STOFFÜBERSICHT MAT3 FÜR CMS, WS 05/06

ERHARD AICHINGER, PETER MAYR

(1) Aus Unterlagen zur elementaren Zahlentheorie:
   (a) * Aus der Sektion **1. Teilbarkeit** alles außer Satz 1.13.
   (b) * Aus der Sektion **2. Lösen von Longruenzen**: Definition 1.14, Satz 1.15 mit Beweis, Satz 1.16 ohne Beweis.
   (c) Aus der Sektion **3. Der Ring** $\mathbb{Z}_n$: Alles bis (einschließlich) Satz 1.24.
   (d) * Aus der Sektion **3. Der Ring** $\mathbb{Z}_n$: Definition 1.26, Satz 1.27 (ohne Beweis). Korollar 1.28 (ohne Beweis).
   (e) * Aus der Vorlesung: Definition eines Körpers; $\mathbb{Z}_n$ ist genau dann ein Körper, wenn n Primzahl ist. In einem Körper kann ein Produkt nur 0 sein, wenn einer der Faktoren 0 ist (mit Begründung).

(2) Aus Unterlagen zu Polynomringen:
   (a) * Aus der Sektion **1. Körper**: Definition 1.1.
   (b) * Alles aus Sektion **2. Polynome**.
   (c) * Aus Sektion **3. Teilbarkeit von Polynomen**: Alles bis (einschließlich) zum Beweis von Satz 1.14.
   (d) * Aus Sektion **4. Polynomfunktionen und Nullstellen**: Alles bis (einschließlich) Satz 1.19.
   (e) Beweis von Satz 1.19.

(3) Aus Unterlagen zu endlichen Körpern:
   (a) * Aus Sektion **1. Definition endlicher Körper**: Definition 1.1.
   (b) * Aus Sektion **2. Körper aus irreduziblen Polynomen**: Alles außer dem Mathematica-Code und dem Satz 1.7.
   (c) Aus Sektion **2. Körper aus irreduziblen Polynomen**: Verständnis des Mathematica-Codes, Satz 1.7.
   (d) * Aus Sektion **3. Eigenschaften endlicher Körper**: Alles bis einschließlich Satz 1.11.
   (e) Beweis von Satz 1.11, soweit in der Vorlesung besprochen.
   (f) * Aus Sektion **3. Eigenschaften endlicher Körper**: Definition 1.13, 1.14, Lemma 1.15, Satz 1.16 (ohne Beweis),
   (g) Aus Sektion **3. Eigenschaften endlicher Körper**: Satz 1.17, Satz 1.18, Satz 1.19.
   (h) * Aus der Vorlesung: Satz von Fermat (ohne Beweis). Definition endlicher zyklischer Gruppen, Definition von Erzeuger, Definition von primitiven Elementen.

Date: January 4, 2006.

(4) Anwendungen: Generalized El Gamal Signature Scheme. Lösen von Gleichungssystemen über endlichen Körpern. Minimaldistanz von Codes. Hamming-Schranke.
(5) Fertigkeiten:
  (a) * Erweiterter Euklidscher Algortihmus in $\mathbb{Z}$.
  (b) * Bestimmen aller Lösungen von $ax \equiv b (\mathrm{mod}\ c)$.
  (c) * $+, -, *$ in $\mathbb{Z}_n$.
  (d) * Invertieren in $\mathbb{Z}_n$.
  (e) * Potenzieren in $\mathbb{Z}_n$.
  (f) * Lösen eines Gleichungssystems in $\mathbb{Z}_p$.
  (g) * Bestimmen von Quotient und Rest für Polynome $f, g \in \mathbb{Z}_p[x]$.
  (h) * Erweiterter Euklidscher Algortihmus in $\mathbb{Z}_p[x]$.
  (i) * $+, -, *$ in $\mathbb{Z}_p[x]/f$.
  (j) * Invertieren von $[g]_f$ in $\mathbb{Z}_p[x]/f$.
  (k) Überprüfen, ob ein $f \in \mathbb{Z}_p[x]$ über $\mathbb{Z}_p$ irreduzibel ist.
  (l) * Bestimmen der multiplikativen Ordnung von $[g]_f$ in $\mathbb{Z}_p[x]/f$.
  (m) Finden eines primitiven Elements von $\mathbb{Z}_p[x]/f$.
  (n) Konstruieren eines endlichen Körpers mit vorgegebener Anzahl von Elementen.
  (o) Durchführen der Rechenoperationen zur digitalen Unterschrift nach El Gamal.

Prüfungsinformation

Die Prüfung besteht aus einem ersten Teil ohne Unterlagen (30.1., 9:40 - 10:40) und einem zweiten Teil (30.1., 11:00-12:30) mit Unterlagen und Computer. Die mit * versehenen Teile sollten Sie ohne Unterlagen wissen. Die nicht mit * versehenen Teile sollten Sie verstanden haben; diese Teile müssen Sie aber nicht auswendig beherrschen. Sie sollen die in der Vorlesung verwendeten Mathematica-Programme in `poliesModP.m` verwenden können (diese werden Ihnen bei der Prüfung zur Verfügung gestellt.) Ebenso sollten Sie alle für die Verschlüsselung nach dem RSA-Verfahren nötigen Rechnungen (also Potenzieren modulo n) mit Mathematica durchführen können.

Typische Prüfungsbeispiele

(1) (ohne Unterlagen)
  (a) Berechnen Sie $\mathrm{ggT}(78, 90)$, und berechnen Sie Zahlen $u, v \in \mathbb{Z}$, sodass $\mathrm{ggT}(78, 90) = 78u + 90v$.
  (b) Bestimmen Sie eine Lösung der Kongruenz $13x \equiv 2 \,(\mathrm{mod}\ 101)$.
  (c) Berechnen Sie das inverse Element von $[5]_7$ in $\mathbb{Z}_7$.
  (d) Was sagt der Satz von Fermat aus? (Hinweis: etwas über den Rest von z^p modulo p.) Formulieren Sie diesen Satz.
(2) (mit Unterlagen) Übungsbeispiele 12.3 und 12.4.