Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 4

In der letzten Tutoriumsstunde wurde ein Algorithmus zum Quadratwurzelziehen modulo einer ungeraden Primzahl behandelt:

Es soll eine Quadratwurzel aus $a \in \mathbb{Z}_p$ gefunden werden.
Man stelle dazu zunächst fest, ob a überhaupt ein Quadrat modulo p ist, indem man mit dem quadratischen Reziprozitätsgesetz die Gleichung $\left(\frac{a}{p}\right)=1$ überprüft bzw. nachrechnet, daß $a^{\frac{p-1}{2}} = 1 \bmod p$.

Es sei $p-1=2^{\alpha}u$, wobei u ungerade.

Aufgabe 1:
a) Zeigen Sie, daß a^u eine $2^{\alpha-1}$-te Einheitswurzel in $\mathbb{Z}_p^*$ ist.
b) Zeigen Sie: Wenn $\left(\frac{\zeta}{p}\right)=-1$, so ist $\eta := \zeta^u$ eine 2^{α}-te primitive Einheitswurzel in $\mathbb{Z}_p^*$.

Man beschaffe sich nun η wie in b) und setze $r := a^{\frac{u+1}{2}}$. Dann ist $r^2 = a^{u+1} = a^u \cdot a$, d.h. bis auf eine $2^{\alpha-1}$-te Einheitswurzel ist r die gesuchte Quadratwurzel. Eine $2^{\alpha-1}$-te Einheitswurzel ist aber eine gerade Potenz von η, und man muß jetzt nur einen entsprechenden Korrekturfaktor in r anbringen.

c) Sei H eine zyklische Gruppe der Ordnung 2^{α} mit dem Erzeuger η und sei $g \in H$.
Finden Sie einen effektiven Algorithmus an zur Berechnung des Exponenten $x \in \mathbb{N}$, für den $g = \eta^x$.
(Effektiv wäre eine Laufzeit proportional zu α, nicht zu 2^{α}.)

e) Finden Sie mit der oben beschriebenen Methode eine Quadratwurzel von 5 in $\mathbb{Z}_{241}$. Benutzen Sie zur Findung des in b) beschriebenen Korrekturfaktors Ihre in c) gefundene Methode.

f) Schreiben Sie ein Pari-Programm `sqr(a,p)`, welches diese Methode implementiert.