Finite Fields

D. S. 34: Let $m(x)$ be a polynomial of deg. d over F. Then
$F[x]_{m(x)} \overset{def}{=} \{a(x) \in F[x] \mid \deg(a(x)) < d\}$

L. S. 34: Let F be a finite field with q elements and let $m(x)$ be a polynomial of deg. d over F. Then $|F[x]_{m(x)}| = q^d$.

L. S. 35: $F[x]_{m(x)}$ is a ring with respect to addition and multiplication modulo $m(x)$.

L. S. 36: $F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} \mid \gcd(a(x), m(x)) = 1\}$

T. S. 37: The ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible.

(T. S. 38): $|GF(a)| = q-1$ for $q = p^e$, p = prim $e \geq 1$

If F is a field $F[x]$ can't be a field.

Proof: At least one element in $F[x]$ has no inverse. Given at least two elements we have $0, 1 \in F$ and $0 \neq 1$. Now we multiply two polynomials of degree d, d', which will yield a polynomial of degree $d+d' \geq d$ as $a_d \cdot b_{d'} \neq 0$ (no zero-divisor). Multiplication only increases the degree, it follows that a polynomial with $d \geq 1$ does not have an inverse. Therefore $F[x]$ is not a field.

Constructing finite field with p^d elements:
- pick $GF(p)$
- pick $m(x)$ of degree d in $GF(p)$ that is irreducible $\Rightarrow GF(p)[x]_{m(x)}$

Ex. monoid: $\langle \mathbb{Z}; +, 0\rangle$
group: $\langle \mathbb{Z}; +, -, 0\rangle$, $\langle \mathbb{Z}[x]; +, -, 0\rangle$
ring: $\langle \mathbb{R}; +, -, 0, \cdot, 1\rangle$, $\mathbb{Z} \times \mathbb{Z}$
finite ring: $\langle \mathbb{Z}_m; +, -, 0, \cdot, 1\rangle$
integ. dom: $\mathbb{Z}$, $\mathbb{Z}_{prime}$, $\mathbb{Q}[x]$
field: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, GF$
finite field: $\mathbb{Z}_{prime}$
} $\langle G; +, -, 0, \cdot, 1\rangle$ are left away for simplicity

Ex. Let F be a finite field, prove that there exists $f(x) \in F[x]$ which has no roots
1. Let $g(x) = \prod_{\alpha \in F} (x - \alpha)$, clearly $g(\alpha) = 0$ for all $\alpha \in F$
2. Now let $f(x) = g(x) + 1$, since $\forall \alpha \in F\ g(\alpha) = 0$ it follows that $\forall h \in F\ f(h) = 1$.

Application: Error-Correcting Code

D. S. 35: A (n,k)-encoding function maps A^k to A^n, where $n > k$, the result is called a codeword.

D. S. 36: An (n,k)-ECC over A with $|A| = q$ is a subset of A^n with cardinality q^k.

D. S. 37: Hamming Distance: number of positions in which two strings over A differ.

D. S. 38: Minimum Distance: minimal Hamming Distance between any two codewords of an ECC C, $d_{min}(C)$

D. S. 39: A decoding function D for an (n,k)-encoding function is a function $D: A^n \to A^k$

D. S. 40: D is t-error correcting for encoding function E if for any $(a_0, \dots, a_{k-1})$ $D((r_0, \dots, r_{n-1})) = (a_0, \dots, a_{k-1})$ for any $(r_0, \dots, r_{n-1})$ with Hamming dist. at most t from $E((a_0, \dots, a_{k-1}))$.
A code is t-error correcting if there exists E and D with $C = \text{Im}(E)$ where D is t-error correcting.

T. S. 41: A ECC with minimum distance d is t-error correcting iff $d \geq 2t+1$

T. S. 42: Let $A = GF(q)$ and let $a_0, \dots, a_{n-1} \in A$. The encoding function $E((a_0, \dots, a_{k-1})) = (a(a_0), \dots, a(a_{n-1}))$, where $a(x) = a_{k-1}x^{k-1} + \dots + a_1 x + a_0$
This ECC has minimum distance $n - k + 1$.

Euler

If p is prime $\varphi(p) = p-1$

If p is prime, a a pos. Int. $\varphi(p^a) = p^a - p^{a-1}$

If a and b are rel. prime $n = ab$ then $\varphi(n) = \varphi(a)\varphi(b)$

If n is pos. Int. with prime factorization $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$
then $\varphi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \dots (p_k^{e_k} - p_k^{e_k-1})$
$= (p_1 - 1) p_1^{e_1-1} \cdot (p_2 - 1) p_2^{e_2-1} \dots (p_k - 1) p_k^{e_k-1}$

Countability

$\{0,1\}^\infty \leq A$
↑ uncount. → thus A uncount.

$A \leq \mathbb{N} \times \mathbb{N}$
↓ count.
thus A ↑ count.

Bei Uncountability oft $\{0,1\}^\infty$

Bei Countability ein wenig kreativer wie $\mathbb{Q}$ $\frac{n}{m}$ $\mathbb{N}^*$

Elements of multiplicative groups $\mathbb{Z}_n^*$ and generators

2	1
3	1 2
4	1 3
5	1 2 3 4
6	1 5
7	1 2 3 4 5 6
8	1 3 5 7
9	1 2 4 5 7 8
10	1 3 7 9
11	1 2 3 4 5 6 7 8 9 10
12	1 5 7 11
13	1 2 3 4 5 6 7 8 9 10 11 12
14	1 3 5 9 11 13
15	1 2 4 7 8 11 13 14
16	1 3 5 7 9 11 13 15
17	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
18	1 5 7 11 13 17
19	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
20	1 3 7 9 11 13 17 19
21	1 2 4 5 8 10 11 13 16 17 19 20
22	1 3 5 7 9 13 15 17 19 21
23	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
24	1 5 7 11 13 17 19 23
25	1 2 3 4 6 7 8 9 11 12 13 14 16 17 18 19 21 22 23 24
26	1 3 5 7 9 11 15 17 19 21 25 25
27	1 2 4 5 7 8 10 11 13 14 16 17 19 20 22 23 25 26
28	1 3 5 9 11 13 15 17 19 23 25 27
29	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
30	1 7 11 13 17 19 23 29
31	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
32	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31
33	1 2 4 5 7 8 10 13 14 16 17 19 20 23 25 26 28 29 31 32
34	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33
35	1 2 3 4 6 8 9 11 12 13 16 17 18 19 22 23 24 26 27 29 31 32 33 34
36	1 5 7 11 13 17 19 23 25 29 31 35
37	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
38	1 3 5 7 9 11 13 15 17 21 23 25 27 29 31 33 35 37
39	1 2 4 5 7 8 10 11 14 16 17 19 20 22 23 25 28 29 31 32 34 35 37 38
40	1 3 7 9 11 13 17 19 21 23 27 29 31 33 37 39
41	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
42	1 5 11 13 17 19 23 25 29 31 37 41
43	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42
44	1 3 5 7 9 13 15 17 19 21 23 25 27 29 31 35 37 39 41 43
45	1 2 4 7 8 11 13 14 16 17 19 22 23 26 28 29 31 32 34 37 38 41 43 44
46	1 3 5 7 9 11 13 15 17 19 21 25 27 29 31 33 35 37 39 41 43 45
47	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 45 44 45 46
48	1 5 7 11 13 17 19 23 25 29 31 35 37 41 43 47
49	1 2 3 4 5 6 8 9 10 11 12 13 15 16 17 18 19 20 22 23 24 25 26 27 29 30 31 32 33 34 36 37 38 39 40 41 43 44 45 46 47 48
50	1 3 7 9 11 13 17 19 21 23 27 29 31 33 37 39 41 43 47 49