12. Bestimmen Sie ein Polynom $f \in \mathbb{F}_5[X]$ mit $f(0) = f(1) = f(4) = 1$ und $f(2) = f(3) = 3$.

13. Wenn die Elemente von $\mathcal{E}(\mathbb{F}_q)$ als Potenzen eines fixen primitiven Elements $b \in \mathbb{F}_q$ dargestellt werden, dann wird die Addition in $\mathbb{F}_q$ durch die Einführung des *Jacobi-Logarithmus* $L(n)$ erleichtert, der durch die Gleichung $1 + b^n = b^{L(n)}$ definiert wird, wobei der Fall $b^n = -1$ ausgeschlossen wird.

    (a) Zeigen Sie, dass dann $b^m + b^n = b^{m+L(m-n)}$ gilt, wannimmer L definiert ist.

    (b) Erstellen Sie eine Tabelle des Jacobi-Logarithmus für $\mathbb{F}_9$.

    (c) Dasselbe für $\mathbb{F}_{17}$.

14. Sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik p. Zeigen Sie, dass es für jedes Element von $\mathbb{F}_q$ genau eine p-te Wurzel in $\mathbb{F}_q$ gibt.

15. Sei $\mathbb{F}_q$ ein endlicher Körper mit ungeradem q. Zeigen Sie, dass ein Element $a \in \mathcal{E}(\mathbb{F}_q)$ genau dann eine Quadratwurzel in $\mathbb{F}_q$ besitzt, wenn $a^{(q-1)/2} = 1$.

16. Sei $\mathbb{F}_q$ ein endlicher Körper, $k \in \mathbb{N}$ und $a \in \mathcal{E}(\mathbb{F}_q)$. Zeigen Sie, dass a genau dann die k-te Potenz eines Elements aus $\mathbb{F}_q$ ist, wenn $q^{(q-1)/d} = 1$, wobei $d = \mathrm{ggT}(q-1, k)$.

17. Zeigen Sie: Jedes Element von $\mathbb{F}_q$ ist eine k-te Potenz eines Elements von $\mathbb{F}_q$ genau dann, wenn $\mathrm{ggT}(q-1, k) = 1$.

18. Sei $a \in \mathbb{F}_q$ und $n \in \mathbb{N}$. Zeigen Sie, dass das Polynom $X^{q^n} - X + na$ in $\mathbb{F}_q[X]$ durch $X^q - X + a$ teilbar ist.

19. Finden Sie eine normale Basis folgender Körper:

    (a) $\mathbb{F}_{17}$,

    (b) $\mathbb{F}_9$,

    (c) $\mathbb{F}_8$.

    Stellen Sie jeweils 1 durch die jeweilige Basis dar.

20. Bestimmen Sie

    (a) die primitiven 4-ten Einheitswurzeln in $\mathbb{F}_9$,

    (b) die primitiven 8-ten Einheitswurzeln in $\mathbb{F}_9$,

    (c) die primitiven 9-ten Einheitswurzeln in $\mathbb{F}_{19}$.

21. Sei ζ eine n-te Einheitswurzel über einem Körper K. Zeigen Sie, dass $1+\zeta+\zeta^2+\cdots+\zeta^{n-1} = n[\zeta = 1]$ (Iverson-Notation).

22. Sei K ein Körper und n eine ungerade natürliche Zahl. Zeigen Sie, dass $K^{(2n)} = K^{(n)}$.

23. Sei p eine Primzahl und $n \in \mathbb{N}$. Zeigen Sie, dass n ein Teiler von $\varphi(p^n - 1)$ ist.