Aufgaben zur Vorlesung
Algorithmen für Zahlen und Primzahlen
Wintersemester 2006/07

Die Lösungen sind in logisch und grammatisch einwandfreien Sätzen zu formulieren. Neben dem unmittelbaren Ergebnis muss auch der Lösungsweg erkennbar sein, also insbesondere die mit dem Computer ausgeführten Rechnungen. Umfangreiche Zwischen- oder Endergebnisse können abgekürzt oder verbal dargestellt werden.

Serie 4 — Abgabetermin: 21.11.

12. (a) Berechnen Sie `CRA((2,11),(5,13),(3,19),(7,23))` und überprüfen Sie das Ergebnis auf Richtigkeit. (2 Pkt.)

    (b) Finden Sie eine Formel für die Berechnung der Restklasse

    $$u = u(x, y, z) \pmod{1495}$$

    mit

    $$u \equiv x \pmod 5,\ u \equiv y \pmod{13},\ u \equiv z \pmod{23}$$

    (4 Pkt.)

13. Die Fibonaccizahlen, die durch die rekursive Bildungsvorschrift $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ für $n > 2$ definiert werden, haben einige bemerkenswerte Eigenschaften.

    (a) Zeigen Sie, dass zwei benachbarte Fibonaccizahlen zueinander teilerfremd sind. (2 Pkt.)

    (b) Nach (a) ist $F_{n-1} \pmod{F_n}$ für $n > 2$ eine prime Restklasse und damit invertierbar. Stellen Sie eine Vermutung für eine Formel zur Berechnung von $F_{n-1}^{-1} \pmod{F_n}$ auf und beweisen Sie diese. (3 Pkt.)

    (c) Beweisen Sie die Beziehung (3 Pkt.)

    $$F_{m+n} = F_{n-1}F_m + F_nF_{m+1} \text{ für } m, n > 1$$

(d) Zeigen Sie, dass F_m ein Teiler von F_n ist, wenn m ein Teiler von n ist. (3 Pkt.)
Damit ist F_n $(n > 4)$ höchstens dann prim ist, wenn n selbst prim ist. Finden Sie alle $n < 1000$, für welche F_n prim ist. (3 Pkt.)

(e*) Beweisen Sie die Beziehung (4 Pkt.)

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}$$