Übungen zur Elementaren Zahlentheorie

-Zentralübung-

Prof. Dr. K. Wingberg
J. Bartels

SS 2007

Zettel für die Zentralübung Mittwoch 2. Mai 2007

---

1 . Aufgabe:
Wir codieren einen Text mithilfe der Primzahlen $p = 17$ und $q = 19$. Deren Produkt ist $n = 323$, $\varphi(pq) = 288$. Anschließend nehmen wir eine zu 288 teilerfremde Zahl $e = 95$. Zusammen ergeben (n, e) den öffentlichen Schlüssel. Man finde einen privaten Schlüssel d dazu.
Mit diesem finde man heraus, welche die verschlüsselte Zahl 294 ursprünglich gewesen ist.

2 . Aufgabe:
Potenzieren mod n
(in der Übung direkt).

Hinweise zum gegenwärtigen Zettel:
1. Aufgabe:
Man gucke sich die Vorlesung, gerade am Anfang genauer an.
2. Aufgabe:
Die Teilbarkeitsbedingungen führen zu einer (etwas größeren) Gleichung, dann Fallunterscheidung.