Kryptologie

Übung, LVA 405.321
C. Fuchs

4. Übungsblatt, SS 2022

30.03.2022

1. Man kann den Euklidischen Algorithmus noch beschleunigen indem man Division mit negativem Rest erlaubt, also $r_j = q_{j+2}r_{j+1} - r_{j+2}$ oder $r_j = q_{j+2}r_{j+1} + r_{j+2}$ je nachdem wo das kleinere r_{j+2} entsteht. Dadurch gilt stets $r_{j+2} \leq r_{j+1}/2$. Vergleiche die Laufzeit für die Paare $(a, b) = (26, 19), (187, 160), (841, 160)$.

2. *Multiplikation zweier großer Binärzahlen*: Sei k die Bitlänge von a, b und ℓ eine fixe ganze Zahl, die sehr viel kleiner als k ist. Man wähle m_i mit $1 \leq i \leq r$, $\ell/2 < m_i < \ell$ für alle i und $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i \neq j$. Wähle $r = \lfloor 4k/\ell \rfloor + 1$. Die Zahl a wird nun als ein r-Tupel $(a_1, \ldots, a_r)$ gespeichert, wobei $a \equiv a_i \pmod{2^{m_i} - 1}$ ist. Zeige, dass a, b und $a \cdot b$ eindeutig bestimmt sind durch das zugehörige r-Tupel und schätze die Laufzeit ab, die man braucht, um das r-Tupel von $a \cdot b$ aus denen von a und b zu berechnen. Warum ist die Wahl $2^{m_i} - 1$ günstig?

3. Sind die Module m_i beim chinesischen Restsatz sehr groß, dann gibt es folgende schnellere Lösungsmöglichkeit, als die in der Vorlesung gezeigte:

   - Die zwei Gleichungen $x \equiv a_1 \mod m_1, x \equiv a_2 \mod m_2$ haben für relativ prime m_1, m_2 die Lösung $x = a_1 + (a_2 - a_1)m_1 \cdot b$ mit $b = m_1^{-1} \mod m_2$.
   - Hat man r Kongruenzen der Form $x \equiv a_i \mod m_i$ für $1 \leq i \leq r$ mit paarweise relativ primen m_i, so ersetzt man die ersten beiden Kongruenzen durch die einzelne Kongruenz $x \equiv a \mod m_1 m_2$, mit a wie vorher. Das wiederholt man sukzessive, bis man eine Lösung für alle Gleichungen hat.

   Analysiere die Laufzeit im Vergleich zum normalen Lösungsverfahren.

4. Ist die Gleichungsanzahl beim Chinesischen Restsatz ≥ 17, dann kann man einen weiteren Kniff einbauen, indem man die Idee von Aufgabe 3 mit einer "Divide und Conquer"-Strategie verbindet, d. h. man teilt die Kongruenzen in gleich große Hälften und verfährt rekursiv weiter. Zum Schluß löst man die einzelnen Teile wie in der letzten Aufgabe. Analysiere wieder die Laufzeit.