MA0609 — Tópicos en Teoría de Números

Basado en las clases impartidas por Adrián Barquero

Notas tomadas por Ignacio Rojas

Verano 2021

Estas notas no están respaldadas por los profesores y han sido modificadas (a menudo de manera significativa) después de las clases. No están lejos de ser representaciones precisas de lo que realmente se dio en clase y en particular todos los errores son casi seguramente míos.

La teoría de curvas elípticas tiene al día de hoy más de 50 años de ser desarrollada continuamente. Fermat estudió ecuaciones que tenían relación con curvas elípticas y es hasta el día de hoy que se pueden ver las relaciones con estos temas. Este tema se puede ver desde las distintas areas de la matemática: análisis, álgebra, geometría... Hay métodos para el uso de firmas digitales y seguridad en tarjetas de crédito que están relacionados con curvas elípticas.

En fín, este tema es de mucho interés en la actualidad. Nosotros nos centraremos en los números racionales siguiendo la línea del libro de Silverman & Tate [2]. En concreto los temas a tratar son los siguientes:

(a) Introducción a geometría proyectiva.

(b) Curvas cúbicas y ecuaciones en forma normal de Weierstrass.

(c) Suma de puntos y la ley de grupo en curvas elípticas.

(d) Puntos de orden finito y el teorema Nagell-Lutz.

(e) La estructura del grupo de puntos racionales en una curva elíptica y el teorema Mordell-Weil.

Requisitos

Se asume un conocimiento básico de teoría de números. Se utilizarán conceptos de teoría de grupos y variable compleja a un nivel básico.

Índice general

Capítulo 1

Curvas elípticas

1.1. Día 1 | 20210105

Introducción a la geometría proyectiva

La vista algebraica

En general hay más de una manera en la que uno puede construir el plano proyectivo y más generalmente el espacio proyectivo en varias dimensiones. A manera de motivación, a la hora de estudiar ciertos problemas en matemática, se llega a observar que es suficiente trabajar con objetos en términos de clases de equivalencia.

Por ejemplo un problema que se discute en el Silverman y Tate [2], al estudiar las soluciones racionales de la ecuación

$$x^N + y^N = 1,$$

se puede ver que si $x = \frac{a}{c}$ y $y = \frac{b}{d}$ son soluciones racionales en su forma más reducida ($\mathrm{mcd}(a, c) = \mathrm{mcd}(b, d) = 1$, y $c, d > 0$) entonces debe ocurrir que $c = d$. Esto se logra después de un breve análisis de divisibilidad. Concluimos que la solución debe tener la forma $x = \frac{a}{c}$ y $y = \frac{b}{c}$.

Esta solución satisface que $a^N + b^N = c^N$ por lo que la solución $\left(\frac{a}{c}, \frac{b}{c}\right)$ del problema en términos racionales genera una solución (a, b, c) de la ecuación homogénea $x^N + y^N = z^N$. La clave aquí es que como la ecuación es homogénea, cualquier múltiplo de (a, b, c) va a ser una solución al mismo problema. Pero como estas soluciones se obtienen de manera relativamente trivial, podríamos querer considerarlas como equivalentes. Este tipo de razonamiento lleva a la definición algebraica del plano proyectivo.

Definición 1.1.1. El plano proyectivo sobre un cuerpo K es el cociente del conjunto

$\{\,(a,b,c) \in K^3 \backslash \{\,(0,0,0)\,\}\,\}$ por la relación

$$(a,b,c) \sim (a',b',c') \iff \exists t \in K^\times (a = ta',\ b = tb', c = tc').$$

Denotamos entonces

$$\mathbb{P}^2_K = \{\, x \in K^3 \backslash \{\, 0 \,\}\,\} \Big/ \sim,$$

y la clase de equivalencia de (a,b,c) la denotamos $[a,b,c]$ y se llamarán sus coordenadas homogéneas.

¿Qué pasa si incluimos el cero en nuestra definición del plano proyectivo?

Bueno, volviendo al ejemplo que presentamos, nos gustaría que nuestras soluciones estén en correspondencia. Claramente $(0,0,0)$ resuelve la ecuación homogénea, pero no la que tiene forma racional. Quizás de manera más interesante, $(1,-1,0)$ resuelve la ecuación homogénea con exponente impar. Pero esta no da una solución de la ecuación racional, entonces podríamos pensar por ejemplo que tenemos $((a_j,b_j,c_j)) \subseteq \mathbb{R}^3$ una sucesión de soluciones reales que converge a $(1,-1,0)$ y $c_j > 0$. Esta sucesión si genera soluciones $\left(\frac{a_j}{c_j}, \frac{b_j}{c_j}\right)$ de la ecuación racional y cuando $j \to \infty$ entonces este par ordenado tiende a $(\infty, -\infty)$. Podemos entonces pensar que las tripletas con tercera coordenada nula corresponden con soluciones que se encuentran en el infinito. Esta clase de puntos en el infinito es fundamental y lo estudiaremos más adelante.

Definición 1.1.2. El espacio proyectivo en n dimensiones sobre un cuerpo K es el conjunto

$$\mathbb{P}^n_K = x \in K^{n+1} \backslash \{\, 0 \,\} \Big/ \sim$$

donde la equivalencia es $x \sim x' \iff \exists t \in K^\times (x = tx')$. De igual manera denotamos la clase de x como $[x]$. Las coordenadas de $[x]$ igualmente se llamarán coordenadas homogéneas.

Más adelante vamos a definir curvas en el espacio proyectivo. En este momento vamos a definir lo que entenderemos como una recta en el plano proyectivo.

Definición 1.1.3. Una recta en el plano proyectivo $\mathbb{P}^2_K$ es el conjunto de puntos $[a,b,c]$ cuyas coordenadas satisfacen una ecuación de la forma

$$\alpha X + \beta Y + \gamma Z = 0,$$

donde $\alpha, \beta, \gamma \in K$ no son todos nulos.

Una visión geométrica

Sabemos que en $\mathbb{R}^2$ vale que dos puntos determinan una única recta y similarmente dos rectas se intersecan en un único punto salvo cuando son paralelas.

1.2. Día n+1 | 20210113

Hemos concluido la lección anterior observando ejemplos de intersecciones entre curvas. Para lograr que dos curvas de grados d_1 y d_2 se intersecaran en $d_1 \cdot d_2$ puntos, necesitábamos trabajar tanto en el plano proyectivo como en $\mathbb{C}$. Continuamos con otro ejemplo:

Ejemplo 1.2.1. Consideramos las curvas

$$C_1 : \ x + y = 2,$$
$$C_2 : \ x^2 + y^2 = 2.$$

La recta C_1 interseca al círculo de forma tangencial en el punto $(1, 1)$. De hecho si

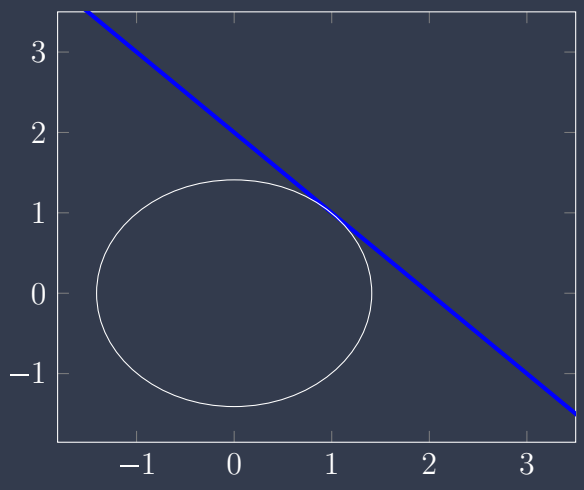

Figura 1.1: aaa

homogenizamos y buscamos las intersecciones de las curvas proyectivas

$$\tilde{C}_1 : \ x + y = 2z,$$
$$\tilde{C}_2 : \ x^2 + y^2 = 2z^2,$$

entonces despejamos $z = \frac{x+y}{2}$. Lo que nos lleva a $x^2 + y^2 = 2\left(\frac{x+y}{2}\right)^2$. Despejando vale que $(X - Y)^2 = 0$ y no podría ocurrir que X, Y son ambos cero y $X = Y$. Esto nos

lleva al punto $[X, X, X] = [1, 1, 1] \in \tilde{C}_1 \cap \tilde{C}_2$ y este punto corresponde al punto afín que ya habíamos encontrado.

Nosotros esperábamos dos puntos de intersección, pero no hay manera ni siquiera pasando por los complejos. Sólo obtenemos un punto de intersección y esto ocurre porque la recta interseca de manera tangencial. Este problema es el análogo al de una variable, recuerde que el teorema fundamental del álgebra garantiza la existencia cierto número de raíces para los polinomios. Lo que no hemos mencionado es la *multiplicidad* de la raíz. En este caso vemos que la misma ecuación $(X - Y)^2 = 0$ nos dice que la raíz tiene multiplicidad dos.

En conclusión sólo encontramos un punto de intersección, incluso después de haber buscado posibles puntos en el infinito. Esto es porque $[1, 1, 1]$ se debe contar con multiplicidad dos y corresponde con el hecho de que ambas curvas se intersecan de manera tangencial en este punto. De hecho, se ve reflejado en que al resolver el sistema de ecuaciones obtuvimos la ecuación $(X - Y)^2 = 0$.

Este no es el único caso en que esto puede ocurrir y el siguiente ejemplo lo ilustra.

Ejemplo 1.2.2. Considere ahora la curvas

$$C_1 : \ y = x,$$
$$C_2 : \ y^2 = x^3.$$

aregar figura Estas curvas se intersecan en dos puntos del plano afín. Al homogenizar obtenemos

$$\tilde{C}_1 : \ X - Y = 0,$$
$$\tilde{C}_2 : \ X^3 - Y^2 Z = 0,$$

y resolviendo llegamos a $X^3 - X^2 Z = 0$ y de aquí que $X = 0$ ó $X = Y = Z$. Si $X = 0$, entonces $Y = 0$ y así Z queda libre lo que nos lleva a los puntos $[1, 1, 1]$ y $[0, 0, 1]$. A diferencia del caso anterior, no hay multiplicidades mayores a uno. Aquí lo que ocurre es que uno de los puntos de intersección es un punto que no es suave. Las rectas cuyas direcciones aproximan la identidad tienen dos puntos de intersección con la curva cuspidal, entonces en el límite, el punto singular $[0, 0, 1]$ tiene multiplicidad dos. agregar figura

Ejemplo 1.2.3. Esta vez consideramos las curvas

$$C_1 : \ x + y + 1 = 0,$$
$$C_2 : \ 2x^2 + xy - y^2 + 4x + y + 2 = 0.$$

Aquel que esté atento podrá notar que

$$2x^2 + xy - y^2 + 4x + y + 2 = (x + y + 1)(2x - y + 2)$$

y así $C_1 \subseteq C_2$ lo que nos dice que la cantidad de puntos de intersección es infinita. Pero entonces las situaciones así no deben entrar en la consideración de los puntos de intersección de manera tan vaga. En el caso de $\mathbb{A}^2_{\mathbb{R}}$ hay infinitos puntos por lo que debemos especificar lo que buscamos.

Definición 1.2.4. Sea $C:\ f(x,y) = 0$ una curva con $f \in K[x,y]$. Si factorizamos f como un producto de polinomios irreducibles $f = \prod_{j=1}^{n} p_j$, entonces los componentes de la curva C son las curvas $C_j:\ p_j(x,y) = 0$. Diremos que C es irreducible cuando tenga un único componente. Es decir, sólo si el polinomio f es irreducible.

Ejemplo 1.2.5. De las curvas estudiadas en el ejemplo anterior, la curva C_1 es irreducible al ser un polinomio lineal y la segunda curva se puede factorizar en dos componentes. Ambas rectas son las componentes irreducibles de esta curva.

Definición 1.2.6. Diremos que dos curvas afines C_1, C_2 no tienen componentes en común si sus componentes irreducibles son distintos.

Un resultado básico en teoría de curvas que no vamos a demostrar es el siguiente:

Proposición 1.2.7. *Si C_1, C_2 son dos curvas afines sin componentes en común, entonces $C_1 \cap C_2$ es un conjunto finito.*

Observación 1.2.8. De manera análoga al caso afín, se definen componentes de curvas proyectivas y la noción de dos curvas proyectivas sin componentes comunes.

El teorema de Bezout es más general que este resultado. Con lo que hemos visto hasta ahora, lo podemos enunciar.bajé a agarrar agua

Por ahora mencionamos las siguientes propiedades:

(a) Si $P \notin C_1 \cap C_2$, entonces $I(C_1 \cap C_2, P) = 0$.

(b) Si $P \in C_1 \cap C_2$ y P es un punto no singular de C_1 y C_2, y si adicionalmente C_1 y C_2 tienen direcciones tangenciales diferentes en P, entonces $I(C_1 \cap C_2, P) = 1$. En este caso, se dice que C_1 y C_2 se intersecan en P de manera transversal.

(c) Si $P \in C_1 \cap C_2$ y C_1 y C_2 no se intersecan transversalmente, entonces $I(C_1 \cap C_2, P) \geqslant 2$.

Teorema 1.2.9 (Bezout). *Sean $C_1, C_2 \subseteq \mathbb{P}^2_{\mathbb{C}}$ sin componentes en común. Entonces vale que*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = \deg(C_1)\deg(C_2).$$

En particular si C_1, C_2 son suaves y únicamente tienen intersecciones transversales, entonces

$$|C_1 \cap C_2| = \deg(C_1)\deg(C_2)$$

y en todo momento se tiene la desigualdad $|C_1 \cap C_2| \leqslant \deg(C_1)\deg(C_2)$.

1.3. Día n+2 | 20210114

Multiplicidad de la intersección de dos curvas

Vamos a estudiar algunas propiedades y ejemplos de cálculo de la multiplicidad o índice de intersecciones $I(C_1 \cap C_2, P)$. Vamos a comenzar con un teorema que establece la existencia de la multiplicidad de la intersección y nos permite hacer cálculos.

Rápidamente para poder simplificar la notación introducimos los conceptos de variedad.

Definición 1.3.1. La variedad afín de f es el conjunto de ceros de f dentro del espacio afín $\mathbb{A}^2$. Denotamos

$$V(f) = \{\, x \in \mathbb{A}^2 : \ f(x) = 0 \,\}$$

y análogamente la variedad proyectiva de F es su conjunto de ceros dentro del espacio proyectivo. Este conjunto es

$$V(F) = \{\, X \in \mathbb{P}^2 : \ F(X) = 0 \,\}.$$

Teorema 1.3.2. *Considere $V(f), V(g)$ dos curvas afines en $\mathbb{A}^2_{\mathbb{C}}$ y $P \in \mathbb{A}^2_{\mathbb{C}}$ dado. Entonces existe un número $I(V(f) \cap V(g), P)$ definido de manera única tal que las siguientes propiedades se satisfacen*:

(a) *$I(V(f) \cap V(g), P) \in \mathbb{Z}_{\geqslant 0}$, a menos que P esté en un componente común de $V(f), V(g)$ y en ese caso $I(V(f) \cap V(g), P) = \infty$.*

(b) *$I(V(f) \cap V(g), P) = 0$ si y sólo si $P \notin V(f) \cap V(g)$.*

(c) *Dos rectas distintas se intersecan con multiplicidad uno en su punto de intersección.*

(d) *$I(V(f) \cap V(g), P) = I(V(g) \cap V(f), P)$.*

(e) *Si* $f = \prod p_i^{\alpha_i}$ *y* $g = \prod q_i^{\beta_i}$*, entonces*

$$I(V(f) \cap V(g), P) = \sum_{i,j} \alpha_i \beta_j I(V(p_i) \cap V(q_j), P).$$

(f) $I(V(f) \cap V(g), P) = I(V(f) \cap V(g + hf), P)$ *para* $h \in \mathbb{C}[x, y]$.

Definición 1.3.3. El número $I(V(f) \cap V(g), P)$ se llama multiplicidad de la intersección de $V(f)$ y $V(g)$ en P.

Ejemplo 1.3.4. (a) x^2 con y

(b) círculo con recta

(c) cuspidal con identidad

Definición 1.3.5. Sea f un polinomio con coeficientes en $\mathbb{C}$ y $P \in V(f)$. La multiplicidad de f en P

Índice Analítico

Bibliografía

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[2] Joseph H. Silverman, John T. Tate, and Springer-Verlag (Nowy Jork). *Rational Points on Elliptic Curves*. Structure and Bonding. Springer-Verlag, 1992.