Universität des Saarlandes
FR 6.1, Mathematik
Prof. Dr. E.-U. Gekeler
Dipl.-Math. M. Gebhardt

4. Übung zur elementaren Zahlentheorie, SS 2003

Aufgabe 1:(*10 Punkte*) Die 5-te Fermat-Zahl ist $F_5 := 2^{2^5} + 1 = 4\ 294\ 967\ 297 = 641 \cdot 6700417$. Sind $a = 2$ bzw. $a = 3$ Euler-Zeugen für F_5?

Aufgabe 2:(*12 Punkte*) Betrachten Sie die Zahl $n = 2821$. Führt man für die ersten 15 Primzahlen a den Solovey-Strassen-Primtest durch, so erhält man folgende Tabelle:

a	$a^{\frac{n-1}{2}} \bmod n$	$\left(\frac{a}{n}\right)$	a	$a^{\frac{n-1}{2}} \bmod n$	$\left(\frac{a}{n}\right)$	a	$a^{\frac{n-1}{2}} \bmod n$	$\left(\frac{a}{n}\right)$
2	1520	-1	13	2171	0	31	155	0
3	1	1	17	1	1	37	1520	1
5	1520	1	19	1520	1	41	1520	1
7	714	0	23	1	-1	43	1	-1
11	1520	1	29	1	-1	47	1520	1

a) Zeigen Sie, daß n eine Carmichael-Zahl ist.

b) Setzen Sie die Tabelle fort für alle a aus $\mathbb{N}$ mit $48 \leq a \leq 55$.

c) Erklären Sie, warum in der obigen Tabelle für $a^{\frac{n-1}{2}} \bmod n$ nur 5 verschiedene Werte auftreten. Wieso tritt insbesondere die Zahl 1520 so oft auf ?

Aufgabe 3:(*8 Punkte*) Schreiben Sie die Zahl 2665 auf vier verschiedene Weisen als Summe von zwei Quadraten. (D.h. finden Sie vier paarweise verschiedene Mengen $\{a_i, b_i\} \subset \mathbb{N}_0$ mit $2665 = a_i^2 + b_i^2$.)

Aufgabe 4:(*10 Punkte*) Sei $(G, \cdot)$ eine endliche abelsche Gruppe. Dann heißt

$$e(G) := \mathrm{kgV}\{ord_G(x) \mid x \in G\} = \min\{n \in \mathbb{N} \mid x^n = 1,\ \forall x \in G\}$$

der *Exponent* von G. Zeigen Sie:

a) Ist G zyklisch der Ordnung n, so gilt $e(G) = n$.

b) Ist H Untergruppe von G, so gilt $e(H)|e(G)$ und $e(G/H)|e(G)$.

c) Ist $p \in \mathbb{P}$ und $p|\#G$, so gilt $p|e(G)$.

d) Die Primteiler von $\#G$ und $e(G)$ sind gleich.

e) $e(G_1 \times G_2) = \mathrm{kgV}(e(G_1), e(G_2))$

Hinweis: In den Aufgaben 1 und 2 können auftretende Additionen und Multiplikationen mit dem Taschenrechner durchgeführt werden.
Da in der Klausur keine Taschenrechner erlaubt sein werden, sollten die Übungen nur dann mit Hilfe eines Taschenrechners bearbeitet werden, wenn dies explizit erwähnt wird.

Abgabe am 30. Mai 2003 vor der Vorlesung