1. Sei p eine Primzahl und $0 \leq j \leq p-1$. Zeigen Sie, dass $\binom{p-1}{j} \equiv (-1)^j \pmod{p}$.
2. Sei R ein kommutativer Ring der Charakteristik $p > 0$ (prim). Zeigen Sie, dass
$$(a-b)^{p-1} = \sum_{j=0}^{p-1} a^j b^{p-1-j}, \qquad a, b \in R.$$
3. Bestimmen Sie die Additions- und Multiplikationstabelle von $\mathbb{F}_2[X]/(X^3+X)$. Handelt es sich um einen Körper?
4. Gibt es ein Polynom $f \in \mathbb{F}_3[X]$, sodass $(X^2+1)f(X) \equiv 1 \pmod{X^3+1}$? Geben Sie gegebenenfalls ein solches an.
5. Gibt es ein Polynom $f \in \mathbb{F}_3[X]$, sodass $(X^4+X^3+X^2+1)f(X) \equiv (X^2+1) \pmod{X^3+1}$? Geben Sie gegebenenfalls ein solches an.
6. Bestimmen Sie $f(2)$ für $f(X) = X^{2007} + X^{308} \in \mathbb{F}_9[X]$.
7. Sei $f \in \mathbb{Z}[X]$ mit $f(0) \equiv f(1) \equiv 1 \pmod{2}$. Zeigen Sie: f hat keine ganzzahligen Nullstellen.
8. Zeigen Sie: $\sum_{\alpha \in \mathbb{F}_q} \alpha = 0$ für Primzahlpotenzen $q > 2$.
9. Bestimmen Sie alle primitiven Elemente (Erzeuger der multiplikativen Gruppe) von
   (a) $\mathbb{F}_7$,
   (b) $\mathbb{F}_{17}$,
   (c) $\mathbb{F}_9$.
10. Schreiben Sie alle Elemente von $\mathbb{F}_{25}$ als Linearkombination von Basiselementen über $\mathbb{F}_5$. Finden Sie ein primitives Element β von $\mathbb{F}_{25}$ und bestimmen Sie für jedes $\alpha \in \mathcal{E}(\mathbb{F}_{25})$ die kleinste nichtnegative ganze Zahl n mit $\alpha = \beta^n$.
11. Sei K ein Körper, dessen Einheitengruppe $\mathcal{E}(K)$ zyklisch ist. Zeigen Sie, dass K endlich ist.

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.

24. Die *Möbiussche μ-Funktion* $\mu : \mathbb{N} \to \{0, \pm 1\}$ ist folgendermaßen definiert:

$$\mu(n) = \begin{cases} (-1)^r, & \text{falls } n = p_1 \dots p_r \text{ für } r \geq 0 \text{ paarweise verschiedene Primzahlen } p_j, \\ 0, & \text{sonst.} \end{cases}$$

Zeigen Sie für $n \in \mathbb{N}$:

$$\sum_{d|n} \mu(d) = [n = 1] \qquad \text{(Iverson-Notation).}$$

25. Zeigen Sie die *Möbiussche Umkehrformel*: Seien $f : \mathbb{N} \to \mathbb{C}$ und $F : \mathbb{N} \to \mathbb{C}$ zwei Funktionen mit

$$F(n) = \sum_{d|n} f(d), \qquad n \in \mathbb{N}.$$

Zeigen Sie, dass dann

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d), \qquad n \in \mathbb{N}$$

gilt.

26. Beweisen Sie:

$$\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d, \qquad n \in \mathbb{N}.$$

Hier ist φ die Eulersche und μ die Möbiussche Funktion.

27. Sei r eine Primzahl und $k \in \mathbb{N}$. Zeigen Sie folgende Formel für das Kreisteilungspolynom G_{r^k}:

$$G_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \dots + x^{(r-1)r^{k-1}}.$$

28. Sei K ein Körper und $n \geq 2$. Zeigen Sie, dass das Polynom

$$x^{n-1} + x^{n-2} + \dots + x + 1$$

nur dann über K irreduzibel sein kann, wenn n eine Primzahl ist.

29. Zeigen Sie die folgenden Eigenschaften von Kreisteilungspolynomen:

(a) $G_{mp}(X) = G_m(X^p)/G_m(X)$ für eine Primzahl p und $m \in \mathbb{N}$ mit $p \nmid m$.

(b) $G_{mp}(X) = G_m(X^p)$ für alle $m \in \mathbb{N}$, die durch die Primzahl p teilbar sind.

(c) $G_{mp^k}(X) = G_{mp}(X^{p^{k-1}})$ für eine Primzahl p und beliebige m, $k \in \mathbb{N}$,

(d) $G_{2n}(X) = G_n(-X)$ für $n \geq 3$ und ungerades n,

(e) $G_n(0) = 1$ für $n \geq 2$,

(f) $G_n(X^{-1})X^{\varphi(n)} = G_n(X)$ für $n \geq 2$, wobei φ die Eulersche Funktion ist,

(g)

$$G_n(1) = \begin{cases} 0, & \text{wenn } n = 1, \\ p, & \text{wenn } n \text{ eine Potenz der Primzahl } p \text{ ist,} \\ 1, & \text{wenn } n \text{ zumindest zwei verschiedene Primfaktoren hat.} \end{cases}$$

30. Bestimmen Sie die Ordnung des Polynoms $(X^2 + X + 1)^5(X^3 + X + 1)$ über $\mathbb{F}_2$.

31. Bestimmen Sie die Ordnung des Polynoms $X^7 - X^6 + X^4 - X^2 + X$ über $\mathbb{F}_3$.

32. Sei $f \in \mathbb{F}_q[X]$ ein Polynom vom Grad $m \geq 1$ mit $f(0) \neq 0$, das in seinem Zerfällungskörper über $\mathbb{F}_q$ lauter einfache Nullstellen $\alpha_1, \ldots, \alpha_m$ besitze. Zeigen Sie, dass die Ordnung von f die kleinste positive ganze Zahl e mit $\alpha_i^e = 1$ für alle $1 \leq i \leq m$ ist.

33. Zeigen Sie, dass $\mathrm{ord}(G_n) = n$ für alle n gilt, für die das Kreisteilungspolynom $G_n \in \mathbb{F}_q[X]$ definiert ist.

34. Sei f irreduzibel über F_q mit $f(0) \neq 0$. Zeigen Sie, dass $\mathrm{ord}(f) = e$ für zu q teilerfremde e genau dann gilt, wenn f das Kreisteilungspolynom G_e teilt.

35. Sei $f \in \mathbb{F}_q[X]$ ein Polynom vom Grad $m \geq 1$ mit $f(0) \neq 0$, das in seinem Zerfällungskörper über $\mathbb{F}_q$ lauter einfache Nullstellen $\alpha_1, \ldots, \alpha_m$ besitze. Wie hängen die Ordnungen von f^b und von f zusammen ($b \in \mathbb{N}$)?

36. Sei $f \in \mathbb{F}_q[X]$ ein nicht-konstantes Polynom mit $f(0) \neq 0$. Zeigen Sie, dass $\mathrm{ord}(f(x^p)) = p\,\mathrm{ord}(f(x))$ gilt, wobei $q = p^n$.

37. Sei $f \in \mathbb{F}_q[X]$ ein normiertes Polynom vom Grad $m \geq 1$. Zeigen Sie, dass f genau dann primitiv über $\mathbb{F}_q$ ist, wenn f ein irreduzibler Faktor des Kreisteilungspolynoms $G_d \in \mathbb{F}_q[X]$ für $d = q^m - 1$ ist.

38. Bestimmen Sie die Anzahl der primitiven Polynome über $\mathbb{F}_q[X]$ vom Grad m.

39. Zeigen Sie, dass es höchstens $(q^n - q)/n$ irreduzible Polynome vom Grad n über $\mathbb{F}_q$ gibt. Zeigen Sie weiters, dass Gleichheit genau dann gilt, wenn n eine Primzahl ist.

40. Zeigen Sie, dass die Kreisteilungspolynome G_{19} und G_{27} denselben Grad haben und beide über $\mathbb{F}_2$ irreduzibel sind.

41. Faktorisieren Sie $X^{32} - X$ über $\mathbb{F}_2$ in irreduzible Faktoren.

42. Faktorisieren Sie das Polynom

$$X^{34} + 2X^{32} + 2X^{30} + 2X^{29} + 2X^{28} + 2X^{27} + 2X^{25} + X^{23} + X^{21} + X^{20} + X^{19} + X^{18} + 2X^{16} + X^{14} + X^{12} + X^{11} + X^{10} + X^9 + X^7 + 2X^5 + 2X^3 + 2X^2 + 2X + 2$$

über

(a) $\mathbb{F}_3$,

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

43. Sei $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ für ein passendes α. Faktorisieren Sie $X^5 + \alpha X^4 + X^3 + (1+\alpha)X + \alpha$ über $\mathbb{F}_4$.

44. Bestimmen Sie die Anzahl der verschiedenen normierten irreduziblen Faktoren von $x^4 + 1$ über $\mathbb{F}_p$ für alle ungeraden Primzahlen p.

45. Der dreifache Paritätscheckcode werde um ein Paritätscheckbit erweitert, d.h., das Wort abc werde durch $abcxyzp$ codiert, wobei

$$a+b+z = a+c+y = b+c+x = a+b+c+x+y+z+p = 0.$$

Was sind die Parameter (Blocklänge, Dimension, Minimaldistanz) dieses Codes?

46. Der ternäre (also über $\mathbb{F}_3 = \{0, +1, -1\}$) $(8, 7)$-Checkcode entsteht durch das Anhängen eines Prüftrits (i.e., einer ternären Ziffer) zu jedem Block der Länge sieben, wobei die Summe der Trits 0 wird. Zeigen Sie, dass dieser Code alle ein-trit Fehler und manche zwei-trit Fehler erkennt.

47. Der Binärcode C habe Prüfmatrix (in Standardform, d.h., die letzten Spalten sind eine Einheitsmatrix) M_C. Der ternäre Code D habe dieselbe Prüfmatrix. Wie ist der Zusammenhang zwischen den Codewörtern von C und D? Zeigen Sie, dass C und D dieselbe Dimension haben. Zeigen Sie: wenn C Minimaldistanz ≥ 3 hat, dann hat D ebenfalls Minimaldistanz ≥ 3.

48. Binäre 16-Bit-Wörter seien zu codieren. Wie viele Check-Bits müssen hinzugefügt werden, um einen ein-bit-korrigierenden Code zu erhalten? Geben Sie die Generatormatrix eines solchen Codes an.

49. Seien C und D lineare Codes der Blocklänge n, wobei C die Dimension m und D die Dimension ℓ habe. Der Code C habe Minimaldistanz d und D habe Minimaldistanz $2d$. Zeigen Sie, dass der Code X, der aus allen Wörtern der Form $(u, u+v)$ mit $u \in C$ und $v \in D$ besteht, ein linearer Code der Blocklänge $2n$, Dimension $m+\ell$ und Minimaldistanz $2d$ ist.

50. Sei D ein linearer $(8, 5)$-Code, wobei die folgenden Paritätschecks einem Wort $abcde$ angefügt werden: $x = a+b+e$, $y = a+b+c+d$ und $z = b+d+e$. Geben Sie eine Tabelle der „Coset leaders“ für alle Syndrome (i.e. $M \cdot x$ für die Prüfmatrix M und $x \in \mathbb{F}_2^8$) an. Geben Sie zwei Fehlermuster vom Gewicht 1 an, die dasselbe Syndrom haben. Konstruieren Sie einen binären $(9, 5)$-Code, der ein-Bit-Fehler korrigieren kann, indem Sie ein weiteres Prüfbit anhängen.

51. Schreiben Sie ein Programm, das einen Text aus den Buchstaben „a“ – „z“, „A“ – „Z“, „0“ – „9“, „ “, „.“, „,“, „:“ codiert, sodass ein-Bit-Fehler korrigiert werden können. Schreiben Sie weiters einen Fehlerprozessor und einen Decodierer.

52. Zeigen Sie, dass ein ternärer Code genau dann alle ein-Trit-Fehler korrigieren kann, wenn keine zwei Spalten der Prüfmatrix Summe oder Differenz 0 haben.

53. Benutzen Beispiel 52, um einen ternären Hammingcode $\text{Hamming}_3(k)$ mit Prüfmatrix $H_{3,k}$ zu konstruieren, wobei die Spalten von $H_{3,k}$ alle von Null verschiedenen ternären Vektoren bestehen, deren erster von Null verschiedener Eintrag gleich $+1$ ist. Bestimmen Sie die Blocklänge und den Dimension des Codes und zeigen Sie, dass er perfekt ist.

54. Beispiel 53 für beliebigen Grundkörper $\mathbb{F}_q$.

55. Geben Sie das kleinste n an, sodass das Polynom

$$X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$$

einen zyklischen Binärcode der Blocklänge n erzeugt. Geben Sie das zugehörige Prüfpolynom an. Codieren Sie damit systematisch das Codewort 11000. Worum handelt es sich bei diesem n?

56. Geben Sie ein Generatorpolynom für

(a) BCH$(4, 3)$

(b) BCH$(5, 4)$

über $\mathbb{F}_2$ an.

57. (a) Zeigen Sie, dass der Körper $\mathbb{F}_{2^{11}}$ ein Element β der Ordnung 23 besitzt.

(b) Sei g das Minimalpolynom von β über $\mathbb{F}_2$. Für welche ganzen Zahlen k ist β^k eine Nullstelle von g?

(c) Geben Sie das Minimalpolynom von β und von β^{-1} an.

(d) Setze

$$M_\beta := \left(\beta^{jk}\right)_{\substack{1\le j\le 4\\ 0\le k\le 22}}.$$

Zeigen Sie, dass $C := \{c \in \mathbb{F}_2^{23} \mid M_\beta c = 0\}$ ein polynomialer Code ist, geben sie sein Generatorpolynom, seine Blocklänge und seine Dimension an.

(e) Geben Sie die Minimaldistanz von C an.

(f) Ist C ein perfekter Code?

58. Ein Wort werde BCH$(4, 3)$-codiert übertragen. Empfangen wird das Wort 10101 11011 11110. Benutzen Sie den Euklidischen Fehlerprozessor, um das Wort zu korrigieren, und decodieren Sie das Ergebnis.

59. Sei $P = \sum_{j\ge 0} a_j X^j$ eine formale Potenzreihe über dem Körper K. Falls g und f Polynome aus $K[X]$ mit $\deg f \le m$ und $\deg g \le n$ sind, sodass

$$g(X)P(X) \equiv f(x) \pmod{X^{m+n+1}},$$

so heißt die rationale Funktion f/g eine Padé-Approximation von P der Ordnung (m, n).

(a) Zeigen Sie, dass für gegebene m und n genau eine Padé-Approximation der Ordnung (m, n) gibt und das Zähler und Nenner bis auf Multiplikation mit einer Konstanten eindeutig bestimmt sind.

(b) Wie kann man Padé-Approximationen mit dem Euklidischen Algorithmus bestimmen?