– Praktikumsaufgabe 5 –

Thema: *Modulare Exponentiation und Diskreter Logarithmus*

Zielstellung: Kennenlernen der Modularen Exponentiation und des Diskreten Logarithmus

1. Implementieren Sie ein Werkzeug, das die modulare Exponentiation verwirklicht, also den Ausdruck
$$y = f(x) = g^x \bmod p$$
berechnet. Die Aufrufsyntax soll
```
./modexp <g> <x> <p>
```
lauten. Nutzen Sie die aus der Vorlesung bekannte Technik der binären Exponentiation.

2. Lösen Sie (ggf. unter Nutzung obigen Werkzeugs)

   a) $y = 4^{13} \bmod 497$,

   b) $4^x \bmod 11 = 3$,

   c) $19^x \bmod 65537 = 10348$.

   Wie lange benötigt der Rechner für den Fall c) in etwa?