Aufgabenzettel 8.

8.1. (a) Man zeige: Sei G eine endliche zyklische Gruppe, deren Ordnung gerade ist. Dann gilt: Das Produkt $\prod_{g\in G} g$ hat die Ordnung 2 (und bekanntlich hat eine derartige Gruppe genau ein Element der Ordnung 2). (Beachte: da G abelsch ist, kommt es bei der Produktbildung $\prod_{g\in G} g$ nicht darauf an, in welcher Reihenfolge multipliziert wird.)

(b) Man folgere aus (a) den "Satz von Wilson": Für jede Primzahl p gilt

$$(p-1)! \equiv -1 \mod p.$$

(Achtung: den Fall $p = 2$ muss man getrennt betrachten).

(c) Man folgere aus (b) den "Satz von Leibniz": Für jede Primzahl p gilt

$$(p-2)! \equiv 1 \mod p.$$

8.2. Zwei Beweise für den Kleinen Fermat. Sei p Primzahl.

(a) Beweis 1. Zeige mit Induktion nach n: Es gilt $n^p \equiv n \mod p$. Folgere daraus: Ist $(n,p) = 1$, so ist $n^{p-1} \equiv 1 \mod p$.

(b) Beweis 2. Zeige: Ist $1 \le a < p$, so liefert die Multiplikation mit $\overline{a}$ eine Permutation der Menge $(\mathbb{Z}/p)^* = \{\overline{1}, \ldots, \overline{p-1}\}$. Folgere daraus: $\prod_{i=1}^{p-1} \overline{ai} = \prod_{i=1}^{p-1} \overline{i}$. Daraus folgt die Behauptung — wieso?.

(c). Man verallgemeinere den Beweis in (b), um den Satz von Euler zu zeigen: Ist $(a,n) = 1$, so ist $a^{\phi(n)} \equiv 1 \mod n$.

8.3. Zeige, dass die Folge der Endziffern der Zahlen n^n (in der Dezimaldarstellung) periodisch ist und gib eine volle Periode an. (Es sei also $n^n \equiv a_n \mod 10$ mit $0 \le a_n \le 9$; zu untersuchen ist die Folge $a_1, a_2, \ldots$.)

8.4. Die Primteiler der Fermat'schen Zahlen. Es sei daran erinnert, dass man $F_n = 2^{2^n} + 1$ mit $n \in \mathbb{N}_0$ die *n-te Fermat'sche Primzahl* nennt.

(a) Zeige: Ist p ein Primteiler von F_n, so ist gibt es ein $k \in \mathbb{N}$ mit $p = k \cdot 2^{n+1} + 1$.

Hinweis: Betrachte die Ordnung von 2 in $(\mathbb{Z}/p)^*$.

(b) Die Zahl $F_5 = 2^{32} + 1$ ist keine Primzahl. Man verwende (a), um mögliche Teiler von F_5 zu suchen. Ohne viel Mühe findet man auf diese Weise einen Teiler — welchen?

8.1. (a) Let G be a finite cyclic group of even order. Show that the product $\prod_{g\in G} g$ has order 2 (we know already that such a cyclic gropu of even order has precisely one element of even order). (Note: since G is abelian, we do not have to specify the order of multiplying the elements in $\prod_{g\in G} g$.)

(b) As a consequence, show the "theorem of Wilson": If p is a prime, then

$$(p-1)! \equiv -1 \mod p.$$

(Note: the case $p = 2$ has to be considered separately).

(c) Derive from (b) the "Theorem of Leibniz": if p is a prime, then

$$(p-2)! \equiv 1 \mod p.$$

8.2. Tow proofs for the Little Fermat Theorem. Let p be a prime.

(a) Proof 1. Use induction along n in order to show: $n^p \equiv n \mod p$. Show that this implies: If $(n,p) = 1$, then $n^{p-1} \equiv 1 \mod p$.

(b) Proof 2. Show: Let $1 \leq a < p$. The multiplication by $\overline{a}$ is a permutation of the set $(\mathbb{Z}/p)^* = \{\overline{1}, \ldots, \overline{p-1}\}$. Show that this imples $\prod_{i=1}^{p-1} \overline{ai} = \prod_{i=1}^{p-1} \overline{i}$. This yields the assertion — why?

(c). Generalize the proof in (b), in order to provide a proof of the Euler Theorem: If $(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.

8.3. Show that the sequence of last digits of the numbers n^n (in the decimal expansion) is periodic and exhibit a full period. (To be precise: let $n^n \equiv a_n \mod 10$ with $0 \leq a_n \leq 9$; we are looking at the sequence $a_1, a_2, \ldots$.)

8.4. The prime divisors of the Fermat numbers. Recall that $F_n = 2^{2^n} + 1$ with $n \in \mathbb{N}_0$ is called the *n-the Fermat number.*

(a) Show: If p is a prime dividing F_n, then there is $k \in \mathbb{N}$ with $p = k \cdot 2^{n+1} + 1$.

Hint: Consider the order of 2 in $(\mathbb{Z}/p)^*$.

(b) The number $F_5 = 2^{32} + 1$ is not a prime. Use (a), in order to find possible divisors of F_5. Without much effort, one finds in this way a proper divisor of F_5 — which one?