Aufgaben: Zwei Quadrate Satz

1. Zeige, dass für eine Primzahl $\mathbb{N} \ni p \equiv 1 \mod (4)$ die zwei ganzen Zahlen $x, y \in \mathbb{Z}$ für welche $p = x^2 + y^2$ gilt bis auf Reihenfolge und Vorzeichen eindeutig bestimmt sind.

   Hinweis: Betrachte $a^2(x^2 + y^2) - x^2(a^2 + b^2)$, wobei $p = a^2 + b^2$ eine andere Lösung ist.

   Lösung:

   Seien, a, b, x, y ganze Zahlen mit $a^2 + b^2 = p = x^2 + y^2$. Dann gilt,

   $$p \mid a^2(x^2 + y^2) - x^2(a^2 + b^2) = a^2y^2 - b^2x^2 = (ay - bx)(ay + bx).$$

   Da p prim ist können wir zwei Fälle unterscheiden.

   1) Fall: $p \mid ay - bx$

   Wir haben

   $$p^2 = (a^2 + b^2)(x^2 + y^2) = (ay - bx)^2 + (ax + by)^2.$$

   Es folgt, dass $p \mid ax + by$ und weiter, dass entweder $ay - bx = 0$ oder $ax + by = 0$.

   1a) Fall: $ay - bx = 0$

   Es gilt dann

   $$y^2p = y^2(a^2 + b^2) = b^2(x^2 + y^2) = b^2p \Rightarrow y = \pm b \Rightarrow x = \pm a.$$

   1b) Fall: $ax + by = 0$

   Es gilt dann

   $$x^2p = x^2(a^2 + b^2) = b^2(y^2 + x^2) = b^2p \Rightarrow x = \pm b \Rightarrow y = \pm a.$$

   2) Fall: $p \mid ay + bx$

   Wir haben

   $$p^2 = (a^2 + b^2)(x^2 + y^2) = (ay + bx)^2 + (ax - by)^2.$$

   Es folgt, dass $p \mid ax - by$ und weiter, dass entweder $ay + bx = 0$ oder $ax - by = 0$.

   2a) Fall: $ay + bx = 0$

   Es gilt dann

   $$y^2p = y^2(a^2 + b^2) = b^2(x^2 + y^2) = b^2p \Rightarrow y = \pm b \Rightarrow x = \pm a.$$

   2b) Fall: $ax - by = 0$

   Es gilt dann

   $$x^2p = x^2(a^2 + b^2) = b^2(y^2 + x^2) = b^2p \Rightarrow x = \pm b \Rightarrow y = \pm a.$$

2. Sei $p \in \mathbb{N}$ eine Primzahl und $x, y \in \mathbb{Z}$ zwei ganze Zahlen, welche teilerfremd zu p sind. Nehme an, dass $p \mid x^2 - xy + y^2$ und folgere, dass entweder $p = 3$ oder $p \equiv 1 \mod (6)$.

Hinweis: $(x+y)(x^2-xy+y^2) = x^3+y^3$.

Lösung:

Es gilt

$$p \mid x^2 - xy + y^2 \mid x^3 + y^3$$

und ferner, da y und p teilerfremd sind, dass $(xy^\star)^3 \equiv -1 \mod (p)$ für ein multiplikatives Inverse $y^\star$ von y modulo p. Sei $z \in \mathbb{Z}$ eine ganze Zahl, sodass $z \equiv xy^\star \mod (p)$. Dann ist die multiplikative Ordnung r von z modulo p ein Teiler von 6, da $z^6 \equiv (-1)^2 \equiv 1 \mod (p)$. Es gilt die Fälle $r = 1, 2, 3, 6$ zu unterscheiden. Falls $r = 1$, dann gilt $z \equiv 1 \mod (p)$ und folglich $x \equiv y \mod (p)$ und $0 \equiv x^2 - xy + y^2 \equiv x^2 \not\equiv 0 \mod (p)$ – ein Widerspruch!

Falls $r = 2$, dann gilt $x^2 \equiv y^2 \mod (p)$ und somit $0 \equiv x^2 - xy + y^2 \equiv y(2y - x) \mod (p)$. Da y und p teilerfremd sind muss also $2y \equiv x \mod (p)$ gelten und somit $y^2 \equiv x^2 \equiv 4y^2 \mod (p)$. Also $p \mid 3y^2$, aber $p \nmid y$ und somit $p \mid 3$, folglich $p = 3$.

Im Fall $r = 3$ gilt $1 \equiv z^3 \equiv -1 \mod (p)$ und somit $p \mid 2$. Aber für zwei ungerade Zahlen x, y gilt $2 \nmid x^2 - xy + y^2$ – ein Widerspruch!

Im Fall $r = 6$ muss $6 \mid p - 1$ gelten, da nach dem kleinen Satz von Fermat gilt $z^{p-1} \equiv 1 \mod (p)$, und es foglt, dass $p \equiv 1 \mod (6)$.