Hugo *Rincon Galeana*

TU Wien, Winter 2019
104.272 Discrete Mathematics, Group 1 (Professor Gittenberger)
12. Exercise, Due 22 January, 2020

111. Prove that for each prime n, we have $(n-1)! \underset{n}{\equiv} -1$. Further show that this only holds when n is prime.

Proof. Lec $r^2 \underset{n}{\equiv} 1$. From the division algorithm, $r = \alpha p + c'$. With $0 \leq c' < p$. Since $c' = 0$ would imply that $r^2 \underset{n}{\equiv} 0$, then $c' \geq 1$. Therefore $r = \alpha p + 1 + c$. Therefore $r^2 = \alpha^2 p^2 + 2\alpha p(1+c) + 1 + 2c + c^2 = \beta p + c(2+c) + 1$. Since $r^2 = \gamma p + 1$, and $c < p$ with p prime, then $p\,|2+c$ or $p\,|c$. Therefore $c \underset{n}{\equiv} p-2$ or $c = 0$. This implies that $r \underset{n}{\equiv} p-1$ or $r \underset{n}{\equiv} 1$. Therefore in $\mathbb{Z}_p$ all elements that are not 1 or $p-1$ are not self-inverse. This implies that $(n-1)! = \prod_{z \in \mathbb{Z}_{\shortmid}{}^*} z = 1 \cdot (p-1) = -1$, since all other elements cancel out with their respective inverses.
Now assume that $(n-1)! \underset{n}{\equiv} -1$. Since $((n-1)!)^2 = 1$, this implies that all $z \in \mathbb{Z}_n$ such that $z \neq 0$ have a product inverse. Therefore n must be prime. ☐

112. Prove that every finite integral domain is a field

Hint: One only has to show that if R is a finite integral domain, then every non-zero element of R is invertible. One starts as follows: let $a \in R, a \neq 0$, and $f : R \to R$ be the function defined by $f(x) = ax$. First prove that f is injective, than notice that f is a function from a finite set to itself.

Proof. We take the hint and let f as defined previously. Notice that f is a group morphism with respect to the product. Notice that since R is an integral domain, then $\ker f = 0$. Therefore f is injective. Since R is finite, then f is bijective. Therefore there exists an element c such that $ac = 1$. This completes the proof that R is a field. ☐

113. Let $\mathbb{K}$ be a field whose characteristic equals a prime number p. Prove the so-called *freshman's dream*:

$$(a+b)^p = a^p + b^p \quad \text{for all } a, b \in \mathbb{K}.$$

Does this statement generalises for more than two summands?

Proof. Recall from the binomial theorem that:
$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$, also notice that $p \,|\binom{p}{i}$ for all $0 < i < p$. Since $\mathbb{K}$ is of characteristic p it follows that $\binom{p}{i} = 0$ for all $0 < i < p$.

Notice that it works for any ammount of summands, that is $\left(\sum_{i=1}^{n} a_i\right)^p = \sum_{i=1}^{n} a_i^p$.
The proof is induction over the number of summands. $\square$

114. Prove that for each odd prime p, there is a field with p^2 elements.

Hint: One has to show that there is an irreducible quadratic polynomial over $\mathbb{Z}_p$, for example of the form $x^2 - a$. To that end, one could show that there exists $a \in \mathbb{Z}_p$ which is not the square of another element in $\mathbb{Z}_p$.

Proof. Consider the function $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $x \mapsto x^2$. Since we are considering $p > 2$, then f is not injective since $1^2 = 1 = (p-1)^2$. Since $\mathbb{Z}_p$ is also finite, then f is not surjective. Therefore, there must exist $a \in \mathbb{Z}_p$ without a square root in $\mathbb{Z}_p$. This implies that $x^2 - a$ is irreducible in $\mathbb{Z}_p[x]$. Notice that $\mathbb{Z}_p[x]/x^2 - a$ is a Galois field with p^2 elements. $\square$

115. Consider the field $\mathbb{Z}_2[x]/m(x) = \mathbb{F}_{256}$ where $m(x) = x^8 + x^4 + x^3 + x + 1$. Hence the residue classes modulo $m(x)$ are $\overline{b(x)} = \overline{b_7x^7 + b_6x^6 + \ldots b_1x + b_0}$ and can be identified with the byte $b_7b_6 \ldots b_1b_0$.

(a) Compute the sum and the product of the two bytes 10010101 and 11001100 in $\mathbb{F}_{256}$.

Proof.

$$\begin{array}{r} 10010101 \\ +\ 11001100 \\ \hline 01011001 \end{array}$$

Notice that multiplying by a fixed element is a linear transformation, therefore it can be defined through the image of the basis as a matrix product. Also notice that $x^8 = x^4 + x^3 + x + 1$ since in $\mathbb{Z}_2$ each element is its own additive inverse. Taking this into consideration, we can consider the product by 10010101 as multiplying the following matrix M with a vertical vector

$$\begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{matrix}$$

Which yields 00101000 $\square$

(b) Compute the multiplicative inverse y^{-1} for $y = 10010101$ in $\mathbb{F}_{256}$.

Proof. We solve the equation $M \cdot y^{-1} = 00000001$ through the diagonalization method.

Which yields the following equation $M'y^{-1} = 00000110$ where M' is the following matrix :

$$\begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

Therefore $y^{-1} = 10001010$ □

116. Let a (n, k)-linear code $C \subseteq \mathbb{F}_q^n$ be given by its generator matrix G. Let H be the generator matrix of the dual code. Show that $GH^T = 0_{k\times(n-k)}$.

    Remark: The check matrix can be defined either to be the generator matrix of the dual code $C^* = \{x \in \mathbb{F}_q^n : x \cdot c = 0$ for all $c \in C\}$ or to be a matrix that satisfies $GH^T = 0$. This exercise shows, that those two definitions are equivalent.

    Proof. Notice that H is of dimension $(n - k) \times n$ and G is of dimension $k \times n$. Therefore GH^T is of dimension $k \times (n - k)$ Consider $(GH^T)_{i,j} = \sum_{k=1}^{n} G_{i,k}H_{j,k} = G_i \cdot H_j = 0$. Since $G_i \in C$ and $H_j \in C^*$. □

117. Compute the dual code C^* of a linear code $C \subseteq \mathbb{F}_2^8$ that is represented by

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Proof. Recall that if a code is systematic, given by a generating matrix $G = [I_k \mid P]$ then the dual code has generating matrix $H = [-P^T \mid I_k]$.

Notice that P is given by

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Since in the code is binary, then $-P = P$, therefore $-P^T$ is given by the following matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

Therefore H is given by

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

□

118. Consider a linear code $C \subseteq \mathbb{F}_2^5$ with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Proof. First we will make the generator matrix systematic through diagonalization.

$$G' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

This yields the following matrix H as a check matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Notice that the code $C = \{00000, 10011, 01001, 11010, 00101, 10110, 01100, 11111\}$

$$H^T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Notice that the minimum distance of this code is 2. Therefore up to 1 errors can be detected and 1 can be corrected.

The correcting scheme can be given as follows:

If $S(v) \in \{01, 10\}$ then simply $\bar{v} = v + S(v)$.

If $S(v) = \{11\}$, then $C' = \{00011, 10000, 01010, 00110, 10101, 01111, 11100\}$

Since the distances can be at most 1, then the corrected code should be $\{00011 \mapsto 10011, 10000 \mapsto 00000, 01010 \mapsto \text{error}, 00110 \mapsto 10110, 10101 \mapsto \text{error}, 01111 \mapsto 11111, 11100 \mapsto 01100\}$ □

119. Let $p(x) = x^3 + 2$ be a generating polynomial of a cyclic $(9, 6)$-linear code over $\mathbb{F}_3$. Determine a generating matrix such that the code is a systematic code, i.e. encoding is done by appending one or more letters at the end of the original words.

Proof. The generator matrix is given by:

$$\begin{pmatrix} 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 \end{pmatrix}$$

Operating the matrix above through elementary operations yields the following systematic generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 \end{pmatrix}$$

□

120. Let $(s_n)_{n\geq 0}$ be a homogeneous linear recurring sequence of order k over a finite field $\mathbb{F}_q$

$$s_{n+k} = a_0 s_n + a_1 s_{n+1} + \ldots + a_{k-1} s_{n+k-1},$$

where $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_q$ are fixed and $s_0, s_1, \ldots, s_{k-1}$ are given. Show that $(s_n)_{n\geq 0}$ has to be a periodic sequence. *Hint: use linear feedback shift registers.*

Proof. Notice that this sequence is generated by a linear shift register with k different registers, each of which has q different possible states. Notice that there are at most q^k different possible states for the linear shift register. This implies that the state of the registers should repeat in q^k different states or less. Therefore the sequence generated is periodic. □