Mathematische Grundlagen der Kryptografie

6. Übungsblatt, SS 2006 — 27.06.2006

54. Faktorisieren Sie mit der FERMAT-Faktorisierung 99296873 und 88169891.

*55. Zeigen Sie: Wenn $n \in \mathbb{N}$ einen Faktor in der Menge

$$\{\sqrt{n} - \sqrt[4]{n}, \ldots, \sqrt{n}, \ldots, \sqrt{n} + \sqrt[4]{n}\}$$

hat, dann funtioniert die FERMAT-Faktorisierung bereits beim ersten Schritt (also für $t = \lfloor\sqrt{n}\rfloor + 1$).

*56. Zeigen Sie, dass man mit der Wahl $k = 2$ (oder allgemeiner $k \in \mathbb{N}$ mit $2|k$ und $4 \not| k$) eine große ungerade Zahl n mit der verallgemeinerten FERMAT-Faktorisierung nicht faktorisieren kann.
Bem: Die verallgemeinerte FERMAT-Methode heißt, man beginnt (für kleine k) mit $t = \lfloor\sqrt{kn}\rfloor + 1$ und erhöht solange, bis man ein Quadrat gefunden hat.

57. Faktorisieren Sie die Zahlen 29895581 und 19578079 mit der verallgemeinerten FERMAT-Methode. Benutzen Sie bei diesem Beispiel nur elementarste Funktionen von `Mathematica`.

In den nächsten beiden Aufgaben sei k jene Zahl, die im POLLARD'schen $p-1$-Verfahren benutzt wird, also für eine gegebene Schranke $B \in \mathbb{N}$ sei

$$k = \prod_{\substack{q_i \in \mathbb{P} \\ q_i^{e_i} \leq B}} q_i^{e_i}$$

wobei $q_1, \ldots, q_L$ die Primzahlen $\leq B$ sind, und $e_i \geq 1$ die größtmögliche Potenz sei, sodass $q_i^{e_i} \leq B$ gilt.

*58. Zeigen Sie, dass $k = \mathrm{kgV}(1, \ldots, B)$ gilt, also k ist das kleinste gemeinsame Vielfache aller Zahlen $1, 2, \ldots, B-1, B$.

*59. Im $p-1$-Verfahren überprüft man den Wert $\mathrm{ggT}(a^k - 1, n)$ für ein zufälliges $a \in \{1, \ldots, n-1\}$. Angenommen man wählt $a = 2$. Dann gibt es natürliche Zahlen $n = p \cdot q$ mit $p < q$ Primzahlen, sodass

$$\mathrm{ggT}(2^k - 1, n) = \mathrm{ggT}(a^{\mathrm{kgV}(1,\ldots,B)} - 1, n) \in \{1, n\}$$

für alle Schranken B, d. h. solche Zahlen lassen sich nie mit der $p-1$-Methode (und $a = 2$) faktorisieren.
Bestimmen Sie alle solche Zahlen $n \leq 1000$.

60. Faktorisieren Sie $n = 89073489106939240931551386805730106 1$ mit der $p-1$-Methode. (Die Zahl befindet sich auch in der Datei `bsp60.txt`.)

59. Man faktorisiere die Zahl 7064009 mithilfe des quadratischen Siebes.

60. Faktorisieren Sie mit dem quadratischen Sieb die Zahl $n = 11111111111111111$ (das sind 17 Einser). Das muss kein lauffähiges Programm sein, wichtig ist, dass jeder Schritt des quadratischen Siebs klar hervorgeht.