Blatt 4

Prof. Dr. N-P. Skoruppa und Dr. Jan Fricke Abgabe: Fr, 2. Mai 08
www.countnumber.de

Aufgabe 1. Finden Sie die kleinsten zusammengesetzten[1] ganzen Zahlen m, die folgende Eigenschaft haben:

Für jede zu m teilerfremde Zahl a gilt $a^{m-1} \equiv 1 \bmod m$.

Aufgabe 2. Auf der Internetseite zur Vorlesung ist eine Nachricht hinterlegt, die folgendermassen verschlüsselt wurde: Zunächst wurde jedes Zeichen des Textes der Nachricht (Buchstaben, Satzzeichen, Leerzeichen, ...) mittels der Python-Funktion `ord()` in eine Zahl $0 \leq z < 256$ verwandelt[2], dann wurde jede dieser Zahlen z mit einer geheimen Zahl M multipliziert, und schließlich wurde die resultierende Folge von Zahlen m nach dem RSA-Verfahren mit öffentlichen Schlüsseln N und e Zahl für Zahl chiffriert. Die Folge der chiffrierten Zahlen und den öffentlichen Schlüssel finden Sie auf der Internetseite zur Vorlesung. Entschlüsseln Sie die Nachricht! Hinweis: Eine der in N aufgehenden Primzahlen können Sie finden, indem Sie die Geburtsjahre von Euler, Gauß und Andrew Wiles addieren und mit der Summe der ersten 10 Glieder der Fibonacci-Folge $0, 1, 1, 2, \ldots$ multiplizieren — das Ergebnis sei die Zahl x — und die Seite `www.nskoruppa.de/x` aufrufen.

Aufgabe 3. Man bestimme ohne Rechenhilfsmittel die jeweils letzten drei Dezimalziffern von 7^{9999}, 11^{9999} und 13^{9999}. (Sie dürfen Ihr Ergebnis natürlich mit einem CAS überprüfen.)

Aufgabe 4. Man finde alle ganzen Zahlen $1 \leq n \leq 1000$ mit der folgenden Eigenschaft: Ist a mit $2 \leq a \leq n$ teilerfremd zu n, dann ist a eine Primzahl.

Beispiele: 12 ist so eine Zahl: Zu 12 teilerfremd sind 5, 7 und 11, das sind alles Primzahlen.

10 ist nicht so eine Zahl: Zu 10 teilerfremd sind 3, 7 und 9, aber 9 ist keine Primzahl.

Zusatzaufgabe: Zeigen Sie, dass es keine solchen Zahlen > 1000 gibt.

Hinweis: Benutzen Sie den Satz von Tschebyscheff (für $n > 1$ gibt es zwischen n und $2n$ eine Primzahl).

---

[1] Eine natürliche Zahl $m > 1$ heißt zusammengesetzt, falls sie keine Primzahl ist.

[2] Für die Rückverwandlung können Sie `chr()` benutzen