Mathematische Grundlagen der Kryptografie

2. Übungsblatt, SS 2006 — 02.05.2006

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

    - Die zwei Gleichungen

      $$x \equiv a_1 \mod m_1 \qquad x \equiv a_2 \mod m_2$$

      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.

    Stellen Sie `Timing`-Vergleiche an.

14. Ist die Gleichungsanzahl beim Chinesischen Restsatz ≥ 17, dann kann man einen weiteren Kniff einbauen, indem man die Idee von Aufgabe 13 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.
    Stellen Sie abermals `Timing`-Vergleiche an.

*15. Schreiben Sie ein Programm in `Mathematica`, dass den chinesischen Restsatz implementiert, wenn man die Bedingung an die paarweise Teilerfremdheit der m_i außer Acht lässt. Das Programm soll nichts ausgeben, wenn keine Lösung existiert (z. B. $x \equiv 1 \mod 5, x \equiv 3 \mod 25$) und sonst die betragskleinste Lösung.

    Hinweise:

    - Zeigen Sie, dass das System

      $$x \equiv a_1 \mod m_1 \qquad x \equiv a_2 \mod m_2 \tag{1}$$

      genau dann eine eindeutige Lösung hat, wenn $a_1 - a_2$ durch $\mathrm{ggT}(m_1, m_2)$ teilbar ist, und dass, wenn es eine Lösung gibt, diese eindeutig ist modulo $\mathrm{kgV}(m_1, m_2)$.
    - Geben Sie eine explizite Formel für die Lösung von (1) an, wenn eine solche existiert.

- Man behandle ein System von r Gleichungen, indem man die ersten beiden zu einer zusammenfasst und damit das System auf ein kleineres reduziert.

16. Berechnen Sie alle Lösungen der Kongruenzen $27x \equiv 72 \bmod 900$ und $9x \equiv 21 \bmod 12$.

17. Konstruieren Sie die folgenden endlichen Körper: $\mathbb{F}_{27}, \mathbb{F}_{25}$, d. h. bestimmen Sie ein irreduzibles Polynom und geben Sie die Liste der Elemente an. Bestimmen Sie außerdem ein primitives Element γ für die jeweilige multiplikative Gruppe und schreiben Sie alle Elemente des Körpers als Potenzen von γ.

*18. Zeigen Sie, dass in einem Körper K der Charakteristik p der sogenannte "freshman's dream" gilt: Für alle $a, b \in K$ und alle $n \geq 0$ ist

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}.$$

19. Konstruieren Sie den $\mathbb{F}_{3^8}$ mit `Mathematica` und finden Sie auch hier ein primitives Element. Verwenden Sie dabei nicht das `Mathematica`-Paket `<<Algebra‘Finite Fields‘`. Benutzen Sie es anschließend um Ihre Ergebnissen zu überprüfen.

20. Finden Sie für $p = 2, 3, 5, 7, 11, 13, 17$ jeweils die kleinste positive ganze Zahl, welche $\mathbb{F}_p^*$ erzeugt und berechne wieviele der Zahlen $1, 2, 3, \ldots, p-1$ noch Erzeuger sind.

*21. Unter welchen Bedingungen an n und p (p prim) ist jedes Element außer 0,1 ein Erzeuger von $\mathbb{F}_{p^n}^*$?