Wolfgang K. Seiler
Tel. 2515

A5, C201

13. April 2018

7. Übungsblatt Zahlentheorie

Aufgabe 1: *(7 Punkte)*

a) $F_n = 2^{2^n} + 1$ sei die n-te Fermat-Zahl. Zeigen Sie: Für alle $n \in \mathbb{N}_0$ ist $2^{F_n - 1} \equiv 1 \bmod F_n$, so daß ein Fermat-Test mit Basis zwei kein F_n als zusammengesetzt erkennen kann.

b) Zeigen Sie, daß für $n \geq 2$ sogar $2^{(F_n-1)/2} \equiv 1 \bmod F_n$ ist!

c) Zeigen Sie mit Eulers Methode, daß jeder ungerade Primteiler p von $a^{2^n} + b^{2^n}$ entweder ein gemeinsamer Teiler von a und b ist oder aber kongruent eins modulo 2^{n+1}.
Hinweis: Überlegen Sie sich, daß für $p \nmid \operatorname{ggT}(a, b)$ mindestens einer der beiden Quotienten a/b und b/a in $\mathbb{F}_p$ existiert, und untersuchen Sie seine Ordnung in $\mathbb{F}_p^\times$!

d) Zerlegen Sie ohne Computerhilfe die Zahl $N = 2^8 + 5^8 = 390\,881$ in ihre Primfaktoren!

Aufgabe 2: *(6 Punkte)*

a) Zeigen Sie, daß $\prod\limits_{k=0}^{n-1} F_k = F_n - 2$ ist!

b) Folgern Sie, daß zwei verschiedene Fermat-Zahlen F_n und F_m stets teilerfremd sind!

c) Machen Sie daraus einen neuen Beweis für den Satz, daß es unendlich viele Primzahlen gibt!

Aufgabe 3: *(7 Punkte)*

Die r-te Mersenne-Zahl ist $M_r = 2^r - 1$.

a) Zeigen Sie: Ist r ein Teiler von s, so ist M_r Teiler von M_s.

b) Ist M_r eine Primzahl, so auch r.

c) Finden Sie die kleinste Primzahl p, für die M_p *keine* Primzahl ist!

d) r sei eine ungerade Zahl. Welche Werte kann M_r modulo 3 und modulo 5 annehmen?

e) Eine natürliche Zahl heißt *vollkommen,* wenn sie gleich der Summe aller von ihr selbst verschiedener Teiler ist. Zeigen Sie: Ist M_p eine Primzahl, so ist $2^{p-1} M_p$ eine vollkommene Zahl.
Bemerkung: Mit Ausnahme der Zeit von 1989–1992 war seit 1952 die größte bekannte Primzahl immer eine Mersenne-Zahl, da es für diese einen einfachen Primalitätstest gibt. Derzeit sind fünfzig Mersennesche Primzahlen bekannt; die größte ist $M_{77\,232\,917}$ mit 23 249 425 Dezimalstellen; siehe www.mersenne.org.

Abgabe bis zum Donnerstag, dem 19. April 2018, um 10.10 Uhr