wir fertig und im zweiten Fall folgt aus $p \mid \overline{\alpha}$, dass $p = \overline{p} \mid \overline{\overline{\alpha}} = \alpha$. Dasselbe gilt natürlich auch für β und somit ist p ein gemeinsamer Teiler

von α und β, welcher keine Einheit ist. Falls $p = 2$ ist, können wir ähnlich argumentieren. Hier haben wir, dass $1 + i \mid 2$ und $1 + i$ ist eine prime Gauss'sche Zahl. Es folgt wieder, dass $1 + i \mid \alpha$ oder $1 + i \mid \overline{\alpha}$. Im zweiten Fall gilt

$$1 + i \mid (-i)(1 + i) = 1 - i = \overline{1 + i} \mid \alpha.$$

Es ist also $1 + i$ keine Einheit, welche α und β teilt.

Lösung 3:

Zuletzt kann man auch wiefolgt argumentieren. Sei $\alpha = a + bi$ und $p \equiv 3 \mod (4)$ eine Primzahl. Dann gilt $p \mid N(\alpha) = a^2 + b^2$. In der Vorlesung haben wir gesehen, dass dann $p \mid a$ und $p \mid b$ gelten muss. Es ist dann $\alpha = p \cdot (\frac{a}{p} + \frac{b}{p}i)$ durch p teilbar. Dasselbe gilt für β. Es sind also α und β nicht teilerfremd, da p ein gemeinsamer Teiler ist. Falls $p = 2$, dann sind entweder a, b beide gerade oder beide ungerade. Im ersten Fall ist α durch 2 teilbar und insbesondere durch $1 + i$ teilbar, da $2 = (1 + i)(1 - i)$. Im zweiten Fall ist

$$\alpha \equiv a + bi \equiv (a - 1) + (b - 1)i \equiv 2 \cdot (\tfrac{a-1}{2} + \tfrac{b-1}{2}i) \equiv 0 \mod (1 + i).$$

Punkteschema :

Für eine vollständige Lösung benötigt es:

(B2) Eine korrekte Begründung für jede Primzahl wieso die Aussage stimmt oder ein entsprechendes Gegenbeispiel. **[3 Punkte]**

Dabei kann maximal ein Punkt abgezoben werden für

- $p = 2$ vergessen, beziehungsweise falsch argumentiert,
- Ungenauigkeiten.

Es können maximal zwei Teilpunkte für Teilresultate erzielt werden. Es gibt simple und fortgeschrittene Teilresultate. Es kann höchstens ein Teilpunkt für simple Teilresultate erzielt werden. Simple Teilresultate sind:

(a) Beweis, dass die Aussage gilt für eine bestimmte Primzahl, **[1 Punkt]**

(b) Für einen primen Teiler δ von p gilt $\delta \mid \alpha$ oder $\delta \mid \overline{\alpha}$, **[1 Punkt]**

(c) Für $p \not\equiv 1 \mod (4)$ gibt es bis auf Multiplikation mit einer Einheit genau eine prime Gauss'sche Zahl, dessen Norm durch p teilbar ist. **[1 Punkt]**

Ein weiterer Punkt beziehungsweise beide Teilpunkte können durch folgende fortgeschrittene Teilresultate erzielt werden:

(d) Reduktion auf α, β prime Gauss'sche Zahlen, **[2 Punkte]**

(e) Für $p \equiv 3 \mod (3)$, teilt p sowohl der Realteil und den Imaginärteil von α. **[2 Punkte]**

Keine Punkte gibt es für folgendes:

- Ein Gegenbeispiel für ein/alle $p \equiv 1 \mod (4)$ sofern der Punkt **(B1)** schon vergeben ist,
- $p \mid \alpha\overline{\alpha}$.

Aufgabe 3: Zeigen Sie, dass es mindestens 24 verschiedene Hurwitz Quaternionen $\alpha \in \mathbb{Z}[i, j, k, \xi]$ gibt mit Norm gleich 2021. Hier ist $\xi = (1 + i + j + k)/2$.

[4 Punkte]

Lösung 1:

Nach dem vier Quadrate Satz von Lagrange gibt es ganze Zahlen $a, b, c, d \in \mathbb{Z}$ mit $a^2+b^2+c^2+d^2 = 2021$. Es gibt also sicher eine Hurwitz Quaternion α mit $N(\alpha) = 2021$, nämlich $\alpha = a + bi + cj + dk$. Die Hurwitz Quaternionen besitzen nun 24 verschiedene Einheiten ϵ. Es sind dann $\epsilon\alpha$ Hurwitz Quaternionen

mit $N(\epsilon\alpha) = N(\epsilon)N(\alpha) = 2021$. Für zwei verschiedene Einheiten ϵ und ϵ' sind dann auch $\epsilon\alpha$ und $\epsilon'\alpha$ verschieden, denn

$$N(\epsilon\alpha - \epsilon'\alpha) = N(\epsilon - \epsilon')N(\alpha) \neq 0 \Rightarrow \epsilon\alpha \neq \epsilon'\alpha.$$

Lösung 2:

Es gilt $2021 = 44^2+9^2+2^2$ durch Permutieren und variieren des Vorzeichens finden wir $4!\cdot 2^3 = 24\cdot 8 > 24$ Quadrupel $(a, b, c, d) \in \mathbb{Z}^4$ von ganzen Zahlen mit $a^2 + b^2 + c^2 + d^2 = 2021$. Jedes solches Quadrupel führt zu einer Hurwitz Quaternion $\alpha = a + bi + cj + dk$ mit $N(\alpha) = 2021$, jene Quaternionen sind dann auch paarweise verschieden voneinander.

Lösung 3:

Man kann auch die Lösungen 1 und 2 kombinieren indem man zum Beispiel bemerkt, dass $2021 = 45^2 - 2^2 = 43 \cdot 47$ und genügend Darstellungen für 43 beziehungsweise 47 findet. Hier sind die Darstellungen $43 = 5^2 + 4^2 + 1^2 + 1^2$ und $47 = 6^2 + 3^2 + 1^2 + 1^2$ hilfreich, denn man kann durch Vertauschen und Vorzeichenwechsel $\frac{4!}{2!} \cdot 2^4 > 24$ Quadrupel ganzer Zahlen generieren, dessen Summe von Quadraten 43 beziehungsweise 47 ergeben. Man folgert nun wie bei Lösung 1.

Lösung 4:

$2021 = 43 \cdot 47$ lässt sich nicht als eine Summe von zwei Quadraten schreiben, nach dem zwei Quadrate Satz (43 ist prim und $43 \equiv 3 \mod (4)$). Nach dem vier Quadrate Satz von Lagrange lässt sich aber 2021 als Summe von vier Quadraten schreiben. Seien also $a, b, c, d \in \mathbb{N}_0$ vier nicht negative ganze Zahlen mit $a^2 + b^2 + c^2 + d^2 = 0$. Durch vertauschen können wir weiter annehmen, dass $a \geq b \geq c \geq d \geq 0$. Es gilt nun $c > 0$, da ansonsten $c = d = 0$ und $2021 = a^2 + b^2$ - ein Widerspruch. Falls wir annehmen, dass keine der Zahlen a, b, c, d nur einmal in $\{a, b, c, d\}$ vorkommt, dann muss $a = b$ und $c = d$ gelten, aber dann wäre $2021 = 2(a^2 + c^2)$ gerade - ein Widerspruch. Sei nun $w \in \{a, b, c, d\}$ eine Zahl, die nur einmal vorkommt. Falls $d = 0$, dann ist $w = d = 0$ zu wählen (Wir haben gezeigt, dass 0 nicht zweimal vorkommen kann). Ferner seien x, y, z die übrigen Zahlen, welche nun sicher positiv sind, dann sind

$$(\pm x, \pm y, \pm z, w),\ (w, \pm x, \pm y, \pm z),\ (\pm z, w, \pm x, \pm y),\ (\pm y, \pm z, w, \pm x)$$

$8 \cdot 4 > 24$ verschiedene Quadrupel ganzer Zahlen, dessen Summe von Quadraten 2021 ergibt. Jedes solches Quadrupel führt dann zu einer Hurwitz Quaternion wie in der zweiten Lösung.

Lösung 5:

Nach dem vier Quadrate Satz von *Jacobi* gibt es

$$8 \sum_{\substack{n|2021 \\ 4\nmid n}} n \geq 8 \cdot 2021 > 24$$

Quadrupel $(a, b, c, d) \in \mathbb{Z}^4$ von ganzen Zahlen mit $a^2 + b^2 + c^2 + d^2 = 2021$. Jedes solches Quadrupel führt dann zu einer Hurwitz Quaternion wie in der zweiten Lösung.

Punkteschema :

Für eine vollständige Lösung benötigt es:

(C) Eine korrekte Begründung für die Existenz von 24 verschiedener Hurwitz Quaternionen mit Norm gleich 2021. [**4 Punkte**]

In den Lösungen 1-5 kann maximal ein Punkt abgezoben werden für

- fehlende Begründung beziehungsweise Bemerkung, dass eine Summe von vier Quadraten gleich 2021 zu einer Hurwitz Quaternion mit Norm gleich 2021 führt,
- fehlende Begründung beziehungsweise Bemerkung, dass alle Hurwitz Quaternionen verschieden sind,

- Ungenauigkeiten.

Die fünfte Lösung wird nur als eine fast vollständige Lösung gewertet, falls der vier Quadrate Satz von Jacobi vollständig und korrekt zitiert wurde. Andernfalls können nur Teilpunkte erzielt werden.

Es können maximal zwei Teilpunkte für Teilresultate erzielt werden, indem folgende Aussagen gezeigt werden:

(a) Es gibt mindestens eine Hurwitz Quaternion mit Norm 2021, beziehungsweise 2021 lässt sich als Summe von vier Quadraten darstellen, [**1 Punkt**]

(b) Es gibt 24 Einheiten in den Hurwitz Quaternionen, [**1 Punkt**]

(c) Es gibt genügend verschiedene Permutationen oder Vorzeichenwechsel um 24 verschiedene Hurwitz Quaternionen zu generieren, sofern eine Lösung einer bestimmten Art gefunden ist. [**1 Punkt**]

(d) Multiplikation einer Hurwitz Quaternion mit Norm 2021 mit den 24 Einheiten führt zu 24 Hurwitz Quaternionen mit Norm 2021, welche paarweise verschieden sind. [**1 Punkt**]

Aufgabe 4: Sei $Q(X,Y) = 9X^2 + 13XY + 5Y^2 \in \mathbb{Z}[X,Y]$ eine binäre quadratische Form.

(a) Bestimmen Sie alle reduzierten binären quadratischen Formen mit ganzen Koeffizienten und Diskriminante gleich -11.

[2 Punkte]

Lösung:
Wir suchen ganze Zahlen $a,b,c \in \mathbb{Z}$ mit $b^2 - 4ac = -11$ und $|b| \leq |a| \leq |c|$. In der Vorlesung haben wir gesehen, dass $|a|, |b| \leq \sqrt{11/3} < 2$ gelten muss. Wir sehen weiter, dass b ungerade sein muss, da $-11 = b^2 - 4ac \equiv b^2 \equiv b \mod (2)$. Dies lässt nur die Option $b = \pm 1$ übrig. Insbesondere gilt $b^2 = 1$. $a = 0$ führt zu keiner Lösung und $a = \pm 1$ führt zu $c = \pm 3$ (mit dem gleichen Vorzeichen). Die einzigen reduzierten binären quadratischen Formen mit Diskriminante -11 sind also von der Form $aX^2 + bXY + cY^2$ mit

$$(a,b,c) = (-1,1,-3), (-1,-1,-3), (1,1,3), \text{ und } (1,-1,3).$$

Punkteschema :
Für eine korrekte und begründete Lösung gibt es zwei Punkte. Für kleine Fehler, so zum Beispiel Unklarheit wie die Vorzeichen zu wählen sind oder Vergessen der negativ definiten Lösungen, kann maximal ein Punkt abgezogen werden.

(b) Bestimmen Sie eine reduzierte binäre quadratische Form $Q' \in \mathbb{Z}[X,Y]$, welche zu Q äquivalent ist.

[2 Punkte]

Lösung 1:
Q ist äquivalent zu

$$\rho(Q, \left(\begin{smallmatrix} 1 & -1 \\ & \end{smallmatrix}\right))(X,Y) = 5X^2 - 13XY + 9Y^2.$$

Letzteres ist ferner äquivalent zu

$$\rho(Q, \left(\begin{smallmatrix} 1 & -1 \\ & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & \end{smallmatrix}\right))(X,Y) = 5X^2 - 3XY + Y^2$$

Wir rechnen weiter

$$\rho(Q, \left(\begin{smallmatrix} 1 & -1 \\ & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ & \end{smallmatrix}\right))(X,Y) = X^2 + 3XY + 5Y^2$$

und

$$\rho(Q, \left(\begin{smallmatrix} 1 & -1 \\ & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ 1 & \end{smallmatrix}\right))(X,Y) = X^2 + XY + 3Y^2.$$

Letzteres ist reduziert. Wir bemerken, dass

$$\rho(Q, \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & \end{smallmatrix}\right)\left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -2 \\ & 1 \end{smallmatrix}\right))(X,Y) = X^2 - XY + 3Y^2$$

auch zu Q äquivalent ist und reduziert.

Lösung 2:

Alternativ können wir auch die Aufgabe (a) benutzen. Jede binäre quadratische Form besitzt eine dazu äquivalente reduzierte Form und Äquivalenz behält die Diskriminante und Definitheit invariant. Q besitzt die Diskriminante -11 und ist postiv definit, da die Diskriminante negativ ist und $9 > 0$. Die einzigen reduzierten positiv definiten binären quadratischen Formen der Diskriminante -11 sind $X^2 \pm XY + 3Y^2$ nach (a). Jene sind aber zueinander äquivalent, da $\rho(X^2 + XY + 3Y^2, \left(\begin{smallmatrix} 1 & -1 \\ & 1 \end{smallmatrix}\right)) = X^2 - XY + 3Y^2$. Folglich gibt es bis auf Äquivalenz nur eine binäre positive definite quadratische Form. Es folgt, dass Q zwingend zur reduzierten Form $X^2+XY+3Y^2$ äquivalent ist.

Punkteschema :

Für eine korrekte und begründete Lösung gibt es zwei Punkte. Für kleine Rechenfehler in einer ansonsten korrekten Lösung wird ein Punkt abgezogen. Maximal ein Teilpunkt kann vergeben werden für

(D2a) Eine der reduzierten Formen in (a) ist zu Q äquivalent. [**1 Punkt**]

(D2b) Anwenden des Algorithmus zur Bestimmung einer äquivalenten reduzierten Form. [**1 Punkt**]

(c) Bestimmen Sie für die Primzahlen $p = 57, 79, 227$ ob -11 kongruent zu einem ganzen Quadrat modulo p ist.

[2 Punkte]

Lösung:

-11 ist kongruent zu einem Quadrat modulo p (ungerade) genau dann wenn $\left(\frac{-11}{p}\right) = 0, 1$. Wir berechnen also das Legendre Symbol. Die gelisteten Primzahlen p sind verschieden/teilerfremd zu 11. Es gilt also nach quadratischer Reziprozität, dass

$$\left(\frac{-11}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{11-1}{2}}\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right).$$

Wir berechnen die Quadrate modulo 11 als die Kongruenzklassen von $0, 1, 4, 9, 16 \equiv 5, 25 \equiv 3 \mod (11)$ (für 6 und grösser gilt $6^2 \equiv (-5)^2 \equiv 5^2 \mod (11)$ ist also schon in der Liste enthalten). Wir finden $57, 79 \equiv 2 \mod (11)$, also kein Quadrat, und $227 \equiv 7 \mod (11)$, auch kein Quadrat. Das heisst für all jene Primzahlen p gilt

$$\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right) = -1,$$

also ist -11 kein Quadrat modulo p.

Alternativ muss man nach der Reduktion von p modulo 11 nur noch $\left(\frac{2}{11}\right)$ und $\left(\frac{7}{11}\right)$ bestimmen. Es gilt

$$\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1$$

und

$$\left(\frac{7}{11}\right) = \left(\frac{-4}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)^2 = (-1)^{\frac{11-1}{2}} = -1.$$

Punkteschema :

Für eine korrekte und begründete Lösung für alle Primzahlen gibt es zwei Punkte. Maximal Teilpunkt kann erzielt werden, für

(D3a) eine korrekte und begründete Lösung für eine der Primzahlen. [**1 Punkt**]

Keine Punkte werden vergeben für die Idee dies mit dem Legendre Symbol und/oder quadratische Reziprozität zu berechnen.

(d) Repräsentiert die Form Q die Zahlen 227 oder $57 \cdot 79$?

[2 Punkte]

Lösung:

Q besitzt die Diskriminante -11. In der Vorlesung haben wir gesehen, dass falls Q eine Zahl n repräsentiert, so muss die Diskriminante -11 ein Quadrat sein modulo $4n$ und somit sicherlich auch modulo n. Für $n = 227$ ist dies nicht der Fall nach (c). Falls -11 ein Quadrat modulo $57 \cdot 79$ wäre, so müsste sicherlich -11 ein Quadrat modulo 57 sein, aber auch dies ist nicht der Fall nach (c). Es folgt, dass Q die Zahlen 227 und $57 \cdot 79$ nicht repräsentiert.

Punkteschema :

Volle Punktzahl werden in den folgenden zwei Fällen vergeben:

- **(D4)** Eine korrekte und begründete Lösung für beide Zahlen, [**2 Punkte**]
- **(D4')** Eine korrekte und begründete Lösung für eine beliebige Zahl n in Abhängigkeit ob -11 ein Quadrat ist modulo $4n$. [**2 Punkte**]

Maximal ein Teilpunkt kann erzielt werden, indem man eines der folgenden Aussagen zeigt:

(a) Eine korrekte und begründete Lösung für eine der Zahlen, [**1 Punkt**]

(b) Q repräsentiert eine Zahl n nicht, falls -11 kein Quadrat modulo $4n$ ist, [**1 Punkt**]

(c) Q repräsentiert eine Zahl n, falls -11 ein Quadrat modulo $4n$ ist. [**1 Punkt**]

Keine Punkte gibt es für die Berechnung der Diskriminante von Q.

Notenskala

Note	Punktzahl
6	16+
5.75	15
5.5	14
5.25	13
5	12
4.75	11
4.5	10
4.25	9
4	8
3.75	7
3.25	6
3	5
2.5	4
2.25	3
1.75	2
1.5	1
1	0