

Eine erste Anwendung von Fermats kleiner Satz : Buch Bemerkung 5.85 Seite 146

Satz von Euler Buch Seite 147

Beispiele 5.87, 5.88, 5.89 Buch Seiten 147-148

Einführung in der Kryptographie: Caesar und Vigenere Kryptosysteme, Buch Seiten 163-168.

Beachten Sie bitte dass der Isomorphismus $\log_p: (\mathbb{Z}/\mathbb{Z}_p^*, \cdot) \longrightarrow (\mathbb{Z}_p, +)$ (Proposition 5.95) sowie Fermats kleiner Satz (Theorem 5.83) und Euler Satz (Theorem 5.86) werden am Montag benutzt. Deswegen es ist eine gute Idee diese bis Montag vor der Vorlesung zu lernen.

Bitte Bemerken Sie dass die Seiten 148-157 wurden schon in den vergangene Wochen beigebracht. Also Kapitel 5 ist jetzt ganz erledigt, (Proposition 5.80 und Theorem 5.105 OHNE BEWEIS).