Demostrar que $\varphi_r(N) = \prod_{i=1}^{n} p_i^{(\alpha_i-1)r^2} \cdot \prod_{j=0}^{r-1} (p_i^r - p_i^j)$;

siendo $N = \prod_{i=1}^{n} p_i^{\alpha_i}$

Plan de la demostración:

(1) • Probar que φ_r es una función aritmética multiplicativa.

(2) • Probar que $\varphi_r(p_i^{\alpha_i}) = \varphi_r(p_i) \cdot p_i^{(\alpha_i-1)r^2}$

(3) • Probar que $\varphi_r(p_i) = \prod_{j=0}^{r-1} (p_i^r - p_i^j)$.

Para demostrar (1) usaré la

Proposición 1: Si $(m,n)=1$ los anillos $M_r(\mathbb{Z}_{n\cdot m})$ y $M_r(\mathbb{Z}_n) \times M_r(\mathbb{Z}_m)$ son isomorfos.

Entonces las unidades: (el cardinal de las unidades):

$$|\mathcal{U}(M_r(\mathbb{Z}_{n\cdot m}))| = |\mathcal{U}(M_r(\mathbb{Z}_n) \times M_r(\mathbb{Z}_m))| =$$

$$= |\mathcal{U}(M_r(\mathbb{Z}_n))| \cdot |\mathcal{U}(M_r(\mathbb{Z}_m))| \Rightarrow \varphi_r(m\cdot n) = \varphi_r(m)\cdot\varphi_r(n).$$

Para probar (2) usaré la

Proposición 2: Sea $M \in M_r(\mathbb{Z}_{p^\alpha})$, sea $\hat{M} = M \pmod p$ con $\hat{M} \in M_r(\mathbb{Z}_p)$. Entonces

M es invertible sii $\hat{M}$ lo es.

Sea $f : M_r(\mathbb{Z}_{p^\alpha}) \longrightarrow M_r(\mathbb{Z}_p)$

$$M \longmapsto f(M) = M \pmod p = \hat{M}$$

Entonces la proposición nos dice que

$f^{-1}(GL_r(\mathbb{Z}/\mathbb{Z}_p)) = GL_r(\mathbb{Z}/\mathbb{Z}_{p^\alpha})$; Uso: $\mathbb{Z}/\mathbb{Z}_p := \mathbb{Z}_p$.

Entonces $\forall \hat{M} \in GL_r(\mathbb{Z}_p)$

$f^{-1}(\hat{M}) = \hat{M} + p \cdot \{$ cualquier matriz de $M_r(\mathbb{Z}_{p^{\alpha-1}}) \} = M \in GL_r(\mathbb{Z}_{p^\alpha})$

luego el número de matrices invertibles en $M_r(\mathbb{Z}_{p^\alpha}) =$

$= |GL_r(\mathbb{Z}_{p^\alpha})| = \varphi_r(p^\alpha) = \underbrace{\varphi_r(p)} \cdot (p^{\alpha-1})^{r^2}$ donde.

$\varphi_r(p) = |GL_r(\mathbb{Z}_p)|$ y $p^{r^2(\alpha-1)} = |M_r(\mathbb{Z}_{p^{\alpha-1}})|$

Para cada elemento de la matriz de $M_r(\mathbb{Z}_{p^{\alpha-1}})$ tengo.

$(1, 2, \dots, p^{\alpha-1})$ posibilidades y son r^2 elementos.

Para probar el punto (3): $\varphi_r(p) = \prod_{j=0}^{r-1} (p^r - p^j)$

Uso la siguiente

Proposición 3: Sea $\mathbb{K}$ un cuerpo, sea $M \in M_r(\mathbb{K})$ L.S.A.E:

(1) M es invertible

(2) Las columnas de M son linealmente independientes

En nuestro caso: sea $\hat{M} = \{\hat{M}_1, \hat{M}_2, \dots, \hat{M}_r\}$ con $\hat{M}_i$ columna i-sima de $\hat{M}$. Entonces $\hat{M}$ es invertible sii $\{\hat{M}_1, \dots, \hat{M}_r\}$ es una base.

El número de matrices invertibles corresponde al número de bases ordenadas.

Para la columna $\hat{M}_1$ hay $(p^r - 1)$ posibilidades $(\hat{M}_1 \neq \bar{0})$

" " " $\hat{M}_2$ " $(p^r - p)$ " (porque tenemos que restar las linealmente dependientes de $\hat{M}_1$, i.e.: $\lambda \cdot \hat{M}_1$ con $\lambda \in \{1, \dots, p\}$.

Para la columna $\hat{M}_3$ hay $(p^r - p^2)$ posibilidades (idem. restar las lin. dep. de $\hat{M}_1$ y $\hat{M}_2$: i.e.: $\lambda_1 \hat{M}_1 + \lambda_2 \hat{M}_2$; $\lambda_1, \lambda_2 \in \{1, \dots, p\}$.

$\dots$

idem $\hat{M}_r$ hay $(p^r - p^{r-1})$

luego $\varphi_r(p) = (p^r-1)\cdot(p^r-p)\cdot(p^r-p^2)\cdot\ldots\cdot(p^r-p^{r-1}) = \prod_{j=0}^{r-1}(p^r-p^j)$

La proposición 2 se demuestra teniendo en cuenta

1.- Sea A un anillo conmutativo entonces

$M \in GL_r(A)$ sii $\det(M) \in \mathcal{U}(A)$

2.- $a \in \mathcal{U}(A)$ sii $a \in \mathcal{U}(A/pA)$.

i.e.: El $\det(M)$ con $M \in GL_r(\mathbb{Z}_{p^\alpha})$ no tiene factor común con p^α sii el $\det(\hat{M})$ con $\hat{M} \in GL_r(\mathbb{Z}_p)$ no tiene factor común con p.

Esto es $\mathcal{U}(\mathbb{Z}_{p^\alpha}) = \{1, 2, \ldots, p-1, p+1, \ldots, 2p-1, 2p+1, \ldots, p^\alpha-1\} =$

$= \{1, \ldots, p^\alpha\} \setminus \{p, 2p, 3p, \ldots, p^2, 2p^2, \ldots, p^\alpha\}$.

por eso $|\mathcal{U}(\mathbb{Z}_{p^\alpha})| = \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

$\mathcal{U}(\mathbb{Z}_p) = \{1, 2, \ldots, p-1\}$; $|\mathcal{U}(\mathbb{Z}_p)| = \varphi(p) = p-1$.

Bibliografía:

- FRALEIGH, Abstract Algebra.