1 Teoría de Números

Coordinador:

- Xavier Vidaux, Departamento de Matemáticas, Universidad de Concepción, Concepción.

Contents

Julia Robinson numbers and arithmetical dynamic of quadratic polynomials

Marianela Castillo Fernández*
Departamento de Ciencias Básicas
Universidad de Concepción Campus Los Ángeles
Los Ángeles, Chile

Abstract

In order to show the undecidability of the theory of a ring of integers of a totally real field of algebraic numbers, J. Robinson defined a set which is always $\{+\infty\}$ or of the form $[\lambda, +\infty)$ or $(\lambda, +\infty)$ for some real number $\lambda \geq 4$. All known examples give either $\{+\infty\}$ or $[4, +\infty)$. In this work, we construct infinitely many fields such that the set is an interval, but not equal to $[4, +\infty)$.

Joint work with:
Xavier Vidaux[1], Departamento de Matemática, Facultad de Ciencias Físicas y Matemáticas, Universidad de Concepción, Concepción, Chile.
Carlos R. Videla[2], Department of Mathematics and Computing, Mount Royal University, Calgary, Canadá.

References

[1] Castillo, Marianela; Vidaux, Xavier; Videla, Carlos, *Julia Robinson numbers and arithmetical dynamic of quadratic polynomial*. Preprint.

[2] Vidaux, Xavier; Videla, Carlos, *Definability of the natural numbers in totally real towers of nested square roots,*. Proc. Amer. Math. Soc. **143**. 4463-4477 (2015).

*Partially supported by Conicyt, e-mail: mcastillo@udec.cl
[1]Partially supported by Fondecyt research projects 1130134 and 1170315, Chile, e-mail: xvidaux@udec.cl
[2]e-mail: cvidela@mtroyal.ca

Rangos de curvas elípticas y progresiones aritméticas de puntos racionales

Natalia García Fritz*
Facultad de Matemáticas
Pontificia Universidad Católica de Chile
Santiago, Chile

Abstract

En 1980, Mohanty [2] conjeturó que en ninguna curva elíptica de Mordell $y^2 = x^3 + b$ se puede encontrar una sucesión de cinco o más puntos racionales cuyas coordenadas x están en progresión aritmética. Uno dice en este caso que los *puntos racionales están en progresión aritmética*. Se conocen muchos ejemplos de sucesiones de largo cuatro [3], pero la pregunta sobre si hay una cota para el largo de estas progresiones aritméticas no ha sido resuelta.

En [1], Bremner conjetura que puntos racionales en progresión aritmética tienden a ser linealmente independientes en el grupo de puntos racionales de la curva elíptica, así que progresiones aritméticas largas deberían venir de curvas elípticas con rango alto.

Junto a Héctor Pastén demostramos, gracias a una generalización del Teorema de Faltings hecho por Remond, que el largo máximo de una progresión aritmética en una curva elíptica E está acotado solamente en términos de $\mathrm{rank}(E)$ y el invariante j de E. Esto nos permite resolver incondicionalmente la conjetura de Mohanty para gran parte de las curvas de Mordell, dar una cota en el largo de progresiones aritméticas para ciertas familias de twists de una curva elíptica, y mostrar que el largo promedio de dichas progresiones aritméticas es acotado, entre otras aplicaciones.

Trabajo realizado en conjunto con:
Héctor Pastén[1], Department of Mathematics, Harvard University, Cambridge MA, USA.

References

[1] Bremner, A., *On arithmetic progressions on elliptic curves.* Experiment. Math. 8 (1999), no. 4, 409-413

[2] Mohanty, S. P., *Integer solutions in arithmetic progression for* $y^2 - k = x^3$. Acta Math. Acad. Sci. Hungar. 36 (1980), no. 3-4, 261-265 (1981).

[3] Ulas, M., *Rational points in arithmetic progressions on* $y^2 = x^n + k$. Canad. Math. Bull. 55 (2012), no. 1, 193-207.

*Parcialmente financiado por proyecto Fondecyt Iniciación 11170192, e-mail: natalia.garcia@mat.uc.cl
[1]Parcialmente financiado por una Benjamin Peirce Fellowship, e-mail: hpasten@math.harvard.edu

El problema diofantino de adición y divisibilidad para subanillos de los números racionales y de funciones racionales sobre campos finitos.

Carlos Martínez Ranero*
Departamento de Matemática
Universidad de Concepción
Concepción, Chile

Abstract

En esta charla demostraremos que la teoría positivo existencial de la estructura $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$, donde S es un conjunto finito no vacío de números primos, es indecidible. Es decir, no existe un algoritmo que pueda decidir si un enunciado arbitrario de la forma

$$\exists x_1, \ldots, \exists x_n \bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) \mid g_i(x_1, \ldots, x_n),$$

donde f_i y g_i son polinomios lineales con coeficientes enteros es cierto o falso en $\mathbb{Z}[S^{-1}]$. Este resultado contrasta con el resultado de L. Lipschitz y Belt'yukov de que los enunciados de esta forma pueden ser decididos sobre $\mathbb{Z}$.

También demostraremos una resultado análogo para subanillos del campo de funciones racionales sobre un campo finito.

Trabajo realizado en conjunto con:
Leonidas Cerda Romero[1], Departamento de Matemática
Universidad de Concepción
Concepción, Chile

*e-mail: cmartinezr@udec.cl
[1]Parcialmente financiado por Senescyt Convocatoria Abierta 2011, e-mail: leonidascerda@udec.cl

Semiretículo Hermiteano (Semi) y Retículo de Rolf.

Ana Cecilia de la Maza*
Departamento de Matemática y Estadística
Universidad de la Frontera
Temuco, Chile

Abstract

Estudiamos el retículo Hermiteano indexado generado por un elemento a sujeto a la relación $a = a^{\perp\perp} \leq b = b^{\perp\perp}$. A pesar de ser un retículo infinito, hemos podido describir sus factores subdirectamente irreducibles de manera recursiva.

Un retículo Hermiteano es un algebra $(L, 0, 1, \cdot, +, ^{\perp}, b)$ tal que $(L, 0, 1, \cdot, +)$ es un retículo modular con cotas 0 , 1, y la operación unaria $^{\perp}$ satisface

$$x \leq (x^{\perp} y)^{\perp} \qquad \forall\ x,\ y \in L \text{ y } 0^{\perp} = 1;$$

b es una constante con $xx^{\perp} \leq b \qquad \forall\ x \in L.$

Si omitimos la operación $+$, hablamos de semiretículo.

Un ejemplo de retículo Hermiteano es el retículo $\mathcal{L}(E)$ formado por los subespacios de un espacio vectorial E sobre un cuerpo k, con una forma bilineal ϕ no degenarada. Ahora la ortogonalidad estará dada por la forma bilineal ϕ, es decir si F es un subespacio de E, $F^{\perp} = \{v \in E | b(v, w) = 0 \forall w \in F\}$. El rol de b es el que juega el subespacio formado por los vectores traza valuada.

Ch. Herrmann in [H] muestra que el semiretículo Hermiteano $S := S[a; a = a^{\perp\perp} \leq b = b^{\perp\perp}]$ es infinito, y que definiendo una nueva operación $\vee$ donde $x \vee y := (x^{\perp} y^{\perp})^{\perp}$, se obtiene un retículo que coincide con el retículo descrito por Rolf en R, p. 587].

En este trabajo estudiamos este semiretículo y el retículo Hermiteano generado por él.

Trabajo realizado en conjunto con:
Remo Moresi[1]

References

[G1] Gross, H.: Quadratic forms in infinite dimensional vector spaces. Birkäuser, Boston (1979)

[G2] Gross, H.: Lattices and infinite-dimensional forms. "The lattice method". Order **4**, 233–256 (1987)

[H] Herrmann, Ch.: Galois lattices. Note di Matematica e Fisica 7, 229–234 (1994)

[R] Rolf, H.L.: The free lattice generated by a set of chains. Pacific J. Math. **8**, 585–595 (1958)

*e-mail:anace.delamaza@ufrontera.cl
[1]e-mail: `romicatj@yahoo.it` Cerfim, Locarno, Switzerland.

Aproximación Diofantina y definibilidad existencial.

Héctor Pastén*
Departamento de Matemáticas
Universidad de Harvard
Cambridge, MA, USA

Abstract

Presentaré una conjetura en aproximación Diofantina que, en términos simples, dice que el acotar funciones de proximidad por funciones de altura no es un problema trivial. Explicaré algunos casos donde es posible demostrar esta conjetura, y analizaré algunas de sus consecuencias. En particular, ella implicaría que los enteros no son existencialmente definibles en los racionales.

*e-mail: hpasten@gmail.com

Cadenas de bases doble para multiplicación escalar

Nicolas Thériault*
Departamento de Matemática y Ciencia de la Computación
Universidad de Santiago de Chile
Santiago, Chile

Abstract

Utilizar cadenas de base doble para representar enteros, en particular cadenas de bases 2 y 3, puede ser beneficioso para la eficiencia de la multiplicación escalar. Sin embargo, se pensaba que encontrar un cadena 2-3 optimal para un escalar dado requiere más tiempo que la multiplicación escalar misma, lo que impedía aplicaciones prácticas de las cadenas 2-3 cuando el escalar se utiliza unas pocas veces (como es el caso en el intercambio de llaves de Diffie y Hellman).

En los últimos años, hubo importantes avances en algoritmos para obtener la cadena de base doble la más corta posible para un entero dado n. En 2008, Doche y Habsieger [3] presentaron una estrategia utilizando un árbol binario que permite obtener una (buena) aproximación) de la cadena minima. En 2015, Capuñay y Thériault [2] presentaron el primer algoritmo determinista que devuelve la cadena minima de un escalar n en tiempo polinomial, pero su complejidad $O((\log n)^{3+\epsilon})$ es demasiado grande para competir con la multiplicación escalar. Recientemente, Bernstein, Chuengsatiansup, y Lange [1] presentaron una estrategia basada en grafos para obtener una complejidad $O((\log n)^{2.5+\epsilon})$, acercandose más a lo deseado.

En este trabajo, adaptamos el algoritmo de Capuñay y Thériault para obtener cadenas mínimas en $O((\log n)^2 \log\log n)$ operaciones de bits y $O((\log n)^2)$ bits de memoria. Eso nos permite obtener cadenas mínimas en unos 0.33 milisegundos para enteros de 256 bits, haciendo posible reducir el costo de la multiplicación escalar para enteros utilizados solamente una vez.

También extendemos el resultado a otras bases dobles y a bases triples. En el caso de ambientes computacionales con memoria limitada, nuestro algoritmo se puede adaptar para devolver la cadena mínima en $O((\log n)^2(\log\log n)^2)$ operaciones de bits y solamente $O(\log n(\log\log n)^2)$ bits de memoria.

Trabajo realizado en conjunto con:
Cristobal Leiva[1], Departamento de Matemática y Ciencia de la Computación, Universidad de Santiago de Chile, Santiago, Chile.

References

[1] Bernstein, Daniel J.; Chuengsatiansup, Chitchanok; Lange, Tanja, *Double-base scalar multiplication revisited*, IACR eprint archive, **2017/037**, (2017).

[2] Capuñay, Alex; Thériault, Nicolas, *Computing Optimal 2-3 Chains for Pairings*, in: Progress in Cryptology – LATINCRYPT 2015, Lecture Notes in Computer Science, **9230**, Springer-Verlag, (2015). 225-244.

[3] Doche, Christophe; Habsieger, Laurent, *A Tree-Based Approach for Computing Double-Base Chains*, in: Information Security and Privacy – ACISP 2008, Lecture Notes in Computer Science, **5107**, Springer-Verlag, (2008). 433-446.

*Parcialmente financiado por el proyecto FONDECYT regular 1151326, e-mail: nicolas.theriault@usach.cl
[1]Parcialmente financiado por el proyecto FONDECYT regular 1151326, e-mail: cristobal.leiva@usach.cl

Interpreting arithmetic in rings of polynomials in a language with addition and coprimality

Javier Utreras*
Departmento de Matemática
Universidad de Concepción
Concepción, Chile

Abstract

In [1], R. Robinson studied the first–order ring structure of various polynomial rings and obtained undecidability results for many of them. In this work, we weaken the multiplication operation to a coprimality relation and generalise Robinson's method to show how to interpret the ring structure of the natural numbers - and hence show undecidability - in the first–order theories polynomial rings of one variable over diverse rings.

References

[1] R. Robinson, *Undecidable rings*. Transactions AMS **70** (1951), 137–159.

*Partially supported by FONDECYT Postdoctorado 3160301, e-mail: javierutreras@udec.cl