Wolfgang K. Seiler
Tel. 2515

B6, B4.08

21. Oktober 2022

7. Übungsblatt Kryptologie

Aufgabe 1:

a) Schreiben Sie $x = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5}}}}$ als gewöhnlichen Bruch!

b) Berechnen Sie die Kettenbruchentwicklung von $\sqrt{15}$!

c) Welche Zahl wird durch den periodischen Kettenbruch

$$y = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}$$

dargestellt? *(Hinweis: Betrachten Sie $z = 1 + 1/y$.)*

Aufgabe 2:

Finden Sie einen Bruch mit höchstens zweistelligem Nenner, der den Bruch $\frac{13579}{24680}$ mit einem Fehler von höchstens einem Tausendstel approximiert!

Aufgabe 3:

a) Die Zahl $N = 955\,353\,719$ ist das Produkt zweier nicht garzu weit voneinander entfernter Primzahlen. Finden Sie diese!

b) Wie viele Versuche hätten Sie gebraucht, wenn Sie nach der klassischen Vorgehensweise Fermats für $x = 1, 2, 3, \ldots$ nacheinander getestet hätten, ob $N + x^2$ ein Quadrat ist?

Aufgabe 4:

Bereits 1931 entwickelten D.H. Lehmer und R.E. Powers folgende Methode zur Faktorisierung ganzer Zahlen: Ist a/b eine Konvergente der Kettenbruchentwicklung von $\sqrt{N}$; so ist $q = a^2 - Nb^2$ eine relativ kleine Zahl; falls $q = x^2$ eine Quadratzahl sein sollte, haben wir eine Relation der Form $a^2 \equiv x^2 \bmod N$, die uns vielleicht zu einer Faktorisierung von N führt.

a) Warum verwenden D.H. Lehmer und R.E. Powers Kettenbrüche und nicht irgendwelche rationalen Approximationen von $\sqrt{N}$?

b) Berechnen Sie die ersten fünf Konvergenten a_i/b_i der Kettenbruchentwicklung von $\sqrt{15}$!

c) Welche davon liefern direkt eine Relation der Form $a_i^2 \equiv x_i^2 \bmod 15$, und wann führt diese Relation zu einer Faktorisierung?

d) Was ändert sich, wenn Sie anstelle der Relation $a_i^2 - 15b_i^2 = q_i$ die Relation

$$a_i^2 \equiv (q_i \bmod 15) \bmod 15$$

verwenden?

Besprechung am Mittwoch, dem 25. Oktober 2022, um 15.30 Uhr