Privatdozent Dr. C. Diem
diem@math.uni-leipzig.de

MATHEMATISCHE GRUNDLAGEN DER KRYPTOGRAPHIE MIT ÖFFENTLICHEN SCHLÜSSELN

PROGRAMMMIER-HAUSAUFGABE NR. 3

1. Implementieren Sie den Miller-Rabin Primzahltest (eigentlich: Zusammengesetze-Zahl-Test) mit einer passenden Anzahl an Wiederholungen derart, dass die Implementierung de facto immer (oder "immer") das richtige Ergebnis liefert.

2. Implementieren Sie den AKS-Primzahltest aus: Agrawal, Kayal und Saxena, PRIMES is in P, Annals of Mathematics **160** (2004)

   Für den ersten Schritt des Algorithmus können Sie eine numerische Wurzel-Funktion verwenden. (Aber bitte so, dass es auch stimmt, d.h.: Bitte Rundungsfehler beachten!). (Sie können danach auch eine numerische log-Funktion verwenden, aber das ist nicht notwendig, weil Sie auch die Länge von zwei_adisch(n) betrachten können und dies umrechnen können.)

   Beachten Sie hier und und bei 1., dass schon viel hierfür vorhanden ist.

3. Implementieren Sie den "Standard"-Irreduzibilitätstest für Polynome über endlichen Körpern. (Dieser Test wird öfters *Rabin-Test* genannt.)

4. Fügen Sie den implementieren Ringen ein Attribut hinzu: ist_endlicher_koerper. Dabei soll dies eine Instanz von PolynomRestklassenring genau dann den Wert True haben, das Attribut ist_endlicher_koerper des Grundrings basisring den Wert True hat und das definierende Polynom irreduzibel ist.

   Fügen Sie dem Irreduzibilitätstest entsprechende Fehlermeldungen hinzu, wenn der Ring nicht korrekt ist. (Andererseits brauchen Sie den Test auch, um ist_endlicher_koerper zu implementieren, aber das ist kein Widerspruch ...)

5. Implementieren Sie eine Funktion endlicher_koerper. Diese soll eine Instanz von GanzzahlRestklassenring (für Primkörper) oder von PolynomRestklassenring (für nicht-Primkörper) zurückgeben.

   i) Zu einer Primzahl p und einer positiven ganzen Zahl n soll sie einen Körper mit p^n Elementen zurückgeben, zu einer Primpotenz $q = p^n$ das Entsprechende. Für $n > 1$ soll der der Grundring (basisring) dann ein Primkörper sein.

   ii) Zu einem Restklassenring F, der ein endlicher Körper ist (genauer: zu einem Objekt F, dessen Typ von Ring abgeleitet ist und das laut Attribut ein endlicher Körper ist) und einer natürlichen Zahl n soll sie einen Erweiterungskörper von Grad n von F zurückgeben. Für $n = 1$ soll dies dann F selbst sein, für $n > 1$ soll der Grundring dann F sein.

   Die Anwendung soll deterministisch sein, d.h. bei zweimaligem Aufruf sollen identifizierbare Ringe (zwei Objekte R, S mit R == S) zurückgegeben werden.

   Um dies zu erreichen, ist es sinnvoll, über die Ringelemente zu iterieren, und hierfür ist die Verwendung von *Iteratoren* in python sinnvoll.

Selbstredend sollen Sie stets verständliche Fehlermeldungen implementieren.

Fertigstellung mit Präsentation bis zum 1.7.