$\mathbb{F}_p^*$ cyclique.

th : Soit K un corps fini, le groupe K^* est cyclique ~~pour tout nombre~~.
En particulier : $\mathbb{F}_p^*$ est cyclique.

Lemme 1 : Soit G un groupe abelien fini; soit $a \in G$; $\omega(a) = n$; soit $b \in G$, $\omega(b) = m$.
il existe un élément de G d'ordre $\text{ppcm}(n, m)$.

preuve : Soit d un diviseur de n; on a $n = dn'$; posons $x = a^{n'} = a^{\left(\frac{n}{d}\right)}$.
Soit r l'ordre de x; on a :
$x^d = a^n = 1$ ce qui donne $r \mid d$.
par ailleurs; $x^r = a^{rn'} = 1$; on conclut que
rn' est un multiple de n;
$n = dn' \mid rn'$ ou encore $d \mid r$ et enfin; ce qui donne $r = d$.
On vient donc de montrer qu'on peut construire un élément d'ordre d pour tout diviseur d de n.
écrivons $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ $\alpha_i \geq 0$.
$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$, $\beta_i \geq 0$

Exemple : $n = 2^2 \times 3^2 \times 5 \times 7^0$

$m = 2 \times 3^5 \times 5 \times 7$

$ppcm(n, m) = 2^2 \times 3^5 \times 5 \times 7.$

supposons que $\alpha_1 > \beta_1$;

posons $d = p_1^{\alpha_1}$; d divise n ; On construit un élément a_1 d'ordre d à partir de n ;

si $\beta_1 > \alpha_1$, on va construire un élément d'ordre $d = p_1^{\beta_1}$ à partir de m.

par chaque i ; On construit donc un élément a_i d'ordre $p_i^{\max(\alpha_i, \beta_i)}$

par construction ; des $p_i^{\max(\alpha_i, \beta_i)}$ sont premiers entre eux, donc : $\left(\prod_{i=1}^{r} a_i\right)$ est un élément d'ordre $p_1^{\max(\alpha_1, \beta_1)} \cdots p_r^{\max(\alpha_r, \beta_r)}$

Lemme 2 : Soit G un groupe commutatif fini. $G = \{g_1, \dots, g_m\}$, ordre $(g_i) = n_i$. Soit $N = ppcm(n_i)$. alors il existe un élément d'ordre N.

Exemple : $n = 2^2 \times 3^2 \times 5 \times 7^0$

$m = 2 \times 3^5 \times 5 \times 7$

$ppcm(n,m) = 2^2 \times 3^5 \times 5 \times 7$

$\max(\alpha_1,\beta_1)$ $\max(\alpha_r,\beta_r)$

plus généralement $ppcm = p_1^{\max(\alpha_1,\beta_1)} \cdots p_r^{\max(\alpha_r,\beta_r)}$

si $\alpha_1 > \beta_1$, on construit un élément a_1 d'ordre $p_1^{\alpha_1}$ on le construit à partir de a.

si $\alpha_1 < \beta_1$ on construit a_1 à partir de b.

par chaque i : On construit un élément a_i d'ordre $p_i^{\max(\alpha_i,\beta_i)}$.

$p_i^{\max(\alpha_i,\beta_i)}$ et $p_j^{\max(\alpha_j,\beta_j)}$ sont premiers entre eux ; l'élément $\left(\prod_{i=1}^{r} a_i\right)$ est d'ordre $p_1^{\max(\alpha_1,\beta_1)} \cdots p_r^{\max(\alpha_r,\beta_r)} = ppcm(n,m)$.

Lemme 2 : Soit G un groupe abélien fini ; $G = \{g_1, \ldots, g_m\}$; $\omega(g_i) = n_i$

Soit $N = ppcm(n_i)$; il existe un élément de G d'ordre N.

preuve : grâce au lemme 1 ; On construit un élément h_1 d'ordre $n_1 = ppcm(n_1, n_2)$.

et un élément h_2 d'ordre $n_2 = ppcm(n_1, n_3)$

$m_2 = ppcm(ppcm(n_1, n_2), n_3) = ppcm(n_1, n_2, n_3)$
et ainsi de suite. On obtient un élément
h_{m-1} d'ordre $N = ppcm(n_1, n_2, \dots, n_m)$.

preuve du théorème : Soit q le nombre d'éléments de K, $|K^*| = q-1$. Soit N le ppcm des ordres des éléments de K^*.

On a : $x^{q-1} = 1$ pour tout $x \in K$; on conclut que $\omega(x) \mid q-1$ pour tout x; $q-1$ est donc un multiple de tous les ordres des éléments de K^*, c'est donc un multiple de N; en particulier $q-1 \geq N$.

Par ailleurs, on a : $x^N = 1$ pour tout $x \in K^*$. Les éléments de K^* qui sont en nombre de $(q-1)$ sont tous racine du polynôme $X^N - 1$; ce polynôme de degré N possède au plus N racines, il s'en suit que : $q-1 \leq N$.

et par suite $N = q-1$.

d'après le lemme 2, il existe un élément a de K^* d'ordre $N = q-1$: autrement dit : a est un générateur de K^* ; i.e $K^* = \langle a \rangle$ est cyclique.

(1) $x^2 - 3x + 12$ dans $\mathbb{F}_{41}$.

$\Delta = \bar{9} - \bar{4}(\bar{12}) = \bar{9} - 4\bar{8} = -3\bar{9} = \bar{2}$.

$2^5 = 3\bar{2} = -\bar{9}$

$2^{10} = 81 = 40 = -1$ dans $\mathbb{F}_{41}$

$2^{20} = 2^{\frac{41-1}{2}} = 1$

2 n'est pas un carré.

Montrons que $\bar{6}$ est un générateur de $\mathbb{F}_{41}$; on a encore $\omega(\bar{6}) = 40$;

$6^2 = -5$; $6^4 = 25$; $6^5 = 27$;

$6^8 = 10$; $6^{10} = -9$, $6^{20} = -1$ et

$6^{40} = 1$;

cherchons une racine carrée de 2.

$2 = 6^{26}$ (6 est un générateur).

donc 6^{13} est une racine de 2 ;

$6^{13} = 24$;

les racines de 2 sont 24 et $-24 = 17$.

$2^{-1} = 6^{40-13}$ ou plus simplement $2^{-1} = \frac{41+1}{2} = 21 = -20$

les solutions sont : $x_1 = 2^{-1}(3 - 24)$ et $x_2 = 2^{-1}(3+24)$

$x_1 = -20(-21)$; $x_2 = -20(27) = -7$

$x_1 = 10$

(2) Soit p un nombre premier, g un générateur de $\mathbb{F}_p^*$; $e_g : \mathbb{Z}/(p-1)\mathbb{Z} \longrightarrow \mathbb{F}_p^*$

$$\bar{k} \longrightarrow g^k.$$

e_g est un isomorphisme de groupe.

prenons un exemple, $p = 31$; On vérifie que $\bar{3}$ est un générateur de $\mathbb{F}_{31}^*$;

A chaque lettre de l'alphabet, correspond un nombre ≤ 31

$A \to 1$, $B \to 2$ ...

Soit le mot VELO

22 5 12 15

$n =$

g^n : 14 26 8 30

Le mot codé est : 14 26 8 30

pour décrypter (le petit message), il faut utiliser e_g (logarithme discret) ; il faut connaître le générateur

Ici 3. Imaginez p un nombre premier grand. il sera très coûteux en temps de calcul.

Exercice :

· $p = 29$;

$g = ?$

mot	?				
n					
g^n	4	13	2	5	27

Quel est le mot ?

(3). Soit l'equation $11x^4 \equiv 1 [19]$.

dans $\mathbb{Z}/19\mathbb{Z}$, l'equation devient :

$\bar{11}\, \bar{x}^{14} = \bar{1}$

$\bar{2}$ est un générateur de $\mathbb{F}_{19}^*$;

$\bar{x} = \bar{2}^k$; l'equation $\Leftrightarrow \bar{11} \cdot \bar{2}^{14k} = 1$

$\bar{11} = \bar{2}^{12}$; $\Leftrightarrow \bar{2}^{14k+12} = 1$

(2 est d'ordre 18!). $\Leftrightarrow 14k + 12 \equiv 0 [18]$

$\Leftrightarrow 7k + 6 \equiv 0 [9]$.

$\Leftrightarrow 7k \equiv -6 [9]$; $4 \times 7k \equiv -24 [9]$

$\Leftrightarrow k \equiv 3 [9]$

$\Leftrightarrow k \equiv 3$ ou $k \equiv 12 [18]$

$\bar{2}^3 \equiv \bar{8}$; $\bar{2}^{12} = \bar{11}$; $x = 8k + 19n$ ou $11 + 19n$.

dans $\mathbb{F}_p$; les racines sont : $\bar{8}$ et $\bar{11} = -\bar{8}$.

(4).