

# Zahlentheorie und Kryptologie, WS 2008/09

Michael Hortmann

## Mögliche Prüfungs/Klausur Fragen

Die folgende Liste wurde anhand des Stoffs der Vorlesung und der Übungen erstellt. Prüfen Sie anhand dieser Fragen Ihr Verständnis.

Was ist ein Blockchiffrieralgorithmus? Wie ist der DES-Algorithmus aufgebaut? Wie funktioniert Cipher-Block-Chaining? Welche Eigenschaften sollte eine kryptographische Hashfunktion besitzen, wozu wird so eine Funktion benötigt?

Was ist der Unterschied zwischen einem Public Key Verschlüsselungssystem und einem klassischen Verschlüsselungssystem wie DES? Wie funktioniert das RSA-Public Key System, wie der Diffie-Hellman Schlüsselaustausch? Was ist eine digitale Signatur? Wie realisiert man sie im RSA-System und wie in Systemen, die auf der Schwierigkeit des Diskreten Logarithmus-Problems beruhen?

Was ist eine zyklische Gruppe? Warum sind Untergruppen zyklischer Gruppen zyklisch? Wie ist die Ordnung eines Elements einer Gruppe definiert? Welches ist die Beziehung zwischen der Ordnung einer Untergruppe und der Anzahl der Restklassen bzgl. dieser Untergruppe? Wann bilden die Restklassen selbst eine Gruppe?

3. Was sind Primelemente und unzerlegbare Elemente eines Rings? Was sind Primideale und maximale Ideale? Warum gibt es unendlich viele Primzahlen? In welchen Ringen können Sie den Satz über die eindeutige Primfaktorzerlegung beweisen? Was sind euklidische Ringe? Wie funktioniert der Euklidische Algorithmus, wie der erweiterte Euklidische Algorithmus? Wie berechnet man Inverse in Euklidischen Ringen bzgl. der Multiplikation? Wieso ist 2 nicht prim in den Gaußschen Zahlen? Ist 2 prim in den Eisensteinschen Zahlen? Welche endlichen Körper kennen Sie, wie werden sie konstruiert? Können Sie das Polynom  $X^p - X$  über  $Z_p[X]$  faktorisieren? Was ist die Eulersche  $\varphi$ -Funktion, wie berechnet man sie? Was ist die Möbiusfunktion, was die Möbius-Inversionsformel? Was besagt der Chinesische Restesatz, wie beweist man ihn?

Wie kann man auch für große Zahlen testen, ob sie prim sind? Wie läßt sich von einem Polynom feststellen, ob es irreduzibel ist? Wie sind Legendre-Symbol und Jacobi-Symbol definiert? Was besagt das Quadratische Reziprozitätsgesetz? Berechnen Sie das Jacobi-Symbol  $\left(\frac{66}{75}\right)$  ! Was ist eine Carmichael Zahl, welche Carmichael-Zahlen kennen Sie?

Warum ist die Charakteristik eines Körpers gleich Null oder eine Primzahl? Wie konstruiert man einen Körper mit  $p^n$  Elementen? Warum ist die multiplikative Gruppe eines endlichen Körpers zyklisch? Wie würden Sie vorgehen, um einen Erzeuger zu finden? Was ist der Frobenius-Automorphismus in einem endlichen Körper?

Wie würden Sie eine Quadratwurzel in Restklassenringen oder in endlichen Körpern berechnen?

Welche Faktorisierungsalgorithmen kennen Sie? Wie funktionieren sie? Wie funktioniert insbesondere die Fermat-Faktorisierung?

Was ist eine Kettenbruchentwicklung? Was hat die Kettenbruchentwicklung von  $\sqrt{n}$  mit der Faktorisierung von  $n$  zu tun? Wozu ist der Bhaskara Brouncker Algorithmus nützlich?

Was ist eine elliptische Kurve über einem Körper  $K$ ?

Wie ist die Addition auf einer elliptischen Kurve definiert?

Zwischen welchen Werten schwankt die Ordnung einer elliptischen Kurve über einem endlichen Körper? (Satz von Hasse)

Wie berechnet man die Ordnung einer elliptischen Kurve, die über dem Körper  $K$  gegeben ist, wenn man sie als Kurve über einem Erweiterungskörper auffaßt?

Was ist das diskrete Logarithmus-Problem?

Auf was für Gruppen ist dieses Problem leicht zu lösen?

Welche Verfahren zur Lösung des DLP-Problems kennen Sie

Wie stellen Sie mit Hilfe von Pari fest, ob eine Zahl eine Primzahl ist? Wie finden Sie eine zufällige Primzahl einer vorgegebenen Größenordnung? Nennen Sie den Pari-Befehl, welcher die Multiplikation  $3 \cdot 5$  in  $\mathbb{Z}_7$  ausführt. Schreiben Sie ein Pari-Programm, welches  $n!$  berechnet.