Temas de teoría de números

Seminario Avanzado

Departamento de Matemáticas

UAM 2006

Lorente Fernando
2005/2006
Cozimah

Un experimento

Entre los matemáticos que tienen algún contacto casual con los libros de Física es muy fácil criticar la falta de rigor, que en algunos casos llega a ser exasperante. Posiblemente a los físicos les parecerá por su lado que los libros de Matemáticas están llenos de hipótesis ridículas y enrevesadas que ocultan las ideas principales (y eso que ninguno de ellos habrá llegado hasta el libro de teoría de conjuntos de Bourbaki, que en una de las primeras páginas establece ufano: "A es una letra").

Varios ejemplos muestran que, desde el punto de vista didáctico y psicológico, los físicos en muchos casos llevan la delantera. No es necesario ir a la divulgación, donde la diferencia es abrumadora. Por ejemplo, la demostración sin rigor del teorema de la divergencia que aparece en los libros de Física al tiempo que se transforman las ecuaciones de Maxwell, le hace sentir al lector que entiende por qué aquello funciona y que además el nombre de "divergencia" está bien puesto. Sin embargo comprender la idea matemática rigurosa lleva a unos requisitos sólidos y unos cálculos abstractos donde todo acaba cuadrando por razones desconocidas.

A lo largo de estos apuntes, y todavía más en las lecciones del curso, se experimentará tratando de inclinar la balanza ligeramente hacia la propedéutica de los físicos: las ideas predominarán sobre las demostraciones. Naturalmente no se pueden hacer Matemáticas con medias verdades o engaños, por ello se indicarán los argumentos que no son completos o las faltas de rigor. Se empleará una notación tomada del ajedrez: (!?) señala un movimiento dudoso, (?!) expresa un nivel mayor de duda y (??) es un paso desastroso.

Madrid, febrero de 2006

Notación básica

Incluso en el conjunto indudablemente protagonista de cualquier curso de teoría de números, los naturales, no hay acuerdo en la notación. Aquí consideraremos que el cero no es un número muy natural (nació después que el resto) y por tanto escribiremos:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}.$$

Alentados por las necesidades tipográficas tendremos el valor de cambiar levemente la notación clásica de las congruencias $a \equiv b \pmod{n}$ debida al gran Gauss, con el significado "$a - b$ es múltiplo de n", por $a \equiv b\ (n)$. Para el máximo común divisor de m y n usaremos la notación abreviada (m, n) que raramente inducirá a confusión con un elemento de $\mathbb{Z}^2$. Así $(m, n) = 1$ significa que m y n son coprimos.

Emplearemos continuamente la *notación de Landau* O y o para ocultar nuestro desconocimiento sobre la forma exacta de términos de error o manifestar nuestro desinterés por ella en favor de una idea sobre su tamaño. Usando esta notación $O(g)$ y $o(g)$, con g positiva en el rango de interés, representan respectivamente funciones f tales que

$$\limsup \frac{|f|}{g} < \infty \qquad \text{y} \qquad \lim \frac{f}{g} = 0.$$

El valor hacia el que tiende la variable se sobreentiende en cada caso y en este curso será típicamente ∞.

La *notación de Vinogradov* $f \ll g$ tiene el mismo significado que $f = O(|g|)$ y se muestra conveniente e intuitiva para manipular desigualdades olvidándose de las constantes. A veces se escribe $f \ll_t g$ para hacer notar que *la constante* O, esto es, el valor de $\limsup |f|/|g|$, depende de un parámetro t y puede no estar uniformemente acotada cuando t varía.

Una variante obvia de la notación de Vinogradov es $f \gg g$ (significando $g \ll f$). También se emplea con cierta frecuncia $f \asymp g$ para indicar $f \ll g \ll f$. Otro autores emplean $f \sim g$ pero entonces se enfrentan al uso más extendido de este símbolo para indicar la igualdad asintótica. Es decir, $f \sim g$ como notación para $\lim f/g = 1$.

Ejemplos: $1/x \ll 1$, $\operatorname{sen} x = O(1)$, $e^x = 1 + x + O(x^2)$ si $x \to 0$, $\int_2^x dt/\log t = (1+o(1))x/\log x \sim x/\log x$, $(x^2+O(x))/(x+o(1)) = x+o(x)$, $x \gg \log x$, $(x+3)^2 \asymp 7x^2$.

Una notación menos universal aunque bastante extendida en la teoría analítica de números es el uso de $e(t)$ para representar $e^{2\pi it}$. Está ligada a la normalización más sencilla de la *transformada de Fourier* y de su *transformada inversa*:

$$\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e(-\xi x)\, dx \qquad \text{y} \qquad f^\vee(x) = \int_{-\infty}^{\infty} f(\xi)e(x\xi)\, d\xi.$$

La fórmula de inversión asegura $(\widehat{f})^\vee$.

Bibliografía general

Un libro de reciente aparición y tremendamente original es:

[**Iw-Ko**] H. Iwaniec, E. Kowalski. Analytic number theory. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

A pesar de su tamaño (615 páginas) mantiene una notoria y agradable economía en las demostraciones que en muchos puntos complementa con explicaciones muy acertadas. El lector puede encontrar allí temas que pocas veces han bajado de los artículos de investigación a los libros de texto. Incluso en los temas clásicos hay giros inesperados.

Con un contenido más clásico y con explicaciones en general muy buenas, cabe destacar:

[**El**] W.J. Ellison. Les nombres premiers. En collaboration avec Michel Mendès France. Publications de l'Institut de Mathématique de l'Université de Nancago, No. IX. Actualités Scientifiques et Industrielles, No. 1366. Hermann, Paris, 1975.

Además contiene muchos ejercicios propuestos.

Un libro bastante enciclopédico con incursiones tanto en la teoría algebraica como analítica y que trata con éxito de minimizar los detalles técnicos, es:

[**Hu**] L.-K. Hua. Introduction to number theory. Springer-Verlag, Berlin-New York, 1982.

El amplitud de la red mundial nos brinda un mundo de buenos textos por un gasto virtual nulo (calidad/precio=∞, aunque quien vende el *toner* tenga otro cálculo). Un curso gemelo de éste con otras direcciones, interesantes ejercicios y un último capítulo muy destacable es:

[**St**] J. Steuding. `http://www.uam.es/jorn.steuding/files/seminario0.pdf`

Otras notas electrónicas dignas de mención por la variedad de temas tratados son:

[**Elk**] N.D. Elkies. `http://www.math.harvard.edu/~elkies/M259.02/index.html`

Para los viajeros interesados en la teoría analítica de números y que tengan poco espacio en su maleta, es muy aconsejable:

[**Da**] H. Davenport. Multiplicative number theory. Third edition. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

En sólo 177 páginas explica muy bien el material clásico. El precio que debe pagar el lector es leer cada línea con cuidado.

Un libro muy cercano y de los pocos de teoría "avanzada" de números escrito en la lengua de Cervantes es:

[**Ci-Co**] J. Cilleruelo y A. Córdoba, La teoría de los números, Mondadori, Madrid, 1992.

Desafortunadamente desde hace años está descatalogado. Aparte de cubrir buena parte del material habitual, hay algunos capítulos destacables, como el dedicado a la teoría aditiva.

En el siguiente título se unen bastantes ventajas (ejercicios, buenas explicaciones, temas variados) y se puede usar, con algunas selecciones, como material para un curso de licenciatura:

[**Ro**] H.E. Rose. A course in number theory. Second edition. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1994.

Para contrarrestrar lo tendencioso de la selección anterior, nada mejor que terminar con un buen libro "algebraico" y en cualquier caso delicioso de leer:

[**Ir-Ro**] K. Ireland, M. Rosen. A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

Propaganda

Si los teoremas se vendieran en las tiendas, los autores se preocuparían de organizar bellos escaparates. Como afortunadamente no es así e incluso los libros académicos más famosos de Matemáticas tienen poca tirada, los matemáticos podemos permitirnos el lujo de escribir para un club selecto de fanáticos.

Esto no deja de tener sus ventajas, por ejemplo causa un gran respeto y tiene la virtud de alejar a molestos visitantes intempestivos, así un "Nadie entre aquí que no sepa geometría" a tiempo aleja a más intrusos que un *cave canem*.

Un peligro indudable es que lleguemos a asustarnos nosotros mismos, a nuestros estudiantes o a los visitantes bienintencionados escribiendo historias sin argumento o capítulos intermedios de una novela sin comienzo. Por poner un ejemplo, el libro "Introducción al álgebra conmutativa" de Atiyah y Macdonald verdaderamente hace honor a su título, además tiene buenas explicaciones y una gran selección de ejercicios, pero ¿qué cosas podríamos poner en el escaparate? ¿qué le podríamos contar a Gauss? En la página 25 se da la definición de sucesión exacta, en la 26 el lema de la serpiente, en la 27 ya hemos pasado a la definición de producto tensorial por su propiedad universal de factorización. Se pide al lector que pruebe que el homomorfismo borde está bien definido, y evidentemente puede hacerlo combinando definiciones, y puede resolver todos los ejercicios del libro pero lo que sobre todo se le exige al lector es que tenga una fe blindada y mantenida hasta un curso de topología en el que el borde sea el borde. ¿Para qué escribir $\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}\big(M, \mathrm{Hom}(N, P)\big)$ (página 32) para indicar que al fijar una variables en una función que tiene dos, se queda sólo con una? El estudiante que supere esta ardua disciplina lingüística esta capacitado para entender los poéticos teoremas futuros, pero ¿no puede haberse quedado alguien valioso desalentado por el camino? Hay demasiadas pirámides invertidas y la sombra de su construcción oculta el punto de apoyo. No hay lugar para tantos teoremas egoístas que responden a preguntas naturales en contextos antinaturales.

Otro peligro es la especialización como excusa para la ignorancia impenitente o la petulancia, y si nos fiamos de Ortega y Gasset cuando coge bríos en su capítulo "La barbarie del especialismo" (de su obra "La rebelión de las masas"): "El resultado más inmediato de este especialismo *no compensado* ha sido que hoy, cuando hay mayor número de 'hombres de ciencia', hay muchos menos 'hombre cultos' que, por ejemplo, hacia 1750". Más allá de esta exageración, ¿no es triste que pueda haber catedráticos de análisis que apenas conozcan una palabra de álgebra, o viceversa? ¿No es aún más triste que se pueda cercenar la educación de un estudiante de Matemáticas permitiéndole que no vea nunca un grupo de Galois o una serie de Fourier?

En las siguientes líneas se muestra un pequeño escaparate con algunos resultados de propaganda que se probarán en el curso y que añaden algo a nuestro conocimiento previo sin necesidad de concatenar definiciones de crucigrama. El lector puede juzgar el género y tomar su decisión. Los supervivientes del curso, hayan sido las explicaciones buenas o malas, por el hecho de haberlo soportado, no tendrán dudas al final y engrosarán el número de los creyentes indubitados. Su fe se tornará en devoción.

¿Se puede decir algo sobre los primos gemelos?

En primer lugar qué son. Nada más que primos impares consecutivos como 3 y 5 o 101 y 103. Se cree que hay infinitos pero habida cuenta que ya tenemos bastantes problemas al pelear con los primos de uno en uno, no estamos como para enfrentarnos a parejas de ellos. No obstante, V. Brun en 1919 demostró que el espaciamiento medio entre parejas de primos gemelos es al menos del orden del cuadrado del espaciamiento medio entre primos y formuló su resultado de una manera más débil pero espectacular: la suma de los inversos de los primos gemelos converge. Con un ordenador y un análisis teórico del error se puede aproximar el límite obteniéndose:

$$\sum_{p \text{ gemelos}} \frac{1}{p} = 1'9021602\ldots$$

¿No es fantástico que uno pueda probar algo de este tipo? Y lo es más sabiendo que en la prueba no se utiliza ninguna finura acerca de la distribución de los primos. Es puramente combinatoria, elemental pero no sencilla. En última instancia se basa en quitar los números n tales que él y $n+2$ tengan factores primos pequeños. Con métodos más avanzados se demuestra que hay infinitos primos p (de hecho un infinito relativamente grande) tales que $p+2$ tiene a lo más dos factores primos.

La venganza contra Goldbach

Es bien conocida la conjetura de Goldbach[1] de que todo número para mayor que 2 se puede escribir como suma de dos primos ($14 = 7+7$, $16 = 3+13$, $18 = 7+11$), y también es conocido, para cualquiera con inquietud aritmética suficiente para estar leyendo este párrafo, que constituye un problema abierto hasta nuestros días. Como en otros problemas de nuestra rigurosa área, todo parece confabularse contra nosotros para que nos quedemos cerca pero no lleguemos. No obstante, con pócimas a base de sesos de matemático, sangre de tinta y pasta de árbol, se han conseguido algunos resultados asombrosos que conceden una pequeña revancha frente a Goldbach. Por ejemplo, si damos por perdida la batalla y pensamos que la conjetura de Goldbach puede fallar para algunos números, ¿en qué proporción podría ser? ¿para menos de un 10 %? ¿para menos de un 2 %? ¿o para un 0'123 %? Resulta que podemos probar que falla en un 0 % de los casos. Esto evidentemente involucra un límite:

$$\lim_{N\to\infty} \frac{\#\{n \leq N \text{ con } 2n \neq p_1 + p_2\}}{N} = 0.$$

Incluso se puede demostrar que este límite tiende con cierta velocidad a cero.

Goldbach también conjeturó que todo número impar mayor que 5 es suma de tres primos. Pues bien, en eso casi se ha vencido porque I.M. Vinogradov probó en 1937 que a partir de cierto número grande (actualmente se sabe que grande $\approx 10^{43000}$, demasiado

[1] En realidad en los tiempos de Euler y Goldbach se consideraba el uno como número primo, de manera que la formulación actual de las conjeturas que hizo Goldbach, conlleva una leve adaptación.

para un ordenador) esta conjetura es cierta. Todavía más, probó que el número de representaciones de un N impar como suma de tres primos se aproxima bien por

$$\frac{N^2}{2(\log N)^3}\prod_{p\not| N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)$$

en el sentido de que el cociente de ambas cantidades tiende a uno. Por alguna misteriosa razón el número de representaciones depende de la factorización. Por otro lado, es asombroso que la demostración original y natural de estos resultados requiera integrales, y en última instancia entender bien qué tipo de resonancias e interferencias puede haber entre osciladores armónicos de frecuencias primas.

El tercer grado

Si queremos estudiar las soluciones racionales de ecuaciones diofánticas de dos variables (esto es lo mismo que resolver ecuaciones diofánticas homogéneas de tres variables), aspirando a ser ordenaditos, podemos dosificar nuestro esfuerzo haciendo una clasificación por el grado de la ecuación.

El caso de primer grado $ax + by = c$ es trivial: se puede despejar "racionalmente" una variable en términos de las otras y dar valores. El caso de segundo grado es un poco más complicado, pero una vez que sabemos si existe una solución (lo cual se puede decidir en tiempo finito resolviendo ciertas congruencias) se parametrizan todas, como en el caso de grado uno. Así por ejemplo todas las soluciones racionales de $x^2 + y^2 = 1$ vienen dadas por $x = (t^2 - 1)/(t^2 + 1)$, $y = 2t/(t^2 + 1)$ para $t = \mathbb{Q}$ ó $t = \infty$.

El caso de grado tres es mucho más complejo y hasta la fecha nadie sabe de ningún algoritmo que permita decidir sin género de dudas en cualquier ejemplo si hay un número finito o infinito de soluciones (para el caso de grado mayor que tres –no reducible a grado menor– hay un profundísimo teorema de calibre medalla Fields, por el que se sabe que el número es siempre finito). Lo más llamativo es que las posibles soluciones tienen una estructura riquísima y el problema aritmético tiene fructíferas interpretaciones algebraicas y geométricas. Una primera reducción es que toda ecuación diofántica "verdaderamente" cúbica se puede escribir tras un cambio de variable como $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$ así que uno puede limitarse a estudiar ese caso.

A modo de ejemplo, digamos que buscamos dos números racionales, un cuadrado perfecto y un cubo perfecto de forma que el primero difiera del segundo en una unidad. En símbolos:

$$y^2 = x^3 + 1.$$

A simple vista se tienen soluciones como $(0, 1)$ o $(2, 3)$. Y podemos "verlas" mejor si las dibujamos como puntos en la curva cúbica definida por la ecuación. Un procedimiento antiguo e ingenioso para hallar un nueva solución a partir de dos consiste en construir la recta que las une y calcular el tercer punto de intersección con la cúbica. En nuestro caso, a partir de $(0, 1)$ y $(2, 3)$ se obtiene $(-1, 0)$. Nada espectacular. Podemos también aplicar la simetría $y \leftrightarrow -y$ o construir la tangente en una solución (ésta es la recta que pasa por ella y por ella misma). Pero en este ejemplo obtenemos sólo cinco soluciones

(y un infinito) porque los puntos acaban "rebotando" unos en otros y se repiten. ¿Es casualidad que estos puntos sea enteros? ¿no buscábamos soluciones racionales? Pues bien, no hace falta esperar al redoble de tambor: el teorema de Lutz-Nagell implica que si un conjunto finito de puntos solución no da soluciones nuevas al proceder como antes, entonces todas las coordenadas son ¡enteras! Además establece un método para encontrar en cualquier ejemplo un conjunto finito maximal de estos puntos.

¿Y si hay infinitas soluciones? Entonces unos pocos puntos que rebotan no pueden ser toda la historia y los denominadores aparecen indefectiblemente. En este caso el teorema de Mordell-Weil nos da un consuelo para matemáticos: el procedimiento anterior de secantes, tangentes y simetrías permite llegar a cualquier solución a partir de un número finito de ellas convenientemente seleccionado. Pero aquí este "convenientemente" permanece sumido en un gran misterio algorítmico. Si uno escarba encuentra nombres raros, y grupos raros, y viene la alianza con las formas modulares y la teoría de Galois, y el último teorema de Fermat... pero hablar de ello aquí es demasiado pretencioso.