

## Elementare Zahlentheorie (Version 2): Übung 6

- (a) Wieviele Elemente der Ordnung 5 gibt es modulo 541 (eine Primzahl)?  
(b) Und wie ist es modulo 441 (eine nicht-prim Zahl)?

2. Sei  $n \in \mathbb{N}$  gegeben, zusammen mit einer Zahl  $a > 1$  wobei

- i.  $a^{n-1} = 1 \pmod n$ ,
- ii.  $a^m \neq 1 \pmod n$  für  $1 \leq m < n - 1$ .

Zeigen Sie, daß  $n$  prim ist.

- (b) Wiederum sei  $n \in \mathbb{N}$  und  $a > 1$  mit

- i.  $a^{n-1} = 1 \pmod n$ ,
- ii.  $a^m \neq 1 \pmod n$  für alle  $m$  mit  $m|n - 1$ .

Zeigen Sie, daß  $n$  prim ist.

3. Sei  $p$  eine ungerade Primzahl und sei  $1 \leq a \leq p - 1$  ein quadratischer Rest modulo  $p$ . Kann es sein, daß  $a$  auch eine Primitivwurzel modulo  $p$  ist?

Allgemeiner: Sei  $a$  eine Primitivwurzel modulo  $p$ . Für welche  $n$  ist die Gleichung

$$x^n = a \pmod p$$

lösbar?