Capítulo 15
Cuerpos finitos

> ...as a longtime worker using only real or complex numbers, [Joseph F. Ritt] referred to finite fields as "monkey fields".
>
> Steven Krantz, "Mathematical Apocrypha Redux"

En este capítulo vamos a construir los cuerpos finitos y ver sus propiedades básicas.

15.0.1. Observación. *Todo cuerpo finito tiene p^n elementos donde p es algún número primo y $n = 1, 2, 3, \ldots$*

Demostración. Un cuerpo finito necesariamente tiene característica p para algún número primo p, y entonces es una extensión finita de $\mathbb{F}_p$. En particular, es un espacio vectorial de dimensión finita n sobre $\mathbb{F}_p$ que tiene p^n elementos. ■

15.0.2. Teorema. *Para todo primo p y $n = 1, 2, 3, \ldots$ existe un cuerpo finito de p^n elementos; específicamente, es un cuerpo de descomposición del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$. En particular, es único salvo isomorfismo.*

Demostración. Consideremos una extensión $\mathbb{F}/\mathbb{F}_p$. Notamos que el polinomio $f := X^{p^n} - X \in \mathbb{F}_p[X]$ no tiene raíces múltiples en $\mathbb{F}$: en efecto, si en $\mathbb{F}[X]$ se tiene

$$X^{p^n} - X = (X - \alpha)^2 \, g$$

para algún X, entonces, tomando las derivadas formales en $\mathbb{F}[X]$, se obtiene

$$-1 = p^n \, X^{p^n - 1} - 1 = 2 \, (X - \alpha) \, g + (X - \alpha)^2 \, g',$$

de donde $(X - \alpha) \mid -1$, lo que es absurdo.

1) Sea $\mathbb{F}/\mathbb{F}_p$ un cuerpo de descomposición de f. Por lo que acabamos de probar, $\mathbb{F}$ contiene p^n raíces distintas de f. Notamos que las raíces de f forman un subcuerpo de $\mathbb{F}$. En efecto, está claro que $f(0) = f(1) = 0$. Sean $\alpha, \beta \in \mathbb{F}$ elementos tales que $f(\alpha) = f(\beta) = 0$; es decir, $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. Luego,

$$(\alpha\beta)^{p^n} = \alpha^{p^n} \, \beta^{p^n} = \alpha\beta,$$

y además

$$(\alpha + \beta)^{p^n} = \sum_{i+j=p^n} \binom{p^n}{i} \alpha^i \, \beta^j = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

usando que $p \mid \binom{p^n}{i}$ para todo $i = 1, \ldots, p^n - 1$. En fin, si $\alpha \neq 0$, entonces

$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}.$$

Por la minimalidad de los cuerpos de descomposición, esto significa que todos los elementos de $\mathbb{F}$ son raíces del polinomio f cuyo grado es p^n, así que $|\mathbb{F}| = p^n$.

2) Viceversa, notamos que si $\mathbb{F}$ es un cuerpo de p^n elementos, entonces $\mathbb{F}$ tiene característica p y $\mathbb{F}_p \subseteq \mathbb{F}$. El grupo multiplicativo $\mathbb{F}^\times$ tiene orden $p^n - 1$, así que todo elemento $\alpha \in \mathbb{F}^\times$ satisface $\alpha^{p^n-1} = 1$ según el teorema de Lagrange, así que $\alpha^{p^n} = \alpha$. Para $\alpha = 0$ esto también trivialmente se cumple. Luego, todos los p^n elementos de $\mathbb{F}$ son raíces del polinomio $f := X^{p^n} - X \in \mathbb{F}_p[X]$ de grado p^n, así que $\mathbb{F}$ es un cuerpo de descomposición de f. Recordemos que un cuerpo de descomposición es único salvo isomorfismo.

■

15.0.3. Notación. En vista del último resultado, se suele hablar de *el cuerpo* de p^n elementos y se usa la notación $\mathbb{F}_{p^n}$, o $\mathbb{F}_q$ donde $q = p^n$.

15.0.4. Comentario. Note que para $n > 1$ el anillo $\mathbb{Z}/p^n\mathbb{Z}$ (los restos módulo p^n) tiene divisores de cero, y en particular no es un cuerpo. Entonces, $\mathbb{F}_{p^n}$ es algo muy diferente de $\mathbb{Z}/p^n\mathbb{Z}$.

Para construir los cuerpos finitos de manera más explícita, notamos que si $\mathbb{F}_{p^n}$ es un cuerpo de p^n elementos, entonces el grupo $\mathbb{F}_{p^n}^\times$ es cíclico (véase el capítulo 7); es decir, existe un generador $\alpha \in \mathbb{F}_{p^n}^\times$ tal que

$$\mathbb{F}_{p^n} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}.$$

Sea $f := m_{\alpha,\mathbb{F}_p}$ el polinomio mínimo de α sobre $\mathbb{F}_p$. Tenemos

$$\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha), \quad [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg f.$$

Pero $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$, así que $\deg f = n$. Esto nos da el siguiente resultado.

15.0.5. Teorema. *Para todo primo p y $n = 1, 2, 3, \ldots$ existe un polinomio irreducible $f \in \mathbb{F}_p[X]$ de grado n.*

15.0.6. Comentario. Si f es un polinomio irreducible en $\mathbb{F}_p[X]$ y $\mathbb{F} := \mathbb{F}_p[X]/(f)$, denotemos por α la imagen de X en el cociente. Este α *no tiene por qué* ser un generador del grupo multiplicativo $\mathbb{F}^\times$. Por ejemplo, consideremos un cuerpo finito de 9 elementos $\mathbb{F} := \mathbb{F}_3[X]/(X^2 + 1)$. En este caso $\alpha^2 = -1$, y luego $\alpha^4 = 1$. Siendo un grupo cíclico de 8 elementos, $\mathbb{F}^\times$ tiene $\phi(8) = 4$ diferentes generadores y son $\alpha + 1$, $\alpha + 2$, $2\alpha + 1$, $2\alpha + 2$.

15.0.7. Ejemplo. He aquí algunos polinomios irreducibles en $\mathbb{F}_p[X]$.

$p = 2$	$p = 3$	$p = 5$
$X^2 + X + 1$	$X^2 + X + 2$	$X^2 + X + 1$
$X^3 + X^2 + 1$	$X^3 + X^2 + X + 2$	$X^3 + X^2 + 3X + 4$
$X^4 + X^3 + X^2 + X + 1$	$X^4 + X^3 + X^2 + X + 1$	$X^4 + X^3 + 2X^2 + X + 3$
$X^5 + X^4 + X^2 + X + 1$	$X^5 + X^4 + 2X^3 + 1$	$X^5 + X^4 + X^3 + 2X^2 + 3X + 1$
$X^6 + X^5 + X^3 + X^2 + 1$	$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$	$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

▲

Entonces, para construir un cuerpo de p^n elementos, se puede tomar un polinomio irreducible $f \in \mathbb{F}_p[X]$ de grado n y pasar al cociente $\mathbb{F}_p[X]/(f)$. Diferentes f dan el mismo resultado, salvo isomorfismo.

15.0.8. Ejemplo. Los polinomios

$$f_1 := X^3 + X + 1,\ f_2 := X^3 + X^2 + 1 \in \mathbb{F}_2[X]$$

son irreducibles y tiene que haber un isomorfismo entre los cuerpos finitos correspondentes

$$\begin{array}{ccc} \mathbb{F}_2[X]/(f_1) & \xrightarrow{\cong} & \mathbb{F}_2[X]/(f_2) \\ & \nwarrow \quad \nearrow & \\ & \mathbb{F}_2 & \end{array}$$

Vamos a definir un homomorfismo

$$\phi\colon \mathbb{F}_2[X] \to \mathbb{F}_2[X] \twoheadrightarrow \mathbb{F}_2[X]/(f_2)$$

tal que $\ker\phi = (f_1)$. En este caso el primer teorema de isomorfía nos daría un homomorfismo inyectivo

$$\overline{\phi}\colon \mathbb{F}_2[X]/(f_1) \xrightarrow{\cong} \operatorname{im}\phi \hookrightarrow \mathbb{F}_2[X]/(f_2),$$

y dado que $|\mathbb{F}_2[X]/(f_1)| = |\mathbb{F}_2[X]/(f_2)| = 8$, este sería automáticamente sobreyectivo. Necesitamos que se cumpla

$$\phi(f_1) = \phi(X^3 + X + 1) = \phi(X)^3 + \phi(X) + 1 \equiv 0 \pmod{X^3 + X^2 + 1}.$$

Se ve que hay tres opciones:

$$\phi_1\colon X \mapsto \overline{X+1}, \quad \phi_2\colon X \mapsto \overline{X^2+1}, \quad \phi_3\colon X \mapsto \overline{X^2+X}.$$

Cada una de estas aplicaciones induce un isomorfismo $\mathbb{F}_2[X]/(f_1) \cong \mathbb{F}_2[X]/(f_2)$. Notamos que los elementos $\overline{X+1}, \overline{X^2+1}, \overline{X^2+X} \in \mathbb{F}_2[X]/(f_2)$ están relacionados de la siguiente manera:

$$\overline{X^2+1} = (\overline{X+1})^2, \quad \overline{X^2+X} = (\overline{X^2+1})^2 = (\overline{X+1})^4$$

(véase §15.2). ▲

Sería interesante saber cuántas posibilidades hay para escoger al polinomio irreducible f. Denotemos por N_n el número de los polinomios mónicos irreducibles en $\mathbb{F}_p[X]$ de grado n. Nuestro objetivo es deducir una fórmula explícita para N_n.

15.1 La fórmula de Gauss

15.1.1. Lema.

1) *Sea k cualquier cuerpo. El polinomio $X^\ell - 1$ divide a $X^m - 1$ en $k[X]$ si y solo si $\ell \mid m$.*

2) *Sea a un entero ≥ 2. El número $a^\ell - 1$ divide a $a^m - 1$ en $\mathbb{Z}$ si y solo si $\ell \mid m$.*

3) *En particular, para un primo p y $d, n \geq 1$ se tiene $(X^{p^d} - X) \mid (X^{p^n} - X)$ si y solo si $d \mid n$.*

Demostración. En la primera parte, escribamos $m = q\ell + r$ donde $0 \leq r < \ell$. Tenemos en $k(X)$

$$\frac{X^m - 1}{X^\ell - 1} = \frac{(X^{q\ell+r} - X^r) + (X^r - 1)}{X^\ell - 1} = X^r \, \frac{X^{q\ell} - 1}{X^\ell - 1} + \frac{X^r - 1}{X^\ell - 1} = X^r \sum_{0 \leq i < q} X^{i\ell} + \frac{X^r - 1}{X^\ell - 1}.$$

Esto es un polinomio si y solamente si $\frac{X^r-1}{X^\ell-1}$ lo es. Pero $r < \ell$, así que la única opción es $r = 0$.

La segunda parte se demuestra de la misma manera. La última parte es una combinación de 1) y 2):

$$(X^{p^d} - X) \mid (X^{p^n} - X) \iff (X^{p^d-1} - 1) \mid (X^{p^n-1} - 1) \iff (p^d - 1) \mid (p^n - 1) \iff d \mid n.$$

■

15.1.2. Lema. *Denotemos por f_d el producto de todos los polinomios mónicos irreducibles de grado d en $\mathbb{F}_p[X]$. Luego,*

$$X^{p^n} - X = \prod_{d \mid n} f_d.$$

Demostración. Ya hemos notado en la prueba de 15.0.2 que el polinomio $X^{p^n} - X$ no tiene raíces múltiples en su cuerpo de descomposición. En particular, $X^{p^n} - X$ no puede tener factores irreducubles múltiples en $\mathbb{F}_p[X]$[*]. Sería entonces suficiente comprobar que un polinomio mónico irreducible $f \in \mathbb{F}_p[X]$ es de grado d divide a $X^{p^n} - X$ si y solo si $d \mid n$.

Consideremos el cuerpo finito

$$\mathbb{F} := \mathbb{F}_p[X]/(f)$$

y denotemos por $\alpha \in \mathbb{F}$ la imagen de X en el cociente. En este caso f es el polinomio mínimo de α sobre $\mathbb{F}_p$. Siendo un cuerpo de p^d elementos, $\mathbb{F}$ es un cuerpo de descomposición del polinomio $X^{p^d} - X \in \mathbb{F}_p[X]$.

1) Si $d \mid n$, entonces, según el lema anterior, $(X^{p^d} - X) \mid (X^{p^n} - X)$. Entonces, todas las raíces de $X^{p^d} - X$ son también raíces de $X^{p^n} - X$, y en particular $\alpha^{p^n} - \alpha = 0$. Tenemos entonces

$$f \mid (X^{p^n} - X).$$

2) Viceversa, si $f \mid (X^{p^n} - X)$, entonces $f(\alpha) = 0$ implica que $\alpha^{p^n} - \alpha = 0$. Además, para cualquier elemento

$$x = a_{d-1}\,\alpha^{d-1} + \cdots + a_1\,\alpha + a_0 \in \mathbb{F},$$

donde $a_0, a_1, \ldots, a_{d-1} \in \mathbb{F}_p$, se tiene

$$x^{p^n} = a_{d-1}\,(\alpha^{p^n})^{d-1} + \cdots + a_1\,(\alpha^{p^n}) + a_0 = x,$$

así que *todos* los elementos de $\mathbb{F}$ son raíces de $X^{p^n} - X$. Se sigue que $(X^{p^d} - X) \mid (X^{p^n} - X)$, y luego $d \mid n$ por el lema anterior.

■

[*] Sin pasar al cuerpo de descomposición, basta notar que si $X^{p^n} - X = f^2\,g$, entonces, tomando las derivadas formales en $\mathbb{F}_p[X]$, se obtiene $2f\,f'\,g + f^2\,g' = -1$, así que $f \mid -1$ y $f \in \mathbb{F}_p^\times$ es una constante invertible.

15.1.3. Ejemplo. Se sigue que para obtener todos los polinomios irreducibles de grado $d \mid n$ en $\mathbb{F}_p[X]$, basta factorizar el polinomio $X^{p^n} - X$ en $\mathbb{F}_p[X]$. Por ejemplo, en $\mathbb{F}_2[X]$ se tiene

$$X^{16} - X = X\,(X+1)\,(X^2+X+1)\,(X^4+X+1)\,(X^4+X^3+1)\,(X^4+X^3+X^2+X+1).$$

y en $\mathbb{F}_3[X]$

$$X^9 - X = X\,(X+1)\,(X+2)\,(X^2+1)\,(X^2+X+2)\,(X^2+2X+2).$$

▲

15.1.4. Corolario. *Se cumple*

$$p^n = \sum_{d|n} d \cdot N_d.$$

Demostración. Basta comparar grados a ambos lados de la identidad $X^{p^n} - X = \prod_{d|n} f_d$ en $\mathbb{F}_p[X]$. ■

Para obtener una fórmula para N_n, se puede usar la fórmula de inversión de Möbius, revisada en el apéndice D.

15.1.5. Teorema (Gauss). *El número de polinomios mónicos irreducibles de grado n en $\mathbb{F}_p[X]$ es igual a*

$$N_n := \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right)\, p^d,$$

*donde μ denota la **función de Möbius**;*

$$\mu(1) := 1, \quad \mu(n) = 0 \text{ si } n \text{ no es libre de cuadrados},$$

y para n libre de cuadrados se pone

$$\mu(p_1 \cdots p_k) := (-1)^k,$$

donde k es el número de diferentes números primos que aparecen en la factorización de n.

Demostración. Consideremos la función $f(n) := n\,N_n$. Luego,

$$F(n) := \sum_{d|n} f(d) = \sum_{d|n} d\,N_d = p^n,$$

usando 15.1.4. La fórmula de inversión de Möbius nos da

$$f(n) = n\,N_n = \sum_{d|n} \mu\left(\frac{n}{d}\right)\, F(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right)\, p^d.$$

■

15.1.6. Ejemplo. Hay

$$\frac{1}{6}\left(\mu(1)\cdot 2^6 + \mu(3)\cdot 2^2 + \mu(2)\cdot 2^3 + \mu(6)\cdot 2\right) = \frac{1}{6}\left(64 - 4 - 8 + 2\right) = 9$$

polinomios mónicos irreducibles en $\mathbb{F}_2[X]$ de grado 6. Factorizando el polinomio $X^{2^6} - X$ en $\mathbb{F}_2[X]$, se puede ver que son

X^6+X+1,	$X^6+X^4+X^3+X+1$,	$X^6+X^5+X^3+X^2+1$,
X^6+X^3+1,	X^6+X^5+1,	$X^6+X^5+X^4+X+1$,
$X^6+X^4+X^2+X+1$,	$X^6+X^5+X^2+X+1$,	$X^6+X^5+X^4+X^2+1$.

He aquí algunos valores de N_n para diferentes p y n.

p \ n	1	2	3	4	5	6
2	2	1	2	3	6	9
3	3	3	8	18	48	116
5	5	10	40	150	624	2 580
7	7	21	112	588	3 360	19 544
11	11	55	440	3 630	32 208	295 020
13	13	78	728	7 098	74 256	804 076
17	17	136	1 632	20 808	283 968	4 022 064
19	19	171	2 280	32 490	495 216	7 839 780

El número de los polinomios mónicos irreducibles de grado n en $\mathbb{F}_p[X]$

▲

En particular, la fórmula de Gauss implica que para todo $n \geq 1$ existe un polinomio mónico irreducible $f \in \mathbb{F}_p[X]$ de grado n en $\mathbb{F}_p[X]$. En efecto,

$$N_n = \frac{1}{n}\left(p^n + \sum_{\substack{d|n \\ d\neq n}} \pm p^d\right) \geq \frac{1}{n}\left(p^n - (p^{n-1} + \cdots + p^2 + p)\right) > 0,$$

dado que

$$p^{n-1} + \cdots + p^2 + p = \frac{p^n - 1}{p - 1} - 1 < p^n.$$

15.2 Automorfismos de cuerpos finitos

La construcción de cuerpo finito de p^n elementos depende de una elección de un polinomio irreducible de grado n en $\mathbb{F}_p[X]$. Aunque probamos su existencia, no hay un modo canónico de escogerlo. Sin embargo, sabemos que todos los cuerpos de orden p^n son isomorfos entre sí. Esto nos lleva a la siguiente pregunta: ¿cuántos automorfismos tiene un cuerpo finito $\mathbb{F}_{p^n}$?

Para un cuerpo K los automorfismos $\sigma\colon K \xrightarrow{\cong} K$ forman un grupo $\mathrm{Aut}(K)$ respecto a la composición.

15.2.1. Teorema. *Para un cuerpo finito $\mathbb{F}_{p^n}$ el grupo de automorfismos $\mathrm{Aut}(\mathbb{F}_{p^n})$ es cíclico de orden n. Específicamente,*

$$\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle \cong \mathbb{Z}/n\mathbb{Z},$$

donde F denota el ***automorfismo de Frobenius***

$$F\colon x \mapsto x^p.$$

Demostración. Notamos primero que F es un automorfismo. Para cualesquiera $x, y \in \mathbb{F}_{p^n}$ tenemos obviamente

$$(xy)^p = x^p\, y^p.$$

Para las sumas, notamos que $\mathbb{F}_{p^n}$ es un cuerpo de característica p, así que

$$(x + y)^p = \sum_{i+j=p} \binom{p}{i} x^i\, y^j = x^p + y^p,$$

puesto que $p \mid \binom{p}{i}$ para $i = 1, \ldots, p-1$. Esto demuestra que F es un homomorfismo $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. Como todo homomorfismo de cuerpos, F es automáticamente inyectivo. Puesto que $\mathbb{F}_{p^n}$ es finito, F es sobreyectivo.

El grupo multiplicativo $\mathbb{F}_{p^n}^\times$ es cíclico y podemos escoger un generador $\alpha \in \mathbb{F}_{p^n}^\times$. Todo elemento $x \in \mathbb{F}_{p^n}^\times$ es de la forma α^i para $i = 0, 1, \ldots, p^n - 2$, y para cualquier automorfismo $\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ se tiene

$$\sigma(\alpha^i) = \sigma(\alpha)^i.$$

Esto demuestra que σ está definido por la imagen de α. Consideremos las potencias del automorfismo de Frobenius

$$F^k := \underbrace{F \circ \cdots \circ F}_{k}\colon x \mapsto x^{p^k}.$$

Tenemos $F^k = \mathrm{id}$ si y solo si $\alpha^{p^k} = \alpha$; es decir, $\alpha^{p^k-1} = 1$ en $\mathbb{F}_{p^n}^\times$. Dado que α tiene orden $p^n - 1$ en el grupo $\mathbb{F}_{p^n}^\times$, lo último sucede si y solo si $(p^n - 1) \mid (p^k - 1)$; es decir, si y solo si $n \mid k$. Podemos concluir que

$$F^0 = \mathrm{id},\ F,\ F^2,\ \ldots,\ F^{n-1}$$

son n diferentes automorfismos de $\mathbb{F}_{p^n}$. Para terminar la prueba, hay que ver que $\mathbb{F}_{p^n}$ no tiene otros automorfismos.

Sea $f = m_{\alpha,\mathbb{F}_p}$ el polinomio mínimo de α sobre $\mathbb{F}_p$. Luego,

$$\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}.$$

En particular,

$$\deg f = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Tenemos $f(\alpha) = 0$, y para cualquier automorfismo $\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ necesariamente

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

así que $\sigma(\alpha)$ debe ser una raíz de f. Pero f, siendo un polinomio de grado n, tiene a lo sumo n raíces, y esto demuestra que $|\operatorname{Aut}(\mathbb{F}_{p^n})| \leq n$. ■

15.2.2. Corolario. *En un cuerpo finito $\mathbb{F}_{p^n}$ todo elemento es una p-ésima potencia.*

Demostración. Se sigue de la sobreyectividad del automorfismo de Frobenius $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. ■

15.2.3. Teorema. *Los subcuerpos de un cuerpo finito $\mathbb{F}_{p^n}$ corresponden a los divisores de n: son precisamente*

$$\mathbb{F}_{p^d} := \{x \in \mathbb{F}_{p^n} \mid x^{p^d} = x\}.$$

Demostración. Primero, si tenemos un subcuerpo $\mathbb{F} \subseteq \mathbb{F}_{p^n}$, entonces necesariamente $\mathbb{F}_p \subseteq \mathbb{F}$ y $|\mathbb{F}| = p^d$ para algún d. Luego,

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}] \cdot d,$$

demuestra que $d \mid n$. Dado que el grupo multiplicativo $\mathbb{F}^\times$ es cíclico de orden $p^d - 1$, los elementos de $\mathbb{F}$ son precisamente las raíces del polinomio $X^{p^d} - X \in \mathbb{F}_p[X]$:

$$\mathbb{F} = \mathbb{F}_d := \{x \in \mathbb{F}_{p^n} \mid x^{p^d} - x = 0\} = \{x \in \mathbb{F}_{p^n} \mid F^d(x) = x\}.$$

donde $F\colon x \mapsto x^p$ denota el automorfismo de Frobenius. Viceversa, para cualquier $d \mid n$ el conjunto $\mathbb{F}_{d^n}$ de arriba tiene p^d elementos: tenemos $(X^{p^d} - X) \mid (X^{p^n} - X)$ y el polinomio $X^{p^n} - X$ se descompone en factores lineales en $\mathbb{F}_{p^n}[X]$. Además, para cualquier cuerpo K y un endomorfismo $\sigma\colon K \xrightarrow{\cong} K$, el conjunto

$$K^\sigma := \{x \in K \mid \sigma(x) = x\}$$

es un subcuerpo de K: esto se sigue de las identidades

$$\sigma(x+y) = \sigma(x) + \sigma(y), \quad \sigma(1) = 1, \quad \sigma(xy) = \sigma(x)\,\sigma(y), \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

■

15.2.4. Ejemplo. Consideremos un cuerpo de $2^6 = 64$ elementos

$$\mathbb{F}_{64} = \mathbb{F}_2[X]/(X^6 + X^5 + X^3 + X^2 + 1).$$

Denotemos por α la imagen de X en el cociente. Tenemos

$$\mathbb{F}_{64} = \{a_5\,\alpha^5 + a_4\,\alpha^4 + a_3\,\alpha^3 + a_2\,\alpha^2 + a_1\,\alpha + a_0 \mid a_i = 0, 1\}.$$

Los elementos fijos bajo el automorfismo de Frobenius $F\colon x \mapsto x^2$ corresponden al subcuerpo

$$\mathbb{F}_2 = \{0, 1\}.$$

Los elementos fijos por $F^2\colon x \mapsto x^4$ corresponden al subcuerpo

$$\mathbb{F}_4 = \{0,\ 1,\ \alpha^4 + \alpha^2 + \alpha,\ \alpha^4 + \alpha^2 + \alpha + 1\}.$$

Los elementos fijos por $F^3\colon x \mapsto x^8$ corresponden al subcuerpo

$$\mathbb{F}_8 = \{0,\ 1,\ \alpha^2 + \alpha,\ \alpha^2 + \alpha + 1,\ \alpha^4 + \alpha,\ \alpha^4 + \alpha + 1,\ \alpha^4 + \alpha^2,\ \alpha^4 + \alpha^2 + 1\}.$$

▲

15.2.5. Comentario. Notamos que $\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle$ es el grupo cíclico de orden n generado por el automorfismo de Frobenius $F\colon x \mapsto x^p$. Los subgrupos de $\mathrm{Aut}(\mathbb{F}_{p^n})$ son precisamente $\langle F^d \rangle$ para $d \mid n$, y entonces hemos obtenido una biyección entre los subcuerpos de $\mathbb{F}_{p^n}$ y los subgrupos de $\mathrm{Aut}(\mathbb{F}_{p^n})$. Esto no es una coincidencia: es un caso particular de la **teoría de Galois**.

15.3 Cuerpos finitos y la reciprocidad cuadrática

Recordemos que para un número entero a y un primo p el **símbolo de Legendre** se define mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } p \nmid a \text{ y } a \text{ es un cuadrado módulo } p, \\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es un cuadrado módulo } p, \\ 0, & \text{si } p \mid a. \end{cases}$$

Tenemos las siguientes propiedades elementales.

a) El símbolo de Legendre es multiplicativo: se tiene

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

para cualesquiera $a, b \in \mathbb{Z}$.

b) Si p es un primo impar, entonces entre los números $\{1, 2, \ldots, p-1\}$ precisamente la mitad son cuadrados módulo p y la mitad no son cuadrados módulo p; en particular,

$$\sum_{0 \le i \le p-1} \left(\frac{i}{p}\right) = 0. \tag{15.1}$$

c) El símbolo de Legendre puede ser interpretado mediante el **criterio de Euler**: si p es un primo impar, entonces

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Todas estas propiedades se deducen fácilmente del hecho de que $\mathbb{F}_p^\times$ sea un grupo cíclico: existe un generador $\alpha \in \mathbb{F}_p^\times$ tal que todo elemento de $\mathbb{F}_p^\times$ es de la forma α^i para algún $i \in \mathbb{Z}$. Luego, α^i es un cuadrado si y solo si i es par (véase el capítulo 7 para los detalles).

El objetivo de esta sección es presentar una aplicación de cuerpos finitos en una prueba de la **ley de reciprocidad cuadrática** de Gauss.

1) Si p y q son diferentes primos impares, entonces

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right) = \begin{cases} +\left(\frac{p}{q}\right), & \text{si } p \equiv 1 \text{ o } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right), & \text{si } p \equiv 3 \text{ y } q \equiv 3 \pmod 4. \end{cases}.$$

2) La **primera ley suplementaria**: si p es un primo impar, entonces

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

3) La **segunda ley suplementaria**: si p es un primo impar, entonces

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

15.3.1. Ejemplo. He aquí una pequeña tabla de los valores de $\left(\frac{p}{q}\right)$.

p \ q	3	5	7	11	13	17	19	23	29	31
-1	$-$	$+$	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$-$
2	$-$	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$-$	$+$
3	0	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$-$	$-$
5	$-$	0	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$+$
7	$+$	$-$	0	$-$	$-$	$-$	$+$	$-$	$+$	$+$
11	$-$	$+$	$+$	0	$-$	$-$	$+$	$-$	$-$	$-$
13	$+$	$-$	$-$	$-$	0	$+$	$-$	$+$	$+$	$-$
17	$-$	$-$	$-$	$-$	$+$	0	$+$	$-$	$-$	$-$
19	$+$	$+$	$-$	$-$	$-$	$+$	0	$-$	$-$	$+$
23	$-$	$-$	$+$	$+$	$+$	$-$	$+$	0	$+$	$-$
29	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$+$	0	$-$
31	$+$	$+$	$-$	$+$	$-$	$-$	$-$	$+$	$-$	0

▲

Notamos que la primera ley suplementaria se deduce inmediatamente del criterio de Euler. Otro modo de verlo: para $\alpha \in \mathbb{F}_p^\times$ se tiene $\alpha^2 = -1$ si y solamente si el orden de α es igual a 4. Entonces, -1 es un cuadrado si y solo si $4 \mid (p-1)$.

Vamos a probar la segunda ley suplementaria y luego la ley principal. Nuestra exposición sigue [IR1990, Chapter 6], pero en lugar de las raíces de la unidad ζ_n usamos los cuerpos finitos, según lo indicado en [IR1990, §7.3].

La segunda ley suplementaria

Antes de probar la ley principal, empecemos por la segunda ley suplementaria. Si p es un primo impar, entonces $p^2 \equiv 1 \pmod 8$, puesto que cualquier cuadrado de un número impar es congruente a 1 módulo 8:

$$1^2 = 1, \quad 3^2 = 9, \quad 5^2 = 25, \quad 7^2 = 49.$$

Consideremos el cuerpo finito $\mathbb{F}_{p^2}$. El grupo multiplicativo $\mathbb{F}_{p^2}^\times$ es cíclico de orden $p^2 - 1$, y dado que $8 \mid (p^2 - 1)$, existe un elemento $\alpha \in \mathbb{F}_{p^2}^\times$ de orden 8. Notamos que

$$(\alpha^4 - 1)(\alpha^4 + 1) = \alpha^8 - 1 = 0.$$

Dado que $\alpha^4 \neq 1$, tenemos $\alpha^4 = -1$, de donde se siguen las identidades

$$\alpha^2 + \alpha^{-2} = 0, \quad \alpha^3 = -\alpha^{-1}.$$

Pongamos

$$\tau := \alpha + \alpha^{-1}.$$

Notamos que $\tau \neq 0$. En efecto, si $\alpha^{-1} = -\alpha$, entonces $\alpha^2 = -1$ y luego $\alpha^4 = 1$, pero no es el caso.

Tenemos

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = (\alpha^2 + 2 + \alpha^{-2})^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right),$$

donde la última igualdad se sigue del criterio de Euler. En consecuencia

$$\alpha^p + \alpha^{-p} = (\alpha + \alpha^{-1})^p = \tau^p = \left(\frac{2}{p}\right)\tau.$$

Dado que α tiene orden 8, la expresión a la izquierda depende solamente del residuo de p módulo 8:

$$\alpha^p + \alpha^{-p} = \left\{ \begin{array}{ll} \alpha + \alpha^{-1} = \tau, & p \equiv \pm 1 \pmod 8 \\ \alpha^3 + \alpha^{-3} = -\tau, & p \equiv \pm 3 \pmod 8 \end{array} \right\} = (-1)^{\frac{p^2-1}{8}}\tau.$$

Comparando las últimas dos identidades, se obtiene

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

15.3.2. Comentario. El mismo argumento funciona para la raíz de la unidad ζ_8 en lugar de α y el anillo $\mathbb{Z}[\zeta_8]$ en lugar de $\mathbb{F}_{p^2}$. En este caso hay que considerar identidades en $\mathbb{Z}[\zeta_8]$ módulo p.

La ley principal

Sean p y q dos diferentes primos impares. Podemos escoger un número $n = 1, 2, 3, \ldots$ tal que

$$q^n \equiv 1 \pmod p$$

(por ejemplo, basta tomar $n = p - 1$). Consideremos el cuerpo finito $\mathbb{F}_{q^n}$. El grupo multiplicativo $\mathbb{F}_{q^n}^\times$ es cíclico de orden $q^n - 1$. Por nuestra elección de n, se tiene $p \mid (q^n - 1)$, así que existe un elemento $\alpha \in \mathbb{F}_{q^n}^\times$ de orden p.

Para $a \in \mathbb{Z}$ pongamos

$$\tau_a := \sum_{0 \leq i \leq p-1} \left(\frac{i}{p}\right) \alpha^{ai} \in \mathbb{F}_{q^n}.$$

En particular, definamos

$$\tau := \tau_1.$$

A partir de ahora y hasta el final de esta sección, todos los sumatorios serán entre 0 y $p - 1$, así que por brevedad vamos a escribir "$\sum_i$" en lugar de "$\sum_{0 \leq i \leq p-1}$".

15.3.3. Lema. *Tenemos*

$$\sum_i \alpha^{ai} = \begin{cases} p, & si\ p \mid a, \\ 0, & si\ p \nmid a. \end{cases}$$

Demostración. Si $p \mid a$, entonces $\alpha^{ai} = 1$ para todo $0 \leq i \leq p - 1$, así que

$$\sum_i \alpha^{ai} = p.$$

Si $p \nmid a$, entonces $\alpha^a \neq 1$, y luego

$$\sum_i \alpha^{ai} = \frac{\alpha^{ap} - 1}{\alpha^a - 1} = 0.$$

■

15.3.4. Proposición (Gauss). *En $\mathbb{F}_{q^n}$ se cumplen las identidades*

1) $\tau_a = \left(\frac{a}{p}\right)\,\tau$.

2) $\tau^2 = (-1)^{\frac{p-1}{2}}\,p$.

Demostración. Si $p \mid a$, entonces

$$\left(\frac{a}{p}\right) = 0.$$

Por otro lado, tenemos $\alpha^{ai} = 1$ para todo $0 \leq i \leq p-1$, dado que el orden de α es igual a p, y luego,

$$\tau_a = \sum_i \left(\frac{i}{p}\right) = 0$$

por (15.1). Si $p \nmid a$, entonces calculamos que

$$\left(\frac{a}{p}\right)\,\tau_a = \sum_i \left(\frac{ai}{p}\right)\,\alpha^{ai} = \sum_j \left(\frac{j}{p}\right)\,\alpha^j = \tau$$

—el símbolo de Legendre $\left(\frac{j}{p}\right)$ y el elemento α^j dependen solo del resto de j módulo p y los números ai para $0 \leq i \leq p-1$ nos dan todos los restos módulo p. Ahora $\left(\frac{a}{p}\right) = \pm 1$, así que al multiplicar la identidad de arriba por $\left(\frac{a}{p}\right)$ nos queda la identidad 1)

$$\tau_a = \left(\frac{a}{p}\right)\,\tau.$$

Probemos la segunda identidad. Notamos que si $p \nmid a$, entonces la identidad 1) nos da

$$\tau_a\,\tau_{-a} = \left(\frac{a}{p}\right)\,\left(\frac{-a}{p}\right)\,\tau^2 = \left(\frac{-1}{p}\right)\,\tau^2,$$

y si $p \mid a$, entonces $\tau_a\,\tau_{-a} = 0$. Luego,

$$\sum_a \tau_a\,\tau_{-a} = \left(\frac{-1}{p}\right)\,(p-1)\,\tau^2. \tag{15.2}$$

Por otro lado, tenemos

$$\tau_a\,\tau_{-a} = \sum_i \sum_j \left(\frac{i}{p}\right)\,\left(\frac{j}{p}\right)\,\alpha^{a\,(i-j)},$$

y sumando estas identidades para $0 \leq a \leq p-1$, se obtiene

$$\sum_a \tau_a\,\tau_{-a} = \sum_i \sum_j \left(\frac{i}{p}\right)\,\left(\frac{j}{p}\right)\,\sum_a \alpha^{a\,(i-j)}.$$

El cálculo del lema 15.3.3 nos dice que

$$\sum_a \alpha^{a\,(i-j)} = \begin{cases} p, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

Entonces,

$$\sum_a \tau_a \, \tau_{-a} = \sum_i \left(\frac{i}{p}\right)^2 p = (p-1)\, p. \tag{15.3}$$

Comparando (15.2) y (15.3), tenemos

$$\left(\frac{-1}{p}\right)(p-1)\,\tau^2 = (p-1)\,p,$$

de donde

$$\tau^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p.$$

■

Estamos listos para probar la ley de reciprocidad cuadrática. Denotemos

$$p^* := (-1)^{\frac{p-1}{2}} p.$$

La segunda identidad de 15.3.4 nos dice que

$$\tau^2 = p^* \quad \text{en } \mathbb{F}_{q^n}.$$

Entonces,

$$\left(\frac{p^*}{q}\right) = 1 \iff \tau \in \mathbb{F}_q \subset \mathbb{F}_{q^n} \iff \tau^q = \tau.$$

(En efecto, si p^* es un cuadrado en $\mathbb{F}_q$, entonces $p^* = x^2$ para algún $x \in \mathbb{F}_q$. Pero en este caso $\tau = \pm x$, así que $\tau \in \mathbb{F}_q$. Viceversa, si $\tau \in \mathbb{F}_q$, entonces $p^* = \tau^2$ es un cuadrado en $\mathbb{F}_q$.) Luego, tenemos en $\mathbb{F}_{q^n}$

$$\tau^q = \left(\sum_i \left(\frac{i}{p}\right) \alpha^i\right)^q = \sum_i \left(\frac{i}{p}\right)^q \alpha^{qi} = \sum_i \left(\frac{i}{p}\right) \alpha^{qi} = \tau_q = \left(\frac{q}{p}\right) \tau,$$

según la primera identidad 15.3.4. Entonces, la condición $\tau^q = \tau$ equivale a

$$\left(\frac{q}{p}\right) = 1.$$

Hemos probado que

$$\left(\frac{p^*}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1.$$

Esto equivale a la identidad

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right).$$

15.3.5. Comentario. Estos cálculos se pueden hacer con la raíz de la unidad ζ_p en lugar de α. En este caso la expresión

$$g_a := \sum_{0 \le a \le p-1} \left(\frac{a}{p}\right) \zeta_p^a, \quad g := g_1$$

se conoce como la **suma cuadrática de Gauss**. Muchas pruebas de la reciprocidad cuadrática, incluso una de las pruebas de Gauss, se basan en la identidad

$$g^2 = \left(\frac{-1}{p}\right) p.$$

En el tratado de Gauss "Disquisitiones Arithmeticae" aparecen ocho pruebas diferentes de la reciprocidad cuadrática, y hoy en día se conocen alrededor de 250[*]. Para más información sobre las leyes de reciprocidad en el contexto histórico, véase el libro [Lem2000].

15.4 Perspectiva: ecuaciones sobre cuerpos finitos

> Presently, the topic which amuses me most is counting points on algebraic curves over finite fields. It is a kind of applied mathematics: you try to use any tool in algebraic geometry and number theory that you know of... and you don't quite succeed!
>
> Una entrevista a Jean–Pierre Serre, 1985

Consideremos un cuerpo finito $\mathbb{F}_q$. Sus extensiones finitas son de la forma $\mathbb{F}_{q^k}$ para $k = 1, 2, 3, \ldots$ Denotemos por

$$\mathbb{A}^n(\mathbb{F}_{q^k}) := \mathbb{F}_{q^k}^n$$

el espacio afín de dimensión n sobre $\mathbb{F}_{q^k}$. Para una colección de polinomios $f_1, f_2, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_n]$, consideremos el conjunto de sus ceros en común en $\mathbb{F}_{q^k}^n$:

$$V(\mathbb{F}_{q^k}) := \{\underline{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_{q^k}) \mid f_1(\underline{x}) = f_2(\underline{x}) = \cdots = f_s(\underline{x}) = 0\}.$$

Este conjunto es finito, siendo un subconjunto de $\mathbb{A}^n(\mathbb{F}_{q^k})$ que tiene q^{kn} elementos. Entonces, cabe preguntarse, cómo el número de elementos de $V(\mathbb{F}_{q^k})$ depende de k. Este problema fue uno de los más importantes en las matemáticas del siglo XX. A saber, esto se estudia mediante **función zeta** definida por

$$Z(V_{/\mathbb{F}_q}, t) := \exp\left(\sum_{k \geq 1} \#V(\mathbb{F}_{q^k}) \, \frac{t^k}{k}\right).$$

Esta expresión también puede ser considerada como una serie formal en $\mathbb{Q}[\![t]\!]$

En 1960 Bernard Dwork probó que $Z(V_{/\mathbb{F}_q}, t)$ es siempre una función racional. En términos de las series formales, esto significa que $Z(V_{/\mathbb{F}_q}, t) = f/g$ para algunos polinomios $f, g \in \mathbb{Q}[t]$. Conociendo esta función racional, se puede considerar los coeficientes de la serie $\log(f/g)$ para recuperar los números $\#V(\mathbb{F}_{q^k})$ para todo $k = 1, 2, 3, \ldots$

La prueba de Dwork está explicada en el libro [Kob1984] y aquí vamos considerar solo un par de casos particulares.

Círculo unitario

El círculo unitario viene dado por la ecuación $X^2 + Y^2 = 1$. Consideremos entonces el conjunto

$$C(\mathbb{F}_q) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_q) \mid x^2 + y^2 = 1\}.$$

Primero, si $q = 2^k$, entonces todo elemento de $\mathbb{F}_{2^k}$ es un cuadrado: para todo $\alpha \in \mathbb{F}_{2^k}$ existe $\beta \in \mathbb{F}_{2^k}$ tal que $\alpha = \beta^2$. Además, este β es único: se tiene

$$X^2 - \alpha = (X - \alpha)^2.$$

[*] Véase http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

Entonces, cualquier $x \in \mathbb{F}_{2^k}$ define un punto único

$$(x, \sqrt{1-x^2}) \in C(\mathbb{F}_{2^k}).$$

Se sigue que

$$\#C(\mathbb{F}_{2^k}) = 2^k.$$

15.4.1. Ejemplo. Sobre $\mathbb{F}_2$, los puntos del círculo $C(\mathbb{F}_2)$ son

$$(1,0),\ (0,1).$$

Sobre el cuerpo

$$\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2+X+1) = \{0,1,\alpha,\alpha+1\}$$

los puntos del círculo $C(\mathbb{F}_4)$ son

$$(0,1),\ (1,0),\ (\alpha,\alpha+1),\ (\alpha+1,\alpha).$$

En efecto, tenemos

$$\alpha^2 = \alpha+1, \quad (\alpha+1)^2 = \alpha.$$

▲

Ahora si q es impar, el problema se vuelve más interesante. Analicemos algunos ejemplos.

15.4.2. Ejemplo. Tenemos

$$\begin{aligned} C(\mathbb{F}_3) &= \{(0,1),\ (0,2),\ (1,0),\ (2,0)\},\\ C(\mathbb{F}_5) &= \{(0,1),\ (0,4),\ (1,0),\ (4,0)\},\\ C(\mathbb{F}_7) &= \{(0,1),\ (0,6),\ (1,0),\ (2,2),\ (2,5),\ (5,2),\ (5,5),\ (6,0)\}. \end{aligned}$$

En el cuerpo

$$\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1) = \{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$$

Los cuadrados son

$$\begin{aligned} 1^2 = 2^2 &= 1,\\ \alpha^2 = (2\alpha)^2 &= 2,\\ (\alpha+1)^2 = (2\alpha+2)^2 &= 2\alpha,\\ (\alpha+2)^2 = (2\alpha+1)^2 &= \alpha. \end{aligned}$$

Luego,

$$\alpha^2 + \alpha^2 = (2\alpha)^2 + (2\alpha)^2 = \alpha^2 + (2\alpha)^2 = 1.$$

Tenemos

$$C(\mathbb{F}_9) = \{(0,1),\ (0,2),\ (1,0),\ (2,0),\ (\alpha,\alpha),\ (\alpha,2\alpha),\ (2\alpha,\alpha),\ (2\alpha,2\alpha)\}.$$

▲

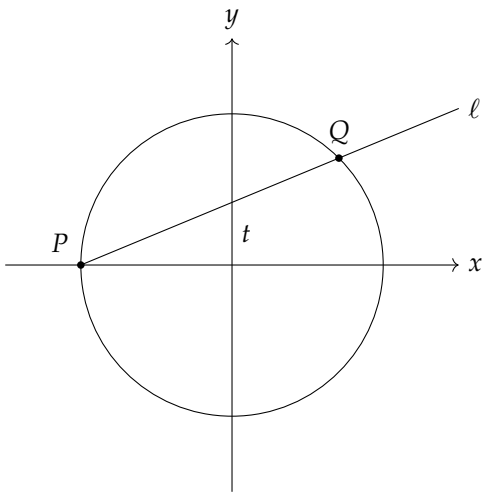
He aquí una pequeña tabla que podemos compilar con ayuda de una computadora:

q:	3	5	7	9	11	13	17	19	23	25	27	29	31	37	41	$\cdots$
q mód 4:	3	1	3	1	3	1	1	3	3	1	3	1	3	1	1	$\cdots$
$\#C(\mathbb{F}_q)$:	4	4	8	8	12	12	16	20	24	24	28	28	32	36	40	$\cdots$

Se nota que $\#C(\mathbb{F}_q) = q \pm 1$. Para explicar qué está pasando, recordemos la parametrización del círculo. Sería instructivo hacer un dibujo del círculo real. El punto $P = (-1, 0)$ siempre está en el circulo. Podemos trazar una recta que pasa por P y tiene otra intersección con el círculo. Esta recta necesariamente tendrá ecuación

$$\ell \colon Y = tX + t$$

para algún t.



La intersección de esta recta con el círculo viene dada por[*]

$$Q = (x, y),\ y = t\,x + t,\ x^2 + y^2 = 1 \Longrightarrow (x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

Viceversa, la recta que pasa por P y $Q = (x, y)$ tiene ecuación

$$Y = t\,X + t, \quad t = \frac{y}{x + 1}.$$

Ahora si trabajamos sobre un cuerpo $\mathbb{F}_q$, puede pasar que $t^2 = -1$. Entonces, lo que tenemos es una aplicación

$$\begin{aligned} \phi \colon \{t \in \mathbb{F}_q \mid t^2 \neq -1\} &\to C(\mathbb{F}_q) \setminus \{(-1, 0)\}, \\ t &\mapsto \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right). \end{aligned}$$

Esta aplicación está bien definida:

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) \neq (-1, 0)$$

[*]El lector probablemente reconocerá las identidades trigonométricas

$$\cos\alpha = \frac{\cos^2(\alpha/2) - \operatorname{sen}^2(\alpha/2)}{\cos^2(\alpha/2) + \operatorname{sen}^2(\alpha/2)} = \frac{1 - \tan^2(\alpha/2)}{1 + \tan^2(\alpha/2)}$$

y

$$\operatorname{sen}\alpha = \frac{2\operatorname{sen}(\alpha/2)\cos(\alpha/2)}{\cos^2(\alpha/2) + \operatorname{sen}^2(\alpha/2)} = \frac{2\tan(\alpha/2)}{1 + \tan^2(\alpha/2)}.$$

si q es impar. Notamos que si para $(x,y) \in C(\mathbb{F}_q)$ tenemos

$$\left(\frac{y}{x+1}\right)^2 = -1,$$

entonces

$$y^2 = -(x+1)^2,$$

y luego la ecuación

$$x^2 + y^2 = x^2 - (x-1)^2 = -2x - 1 = 1$$

nos dice que $(x,y) = (-1,0)$. Entonces, tenemos una aplicación bien definida

$$\psi\colon C(\mathbb{F}_q) \setminus \{(-1,0)\} \to \{t \in \mathbb{F}_q \mid t^2 \neq -1\},$$
$$(x,y) \mapsto \frac{y}{x+1}.$$

Las aplicaciones ϕ y ψ son mutualmente inversas:

$$\psi \circ \phi(t) = t, \quad \phi \circ \psi(x,y) = (x,y)$$

para cualesquiera $t \in \mathbb{F}_q$ con $t^2 \neq 1$ y $(x,y) \in C(\mathbb{F}_q)$ con $x \neq -1$. Esta biyección nos permite concluir que

$$\#C(\mathbb{F}_q) - 1 = \#\{t \in \mathbb{F}_q \mid t^2 \neq -1\}.$$

Ahora si -1 es un cuadrado en $\mathbb{F}_q$, la ecuación $t^2 = -1$ tiene dos soluciones. Tenemos entonces

$$\#C(\mathbb{F}_q) = \begin{cases} q+1, & \text{si } -1 \text{ no es un cuadrado en } k, \\ q-1, & \text{si } -1 \text{ es un cuadrado en } k. \end{cases}$$

Falta notar que -1 es un cuadrado en $\mathbb{F}_q^\times$ si y solamente si $q \equiv 1 \pmod 4$ (véase el ejercicio 15.9). Resumamos nuestros resultados.

15.4.3. Proposición. *Se tiene*

$$\#C(\mathbb{F}_q) = \begin{cases} q, & \text{si } q \text{ es par}, \\ q+1, & \text{si } q \equiv 3 \pmod 4, \\ q-1, & \text{si } q \equiv 1 \pmod 4. \end{cases}$$

Calculemos la función zeta correspondiente

$$Z(C_{/\mathbb{F}_q}, t) := \exp\left(\sum_{k\geq 1} \#C(\mathbb{F}_{q^k})\,\frac{t^k}{k}\right).$$

1) Si q es par, enconces $\#C(\mathbb{F}_{q^k}) = q^k$ y tenemos

$$Z(C_{/\mathbb{F}_q}, t) = \exp\left(\sum_{k\geq 1} \frac{(qt)^k}{k}\right).$$

Recordemos la serie para el logaritmo

$$\log(1+t) = \sum_{k\geq 1} (-1)^{k+1}\,\frac{t^k}{k} = t - \frac{t^2}{2} + \frac{t^3}{3} - \frac{t^4}{4} + \cdots$$

Luego,

$$-\log(1-t) = \sum_{k\geq 1} \frac{t^k}{k} = t - \frac{t^2}{2} + \frac{t^3}{3} - \frac{t^4}{4} + \cdots$$

En nuestro caso, tenemos

$$Z(C_{/\mathbb{F}_q}, t) = \exp(-\log(1-qX)) = \frac{1}{1-qX}.$$

2) Si $q \equiv 3 \pmod 4$, entonces $q^k \equiv (-1)^k \pmod 4$, de donde se obtiene

$$\#C(\mathbb{F}_{q^k}) = \begin{cases} q^k + 1, & \text{si } k \text{ es impar,} \\ q^k - 1, & \text{si } k \text{ es par.} \end{cases}$$

Luego,

$$Z(C_{/\mathbb{F}_q}, t) = \exp\left(\sum_{k\geq 1} \frac{(q\,t)^k}{k} + \sum_{k\geq 1} (-1)^{k+1} \frac{t^k}{k}\right) = \exp(-\log(1-qt) + \log(1+t)) = \frac{1+t}{1-qt}.$$

3) De la misma manera, si $q \equiv 1 \pmod 4$, entonces $q^k \equiv 1 \pmod 4$ para todo $k = 1, 2, 3, \ldots$ y

$$\#C(\mathbb{F}_{q^k}) = q^k - 1.$$

La función zeta entonces viene dada por

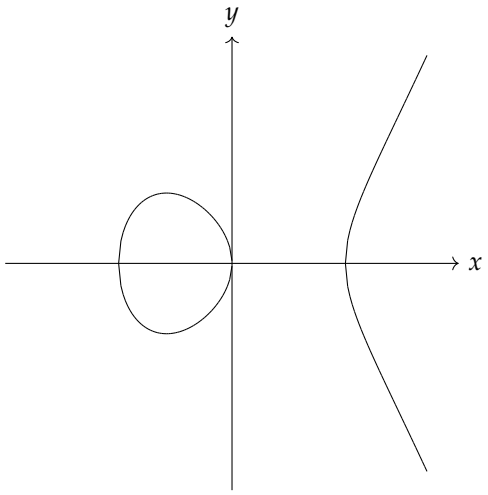
$$Z(C_{/\mathbb{F}_q}, t) = \exp\left(\sum_{k\geq 1} \frac{(q\,t)^k}{k} - \sum_{k\geq 1} \frac{t^k}{k}\right) = \exp(-\log(1-qt) + \log(1-t)) = \frac{1-t}{1-qt}.$$

La curva $Y^2 = X^3 - X$

Consideremos el conjunto

$$E_0(\mathbb{F}_q) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_q) \mid y^2 = x^3 - x\}.$$

He aquí la gráfica de los puntos reales de la curva $y^2 = x^3 - x$:



De nuevo, nuestro objetivo sería investigar cómo la cardinalidad de $E_0(\mathbb{F}_q)$ depende de q. Como en el caso del círculo unitario, si $q = 2^k$, entonces para todo $x \in \mathbb{F}_q$ existe un único y tal que $y^2 = x^3 - x$. Se sigue que

$$\#E_0(\mathbb{F}_{2^k}) = 2^k.$$

En característica diferente de 2, no todo elemento es un cuadrado y el problema es mucho más interesante.

15.4.4. Ejemplo.

$$\begin{aligned}
\#E_0(\mathbb{F}_3) &= \{(0,0),(0,1),(0,2)\},\\
\#E_0(\mathbb{F}_5) &= \{(0,0),(0,1),(0,4),(1,2),(2,3),(3,3),(2,3)\},\\
\#E_0(\mathbb{F}_7) &= \{(0,0),(0,1),(0,6),(1,5),(2,4),(5,4),(6,5)\}.
\end{aligned}$$

▲

Con ayuda de una computadora compilemos una pequeña tabla:

q:	3	5	7	9	11	13	17	19	23	25	27	29	31	37	41	$\cdots$
q mód 4:	3	1	3	1	3	1	1	3	3	1	3	1	3	1	1	$\cdots$
$\#E_0(\mathbb{F}_q)$:	3	7	7	15	11	7	15	19	23	31	27	39	31	39	31	$\cdots$

Aquí se nota un patrón:

$$\#E_0(\mathbb{F}_q) = q, \quad \text{si } q \equiv 3 \pmod 4,$$

y esto es lo que vamos a probar en esta sección.

Usando el hecho de que el grupo $\mathbb{F}_q^\times$ sea cíclico de orden $q-1$, se puede ver que precisamente la mitad de los elementos de $\mathbb{F}_q^\times$ son cuadrados y la mitad no son cuadrados, con la siguiente "tabla de multiplicación"[*]:

$\times$	cuadrado	no-cuadrado
cuadrado	cuadrado	no-cuadrado
no-cuadrado	no-cuadrado	cuadrado

Consideremos la función

$$f(x) := x^3 - x.$$

Primero notamos que la ecuación $f(x) = 0$ tiene tres diferentes soluciones $x = 0, \pm 1$. Esto nos da tres puntos

$$(0,0),\ (1,0),\ (-1,0) \in E_0(\mathbb{F}_q).$$

Asumamos que $q \equiv 3 \pmod 4$. En este caso -1 no es un cuadrado en $\mathbb{F}_q^\times$. Ahora si $x \neq 0, \pm 1$, tenemos $f(x) \neq 0$. Dado que $f(x) = -f(-x)$ y -1 no es un cuadrado, precisamente un elemento entre $f(x)$ y $f(-x)$ es un cuadrado. Se sigue que exactamente para la mitad de los $x \neq 0, \pm 1$, el elemento $f(x)$ es un cuadrado. En este caso la ecuación

$$y^2 = f(x)$$

tiene dos soluciones $y \in \mathbb{F}_q^\times$. Luego,

$$\#E_0(\mathbb{F}_q) = 3 + 2 \cdot \frac{q-3}{2} = q.$$

15.4.5. Proposición. *Si q es par o $q \equiv 3 \pmod 4$, entonces*

$$\#E_0(\mathbb{F}_q) = q.$$

[*]Véase el ejercicio 15.8.

Por otro lado, cuando $q \equiv 1 \pmod 4$, las cosas se vuelven mucho más interesantes. Para formular la respuesta, recordemos que el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ es un dominio de factorización única. Recordemos (de los ejercicios del capítulo anterior) que un primo impar p es primo en $\mathbb{Z}[\sqrt{-1}]$ si $p \equiv 3 \pmod 4$ y si $p \equiv 1 \pmod 4$, entonces

$$p = N(\pi) = \pi\,\overline{\pi} = a^2 + b^2$$

para un primo $\pi = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$. Notamos que los números a y b no son nulos y tienen diferente paridad, así que hay ocho diferentes opciones para escoger este π que corresponden al cambio del signo de a y de b y el intercambio de a con b. Se puede escoger uno de estos π que es **primario** en el siguiente sentido.

15.4.6. Definición. Se dice que un entero de Gauss no invertible $\alpha = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ es **primario** si $\alpha \equiv 1 \pmod{2 + 2\sqrt{-1}}$. Esto sucede si y solo si se cumple una de las dos condiciones:

1) $a \equiv 1$ y $b \equiv 0 \pmod 4$;

2) $a \equiv 3$ y $b \equiv 2 \pmod 4$.

15.4.7. Ejemplo. Si pedimos que $N(\pi) = 5$, entonces hay 8 posibilidades:

$$\pi = 2 \pm \sqrt{-1},\ \ -2 \pm \sqrt{-1},\quad 1 \pm 2\sqrt{-1},\ \ -1 \pm 2\sqrt{-1}.$$

Los elementos primarios son $-1 \pm 2\sqrt{-1}$. ▲

15.4.8. Teorema ([IR1990, §18.4, Theorem 5]). *Sean p un número primo tal que $p \equiv 1 \pmod 4$ y $\pi \in \mathbb{Z}[\sqrt{-1}]$ un entero de Gauss tal que $N(\pi) = p$ y π es primario. Entonces,*

$$\#E_0(\mathbb{F}_p) = p - 2\,\mathrm{Re}\,\pi.$$

15.4.9. Ejemplo. He aquí una pequeña tabla de los π como en el teorema y el número de puntos correspondiente en la curva.

p:	5	13	17	29	37	41	$\cdots$
π:	$-1 \pm 2\sqrt{-1}$	$3 \pm 2\sqrt{-1}$	$1 \pm 4\sqrt{-1}$	$-5 \pm 2\sqrt{-1}$	$-1 \pm 6\sqrt{-1}$	$5 \pm 4\sqrt{-1}$	$\cdots$
$\#E_0(\mathbb{F}_p)$:	7	7	15	39	39	31	$\cdots$

▲

Para obtener los números $\#E_0(\mathbb{F}_{p^k})$ nos puede ayudar la función zeta. Por ciertas razones, es más conveniente añadir a E_0 un punto extra, denotado por O, y trabajar con

$$E := E_0 \cup \{O\}.$$

Entonces,

$$\#E(\mathbb{F}_q) = E_0(\mathbb{F}_q) + 1.$$

15.4.10. Teorema. *Para q impar se tiene*

$$Z(E_{/\mathbb{F}_q}, t) = \frac{1 - at + qt^2}{(1-t)\,(1-qt)} + 1, \quad \textit{donde } a = q + 1 - \#E(\mathbb{F}_q).$$

El lector interesado puede consultar [Sil2009, §V.2] y [Kob1993, §II.1–2] para más detalles. En nuestro caso tenemos

p:	3	5	7	11	13	$\cdots$
$\#E(\mathbb{F}_p)$:	4	8	8	12	8	$\cdots$
$p+1-\#E(\mathbb{F}_p)$:	0	-2	0	0	6	$\cdots$

Las funciones zeta correspondientes son entonces

$$Z(E_{/\mathbb{F}_3},t) = \frac{1+3t^2}{(1-t)\,(1-3t)},$$
$$Z(E_{/\mathbb{F}_5},t) = \frac{1+2t+5t^2}{(1-t)\,(1-5t)},$$
$$Z(E_{/\mathbb{F}_7},t) = \frac{1+7t^2}{(1-t)\,(1-7t)},$$
$$Z(E_{/\mathbb{F}_{11}},t) = \frac{1+11t^2}{(1-t)\,(1-11t)},$$
$$Z(E_{/\mathbb{F}_{13}},t) = \frac{1-6t+13t^2}{(1-t)\,(1-13t)},$$

de donde se calculan las series[*]

$$\log Z(E_{/\mathbb{F}_3},t) = 4\,t + \frac{16}{2}\,t^2 + \frac{28}{3}\,t^3 + \frac{64}{4}\,t^4 + \frac{244}{5}\,t^5 + \cdots$$
$$\log Z(E_{/\mathbb{F}_5},t) = 8\,t + \frac{32}{2}\,t^2 + \frac{104}{3}\,t^3 + \frac{640}{4}\,t^4 + \frac{3208}{5}\,t^5 + \cdots$$
$$\log Z(E_{/\mathbb{F}_7},t) = 8\,t + \frac{64}{2}\,t^2 + \frac{344}{3}\,t^3 + \frac{2304}{4}\,t^4 + \frac{16\,808}{5}\,t^5 + \cdots$$
$$\log Z(E_{/\mathbb{F}_{11}},t) = 12\,t + \frac{144}{2}\,t^2 + \frac{1332}{3}\,t^3 + \frac{14\,400}{4}\,t^4 + \frac{161\,052}{5}\,t^5 + \cdots$$
$$\log Z(E_{/\mathbb{F}_{13}},t) = 8\,t + \frac{160}{2}\,t^2 + \frac{2216}{3}\,t^3 + \frac{28\,800}{4}\,t^4 + \frac{372\,488}{5}\,t^5 + \cdots$$

Tenemos entonces

p:	3	5	7	11	13	$\cdots$
$\#E(\mathbb{F}_p)$:	4	8	8	12	8	$\cdots$
$\#E(\mathbb{F}_{p^2})$:	16	32	64	144	160	$\cdots$
$\#E(\mathbb{F}_{p^3})$:	28	104	344	1332	2216	$\cdots$
$\#E(\mathbb{F}_{p^4})$:	64	640	2304	14 400	28 800	$\cdots$
$\#E(\mathbb{F}_{p^5})$:	244	3208	16 808	161 052	372 488	$\cdots$

El conteo de soluciones de ecuaciones polinomiales es un tema muy profundo. Por ejemplo, este es el hilo conductor del libro [IR1990].

15.5 Cerradura algebraica de $\mathbb{F}_p$

Consideremos un cuerpo finito $\mathbb{F}_p$. Sus extensiones son cuerpos finitos $\mathbb{F}_{p^n}$. Recordemos que si $m \mid n$, entonces $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$; específicamente, un subcuerpo de p^n elementos contiene un subcuerpo único de p^m

[*]Un ejemplo de este cálculo en PARI/GP:

```
? log ((1+3*t^2)/((1-t)*(1-3*t)))
% = 4*t + 8*t^2 + 28/3*t^3 + 16*t^4 + 244/5*t^5 + ...
```

elementos. Respecto a estas inclusiones, podemos tomar

$$\mathbb{F}_{p^\infty} := \bigcup_{n\geq 1} \mathbb{F}_{p^n}.$$

A saber, los elementos de $\mathbb{F}_{p^\infty}$ son $x \in \mathbb{F}_{p^m}$ e $y \in \mathbb{F}_{p^n}$, y para calcular $x\,y$ o $x \pm y$, hay que encajar x e y en $\mathbb{F}_{p^{\mathrm{mcm}(m,n)}}$. Se ve que esto es un cuerpo y es una extensión infinita de $\mathbb{F}_p$.

Todo polinomio $f \in \mathbb{F}_{p^\infty}[X]$ tendrá sus coeficientes en algún cuerpo finito $\mathbb{F}_{p^n}$ para n suficientemente grande, y el cuerpo de descomposición de f, siendo una extensión finita de $\mathbb{F}_{p^n}$, también será de la forma $\mathbb{F}_{p^N}$ y será un subcuerpo de $\mathbb{F}_{p^\infty}$. Esto demuestra que $\mathbb{F}_{p^\infty}$ es un cuerpo algebraicamente cerrado. Siendo la unión de extensiones finitas de $\mathbb{F}_p$, es una extensión algebraica de $\mathbb{F}_p$. Entonces, $\mathbb{F}_{p^\infty}$ es una cerradura algebraica de $\mathbb{F}_p$.

Sería interesante calcular el grupo de automorfismos $\mathrm{Aut}(\mathbb{F}_{p^\infty})$. Notamos que para todo automorfismo $\sigma\colon \mathbb{F}_{p^\infty} \xrightarrow{\cong} \mathbb{F}_{p^\infty}$ y todo polinomio $f \in \mathbb{F}_p[X]$ se cumple $f(\sigma(x)) = \sigma(f(x))$ para todo $x \in \mathbb{F}_{p^\infty}$. En particular, σ preserva los subcuerpos

$$\mathbb{F}_{p^n} = \{x \in \mathbb{F}_{p^\infty} \mid x^{p^n} - x = 0\},$$

y la restricción de σ a $\mathbb{F}_{p^n}$ es algún automorfismo de $\mathbb{F}_{p^n}$. Recordemos nuestro cálculo de los automorfismos de $\mathbb{F}_{p^n}$ en 15.2.1:

$$\begin{aligned} \mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle &\cong \mathbb{Z}/n\mathbb{Z}, \\ F^k &\mapsto [k]_n, \end{aligned}$$

donde $F\colon x \mapsto x^p$ es el automorfismo de Frobenius. Puesto que $\mathbb{F}_{p^\infty}$ es la unión de los $\mathbb{F}_{p^n}$, el automorfismo σ está definido de modo único por sus restricciones a $\mathbb{F}_{p^n}$. Notamos que si $m \mid n$, entonces el automorfismo $F^k\colon \mathbb{F}_{p^n}$ se restringe al automorfismo $F^\ell\colon \mathbb{F}_{p^m} \xrightarrow{\cong} \mathbb{F}_{p^m}$, donde $k \equiv \ell \pmod{m}$. Estas consideraciones nos llevan a la siguiente descripción de grupo de automorfismos de $\mathbb{F}_{p^\infty}$:

$$\mathrm{Aut}(\mathbb{F}_{p^\infty}) \cong \widehat{\mathbb{Z}} := \{(x_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z} \mid x_n \equiv x_m \pmod{m} \text{ para todo } m \mid n\}.$$

Este grupo se llama el grupo de los **enteros profinitos** y tiene cardinalidad $2^{\aleph_0}$. (Aunque muy grande, considerado como un **grupo topológico**, el grupo $\widehat{\mathbb{Z}}$ deja de ser tan asombroso; de hecho, es un grupo muy natural e importante en aritmética.)

15.6 Ejercicios

Ejercicio 15.1.

1) *Encuentre polinomios irreducibles de grado* 2

$$f \in \mathbb{F}_2[X] \quad y \quad g \in \mathbb{F}_3[X].$$

2) *Consideremos los cuerpos finitos*

$$\mathbb{F}_4 := \mathbb{F}_2[X]/(f) \quad y \quad \mathbb{F}_9 := \mathbb{F}_3[X]/(g)$$

de orden 4 *y* 9 *respectivamente. Escriba las tablas de adición y multiplicación para* $\mathbb{F}_4$ *y* $\mathbb{F}_9$.

3) *Encuentre el orden de cada elemento del grupo multiplicativo* $\mathbb{F}_4^\times$ *y* $\mathbb{F}_9^\times$.

4) *Consideremos la ecuación*

$$y^2 = x^3 - x.$$

Enumere todas sus soluciones $(x, y) \in R^2$, *donde*

$$R = \mathbb{F}_2,\ \mathbb{F}_3,\ \mathbb{F}_4,\ \mathbb{F}_9,\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z}.$$

Ejercicio 15.2. *Sea* $q = p^k$ *donde* p *es primo y* $k = 1, 2, 3, \ldots$ *Demuestre que para cualquier* $n = 1, 2, 3, \ldots$ *existe un polinomio mónico irreducible* $f \in \mathbb{F}_q[X]$ *de grado* n. *(Lo probamos en clase para* $k = 1$.*)*

Ejercicio 15.3. *Encuentre isomorfismos explícitos entre los cuerpos*

$$\mathbb{F}_3[X]/(X^2+1), \quad \mathbb{F}_3[X]/(X^2+X+2), \quad \mathbb{F}_3[X]/(X^2+2X+2).$$

Ejercicio 15.4. *Encuentre los polinomios mónicos irreducibles de grado* 3 *en* $\mathbb{F}_2[X]$ *factorizando* $X^8 - X$.

Ejercicio 15.5. *Sean* p *un número primo y* $n = 1, 2, 3, \ldots$ *Para* $\alpha \in \mathbb{F}_{p^n}$ *definamos*

$$N(\alpha) := \alpha\, \alpha^p\, \alpha^{p^2} \cdots \alpha^{p^{n-1}}.$$

1) *Demuestre que* $N(\alpha) \in \mathbb{F}_p$ *para todo* $\alpha \in \mathbb{F}_{p^n}$.

2) *Demuestre que*

$$N(\alpha\beta) = N(\alpha)\, N(\beta), \quad N(a\alpha) = a^n\, N(\alpha)$$

para cualesquiera $a \in \mathbb{F}_p$, $\alpha, \beta \in \mathbb{F}_{p^n}$.

3) *Demuestre que el homomorfismo de grupos multiplicativos* $N\colon \mathbb{F}_{p^n}^\times \to \mathbb{F}_p^\times$ *es sobreyectivo.*

Indicación: demuestre que $|\ker N| = \frac{p^n-1}{p-1}$ *e use el primer teorema de isomorfía.*

Ejercicio 15.6. *Sean* p *un número primo y* $n = 1, 2, 3, \ldots$ *Para el cuerpo finito* $\mathbb{F}_{p^n}$ *y un elemento* $\alpha \in \mathbb{F}_{p^n}$ *definamos* $T(\alpha) := \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$.

1) *Demuestre que* $T(\alpha) \in \mathbb{F}_p$.

2) *Demuestre que* $T\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ *es una aplicación* $\mathbb{F}_p$*-lineal.*

3) *Demuestre que la aplicación* $T\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ *es sobreyectiva.*

Ejercicio 15.7. *Sean p y q dos diferentes primos impares. Demuestre que el número de polinomios mónicos irreducibles de grado q en $\mathbb{F}_p[X]$ es igual a $\frac{1}{q}(p^q - p)$.*

Ejercicio 15.8. *Sea k un cuerpo.*

1) *Demuestre que los cuadrados en el grupo multiplicativo $k^\times$ forman un subgrupo*
$$(k^\times)^2 := \{\alpha \in k^\times \mid \alpha = x^2 \text{ para algún } x \in k^\times\} \subseteq k^\times.$$
2) *Enumere los cuadrados en el grupo $\mathbb{F}_9^\times$ para el cuerpo $\mathbb{F}_9$ construido en el ejercicio anterior.*
3) *Calcule el grupo cociente $k^\times/(k^\times)^2$ para $k = \mathbb{R}$ y $k = \mathbb{F}_q$, donde $q = p^k$ (considere por separado el caso de $p = 2$ y p impar).*

Ejercicio 15.9. *Sea $q = p^k$ donde p es un primo impar y $k = 1, 2, 3, \ldots$*

1) *Demuestre que -1 es un cuadrado en $\mathbb{F}_q$ si y solamente si -1 tiene orden 4 en el grupo cíclico $\mathbb{F}_q^\times$.*
2) *Concluya que -1 es un cuadrado en $\mathbb{F}_q$ si y solamente si $q \equiv 1 \pmod 4$.*
3) *Exprese -1 como un cuadrado en $\mathbb{F}_9$.*

Ejercicio 15.10 (generalización de 15.8). *Sea $q = p^k$ donde p es primo y $k = 1, 2, 3, \ldots$ Asumamos que $q \equiv 1 \pmod n$.*

1) *Demuestre que para todo $\alpha \in \mathbb{F}_q^\times$ la ecuación $x^n = \alpha$ o no tiene soluciones, o tiene n soluciones.*
2) *Demuestre que el subconjunto*
$$\{\alpha \in \mathbb{F}_q^\times \mid \alpha = x^n \text{ para algún } x \in \mathbb{F}_q^\times\}$$
es un subgrupo de $\mathbb{F}_q^\times$ de orden $\frac{q-1}{n}$.
3) *Por ejemplo, encuentre el subgrupo de cubos en $\mathbb{F}_{13}^\times$.*

Ejercicio 15.11. *Supongamos que p es un primo tal que $p \equiv 3 \pmod 4$. Demuestre que el anillo cociente $\mathbb{Z}[\sqrt{-1}]/(p)$ es un cuerpo de p^2 elementos.*

Ejercicio 15.12. *Para un entero de Gauss no invertible $\alpha = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ demuestre que*
$$\alpha \equiv 1 \pmod{2 + 2\sqrt{-1}}$$
si y solo si se cumple una de las dos condiciones:

1) *$a \equiv 1$ y $b \equiv 0 \pmod 4$;*
2) *$a \equiv 3$ y $b \equiv 2 \pmod 4$.*

Ejercicio 15.13. *Usando los resultados que vimos en clase, encuentre la cardinalidad del conjunto*
$$E_0(\mathbb{F}_p) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_p) \mid y^2 = x^3 - x\}$$
para $p = 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Ejercicio 15.14. *Demuestre que si $p \equiv 1 \pmod 4$, entonces el número $\#E(\mathbb{F}_p) = \#E_0(\mathbb{F}_p) + 1$ es siempre divisible por 4.*

Ejercicio 15.15. *Consideremos*

$$Z(t) = \frac{1 + 3\,t + 5t^2}{(1-t)\,(1-5\,t)} \in \mathbb{Q}(t).$$

1) *Exprese $Z(t)$ como una serie*

$$1 + \underbrace{a_1\,t + a_2\,t^2 + a_3\,t^3 + a_4\,t^4 + \cdots}_{=:f} \in \mathbb{Q}[\![t]\!]$$

(calcule por lo menos los coeficientes a_1 y a_2).

2) *Calcule los coeficientes b_1 y b_2 de la serie*

$$\log(1+f) := \sum_{k\geq 1} (-1)^{k+1}\,\frac{f^k}{k} = b_1\,t + \frac{b_2}{2}\,t^2 + \frac{b_3}{3}\,t^3 + \frac{b_4}{4}\,t^4 + \cdots \in \mathbb{Q}[\![t]\!]$$

Ejercicio 15.16. *Consideremos el espacio afín de dimensión n sobre el cuerpo finito $\mathbb{F}_{q^k}$:*

$$\mathbb{A}^n(\mathbb{F}_{q^k}) = \mathbb{F}_{q^k}^n.$$

Encuentre la expresión racional para la función zeta

$$Z(\mathbb{A}^n_{/\mathbb{F}_q}, t) := \exp\left(\sum_{k\geq 1} \#\mathbb{A}^n(\mathbb{F}_{q^k})\,\frac{t^k}{k}\right).$$

Ejercicio 15.17. *Para los conjuntos*

$$\begin{aligned} V_1(\mathbb{F}_{q^k}) &:= \{(x,y) \in \mathbb{A}^2(\mathbb{F}_{q^k}) \mid xy = 0\},\\ V_2(\mathbb{F}_{q^k}) &:= \{(x,y) \in \mathbb{A}^2(\mathbb{F}_{q^k}) \mid x^2 - y^2 = 0\},\\ V_3(\mathbb{F}_{q^k}) &:= \{(x,y,z) \in \mathbb{A}^3(\mathbb{F}_{q^k}) \mid x^2 = y^2 = z^2\} \end{aligned}$$

encuentre la expresión racional para $Z(V_{1/\mathbb{F}_q}, t)$, $Z(V_{2/\mathbb{F}_q}, t)$, $Z(V_{3/\mathbb{F}_q}, t)$.

Ejercicio 15.18. *Demuestre que si F es un cuerpo de característica diferente de 2 (posiblemente infinito), entonces existe una biyección entre los conjuntos*

$$\begin{aligned} V_1(F) &:= \{(x,y) \in \mathbb{A}^2(F) \mid xy = 0\},\\ V_2(F) &:= \{(x,y) \in \mathbb{A}^2(F) \mid x^2 - y^2 = 0\}. \end{aligned}$$

Ejercicio 15.19. *Sea p un número primo. Consideremos el polinomio $f := X^2 + X + 1 \in \mathbb{F}_p[X]$.*

1) *Demuestre que f es irreducible si y solo si $p \equiv 2 \pmod 3$.*

2) *¿Para cuáles p el polinomio f es separable?*

Ejercicio 15.20. *¿Para cuáles p el polinomio $f := X^2 + X + 2 \in \mathbb{F}_p[X]$ es irreducible? ¿separable?*

Ejercicio 15.21. *Sean p un número primo y $a \in \mathbb{F}_p$ un elemento no nulo. Consideremos el polinomio*

$$f := X^p - X + a \in \mathbb{F}_p[X].$$

En este ejercicio vamos a probar que f es irreducible.

1) *Demuestre que f es separable.*

2) *Sea L un cuerpo de descomposición de f y sea $\alpha \in L$ un elemento tal que $f(\alpha) = 0$. Demuestre que las raíces de f en L son $\alpha, \alpha + 1, \ldots, \alpha + p - 1$.*

3) *Asumamos que $f = gh$ donde $g, h \in \mathbb{F}_p[X]$ son polinomios mónicos y $\deg g, \deg h < \deg f$. Analizando la suma de las raíces de g o h, concluya que $\alpha \in \mathbb{F}_p$.*

4) *Demuestre que en este caso f se descompone en factores lineales en $\mathbb{F}_p[X]$ y deduzca una contradicción.*

Bibliografía

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4

[Kob1984] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003
http://dx.doi.org/10.1007/978-1-4612-1112-9

[Kob1993] _____, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR1216136
https://doi.org/10.1007/978-1-4612-0909-6

[Lem2000] Franz Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer-Verlag Berlin Heidelberg, 2000.
http://dx.doi.org/10.1007/978-3-662-12893-0

[Sil2009] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094
https://doi.org/10.1007/978-0-387-09494-6