Mathematische Grundlagen der Kryptografie

1. Übungsblatt, SS 2006 — 14.03.2006

1. Berechnen Sie den $\mathrm{ggT}(360, 296)$ auf zwei verschiedene Arten: (a) durch Berechnung der Primfaktorzerlegung der beiden Zahlen und damit der Primfaktorzerlegung des ggT; (b) durch den Euklidischen Algorithmus.

2. Für jedes der folgenden Paare finde man den ggT mithilfe des Euklidischen Algorithmus und stelle ihn als Linearkombination der beiden Zahlen dar:

   $$(a)\, 26, 19;\ \ (b)\, 187, 160;\ \ (c)\, 841, 160.$$

3. Berechnen Sie die Inversen (falls vorhanden) von

   (a) 15 im Restklassenring $\mathbb{Z}_{49}$.

   (b) 23 im Restklassenring $\mathbb{Z}_{59}$.

   (c) 26 im Restklassenring $\mathbb{Z}_{143}$.

4. Man kann den Euklidischen Algorithmus noch beschleunigen indem man Divisionen 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 $r_{j+2} \leq \frac{1}{2}r_{j+1}$. Implementieren Sie beide Varianten in `Mathematica` und vergleichen Sie die Laufzeit. (**Hinweis:** Der Befehl lautet `Timing[`*expr*`]`.)

5. Zeigen Sie:

   $$\mathrm{ggT}(2^n - 1, 2^m - 1) = 1 \ \Leftrightarrow\ \mathrm{ggT}(n, m) = 1.$$

6. Konstruieren Sie ein Element der Ordnung 103 in der primen Restklassengruppe $\mathbb{Z}_{1237}$

7. Die Euler'sche φ-Funktion ist gegeben durch

   $$\varphi(n) = \#\{1 \leq k < n \mid \mathrm{ggT}(n, k) = 1\} = |\mathbb{Z}_n^*|.$$

   Beweisen Sie, dass $\varphi(n)$ multiplikativ ist, sprich $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$, wann immer $\mathrm{ggT}(m, n) = 1$.

8. Überlegen Sie sich unterschiedliche Implementationen von $\varphi(n)$ in `Mathematica`. Verwenden Sie dabei unterschiedliche Definitionen von φ. Vergleichen Sie die Laufzeit ihrer Funktion mit der in `Mathematica` vorhandenen Funktion `EulerPhi[n]`.

9. Berechnen Sie $3^{1000000} \bmod 77$.

10. Beweisen Sie den Satz von Wilson: für jede Primzahl p gilt

$$(p-1)! \equiv -1 \bmod p.$$

11. 5 Seeleute sammeln auf einer Insel einen Haufen Kokosnüsse und beschließen, diesen am nächsten Morgen untereinander aufzuteilen. Während der Nacht wacht einer der Seeleute auf, zählt die Kokosnüsse, gibt eine davon dem Affen, der immer um das

    Lager herumschwänzelte und nimmt sich vom Rest genau ein Fünftel mit. Später in derselben Nacht, wacht ein zweiter Seemann auf und verfährt auf die exakt selbe Weise und es kam, dass auch die drei restlichen Seeleute dasselbe taten (eine Nuss dem Affen, vom Rest ein Fünftel für sich), ohne dass einer was vom anderen bemerkte.
    Am nächsten Morgen, als alle erwachen, schenken die Seeleute dem wartenden Affen eine Nuss und teilen den Rest in fünf gleich große Teile. Wieviele Nüsse hatten die Seeleute ursprünglich gesammelt?

12. **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 $1 \leq i \leq r$, $\frac{\ell}{2} < m_i < \ell$ für alle i und $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i \neq j$. Wir wählen $r = \lfloor \frac{4k}{\ell} \rfloor + 1$. Die Zahl a wird nun als ein r-Tupel $(a_1, \ldots, a_r)$ gespeichert, wobei $a \equiv a_i \bmod 2^{m_i} - 1$ ist.
    Zeigen Sie, dass a, b und $a \cdot b$ eindeutig bestimmt sind durch das zugehörige r-Tupel und schätzen Sie 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?