Mathematische Grundlagen der Kryptografie

3. Übungsblatt, SS 2006 — 16.05.2006

*22. Man beweise: Eine rein quadratische Kongruenz $x^2 \equiv a \bmod m$ mit $\mathrm{ggT}(a, m) = d =: e^2 f$, wo f quadratfrei ist, ist genau dann lösbar, wenn $\mathrm{ggT}(f, \frac{m}{d}) = 1$ und $f\frac{a}{d}$ ein quadratischer Rest mod $\frac{m}{d}$ ist.

23. Man zeige, dass für jede ungerade Zahl a gilt:

    (a) $x^2 \equiv a \bmod 2$ hat mod 2 genau eine Lösung,

    (b) $x^2 \equiv a \bmod 4$ ist genau dann lösbar, wenn $a \equiv 1 \bmod 4$, und die Kongruenz besitzt in diesem Fall genau zwei mod 4 inkongruente Lösungen,

    (c) $x^2 \equiv a \bmod 8$ ist genau dann lösbar, wenn $a \equiv 1 \bmod 8$, und die Kongruenz besitzt in diesem Fall genau vier mod 8 inkongruente Lösungen.

*24. Sei p eine ungerade Primzahl, und seien $a, b \in \mathbb{Z}$ zu p teilerfremd. Man zeige, dass dann gilt:

    (a) Aus $a \equiv b \bmod p$ folgt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

    (b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

    (c) $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$,

    (d) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

*25. Seien p_1, p_2 verschiedene Primzahlen, $n = p_1 p_2$ und $a \in \mathbb{Z}$. Man zeige, dass alle Lösungen von

$$x^2 \equiv a \bmod n$$

mit Hilfe der quadratischen Kongruenzen

$$x_1^2 \equiv a \bmod p_1$$
$$x_2^2 \equiv a \bmod p_2$$

bestimmt werden können.

26. Man überprüfe, ob 138 ein quadratischer Rest mod 493 ist.

27. Man bestimme sämtliche Lösungen der Kongruenz $x^2 \equiv 81 \bmod 247$.

28. Desgleichen verfahre man für die Kongruenz $x^2 \equiv 82 \bmod 143$.

29. Schreiben Sie ein `Mathematica`-Programm um den Alorithmus von TONELLI zu implementieren.

*30. Der folgende Algorithmus nach SHANKS ist eine leichte Verbesserung des obigen Algorithmus.
Sei p eine Primzahl und a ein quadratischer Rest modulo p. Man schreibe $p-1 = 2^t q$, q ungerade. Sei h ein quadratischer Nichtrest modulo p.
Setze $z := h^q \ (p)$. Dann gilt: $z^{2^{t-1}} \equiv -1 \ (p)$ wegen dem EULERschen Kriterium.

- Definiere v, w durch: $v \equiv a^{\frac{q+1}{2}} \ (p)$, $w \equiv a^q \ (p)$.
- Ist $w = 1$, dann ist v die gesuchte Lösung für $x^2 \equiv a \ (p)$.
- Wenn nicht, dann bestimmt man das kleinste k sodass $w^{2^k} \equiv 1 \ (p)$ gilt. Da $w^{2^{t-1}} \equiv 1 \ (p)$ ist, muss $k \leq t-1$ sein. Dann ersetzt man $z \leftarrow z^{2^{t-k}} \ (p)$, $t \leftarrow k$, $v \leftarrow v \cdot z^{2^{t-k-1}} \ (p)$ und $w \leftarrow w \cdot z^{2^{t-k}}$ und überprüft wieder, ob $w = 1$ gilt, ansonsten wiederholt man den Vorgang.
  Der Algorithmus terminiert, da t in jedem Schritt zumindest um 1 verringert wird.

Zeigen Sie, dass in jedem Schritt des Algorithmus' die Kongruenzen

$$a \cdot w \equiv v^2 \ (p), \qquad z^{2^{t-1}} \equiv -1 \ (p), \qquad w^{2^{t-1}} \equiv 1 \ (p)$$

erhalten bleiben und dass der Algorithmus funktioniert.

31. Testen Sie die beiden Algorithmen anhand einiger zufällig generierter Beispiele und vergleichen Sie die Lösungen mit jenen von `Solve[{`$x^2 = a$`,Modulus==p}]`. Vergleichen Sie auch die Laufzeiten.