Sistemas de Ecuaciones Polinomiales y Funciones Zeta

EDWIN LEÓN CARDENAL

UNIDAD ZACATECAS

Octubre de 2014
CIMPS 2014

Contents

Contents

Definición

Un sistema de ecuaciones polinomiales es un sistema de la forma:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

en donde los f_i son polinomios en las variables $x_1, \ldots, x_n$ que pueden ser enteras, racionales, reales o complejas por ejemplo.

Definición

Un sistema de ecuaciones polinomiales es un sistema de la forma:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

en donde los f_i son polinomios en las variables $x_1, \ldots, x_n$ que pueden ser enteras, racionales, reales o complejas por ejemplo.Cuando las variables pertenecen a un campo finito (división en clases $\mathbb{Z}$) se dice que es un sistema de congruencias y se escribe usualmente

$$\begin{cases} f_1(x_1, \ldots, x_n) \equiv 0 \mod r \\ \vdots \\ f_m(x_1, \ldots, x_n) \equiv 0 \mod r. \end{cases}$$

Soluciones

En general encontrar las soluciones a un sistema de ecuaciones o de congruencias es difícil y depende de varios parámetros, cómo el grado de los polinomios, el número de variables y de ecuaciones y la estructura de base ($\mathbb{Z}$, $\mathbb{R}$, etc.)

Soluciones

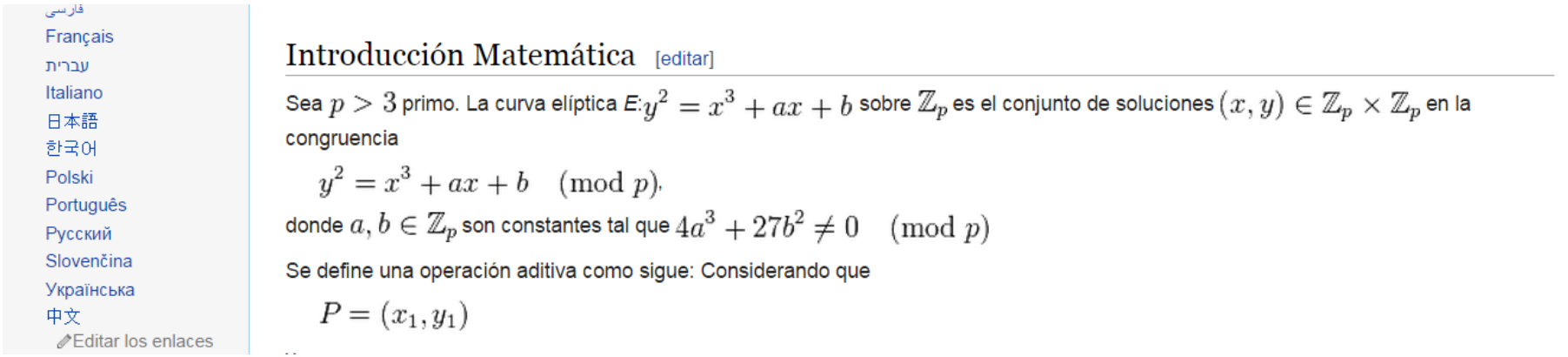
En general encontrar las soluciones a un sistema de ecuaciones o de congruencias es difícil y depende de varios parámetros, cómo el grado de los polinomios, el número de variables y de ecuaciones y la estructura de base ($\mathbb{Z}$, $\mathbb{R}$, etc.)
En el caso de las congruencias hay sólo un número finito de posibilidades por lo que el problema de hallar soluciones es "susceptible" de programación.

Criptoseguridad

La Criptografía de Curva Elíptica [Koblitz/ Miller, 1985] es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves más cortas que algunos métodos antiguos (RSA), al tiempo que proporcionan un nivel de seguridad equivalente.

Criptoseguridad

La Criptografía de Curva Elíptica [Koblitz/ Miller, 1985] es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves más cortas que algunos métodos antiguos (RSA), al tiempo que proporcionan un nivel de seguridad equivalente.


فارسی
Français
עברית
Italiano
日本語
한국어
Polski
Português
Русский
Slovenčina
Українська
中文
Editar los enlaces

Introducción Matemática [editar]

Sea $p > 3$ primo. La curva elíptica E: $y^2 = x^3 + ax + b$ sobre $\mathbb{Z}_p$ es el conjunto de soluciones $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ en la congruencia

$$y^2 = x^3 + ax + b \pmod{p},$$

donde $a, b \in \mathbb{Z}_p$ son constantes tal que $4a^3 + 27b^2 \neq 0 \pmod{p}$

Se define una operación aditiva como sigue: Considerando que

$$P = (x_1, y_1)$$

Algoritmos y Complejidad Computacional

Dado un sistema de ecuaciones polinomiales sobre los racionales, por ejemplo, queremos contestar preguntas sobre sus soluciones. Según la tradición en informática, los problemas se especifican por sus parámetros sintácticos. En el caso que nos compete, esto significa buscar un algoritmo que, dados enteros d, n y m, calcula las soluciones de un sistema de m polinomios en n variables de grado total acotado por d cuando éste define una variedad de dimensión cero.

Algoritmos y Complejidad Computacional

Dado un sistema de ecuaciones polinomiales sobre los racionales, por ejemplo, queremos contestar preguntas sobre sus soluciones. Según la tradición en informática, los problemas se especifican por sus parámetros sintácticos. En el caso que nos compete, esto significa buscar un algoritmo que, dados enteros d, n y m, calcula las soluciones de un sistema de m polinomios en n variables de grado total acotado por d cuando éste define una variedad de dimensión cero.

Hecho

Es sabido que este problema es $P^{\#}-$duro y que el problema de decidir si un sistema definido sobre $\mathbb{Z}$ define o no la variedad vacía es $NP-$ y $NP_{\mathbb{C}}-$duro.

Contents

Problema

Dado $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ estimar el número de soluciones a

$$f(x_1, \ldots, x_n) \equiv 0 \mod r, \quad r \in \mathbb{N}.$$

Problema

Dado $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ estimar el número de soluciones a

$$f(x_1, \ldots, x_n) \equiv 0 \mod r, \quad r \in \mathbb{N}.$$

El teorema chino de los restos permite reducir el problema anterior al problema de estimar el número de soluciones a

$$f(x_1, \ldots, x_n) \equiv 0 \mod p^k, \quad \forall k \geq 1.$$

Problema

Dado $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ estimar el número de soluciones a

$$f(x_1, \ldots, x_n) \equiv 0 \mod r, \quad r \in \mathbb{N}.$$

El teorema chino de los restos permite reducir el problema anterior al problema de estimar el número de soluciones a

$$f(x_1, \ldots, x_n) \equiv 0 \mod p^k, \quad \forall k \geq 1.$$

Theorem

$f(x_1, \ldots, x_n) \equiv 0 \mod p^k$, *es soluble* $\forall k \geq 1$ *si y sólo si*
$f(x_1, \ldots, x_n) = 0$, *es soluble en* $\mathbb{Z}_p$.

$\mathbb{Z}_p$ es el anillo de los enteros $p-$ádicos que definiremos después del siguiente ejemplo.

Ejemplo

Sean $n = m = 1$ y consideremos $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. Estudiemos las congruencias

$$x^2 \equiv 2 \mod 7^k \quad \forall k \geq 1.$$

k=1. Se puede verificar fácilmente que las soluciones son $x_0 \equiv \pm 3 \mod 7$.

Ejemplo

Sean $n = m = 1$ y consideremos $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. Estudiemos las congruencias

$$x^2 \equiv 2 \mod 7^k \quad \forall k \geq 1.$$

k=1. Se puede verificar fácilmente que las soluciones son $x_0 \equiv \pm 3 \mod 7$.

k=2. Notemos que toda solución a $x^2 \equiv 2 \mod 7^2$ también satisface $x^2 \equiv 2 \mod 7$. Luego una solución a $x^2 \equiv 2 \mod 7^2$ debe ser de la forma $x_0 + 7t_1$ para $x_0 \equiv \pm 3 \mod 7$ y algún $t_1 \in \mathbb{Z}/7\mathbb{Z}$. Sea $x_1 = 3 + 7t_1$, entonces

$$x_1^2 \equiv 2 \mod 7^2 \Rightarrow (3 + 7t_1)^2 \equiv 2 \mod 7^2$$
$$\Rightarrow 9 + 42t_1 + 49t_1^2 \equiv 2 \mod 7^2,$$

dividiendo por 7 y reduciendo obtenemos

$$1 + 6t_1 \equiv 0 \mod 7 \Rightarrow t_1 \equiv 1 \mod 7.$$

Así que $x_1 = 3 + 1 \cdot 7 \mod 7^2$.

Cont. Ejemplo

k=3. Si x_2 es solución a $x^2 \equiv 2 \mod 7^3$ entonces $x_2 = x_1 + t_2 7^2$, con x_1 como antes y $t_2 \in \mathbb{Z}/7\mathbb{Z}$. En consecuencia

$$(x_1 + t_2 7^2)^2 \equiv 2 \mod 7^3 \Rightarrow t_2 \equiv 2 \mod 7$$
$$\Rightarrow x_2 = 3 + 1 \cdot 7 + 2 \cdot 7^2 \mod 7^3.$$

Cont. Ejemplo

k=3. Si x_2 es solución a $x^2 \equiv 2 \mod 7^3$ entonces $x_2 = x_1 + t_2 7^2$, con x_1 como antes y $t_2 \in \mathbb{Z}/7\mathbb{Z}$. En consecuencia

$$(x_1 + t_2 7^2)^2 \equiv 2 \mod 7^3 \Rightarrow t_2 \equiv 2 \mod 7$$
$$\Rightarrow x_2 = 3 + 1 \cdot 7 + 2 \cdot 7^2 \mod 7^3.$$

$k \geq 4$ Continuando este proceso podemos obtener $x_0, x_1, x_2, \ldots, x_k$, en donde

$$x_0 \equiv 3 \mod 7,\ x_1 \equiv x_0 \mod 7,\ x_2 \equiv x_1 \mod 7^2, \ldots,$$
$$x_k \equiv x_{k-1} \mod 7^k,$$

y

$$x_k^2 \equiv 2 \mod 7^{k+1}.$$

Los enteros $p-$ádicos $\mathbb{Z}_p$.

Definition

Una sucesión de enteros $\{x_k\}$ que satisface

$$x_k \equiv x_{k-1} \mod p^k \quad \forall k \geq 1,$$

determina unívocamente un entero $p-$ádico.

Los enteros $p-$ádicos $\mathbb{Z}_p$.

Definition

Una sucesión de enteros $\{x_k\}$ que satisface

$$x_k \equiv x_{k-1} \mod p^k \quad \forall k \geq 1,$$

determina unívocamente un entero $p-$ádico.

De estas observaciones tenemos que la congruencia $\mod p^k$ es soluble siempre que la congruencia $f(x_1, \ldots, x_n) \equiv 0 \mod p$ sea soluble y se puedan seguir “levantando" las soluciones.

Los enteros $p-$ádicos $\mathbb{Z}_p$.

Definition

Una sucesión de enteros $\{x_k\}$ que satisface

$$x_k \equiv x_{k-1} \mod p^k \quad \forall k \geq 1,$$

determina unívocamente un entero $p-$ádico.

De estas observaciones tenemos que la congruencia $\mod p^k$ es soluble siempre que la congruencia $f(x_1, \ldots, x_n) \equiv 0 \mod p$ sea soluble y se puedan seguir “levantando" las soluciones.

Lema de Hensel

Lemma

Si $f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$ *y* $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_p^n$ *satisface* $f(\alpha_1, \ldots, \alpha_n) \equiv 0 \mod p$ *y para algún índice* $i = 1, \ldots, n$ *se tiene*

$$f'_{x_i}(x_1, \ldots, x_n) \not\equiv 0 \mod p,$$

entonces existen enteros p−ádicos $\beta_1, \ldots, \beta_n$ *tales que*

$$f(\beta_1, \ldots, \beta_n) = 0$$

y $\beta_1 \equiv \alpha_1 \mod p, \ldots, \beta_n \equiv \alpha_n \mod p.$

Lema de Hensel

Lemma

Si $f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$ *y* $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_p^n$ *satisface* $f(\alpha_1, \ldots, \alpha_n) \equiv 0 \mod p$ *y para algún índice* $i = 1, \ldots, n$ *se tiene*

$$f'_{x_i}(x_1, \ldots, x_n) \not\equiv 0 \mod p,$$

entonces existen enteros p−ádicos $\beta_1, \ldots, \beta_n$ *tales que*

$$f(\beta_1, \ldots, \beta_n) = 0$$

y $\beta_1 \equiv \alpha_1 \mod p, \ldots, \beta_n \equiv \alpha_n \mod p$.

En estos casos se puede contar el número de soluciones a sistemas de congruencias mod p^k.

Número de Soluciones

Qué ocurre en el caso general con el número de soluciones módulo p^k? Qué comportamiento tiene este número de soluciones cuando k es muy grande?

Número de Soluciones

Qué ocurre en el caso general con el número de soluciones módulo p^k? Qué comportamiento tiene este número de soluciones cuando k es muy grande? Sea $f(x) = f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$. Denotemos con N_k el número de elementos del conjunto

$$\{x + p^k \mathbb{Z}_p^n \mid x \in \mathbb{Z}_p^n \text{ y } f(x) \equiv 0 \mod p^k\},$$

para $k \geq 1$ con $N_0 = 1$. Entonces la serie de Poincaré asociada a f es la serie formal

$$P_f(t) = \sum_{k=0}^{\infty} N_k p^{-nk} t^k.$$

Nota

$P_f(t)$ es una función racional en t. Esto es equivalente a afirmar que la sucesión $\{N_k\}$ es una sucesión lineal recurrente, es decir que a partir de cierto índice, los coeficientes N_k se pueden calcular a partir de $N_0, \ldots, N_{k-1}$ mediante una función lineal.

Funciones Zeta $p-$ádicas

Dado $f(x) = f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n] \setminus \mathbb{Z}_p$ y s un número complejo con $Re(s) > 0$, tenemos

$$Z(s, f) := \int_{\mathbb{Z}_p^n} |f(x)|_p^s \, d^n x, \quad Re(s) > 0,$$

donde $|\cdot|_p$ es un valor absoluto $p-$ádico y $d^n x$ es una medida de Haar.

Funciones Zeta $p-$ádicas

Dado $f(x) = f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n] \setminus \mathbb{Z}_p$ y s un número complejo con $Re(s) > 0$, tenemos

$$Z(s, f) := \int_{\mathbb{Z}_p^n} |f(x)|_p^s \, d^n x, \quad Re(s) > 0,$$

donde $|\cdot|_p$ es un valor absoluto $p-$ádico y $d^n x$ es una medida de Haar. Se puede probar que $Z(s, f)$ es una función holomorfa en el semiplano $Re(s) > 0$. La conexión entre $Z(s, f)$ y la serie de Poincaré asociada a f está dada por:

Proposition

$$P_f(t) = \frac{1 - tZ(s, f)}{1 - t}, \quad con \;\; t = p^{-s} \; y \;\; Re(s) > 0.$$

El Teorema de Igusa

Theorem

Sea $f(x) = f(x_1, \ldots, x_n) \in \mathbb{Q}_p[[x_1, \ldots, x_n]]$. *Entonces existe un número finito de parejas* $(N_E, v_E) \in (\mathbb{N} \setminus \{0\})^2$, $E \in T$, *tales que*

$$\prod_{E \in T} (1 - p^{v_E - sN_E}) Z(s, f)$$

es un polinomio en p^{-s} *con coeficientes racionales.*

Algunos Problemas

- De la discusión anterior tenemos que para $p = 2$, calcular la función $Z(s, f)$ es un problema $NP-$completo.

Algunos Problemas

- De la discusión anterior tenemos que para $p = 2$, calcular la función $Z(s, f)$ es un problema $NP-$completo. **León-Cardenal, E. An algorithm for computing the local zeta function of an hyperelliptic curve. Aportaciones matemáticas. Comunicaciones, 41 (2010), 23-43.**

Algunos Problemas

- De la discusión anterior tenemos que para $p = 2$, calcular la función $Z(s, f)$ es un problema $NP-$completo. **León-Cardenal, E. An algorithm for computing the local zeta function of an hyperelliptic curve. Aportaciones matemáticas. Comunicaciones, 41 (2010), 23-43.**
- Hay muchos problemas interesantes y conexiones sorprendentes acerca de $Z(s, f)$ y sus polos, así como sus generalizaciones y especializaciones en diferentes contextos matemáticos.

Contents

From Zeta Functions to Big Data and Cybersecurity

Gracias!