Kryptologie

Übung, LVA 405.321
C. Fuchs

12. Übungsblatt, SS 2022

08.06.2022

1. Zeige, dass

$$\sum_{i=0}^{n-m}(-1)^i\frac{1}{m+i}\binom{n-m}{i}=\int_0^1 x^{m-1}(1-x)^{n-m}dx=\frac{1}{m}\binom{n}{m}^{-1}$$

   für alle $1\leq m\leq n$ gilt. Folgere daraus, dass $\mathrm{kgV}(1,2,\ldots,n)>2^n$ für alle $n\geq 7$ erfüllt ist.

2. Sei p ein Primteiler von n. Zeige, dass aus $(X+a)^n\equiv X^n+a \bmod (n,X^r-1)$ auch $(X+a)^m\equiv X^m+a \bmod (p,X^r-1)$ für alle $m\in\{(n/p)^ip^j;i,j\geq 0\}$ folgt.

3. Zeige für $\ell=\lfloor\sqrt{\varphi(r)}\log n/\log 2\rfloor$ und $t>(\log n/\log 2)^2$, dass

$$n^{\sqrt{t}}<\binom{t+\ell}{t-1}.$$

4. Erstelle ein Pratt-Zertifikat zu 104729.