Aufgabe 1: Zeigen Sie, dass 1 und -1 die einzigsten Einheiten von $\mathbb{Z}[\sqrt{-5}]$ sind.

Es sei $\zeta := \sqrt{-5}$ und $\alpha := a + b\zeta$ sei eine Einheit von $\mathbb{Z}[\sqrt{-5}]$. Dann gibt es ein $\gamma = x + y\zeta$ mit $1 = \alpha\gamma$. Es ist

$$\begin{aligned}(a + b\zeta)(x + y\zeta) &= (ax + \zeta^2 by) + (ay + xb)\zeta \\ &= (ax - 5by) + (ay + xb)\zeta = 1 \\ &\Rightarrow ay + xb = 0, ax - 5by = 1\end{aligned}$$

Wir setzen $x = -ay/b$ in $ax - 5by = 1$ ein:

$$\begin{aligned}-a^2y/b - 5by =& 1 \Leftrightarrow y(-a^2/b - 5b) = 1 \\ \Leftrightarrow& y(-a^2 - 5b^2)1/b = 1 \\ \Leftrightarrow& y = b/(-a^2 - 5b^2)\end{aligned}$$

Durch Einsetzen erhalten wir $x = \frac{-a}{-a^2-5b^2} = \frac{a}{a^2+5b^2}$ und $y = \frac{-b}{a^2+5b^2}$. Es muss aber $\gamma = x + y\zeta \in \mathbb{Z}[\sqrt{-5}]$ sein, deswegen müssen x, y ganze Zahlen sein, deswegen muss $a^2 + 5b^2 = \pm 1$ sein mit $a, b \in \mathbb{Z}$. Das ist aber nur für $a = \pm 1$ und $b = 0$ möglich. Deswegen sind $1, -1$ die einzigsten Einheiten des Ringes.

Aufgabe 2: Zeigen Sie, dass $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ ein euklidischer Ring ist.

Wir verwenden die Norm-Funktion $N(\alpha) = |\alpha|^2$.

Wir zeigen, das wir damit eine Division mit Rest in $R := \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ durchführen können. Seien dazu Elemente $a, b \in R$ gegeben, wir wollen b als $b = aq + r$ schreiben mit $N(r) < N(a)$.

Dazu stellen wir uns das Gitter $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-3}}{2}$ vor (selber Skizze machen oder Abbildung 2.19 in Kapitel 11 im Artin auf diesen Fall übertragen). Die Kantenlängen (Normen der Kanten) der Grundmasche sind: 1 (0 nach 1) und ebenfalls 1 (die Kante von 0 nach $x := \frac{1+\sqrt{-3}}{2}$ hat Norm $|x|^2 = x\bar{x} = \frac{1}{4}4$). Die Diagonale von 1 nach x hat ebenfalls die Norm 1. Die untere Kante, die linke Kante und die Diagonale bilden ein gleichseitiges Dreieck, der Winkel zwischen unterer und linke Kante ist 60 Grad.

Im Gleichseitigen Dreieck mit Kantenlänge 1 ist der Radius dem Umkreises $\sqrt{3}^{-1}$ bzw. $(2(\sin 60))^{-1} = 0.57... < 1$. Das bedeutet jeder Punk im Inneren hat einen Abstand kleiner gleich $\delta := \sqrt{3}^{-1}$ von einem der Gitterpunkte.

In dieses Gitter stellen wir uns das Ideal $(a)R$ also das mit (der komplexen Zahl) a multiplizierte Gitter eingezeichnet vor. Die Kanten dieses Gitters haben die Norm $|a|^2$ (die Norm ist die quadrierte Kantenlänge). Die Diagonalen haben ebenfalls die Kantenlängen a und Norm a^2.

Wir halten fest: Jeder Punkt im Inneren einer Masche von $(a)R$ hat bzgl. unserer Norm einen Abstand von höchstens $\delta^2 a^2$ zu einer Ecke von $(a)R$.

Zurück zu unserem Problem. Wir müssen zeigen, dass zu $a, b \in R$ eine Darstellung der Form $b = aq + r$ möglich ist. aq ist aus dem Ideal bzw. Gitter $(a)R$. Der Punkt b ist aus R. Wir haben gerade gezeigt, dass jeder Punkt aus dem Inneren einer Masche von $(a)R$, also auch jeder Punkt von R aus dem Inneren der Masche, einen quadrierten Abstand $\leq \delta^2 a^2$ zu einer Ecke der Masche hat.

Das bedeutet, wir können zu einem beliebigen $b \in R$ ein Element des Gitter $(a)R$ finden mit $b = aq + r$ und $N(r) \leq \delta^2 a^2$. Hierbei ist a^2 die Norm von a, also $N(r) < N(a)$.

(In der ursprünglichen Fassung der Aufgabe mit $\mathbb{Z}[\sqrt{-3}]$ geht diese Begründung nicht, da die Diagonale in der Masche die Norm $1 - (\sqrt{-3}^2) = 4$ hätte, und der Punkt auf der halben Diagonalen die Norm 1 hätte. Für das Gitter $(a)R$ würde das bedeuten, dass Punkte im Inneren mit Abstand (Norm) a zu den Ecken existieren, das würde auf $N(r) = N(a)$ hinauslaufen.)

Aufgabe 3: Berechnen Sie mit SAGE die Gruppe der Einheiten des Ringes $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Wir untersuchen zuerst die Relation in dem Ring $R := \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Es sei $\zeta := \frac{1+\sqrt{5}}{2}$, dann gilt:

$$\begin{aligned}\zeta = \frac{1+\sqrt{5}}{2} &\Leftrightarrow 2\zeta = 1 + \sqrt{5} \Leftrightarrow 2\zeta - 1 = \sqrt{5} \\ &\Leftrightarrow (2\zeta - 1)^2 = 5 \Leftrightarrow 4\zeta^2 - 4\zeta + 1 = 5 \Leftrightarrow \zeta^2 - \zeta - 1 = 0 \\ &\Leftrightarrow \zeta(\zeta - 1) = 1\end{aligned}$$

An der letzten Zeile erkennen wir, dass $\pm\zeta$ und $\pm(\zeta - 1)$ Einheiten sind, genauso wie $\pm\zeta^n$ und $\pm(\zeta-1)^n$. Da $\pm\zeta^n = \pm(\zeta-1)^{-n}$ ist, ist $\{\pm\zeta^n \mid n \in \mathbb{Z}\}$ $= \{(-1)^{n_1}\zeta^{n_2} \mid n_1, n_2 \in \mathbb{Z}\}$ die Einheitengruppe des Ringes.

Das können wir mit SAGE überprüfen:

```
sage: y=(1+sqrt(5))/2
sage: y.minpoly()
x^2 - x - 1
sage: (y.minpoly() +1).factor()
(x - 1) * x
sage: P.<x>=PolynomialRing(ZZ,'x')
sage: R=P.quotient_ring(x^2-x-1,'z')
sage: z=R.0
sage: z
z
sage: z^(-1)
z - 1
sage: z^(-5)
5*z - 8
sage: (z-1)^5
5*z - 8
sage: for k in range(10):
    n = randint(-1000,1000)
    if z^n==(z-1)^(-n):
        print "ok:", n
    else:
        print "Fehler:",n
ok: 341
ok: -637
ok: -837
ok: 223
ok: 958
ok: -673
ok: -457
ok: 981
ok: -430
ok: -758
```

Aufgabe 4: Implementieren Sie in SAGE den euklidischen Algorithmus für $\mathbb{Z}$ unter alleiniger Verwendung von Division mit Rest.

```
def euklid_algo(a, b ):
    "Berechnet den ggt von a und b mittels euklidischem Algor
    a= abs(a) # es reicht sogar lediglich am Ende
    b= abs(b) # return abs(a) zu sagen
    while b != 0:
        r= a%b
        a= b
        b= r
    return a
```

Aufgabe 5: Sei p eine Primzahl. Es heisst a ein quadratischer Rest modulo p, falls es ein $b \in \mathbb{F}_p$ gibt, mit $b^2 \equiv a \pmod{p}$. Schreiben Sie in SAGE eine Funktion, die durch Probieren feststellt, ob ein a ein quadratischer Rest modulo p ist.

1. Für wieviele der ersten 100 Primzahlen ist $a = -1$ ein quadratischer Rest?
2. Für wieviele der ersten 100 Primzahlen ist $a = 2$ ein quadratischer Rest?
3. Erkennen Sie ein Muster?

```
def is_QR(a, p):
    "Testet, ob es ein b mit b^2 kongruent a mod p gibt."
    RKR= IntegerModRing(p)
    a= RKR(a)
    for b in RKR:
        if RKR(b^2) == a:
            return True
    return False

def count(a, n =100 ):
    return sum([1 for p in primes_first_n(n) if is_QR(a,p)])

print "a=-1: ", count( -1 )
# 48
print "a=2: ",  count(  2 )
# 48

def MusterSucheMinus1(n=100):
    for p in primes_first_n(n):
        if is_QR(-1,p): print p, p%4
        else: print "  ",p, p%4
# MusterSucheMinus1()
```

```
  #   Vermutung -1 ist QR mod p, falls p kong 1 mod 4
  #   ja, wegen legendre(-1,p) = (-1)^((p-1)/2)
25
  def MusterSuche2(n=100):
      for p in primes_first_n(n):
          if is_QR(2,p): print (p^2-1 )/8 # gerade
          else: print "    ", (p^2-1 )/8 # ungerade
30 #MusterSuche2()
  #   Vermutung: 2 ist QR mod p, falls (p^2-1)/8 gerade ist
```