

### **Karatsuba-Multiplikation in endlichen Körpern**

Multipliziert man  $n$ -stellige ganze Zahlen wie in der Schule gelernt, so muss man  $n^2$  Operationen durchführen. Karatsuba hat gezeigt, dass sich durch geschicktes Zusammenfassen von Termen dieser Aufwand auf  $n^{1.584\dots}$  reduzieren lässt. Knuth zeigt, dass sich auf diese Weise sogar  $n^{1+\epsilon}$  erreichen lässt, allerdings wird der Verwaltungsaufwand dabei mit sinkendem  $\epsilon$  immer größer.

In dieser Arbeit soll das Analogon der Multiplikation nach Karatsuba für endliche Körper ausgearbeitet werden. Diese Multiplikation soll anschließend auf das Wurzelziehen modulo  $p$  angewandt werden.