Dr. Dirk Frettlöh 8.5.2019

Übungen zur Vorlesung Kryptographie

Blatt 5

Aufgabe 17: (Legendresymbole berechnen)
Berechnen Sie die Werte der folgenden Legendresymbole von Hand, nur mit Hilfe der Rechenregeln L1 bis L6 aus der Vorlesung. (Obacht: unten muss also immer eine Primzahl stehen! 139, 383 und 997 *sind* Primzahlen.)

$$\left(\frac{102}{139}\right), \quad \left(\frac{164}{383}\right), \quad \left(\frac{296}{997}\right).$$

Geben Sie bei jeder Umformung an, welche Regel Sie benutzen.

Aufgabe 18: (Zaubern mit Legendresymbolen)
Zeigen Sie:
(a) Falls p eine Primzahl ist mit $p \equiv 1 \bmod 12$, dann ist 3 ein quadratischer Rest $\bmod p$.
(b) Ist $p > 3$ eine Primzahl, die Teiler von $a^2 + 3$ ist (für ein $a \in \mathbb{N}$), dann ist $p \equiv 1 \bmod 3$.

Aufgabe 19: (Eulerlügner bzw Solovay-Strassen-Lügner)
Sei $n \in \mathbb{N}$ keine Primzahl, aber ungerade. Eine Zahl $a \in Z_n$ heißt **Eulerlügner** mod n, falls $\mathrm{ggT}(a, n) = 1$ und $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$.

Finden Sie jeweils eine ungerade Nicht-Primzahl n, so dass die Anzahl aller Eulerlügner für n

(a) genau 1 ist;
(b) genau 2 ist;
(c) ungerade ist, und größer als 1;
(d) genau 80 ist.

Aufgabe 20: (Rechnen mit Jacobisymbolen)
(a) Zeigen Sie: Ist a ein Eulerlügner mod n, so ist auch $n - a$ ein Eulerlügner mod n.
(b) Beweisen Sie die Rechenregel J4 für das Jacobisymbol: $\left(\frac{nn'}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{n'}{m}\right)$.

Sie dürfen die Rechenregeln L1-L6 für die Legendresymbole benutzen.

Einige Aufgaben können/sollten auch durch Pogrammieren gelöst werden. Falls Sie Programmcode abgeben, beschreiben Sie auf jeden Fall auch, wie Sie vorgingen.

Abgabe: Mittwoch 15.5.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Dienstag	Philipp Braukmann	pbraukmann@techfak.uni-bielefeld.de
Donnerstag	Oliver Tautz	otautz@techfak.uni-bielefeld.de