WOLFGANG K. SEILER
Tel. 2515

A5, C201

18. März 2014

6. Übungsblatt Zahlentheorie

Aufgabe 1: *(3 Punkte)*

Die Zahl $p = (6t+1)(12t+1)(18t+1)$ sei eine CARMICHAEL-Zahl.

a) Zeigen Sie: Es gibt $1296t^3$ Zahlen a zwischen 1 und $p-1$, für die p den FERMAT-Test besteht.

b) Wie verhält sich die Wahrscheinlichkeit dafür, daß p für eine zufällige Basis a den FERMAT-Test besteht, wenn t gegen unendlich geht?

Aufgabe 2: *(2 Punkte)*

Zeigen Sie, daß 41041 eine CARMICHAEL-Zahl ist!

Aufgabe 3: *(6 Punkte)*

a) $F_n = 2^{2^n} + 1$ sei die n-te FERMAT-Zahl. Zeigen Sie: Für $n \geq 2$ ist $2^{(F_n-1)/2} \equiv 1 \bmod F_n$.

b) 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 $\mathbb{F}_p^\times$!

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

Aufgabe 4: *(6 Punkte)*

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

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

c) Folgern Sie daraus, daß es unendlich viele Primzahlen gibt!

Aufgabe 5: *(3 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) 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. Der derzeitige Rekordhalter ist $M_{57\,885\,161}$ mit fast $17\frac{1}{2}$ Millionen Dezimalstellen; siehe www.mersenne.org.

Abgabe bis zum Dienstag, dem 25. März 2014, um 11.55 Uhr