Aufgabenzettel 9.

9.1. Zeige: Jede Fermat-Zahl $F_n = 2^{2^n} + 1$, jede Mersenne-Zahl $M = 2^p - 1$ (mit p Primzahl) ist selbst entweder eine Primzahl oder aber Pseudo-Primzahl zur Basis 2.

9.2. Lineare Codierung (nicht sehr sicher!) Unter einer Codierung der Zahlen $0 \leq a < m$ verstehen wir eine bijektive Abbildung $\mathbb{Z}/m \to \mathbb{Z}/m$.

(a) Zeige: Sind r, s natürliche Zahlen mit $(m, r) = 1$, so ist $\overline{a} \mapsto \overline{ra + s}$ eine Codierung der Zahlen $0 \leq a < m$ (wir nennen dies eine *lineare* Codierung).

(b) Für vorgegebenes m, wieviele lineare Codierungen gibt es?

(c) Zeige: Die Umkehrabbildung einer linearen Codierung ist wieder eine lineare Codierung.

(d) Es sei $m = 50$. Aufgrund von Häufigkeitsanalysen habe man festgestellt, dass die codierten Zahlen 12 und 31 im Klartext 5 (=e) und 14 (=n) bedeuten. Man bereche daraus die Codierungszahlen r, s.

9.3. RSA. (a) Alice verschlüsselt die Nachricht m mit dem öffentlichen Schlüssel $[51, 11]$. Der verschlüsselte Text sei 31. Bobs privater Schlüssel sei $[51, 3]$. Bestimme, falls möglich, den Klartext.

(b) Alice verschlüsselt die Nachricht m mit dem öffentlichen Schlüssel $[33, 7]$. Der verschlüsselte Text sei 9. Bobs privater Schlüssel sei ebenfalls $[33, 7]$. Bestimme, falls möglich, den Klartext.

Achtung: Man überprüfe jeweils, ob der private Schlüssel überhaupt zum öffentlichen Schlüssel passt!

9.4. Sei p eine Primzahl, sei $k \in \mathbb{N}$. Zeige:

$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} -1 \mod p & \text{falls} \quad (p-1) \mid k, \\ 0 \mod p & \text{andernfalls.} \end{cases}$$

Hinweis: Verwende die Existenz einer Primitivwurzel modulo p (und die Formel für eine geometrische Summe).

9.1. Claim: Any Fermat number $F_n = 2^{2^n}+1$, any Mersenne number $M = 2^p-1$ with p a prime is either itself a prime or else a pseudo prime for the basis 2. Prove it!

9.2. Linear Codes (not very secure!) We consider bijective maps $\mathbb{Z}/m \to \mathbb{Z}/m$.

(a) Show: If r, s are natural numbers with $(m, r) = 1$, then the map $\overline{a} \mapsto \overline{ra+s}$ is bijective. Such a map will be said to be a *lineare code*.

(b) For given n, how many linear codes $\mathbb{Z}/m \to \mathbb{Z}/m$ do exist?

(c) Show: The inverse of a linear code is again a linear code.

(d) Consider the case $m = 50$ and assume a linear code has been used. Now someone has found out (say looking at the distribution of numbers) that the encoded numbers 12 and 31 correspond to the unencoded numbers 5 (=e) and 14 (=n), respectively. Show that this is sufficient in order to calculate the numbers r, s.

9.3. RSA. (a) Alice encodes the message m with the public key $[51, 11]$. Bobs private key is supposed to be $[51, 3]$. Assume that the encoded message is 31. Calculate, if possible, m.

(b) Alice encodes the message m with the public key $[33, 7]$. Bobs private key is supposed to also $[33, 7]$. Assume that the encoded message is 31. Calculate, if possible, m.

Note: Check first, whether the public key and the private key fit to each other!

9.4. Let p be a prime, let $k \in \mathbb{N}$. Show:

$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} -1 \mod p & \text{if } (p-1) \mid k, \\ 0 \mod p & \text{otherwise.} \end{cases}$$

Hint: Use the existence of a primitive root modulo p (as well as the formula for a geometric sum).