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

MATHEMATISCHE GRUNDLAGEN DER KRYPTOGRAPHIE MIT ÖFFENTLICHEN SCHLÜSSELN

Es wird insgesamt drei Programmierhausaufgaben geben. Die Aufgaben sollen in python unter Zuhilfenahme des von mir implementierten Pakets Tocas implementiert werden. Dies finden Sie auf dem Gitlab-Server des Instituts für Informatik. Es ist frei verfügbar unter `https://git.informatik.uni-leipzig.de/diem/tocas`.

Hier sind die ersten beiden Aufgaben.

Die erste Aufgabe soll jeder von Ihnen alleine anfertigen. Die zweite und die dritte Aufgabe sollen Sie dann genau wie das Projekt im Zweierteam bearbeiten.

PROGRAMMMIER-HAUSAUFGABE NR. 1

Implementieren Sie Klassen für den Ring der rationalen Zahlen und die rationalen Zahlen. Diese zwei Klassen sollen heißen: Bruchzahlring und BruchzahlringElement. Sie sollen von den Klassen Ring und RingElement abgeleitet werden. Sie müssen damit also die in diesen Klassen als abstrakt gekennzeichneten Methoden implementieren.
Es soll die folgenden Konstruktoren geben:

- Bruchzahlring() erzeugt die rationalen Zahlen. Hiermit soll ein fester solcher Körper, genannt Q, instanziiert werden (in Analogie zu Z).
- Mittels von Konstruktoren von BruchzahlringElement sollen die folgenden Konstruktionen möglich sein:
  - Für eine ganze Zahl a: $a/1$ in dem festen Körper.
  - Für Tupel (a, b) ganzer Zahlen mit $b \neq 0$: $\frac{a}{b}$ in dem festen Körper.
  - Für eine rationale Zahl: die Zahl selbst. (Wir wollen immer so einen "Identitäts-Konstruktor" haben.

Die Elemente sollen immer als gekürzte Brüche mit positivem Nenner gespeichert werden. (Das kann man hier als Normalform betrachten.) Für das Kürzen können Sie die Methode Ganzzahlring.ext_ggt verwenden.

PROGRAMMIER-HAUSAUFGABE NR. 2

1. Implementieren Sie eine statische Methode ext_ggt der Klasse Polynomring zum Berechnen des ggT zweier Polynome über einem (demselben) Körper.

   Es sollte überprüft werden, dass die beiden Polynome in einem Polynomring zu vergleichbaren Grundringen (basisring) liegen. Sie sollten dann aber davon ausgehen, dass dieser Ring ein Körper ist. (Wenn er es nicht ist, könnte die Rechnung fehlschlagen, weil man in ihm nicht invertieren kann.)

2. Implementieren Sie Klassen PolynomRestklassenring und PolynomRestklassenringElement für das Rechnen in Restklassenringen der Form $K[x]/(f)$ für einen Körper K und ein nicht-triviales Polynom $f \in K[x]$.

   Gehen Sie dabei davon aus, dass ein dass ein Objekt K vom Typ Ring gegeben ist, welches einen Körper beschreibt, sowie ein Element f, das f beschreibt. (Wir überprüfen nicht, ob K tatsächlich ein Körper ist.)

   Es gibt zwei naheliegende Möglichkeiten, die Elemente darzustellen:

   i. Sie gehen analog zu den Klassen GanzzahlRestklassenring und GanzzahlRestklassenringElement vor. Dann werden die Elemente von $K[x]/(f)$ durch Polynome von Grad $<$ Grad(f) dargestellt.
   ii. Sie stellen die Elemente in der Polynomialbasis $[1]_f, [x]_f, \ldots, [x^{\deg(f)-1}]_f$ dar. Der Koeffizientenvektor sollte vom Typ RingTupel sein.

   Natürlich sind die beiden Möglichkeiten eng verwandt, aber die Implemtierung ist trotzdem recht verschieden. Sie sollten sich für eins von beidem entscheiden.

   Gehen Sie für das Invertieren davon aus, dass der Grundring ein Körper ist. (Oder anders ausgedrückt: Machen Sie sich keine Gedanken darüber, ob Elemente aus dem Grundring nun invertierbar sind oder nicht. Wenn sie es nicht sind, gibt es halt eine Fehlermeldung.)

   Die folgenden Konstruktoren sollten verfügbar sein:

   - Für einen Körper K (gegeben durch K vom Typ Ring) und ein Polynom $f \in K[x]$ (gegeben durch f) liefert PolynomRestklassenring(f) ein Objekt, das den Ring $K[x]/(f)$ beschreibt.
   - Es sei R ein Ring, $f \in K[x]$ von Grad n. Dann sollen mittels Konstruktoren von PolynomringElement die folgenden Konstruktionen möglich sein:
     - Für ein Element $r \in K$ (dem Basisring): $r \in K[x]/(f)$.
     - Für ein Element $h \in K[x]$: $[h]_f \in K[x]/(f)$.
     - Für $g \in K[x]$ mit $f \mid g$ und ein Element $a \in K[x]/(g)$: das Bild von a in $K[x]/(f)$. (Als Spezialfall für $f = g$ erhalten wir einen "Identitäts-Konstruktor".)
     - Für ein Tupel $(a_0, \ldots, a_{n-1}) \in K^{n-1}$: $\sum_{i=0}^{n} a_i \cdot [x]_f^i \in K[x]/(f)$.

3. Implementieren Sie eine Instanzmethode zufaellig von PolynomRestklassenring.

   Diese soll ein zufälliges Element liefern, wenn der Ring durch wiederholte Anwendung von PolynomRestklassenring auf einen mit Restklassenring erzeugten Ring erzeugt worden ist. (Ansonsten kann sie einen Fehler werfen. Sie können noch ein Attribut für "gute" Ringe vorsehen, so dass die Fehlermeldung noch ein wenig netter wird.)

Fertigstellung mit Präsentation bis zum 3.6.