Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 3

Aufgabe 1

Man setze $\omega := -1/2 + \sqrt{3}/2$. Der Ring der Eisensteinschen Zahlen $E = \{ m + n\omega \mid m, n \in \mathbb{Z} \}$ ist ein Unterring von $\mathbb{C}$ und als Euklidischer Ring ein Hauptidealring. Daher sind die Primelemente in diesem Ring gerade die unzerlegbaren Elemente.

a)Man finde eine notwendige und hinreichende Bedingung dafür, daß eine Primzahl in $\mathbb{Z}$ auch im Ring *E* prim ist.
(Um einen Eindruck zu gewinnen, untersuche man zunächst die Elemente 2,3,5,7,11,13 in *E*.)

b) Man gebe einige Primzahlen in *E* an, die nicht assoziiert zu Primzahlen in $\mathbb{Z}$ sind.

Aufgabe 2

Zeigen Sie, daß das Polynom $f = x^5 + x^2 + 1$ irreduzibel in $\mathbb{Z}_2[X]$ ist.
Damit ist $K := \mathbb{Z}_2[X] / < f >$ ein Körper. Die Elemente dieses Körpers lassen sich als Polynome in $\mathbb{Z}_2[X]$ vom Grad kleiner gleich 4 auffassen, bzw. als Bitstrings der Länge kleiner gleich 5.
(Dabei ist wird der Bitstring 01001 interpretiert als das Polynom x^3+1.) Es ist $|K| = 32$.

Finden Sie mit Hilfe des Erweiterten Euklidischen Algorithmus das Inverse von 101 in *K*.

Aufgabe 3

Sei *p* die kleinste Primzahl, die größer als 2^{1000} ist.
a) Berechnen Sie im Körper $\mathbb{Z}_p$ eine Quadratwurzel von 2!
b) Sei $q = p^2$. Benutzen Sie das Ergebnis von a), um im Restklassenring $\mathbb{Z}_q$ eine Quadratwurzel von 2 zu berechnen.

c) Die folgende Zahl *n* ist das Produkt zweier zufälliger Primzahlen: *n*=
28415608352022230560999742274479309012797651162709355164498588370827372069690206
55909769630731423510476439424668375133121303105102416219095329902488904573290390
47975958887947569867996346346419509114479712512026624153253745272128921635596432
93405594495419327826696894439417897278062381101105591960279605763434956627995408
47007754426421843287069748768000950909780982800804887697669266556898446025587024
91230290781827038800490940919880556113436488013356538011767436484209320033110773
17200086903656162720295759397453265556180180156360992061922894503250524868611569
33290658405304911623875164550049860038619800662416755 47

Sei nun *a*=
23856273010426103138016280543014699717121135931055591093919217137345188694647431
16559078300029364364625642351631613607031793664407236424417462562534192530723867
80202313915345255747221980483664157690711093193834492880482747107870088643681545
09265208737518758477151400269975576152897523735598683547274301271487782531054570

2760137447207137644745039154904425036833856632909978904984637799084273820908665964976515899545531614344544086222544430665730251587738094898279882816688117144869872110309455856561865554536570249204407286728464820970617813205624076018014705374134778609827468927285277621395034798507581897847469152

Überprüfen Sie, daß in $\mathbb{Z}_n$ gilt: $a^2 = 1$, und benutzen Sie dies, um die Faktorisierung von *n* zu finden.