Algoritmo LLL y factorización de polinomios a coeficientes racionales

Florence Gillibert (PUCV Valparaíso)

En esta charla nos enfocamos sobre el problema de factorización de polinomios a coeficientes racionales. Sea f un polinomio a coeficientes en $\mathbb{Q}$ de grado n. Para factorizar f, nos podemos reducir al caso donde f es mónico a coeficientes enteros, y no tiene factores múltiplos. Observamos que si f_0 es un divisor no trivial de f, es posible encontrar una cota superior M sobre los coeficientes de f_0 a partir de los coeficientes de f. Encontramos el discriminante de f, y reducemos los coefficientes de f módulo un número primo p lo cual no divide al discriminante de f en tal manera que $f \mod p$ no tiene factores múltiplos. El algoritmo de Berlekamp nos permite descomponer $f \mod p$ como producto de factores irreducibles sobre $\mathbb{Z}/pZ$. Si f no es irreducible modulo p, entonces existe una descomposiciíon no trivial $f \mod p = f_1 f_2$ con f_1 y f_2 coprimos, a coeficientes en $\mathbb{Z}/pZ$. Para todo $r \in \mathrm{N}$, el lema de Hensel nos permite levantar esta descomposición modulo p^r en manera única : $f \equiv \tilde{f}_1 \tilde{f}_2 \mod p^r$. Ahora eligo r tal que que $p^r \geq M$. Entonces es posible saber si f tiene una descomposición $f = g_1 g_2$ con $(g_1, g_2) \in \mathbb{Z}[x]^2$ y $f_1 \equiv g_1 \mod p$, $f_2 \equiv g_2 \mod p$. Si f tiene, entonces g_1 y g_2 son los únicos polinomios en $\mathbb{Z}[x]$ a coeficientes $\leq M$ tales que $\tilde{f}_1 \equiv g_1 \mod p^r$ y $\tilde{f}_1 = g_1 \mod p^r$. Así puedo testar todas las descomposiciones en producto de dos factores de $f \mod p$, y deducir la descomposición de f en producto de factores irreducibles.

El problema es que en el peor caso, f es irreducible sobre $\mathbb{Q}$, pero tiene $n = \mathrm{grado}(f)$ factores modulo p. Yo tendría que hacer 2^n verificaciones antes de declarar que f es irreducible sobre $\mathbb{Q}$! Por esta razón, el algoritmo no es considerado eficaz. Buscamos un algoritmo de complejidad polinomial, es decir un algoritmo que nos induce a hacer un número de operaciones acotado para una función polinomial del tamaño de f. Aquí el tamaño se refiere al número de dígitos que necesitaría para listar los coeficientes de f en binario. Si cada coefficiente de f es de tamaño l entonces f es de tamaño nl. Un algoritmo que necesita repetir 2^n veces una operación no es polinomial.

Por esta razón vamos a hablar del algoritmo LLL [**?**]. Este algoritmo ocupa un plazo muy importante en teoría algebraica de números. Consideramos $n \in \mathrm{N}$ un entero y L un retículo en $\mathbb{R}^n$ (es decir un $\mathbb{Z}$-modulo libre de rango n incluido en $\mathbb{R}^n$). Dada una base de L, quiero encontrar otra base con vectores de normas las más pequeãs posibles. El algoritmo LLL nos da una respuesta parcial a este problema, permitendo encontrar una base de L con vectores de tamaño limitado. En aplicación de éste, existe un algoritmo de factorización de los polinomios a coeficientes racionales en tiempo polinomial.

Références

[LLL] A. Lenstra, H. Lenstra, L. Lovász, *Factoring Polynomials with Rational Coefficients Math Ann* **261** *pp. 515-534 (1982).*