TEORÍA DE NÚMEROS

Curso 1999/2000

U.A.M. Departamento de Matemáticas

I. Divisibilidad [1], [2], [3]

-Repaso de congruencias y números primos. Teorema de factorización. Algoritmo de Euclides. Congruencias de Euler-Fermat y Wilson. Teorema chino del resto. Lema de Hensel. Objetivos: Recordar las manipulaciones básicas relativas a la divisibilidad y las congruencias. Seguramente el único material nueva sea la definición de la función ζ y el lema de Hensel.

-Funciones aritméticas. Funciones multiplicativas. Relación entre $f(n)$ y $F(n) = \sum_{d|n} f(d)$, función de Möbius. Series de Dirichlet. Estimación de funciones aritméticas, fórmula de sumación de Abel. Objetivos: Entender que las funciones aritméticas multiplicativas están determinadas por su valor en los primos y potencias de primos, y que en muchos casos se pueden obtener expresiones aproximadas para sus promedios. Respecto a este último punto, las únicas fórmulas empleadas serán la relación $\sum_{n\leq N} F(n) = \sum_{n\leq N}[N/n]f(n)$ y la fórmula de sumación de Abel.

-La distribución de los números primos. Teorema de Chebychev. Teorema de Chebychev. Postulado de Bertrand. Teorema del número primo. Objetivos: Esta sección tiene una gran componente histórica: se pretende enunciar resultados acerca de la distribución de los primos, como el teorema de Chebychev, que son previos al teorema del número primo y, siendo más débiles, admiten una demostración más asequible (pero muy elaborada).

II. Formas cuadráticas [1], [4]

-Ley de reciprocidad cuadrática. Residuos y no residuos cuadráticos. Símbolo de Legendre. Ley de reciprocidad cuadrática. Símbolo de Jacobi. Objetivos: Saber manipular el símbolo de Legendre y la generalización de Jacobi para reconocer los residuos cuadráticos y, en particular, resolver cualquier congruencia cuadrática.

-Enteros algebraicos en $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{d})$. Enteros gaussianos. Primos gaussianos y factorización. Representaciones como suma de dos cuadrados. Enteros algebraicos en $Q(\sqrt{d})$. Objetivos: Entender la relación entre la aritmética (factorización, primos, etc.) de los enteros gaussianos, $\mathbb{Z}[i]$, y la representación de un número como suma de dos cuadradospara resolver completamente este último problema. Notar que, al igual que los enteros gaussianos son los enteros algebraicos en $\mathbb{Q}(i)$, $\mathbb{Z}[\sqrt{d}]$ son los enteros algebraicos en $\mathbb{Q}(\sqrt{d})$ para $d \equiv 2, 3\ (4)$.

-Número de clases de ideales. Repaso de la teoría de ideales. Ideales primos en $\mathbb{Z}[\sqrt{d}]$ (caso $d \equiv 2, 3\ (4),\ d < -1$). Grupo de clases y número de clases. Objetivos: Entender la introducción de los ideales como un artificio teórico para evitar la falta de factorización única. Saber decidir la descomposición de un primo $p \in \mathbb{Z}$ en ideales en $\mathbb{Z}[\sqrt{d}]$ y la relación con las soluciones de $x^2 - dy^2 = n$ (siempre en el caso $d \equiv 2, 3\ (4),\ d < -1$). Comprender que el estudio de estas soluciones pasa por el conocimiento del grupo de clases cuyo orden, el número de clases, admite una fórmula explícita.

III. Aproximación diofántica [**1**], [**2**]

-Números irracionales. Teorema de Dirichlet. Teorema de Dirichlet en aproximación diofántica. Irracionalidad de algunos números. Números algebraicos y trascendentes. Equidistribución de la parte fraccionaria de $n\alpha$ para $\alpha \in \mathbb{R} - \mathbb{Q}$. Objetivos: Lo fundamental es comprender que hay una relación entre la irracionalidad de un número y su aproximación por racionales, así cuando $|\alpha - a_n/b_n|$ tiende "rápido" a cero, α es irracional, y si tiende "muy rápido" se puede llegar a probar la trascendencia de α. Saber que la sucesión $c_n = \mathrm{Frac}(n\alpha)$ está equidistribuida en $[0, 1]$, es decir, ocupa con igual probabilidad subintervalos de la misma longitud.

-Fracciones continuas. Convergentes. Aproximación óptima. Mejora del teorema de Dirichlet. Fracciones continuas periódicas. Objetivos: Saber hallar (con ayuda de una calculadora) los primeros términos y las primeras convergentes de la fracción continua de un número dado. Las convergentes dan en algún sentido la mejor aproximación por racionales, lo que permite ciertas mejoras en el teorema de Dirichlet en aproximación diofántica. Conocer que las fracciones infinitas periódicas corresponden a irracionales cuadráticos.

IV. Ecuaciones diofánticas [**1**], [**2**], [**3**]

-Ternas pitagóricas. Puntos racionales en una cónica. Fórmula para las ternas pitagóricas. Objetivos: Saber encontrar parametrizaciones racionales de cónicas con un punto racional y deducir, en particular, la fórmula para las ternas pitagóricas.

-Ecuación de Pell. Solubilidad de la ecuación de Pell. Ecuación de Pell y fracciones continuas. Objetivos: Saber expresar la solución completa de la ecuación de Pell.

-Último teorema de Fermat para $n = 3k$, $4k$. El caso $n = 4$, descenso infinito. El caso $n = 3$ y la aritmética en $\mathbb{Z}[(-1 + i\sqrt{3})/2]$. Objetivos: La única motivación de esta sección es histórica por la relevancia del problema en el desarrollo de la teoría de los números y ciertas partes del álgebra. Basta con conocer que hay pruebas asequibles del último teorema de Fermat en los casos $n = 3$ y $n = 4$.

V. Curvas elípticas [**1**]

-Ley de grupo. Definición de curva elíptica, forma canónica. Adición de puntos. Objetivos: Aprender a sumar puntos de una curva elíptica escrita en forma canónica.

-Teorema de Mordell-Weil. Enunciado del teorema de Mordell-Weil. Teorema de Siegel. Algunas conjeturas y datos computacionales. Objetivos: Comprender que el grupo de Mordell-Weil permite conocer la estructura de los puntos racionales en una curva elíptica. El teorema correspondiente afirma que dicho grupo está finitamente generado pero todavía quedan muchas cuestiones sin resolver.

Profesor: Fernando Chamizo Despacho: C-XV-307

Bibliografía:

[**1**] H.E. Rose. *A Course in Number Theory*. Clarendon Press 1988.

[**2**] J. Cilleruelo, A. Córdoba. *La Teoría de los Números*. Biblioteca Mondadori 1992.

[**3**] G.H. Hardy, E.M. Wright. *An introduction to the Theory of Numbers*. Clarendon Press 1938.

[**4**] H. Cohn. *Advanced Number Theory*. Dover 1980.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 8**

1) Hallar todas las soluciones racionales de $X^2 - Y^2 = X^3 + XY^2 - 2YX^2 - 2Y^3$. (*Indicación*: En $(0,0)$ hay un punto doble).

2) Hallar todas las soluciones racionales de $Y^2 = X^3 - 3X + 2$.

3) Reducir la curva elíptica $E: Y^2 + 4XY = 3X^3 + 5X^2 + 1$ a su forma canónica.

4) Sea $E: Y^2 = P(X)$ con $P(X) = X^3 + AX + B$. Demostrar que E es una curva elíptica si y sólo si $\mathrm{mcd}(P', P) = 1$. Deducir que E es una curva elíptica si y sólo si $4A^3 + 27B^2 \neq 0$.

5) Sean $P = (1,1)$, $Q = (-1,3)$, $R = (-1,-3)$ puntos de la curva elíptica $E: Y^2 = X^3 - 5X + 5$. Hallar $P + R$, $P - R$ y $2P + Q + R$.

6) Hallar el orden de $P = (-3,2)$ en la curva elíptica $E: Y^2 + 2(X+1)Y = X^3 - X^2 - 2X + 26$.

7) Calcular el orden de $P = (2,3)$ en la curva elíptica $E: Y^2 = X^3 + 1$.

8) Sean $P = (-1,1)$, $Q = (1,2)$ puntos de la curva elíptica $E: Y^2 = X^3 + \frac{1}{2}X + \frac{5}{2}$. Hallar $2P$ y $2Q$.

9) Sea $E: Y^2 = X^4 + 2\alpha X^2 + \beta$, con $\beta \neq 0, \alpha^2$. Demostrar, reduciéndola a su forma canónica con el cambio $U = X^2 + Y + \alpha$, $V = X(X^2 + Y + \alpha)$, que E es una curva elíptica. Concluir que $Y^2 = (1 + aX^2)(1 + bX^2)$ también lo es para $0 < a < b$.

10) Sea $S(d_1, d_2) = \{(x,y,z) \in \mathbb{Z}^3 \,/\, x^2 - d_1 y^2 = 1,\ z^2 - d_2 y^2 = 1\}$ con $d_1, d_2 \in \mathbb{Z}^+$ distintos. Utilizando el teorema de Siegel, el problema anterior y que $(x,y,z) \in S(d_1,d_2)$ implica $(xz)^2 = (1 + d_1 y^2)(1 + d_2 y^2)$, demostrar que $|S(d_1,d_2)| < \infty$.

11) Demostrar que el grupo de Mordell-Weil de $E: Y^2 = X^4 + 1$ es isomorfo a $\mathbb{Z}_3$. (*Indicación*: Utilizar la demostración del caso $n = 4$ del Último Teorema de Fermat).

12) Hallar el grupo de Mordell-Weil de $E: Y^2 = X^3 - 1/108$ usando el cambio $X = (3U + 3V)^{-1}$, $Y = (U - V)(6U + 6V)^{-1}$.

13) Si E es una curva elíptica, se define $E[m] = \{P \in E \,/\, mP = O\}$. Comprobar que $E[m]$ es un grupo para todo $m \in \mathbb{Z}^+$. Hallar una curva elíptica (sobre $\mathbb{Q}$) tal que $E[2] = \{O\}$. ¿A qué grupo es isomorfo $E[2]$ si consideramos E definida sobre $\mathbb{C}$?

14) Sabiendo que la curva elíptica $E: Y^2 = X^3 + X + 1$ sobre $\mathbb{Z}_{103}$ tiene 87 puntos (contando también O), hallar el número de puntos de $E_d: dY^2 = X^3 + X + 1$ donde $103 \nmid d$. (*Indicación*: Distínganse dos casos según d sea o no sea residuo cuadrático módulo 103).

15) Sea N_p el número de puntos de una curva elíptica sobre $\mathbb{Z}_p$ (incluyendo O). La *desigualdad de Hasse* es un profundo resultado que afirma que $|N_p - p - 1| < 2\sqrt{p}$. Comprobar esta desigualdad para $E: Y^2 = X^3 + X + 1$ con $p = 5$ y $p = 7$.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 7**

1) Demostrar que si un triángulo rectángulo tiene lados de longitud entera, entonces su perímetro divide al doble de su área.

2) Hallar todos los triángulos rectángulos de hipotenusa uno cuyos lados sean números racionales con denominador menor o igual que 50.

3) Hallar todas las soluciones racionales de $X^2 + X + 3Y^2 - XY = 4$.

4) Utilizar la fórmula que da las soluciones racionales de $X^2 + 9Y^2 - 5XY - 2Y = 1$ para hallar una solución entera positiva de $x^2 + 9y^2 - 5xy - 134y = 67^2$.

5) Proceder como en el caso de las ternas pitagóricas para hallar una fórmula que produzca todas las ternas de cuadrados perfectos en progresión aritmética.

6) Utilizar el hecho de que $X^2 + Y^2 = 1$ si y sólo si $(X + Y)^2 + (Y - X)^2 = 2$ para resolver el problema anterior de una forma más fácil.

7) Hallar todas las soluciones enteras de $x^2 - 7y^2 = 1$. Hallar también las soluciones racionales.

8) Demostrar que $x^2 - 161y^2 = 23z^2 + 5$ no tiene solución en enteros.

9) Hallar todas las soluciones enteras de $x^2 - 59y^2 = 1$. ¿Para cuántas de ellas x^2 tiene menos de 9 cifras? (Nota: Estas soluciones son las que podríamos comprobar con una calculadora de bolsillo).

10) Sea r la razón aúrea, $r = (1 + \sqrt{5})/2$, y sean $A_n, B_n \in \mathbb{Q}$ con $A_n + B_n\sqrt{5} = r^{2n+1}$, $n \in \mathbb{N}$. Demostrar que $(x, y) = (2A_n, 2B_n)$ son soluciones enteras (y positivas) de $5y^2 = x^2 + 4$.

11) Demostrar que las soluciones enteras de la ecuación exponencial $x^6 = y^6 + 103^z$ son únicamente las soluciones triviales $(x, y, z) = (\pm 103^n, 0, 6n)$ con $n \in \mathbb{N}$.

12) Demostrar que $\dfrac{1}{x^4} + \dfrac{1}{y^4} = \dfrac{1}{z^2}$ no tiene solución en enteros.

13) Hallar una fórmula para las soluciones $x, y, x \in \mathbb{Z} - \{0\}$ de $\dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = 0$. (*Indicación*: Escríbase $x = dA$, $y = dB$ con A y B coprimos).

14) Demostrar que las soluciones enteras de la ecuación $x^4 - 5x^2y^2 + 6y^4 + 3 = 0$ son únicamente $(x, y) = (\pm 3, \pm 2)$.

15) Sean $(x_1, y_1), (x_2, y_2), (x_3, y_3) \ldots$ las soluciones en $\mathbb{Z}^+$ de $5y^2 = x^2 + 4$ escritas en orden creciente. Hallar algunas de ellas y escribir la sucesión $y_1,\ (x_1 + y_1)/2,\ y_2,\ (x_2 + y_2)/2,\ y_3,\ (x_3 + y_3)/2 \ldots$ ¿Qué sucesión es? Inténtese demostrarlo rigurosamente.

16) El teorema de Thue-Siegel-Roth afirma que dado un número algebraico e irracional, α; para cada $\sigma > 2$ existe una constante C tal que $|x - a/b| > C/b^\sigma$ para todo $a/b \in \mathbb{Q}$. Deducir el siguiente teorema de Thue-Siegel: "Si $t^n + a_{n-1}t^{n-1} + \ldots + a_1t + a_0$ es irreducible en $\mathbb{Z}[t]$ y $n > 2$, entonces, para cada $K \in \mathbb{Z}$, la ecuación $x^n + a_{n-1}x^{n-1}y + \ldots + a_1xy^{n-1} + a_0y^n = K$ sólo tiene un número finito de soluciones enteras".

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 6**

1) Hallar las fracciones continuas de $\sqrt{5}$ y de $\sqrt{11}$.

2) Hallar el valor de los números reales cuyas fracciones continuas son $[\overline{2,3}]$, $[1,1,\overline{1,4}]$ y $[5,\overline{2,10}]$.

3) Para $n \in \mathbb{Z}^+$, demostrar que $\sqrt{n^2+1} = [n,\overline{2n}]$ y que $\sqrt{n(n+1)} = [n,\overline{2,2n}]$.

4) ¿Cuál es la fracción continua de $(n+\sqrt{n^2+4})/2$ con $n \in \mathbb{Z}^+$?

5) Sean a y b coprimos y sea p_{n-1}/q_{n-1} la penúltima convergente de a/b, demostrar que $(x,y) = \pm(q_{n-1}, -p_{n-1})$ es una solución de $ax+by = \pm 1$. Utilizar este método para resolver $19x+12y = 1$ en enteros.

6) Escogiendo un número real "al azar" en el intervalo $(0,1)$, ¿cuál es la probabilidad de que el primer coeficiente (no nulo) de su fracción continua tenga tres cifras?

7) Sean α_1 y α_2 las dos raíces de un polinomio, $P \in \mathbb{Z}[x]$, de segundo grado. Demostrar que si $\alpha_1 = [\overline{a,b,c,d}]$ con $a,b,c,d \in \mathbb{Z}^+$, entonces $-1/\alpha_2 = [\overline{d,c,b,a}]$. (*Indicación*: Comenzar demostrando que el P se obtiene despejar en $x = [a,b,c,d+\dfrac{1}{x}]$).

8) Utilizar el resultado del ejercicio anterior (que es un teorema de importancia menor debido a E. Galois) para calcular la fracción continua de $(\sqrt{6}-1)/2$ sin usar la calculadora partiendo de que $(\sqrt{6}+1)/2 = [\overline{1,1,2,1}]$.

9) ¿Cuál es la mejor aproximación racional de π con denominador menor que 12? ¿y con denominador menor que 120?

10) Demostrar que si $x,y > 0$ es una solución en enteros de $x^3 - dy^3 = 1$ con $d \geq 5$, entonces x/y es una convergente de $\sqrt[3]{d}$. Utilizar este hecho para hallar una solución de $x^3 - 17y^3 = 1$. (*Indicación*: $x^3 - a^3 = (x-a)(x^2+ax+a^2)$ para $a \in \mathbb{R}$).

11) Un año solar dura $365'24223379\ldots$ días, pero el calendario oficial le asigna 365 días añadiendo 97 nuevos días cada 400 años, correspondiendo a los años bisiestos. Mejorar la aproximación oficial usando fracciones continuas. (Nota: En 400 años sólo hay 97 bisiestos, porque se suprime uno cada 100 años excepto si el número de siglo es divisible por 4).

12) Sea A una matriz 2×2 con autovalores distintos λ_1, λ_2 y autovectores correspondientes $\vec{w}_1$, $\vec{w}_2$. Demostrar que $\vec{v}_n = C_1\lambda_1^n\vec{w}_1 + C_2\lambda_2^n\vec{w}_2$, donde C_1, C_2 son constantes arbitrarias, es la solución general de la ecuación recurrente $\vec{v}_{n+1} = A\vec{v}_n$. Utilizar este hecho para hallar una fórmula explícita para las convergentes de $\sqrt{2}-1 = [0,\overline{2}]$.

13) Se llaman números de Fibonacci a los términos de la sucesión 1,1,2,3,5,8,13,... que satisface $f_1 = f_2 = 1$, $f_{n+2} = f_{n+1} + f_n$. Demostrar que f_{n+2}/f_{n+1} es la n-ésima convergente de la razón aúrea $(1+\sqrt{5})/2$. Utilizar el problema anterior para hallar una fórmula explícita para f_n.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 5**

1) Demostrar que $\sqrt[5]{33}-\sqrt{3}$ es irracional. (*Indicación*: Hay una demostración breve usando que $\sqrt[5]{33}$ y $\sqrt{3}$ son enteros algebraicos).

2) Demostrar que el logaritmo decimal de un racional positivo, o bien es entero o bien es irracional.

3) Hallar tres fracciones a/b tales que $|\sqrt{6}-a/b|<b^{-2}$.

4) Demostrar que $\sum 10^{-n^2}$ y $\sum(-1)^n n^{-1}2^{-n!}$ son irracionales.

5) Sea c_n la n-ésima cifra decimal de π, demostrar que $\sum(-1)^n(n+c_n)^{-1}(n!)^{-n}$ es irracional.

6) Sea $\alpha=e^{(-1+\sqrt{5})/4}\cos\left(\sqrt{\frac{5+\sqrt{5}}{8}}\right)+e^{(-1-\sqrt{5})/4}\cos\left(\sqrt{\frac{5-\sqrt{5}}{8}}\right)$. Sabiendo que $\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}$, deducir $2\alpha=e^{\zeta}+e^{\zeta^2}+e^{\zeta^3}+e^{\zeta^4}$ con $\zeta=e^{2\pi i/5}$ y utilizar esta fórmula para probar que α es irracional.

7) Demostrar que $a_n=(1+\frac{3}{4}\sqrt{2})(1+\sqrt{2})^n+(1-\frac{3}{4}\sqrt{2})(1-\sqrt{2})^n$ es entero para todo $n\in\mathbb{N}$ y que $|\sqrt{2}-1-a_n/a_{n+1}|<a_{n+1}^{-2}$.

8) Sean $\alpha=0'1234567891011\ldots$ y $\beta=0'235711131719\ldots$ Demostrar que α y β son irracionales. (*Indicación*: Basta ver que no son decimales periódicos).

9) Demostrar que $\pi+e$ y πe no pueden ser ambos racionales (Nota: Todavía no se conoce si alguno lo es). Demostrar que al menos uno de ellos es trascendente.

10) Demostrar que $\sum 2^{-n^n}$ es trascendente.

11) Demostrar que $\sum n^{-4}\mathrm{cosec}(2\pi n\sqrt{2})$ y $\sum n^{-5}\mathrm{cosec}(2\pi n\sqrt[3]{2})$ convergen.

12) Demostrar que la parte fraccionaria de $n!e$ no está equidistribuida.

13) Demostrar que la parte fraccionaria de $(1+\frac{3}{4}\sqrt{2})(1+\sqrt{2})^n$ no está equidistribuida.

14) Demostrar que si α es irracional entonces existe $n\in\mathbb{N}$ tal que la parte fraccionaria de $n\alpha$ tiene un 3 en el lugar 1000. Probar también que casi todo $0<x<1$ (en el sentido de la medida) contiene la cifra 7 en su desarrollo decimal.

15) El código ASCII asigna a cada número $0\le n<256$ un carácter (o símbolo gráfico o de control). Así pues, utilizando base 256 podemos "leer" cada número $0<x<1$. Por ejemplo, $\log\frac{35}{27}=\frac{66}{256}+\frac{111}{256^2}+\frac{83}{256^3}+\frac{97}{256^4}+\ldots\to$ BoSa.... Demostrar que existe $n\in\mathbb{N}$ tal que la parte fraccionaria de $n\pi$ comienza con el texto completo de "El Quijote". Probar que casi todo $x\in(0,1)$ contiene todos los libros del mundo. (*Indicación*: Proceder como en el problema anterior).

16) Sea $L(n)$ la parte fraccionaria de $\log n$. Dar una fórmula aproximada para el cardinal de los $1\le n\le N$ tales que $L(n)<1/2$ y deducir que $L(n)$ no está equidistribuida.

17) En el primer examen saco un $8|\mathrm{sen}\,3|$, en el segundo $8|\mathrm{sen}\,6|$, en el tercero $8|\mathrm{sen}\,9|$ y así sucesivamente. Demostrar que si el número de exámenes es suficientemente grande la media me saldrá aprobado.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 4**

En toda esta hoja d designa a un libre de cuadrados con $d < -1$, $d \equiv 2, 3\ (4)$, $\mathcal{H}_d$ es el grupo de clases de $\mathbb{Z}[\sqrt{d}]$ y p, p_1, $p_2, \ldots$ etc. representan primos impares (distintos).

1) Demostrar que $\left((1+\sqrt{5})/2\right)^n + \left((1-\sqrt{5})/2\right)^n \in \mathbb{Z}$ para todo $n \in \mathbb{N}$. (*Indicación*: Probar que es racional y entero algebraico).

2) Demostrar que cada término de la sucesión $x_{n+1} = \sqrt{2+\sqrt{3+x_n}}$ con $x_0 = 0$, es un entero algebraico. ¿Es también $\lim x_n$, si existe, un entero algebraico?

3) Comprobar que $(3+2\sqrt{2})^n$, $n \in \mathbb{N}$, son unidades distintas en $\mathbb{Z}[\sqrt{2}]$ y utilizarlas para demostrar que $x^2 - 2y^2 = 7$ tiene infinitas soluciones enteras. Hallar tres positivas.

4) Utilizar las soluciones enteras obvias de $x^2 + 37y^2 = 38$ y $x^2 + 37y^2 = 41$ para hallar una solución de $x^2 + 37y^2 = 1558 = 38 \cdot 41$.

5) Demostrar de manera elemental, sin usar la teoría de ideales, que si $\left(\frac{d}{p}\right) = -1$ entonces la ecuación $x^2 - dy^2 = p^\alpha$ no tiene solución entera si α es impar, y si α es par las únicas soluciones enteras son $(\pm p^{\alpha/2}, 0)$.

6) Demostrar que si I es un ideal en $\mathbb{Z}[\sqrt{d}]$ entonces $I^{|\mathcal{H}_d|}$ es principal. Deducir el siguiente resultado similar a uno probado por Jacobi antes de que naciera la teoría de ideales: "Si $d \equiv 1\ (p)$, $x^2 - dy^2 = p^{|\mathcal{H}_d|}$ tiene solución en enteros".

7) Suponiendo que $|\mathcal{H}_d| = 1$, $\left(\frac{d}{p_1}\right) = \left(\frac{d}{p_2}\right) = \ldots = \left(\frac{d}{p_k}\right) = 1$, hallar una fórmula para el número de divisores de $p_1 p_2 \ldots p_k$ en $\mathbb{Z}[\sqrt{d}]$.

8) Repetir el problema anterior suponiendo además que ninguna de las ecuaciones $x^2 - dy^2 = p_j$ tiene solución en enteros y que ahora $|\mathcal{H}_d| = 2$.

9) Estudiar si el ideal $(29, 13+\sqrt{-5})$ es principal en $\mathbb{Z}[\sqrt{-5}]$.

10) Hallar el número de clases de $\mathbb{Z}[\sqrt{-10}]$, esto es, $|\mathcal{H}_{-10}|$ y calcular el número de soluciones enteras de $x^2 + 10y^2 = 7^n$.

11) Sea $I = (3, 1+\sqrt{-17})$. Demostrar que $I^2 = (9, 1+\sqrt{-17})$ no es principal y que $I^4 = (8-\sqrt{-17})$. Concluir (sin hallarlo) que $|\mathcal{H}_{-17}|$ es múltiplo de 4.

12) Factorizar (3) y (41) en $\mathbb{Z}[\sqrt{-5}]$ y hallar el número de soluciones enteras de $x^2 + 5y^2 = 123^n$.

13) Sabiendo que $\mathcal{H}_{-26} \approx \mathbb{Z}_6$ y que el ideal $(5, 2+\sqrt{-26})$ corresponde a $\overline{1}$, hallar el número de soluciones enteras de $x^2 + 26y^2 = 5^{10}$.

14) Hallar, en general, el número de soluciones de $x^2 + 26y^2 = 5^n$ en función de n.

15) Comprobar que $2x^2 + 2xy + 3y^2 = n$ equivale a $(3y+x)^2 + 5x^2 = 3n$. Utilizar este hecho para demostrar que si $x^2 + 5y^2 = p$ tiene solución en enteros entonces $2x^2 + 2xy + 3y^2 = p$ no la tiene.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 3**

En esta hoja p representa siempre un primo impar

1) Probar que x^2+1 tiene 4 raíces en $\mathbb{Z}_{65}$ (no es necesario hallarlas). ¿Cómo puede ser si tiene grado 2? ¿Cuántas tiene en $\mathbb{Z}_{169}$?

2) Demostrar $2^2 \cdot 4^2 \cdot \ldots \cdot (p-1)^2 \equiv 1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2}\ (p)$.

3) ¿La suma de tres cuadrados consecutivos puede ser un múltiplo de 19?

4) Calcular $\left(\frac{3}{p}\right)$.

5) Caracterizar los p para los que $x^2-2x+6 \equiv 0\ (p)$ tiene solución.

6) Rehacer el problema 12 de la Hoja 1 ($p \,|\, 4n^2+1 \ \Rightarrow\ p \equiv 1\ (4)$) utilizando residuos cuadráticos.

7) Demostrar por inducción $a^{\phi(p^k)/2} \equiv \left(\frac{a}{p}\right)\ (p^k)$ para $k \in \mathbb{Z}^+$.

8) Demostrar que si $p = 2^n+1$, esto es, si es primo de Fermat, entonces $\overline{g}$ es un generador de $\mathbb{Z}_p^*$ si y sólo si g es no residuo módulo p.

9) En uno de los primeros microordenadores personales, la n-ésima vez que se accedía a su generador de números aleatorios se obtenía el número $\texttt{RND}(n) = (x_n - 1)/65536$ donde $x_n \equiv 75^n\ (65537)$ con $0 < x_n < 65537$. Sabiendo que $65537 = 2^{16}+1$ es primo, averiguar el valor de $\texttt{RND}(32768)$. ¿Cuándo se repiten por primera vez los números generados por $\texttt{RND}(n)$? (*Indicación*: Utilizar el problema anterior)

10) Calcular los símbolos de Legendre $\left(\frac{175}{257}\right)$, $\left(\frac{15}{103}\right)$, $\left(\frac{136}{137}\right)$.

11) Calcular los símbolos de Jacobi $\left(\frac{3}{35}\right)$, $\left(\frac{403}{803}\right)$, $\left(\frac{133}{169}\right)$.

12) Comprobar que $x^2 \equiv 32\ (33)$ no tiene solución y sin embargo $\left(\frac{32}{33}\right) = 1$.

13) Factorizar $3+11i$ en $\mathbb{Z}[i]$.

14) Hallar el número de representaciones como suma de dos cuadrados de 29000000.

15) Hallar al menos dos soluciones de $x^2+y^2 = 9945 = 3^2 \cdot 5 \cdot 13 \cdot 17$ con $0 < x < y$.

16) Demostrar que $r(n) = 4 \sum_{(2k+1)|n} \left(\frac{-1}{2k+1}\right)$. ¿Es $r(n)/4$ multiplicativa?

17) Sea $\widetilde{r}(n) = \left|\{(a,b) \in \mathbb{Z}^2 : a^2+b^2 = n, \text{ con } a \text{ y } b \text{ primos entre sí (coprimos)}\}\right|$. Demostrar que $r(n) = \sum_{d^2|n} \widetilde{r}(n/d^2)$ y deducir $\widetilde{r}(n) = \sum_{d^2|n} \mu(d) r(n/d^2)$.

18) Si $\pi/4 < \alpha_1 < \alpha_2 < \pi/2$ son los argumentos de dos primos gaussianos, demostrar que $\lambda\alpha_1 + \mu\alpha_2 \neq 0$ para $(\lambda,\mu) \in \mathbb{Z}^2 - \{(0,0)\}$. Deducir que $\operatorname{arc\,tg} 2/\operatorname{arc\,tg}(3/2) \notin \mathbb{Q}$.

19) Sea $\mathcal{P}_{30}(x)$ el conjunto de primos gaussianos, z, con argumento $0 < \alpha < \pi/6$ y $|z|^2 \leq x$. Sabiendo que $\lim_{x\to+\infty} 3\left|\mathcal{P}_{30}(x)\right| \frac{\log x}{x} = 1$, hallar $\lim_{x\to+\infty} \frac{1}{x} \sum_{z \in \mathcal{P}_{30}(x)} \log|z|$.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 2**

1) Calcular la probabilidad de que un número "escogido al azar" no sea divisible por ningún cuadrado mayor que 1.

2) Escribir $\sum_{n=1}^{\infty} d(n)n^{-s}$ en términos de la función ζ.

3) Repetir el problema anterior cambiando $d(n)$ por $\sigma(n)$ (la suma de los divisores).

4) Demostrar que $\sum_{n=1}^{\infty} d^2(n)n^{-s} = \zeta^4(s)/\zeta(2s)$. Nota: Este problema es más difícil que los dos anteriores.

5) Utilizar la fórmula de sumación de Abel para demostrar

a) $\sum_{n\le N} n^{-3/4} = 4N^{1/4} + C + O(N^{-3/4})$ b) $\sum_{n\le N} \log n = N\log N - N + O(\log N)$

donde C es una constante.

6) Hallar fórmulas aproximadas para los promedios de $f_1(n) = n\,d(n)$ y de $f_2(n) = \sqrt{n}\,\phi(n)$ en el intervalo $[1, N]$ con N grande.

7) Demostrar que $d(n) \neq O(\log n)$.

8) Se dice que p es un primo gemelo si p y $p+2$ son primos. Se conjetura que hay infinitos primos gemelos pero sólo se sabe que hay $O(N/\log^2 N)$ de ellos menores o iguales que N. Demostrar que la suma de los inversos de los primos gemelos converge y que, si hay infinitos, el n-ésimo primo gemelo satisface $p_n > Cn\log^2 n$ donde $C > 0$ es una constante.

9) Sea $c(n) = 1$ si n se puede escribir como suma de dos cuadrados y $c(n) = 0$ en otro caso. (Ej. $c(5) = c(2^2 + 1^2) = 1$, $c(9) = c(3^2 + 0^2) = 1$, $c(7) = 0$). Utilizando que $|z||w| = |zw|$ para $z, w \in \mathbb{C}$, demostrar que c es multiplicativa. Sea $C(n) = c(1) + c(2) + \ldots + c(n)$, sabiendo que $\lim C(n)\sqrt{\log n}\,/n = 1$, demostrar que si a_n es el n-ésimo número representable como suma de dos cuadrados $\lim n\sqrt{\log n}\,/a_n = 1$.

10) El postulado de Bertrand también se cumple si reemplazamos el intervalo $(n, 2n]$ por $(x, 2x-7]$ para $x \ge 9$. Sabiendo esto, demostrar que todo número mayor que 6 se puede escribir como suma de primos distintos.

11) Demostrar que $\sum_{n\le N} n^{-1}$ no es entero para ningún $N \ge 2$. (*Indicación*: Encontrar un primo que divida al denominador pero no al numerador).

12) Estudiar si la serie $\sum(p\log p)^{-1}$ converge.

13) Usando el teorema del número primo, aproximar las sumas $\sum_{p\le x} p$ y $\sum_{p\le x} p^2$.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja 1**

1) Sabiendo que π^2 es irracional, demostrar que hay infinitos primos. (*Indicación*: Utilícese $\zeta(2) = \pi^2/6$).

2) Sea $\mathcal{H} = \{5, 9, 13, 17, 21, \ldots\}$. Decimos que $n \in \mathcal{H}$ es $\mathcal{H}$-primo si no tiene divisores propios en $\mathcal{H}$. Demostrar que la factorización en $\mathcal{H}$-primos no es única.

3) Demostrar que hay infinitos primos de la forma $6n - 1$.

4) Hallar $\prod_p (p^2-1)^2/(p^4-1)$ y $\prod_p (1+p^{-2})$. Nota: $\zeta(4) = \pi^4/90$.

5) Si contamos con los dedos de una mano de la forma habitual (comenzando por el índice y acabando en el pulgar), ¿en qué dedo terminará la cuenta hasta 7^{7^7}?

6) Sea $F(n) = 2^n + 1$ con $n \in \mathbb{Z}^+$. Demostrar que si $F(n) = r \cdot s$, con $r, s > 1$, entonces las máximas potencias de 2 que dividen a $r-1$ y a $s-1$ coinciden.

7) Los números $F(n)$ del ejercicio anterior se llaman *primos de Fermat* si son primos (sólo se conocen cinco de ellos) y *números de Fermat* si $n = 2^k$, $k \in \mathbb{N}$. Demostrar que los primos de Fermat son números de Fermat y que dos números de Fermat son siempre coprimos. (*Indicación*: Probar que si a es impar $2^b + 1 | 2^{ab} + 1$).

8) He comprado bolígrafos a 101 ptas y rotuladores a 140 ptas. Si me he gastado en total 2993 ptas, ¿cuántos he comprado de cada?

9) Hallar todas las soluciones de $x^4 + 3x^2 + 2 \equiv 0$ (45).

10) Hallar en cuántos ceros termina 131!

11) Demostrar que hay infinitos números que no son suma de dos ni de tres cuadrados. (*Indicación*: ¿Qué ocurre en $\mathbb{Z}_8$?)

12) Demostrar que si un primo, p, divide a $4n^2 + 1$ con $n \geq 1$, entonces $4|p-1$. (*Indicación*: Sea $\overline{g}$ un generador de $\mathbb{Z}_p^*$ y α tal que $g^\alpha \equiv 2n$ (p). Probar que $4\alpha/(p-1)$ es un entero impar).

13) Hallar una fórmula para la suma de las raíces cuadradas de los divisores de un número.

14) Demostrar que si $F(n)$ es multiplicativa, $f(n) = \sum_{d|n} F(d)\mu(n/d)$ también lo es.

15) Calcular la suma de $d^{-1}\phi(d)$ sobre todos los divisores de un millón.

16) Hallar $\sum_{d|n} |\mu(d)|$ en términos de la factorización de n.

17) Demostrar que si a y n son coprimos, n divide a $\sum_{d|n} a^d \mu(n/d)$.

18) Sea la función $\Lambda(n) = \log p$ si $n = p^\alpha$, $\alpha \geq 1$, y $\Lambda(n) = 0$ en otro caso. Hallar $\sum_{d|n} \mu(d)\Lambda(n/d)$.

19) Fijado $K \in \mathbb{N}$, sea $R_K(n) = \sum_j e^{2\pi i j K/n}$ donde j recorre los números $1 \leq j \leq n$ con $(j, n) = 1$. Demostrar que $R_K(n)$ es multiplicativa.

20) Con la notación del ejercicio anterior, hallar una fórmula para $R_1(n)$.

TEORÍA DE NÚMEROS **Curso 1999/2000** **Hoja E**

1) a) Hallar una fórmula exacta para $f(n) = \sum_{d|n} d|\mu(d)|$ en términos de la factorización de n. b) La suma de los divisores positivos de la forma $6k+1$ de un número, ¿es una función multiplicativa? c) ¿Qué hora es 19^{1999} horas después de las once?

2) Caracterizar mediante condiciones de congruencia los primos, $p > 3$, tales que $x^2 + 4x + 7 \equiv 0 \ \ (p)$ tiene solución.

3) Sea $\alpha = \sum 5^{-n^5}$. Demostrar las siguientes afirmaciones: a) α es un número irracional. b) $\beta = \sqrt{3+\sqrt{\alpha}}$ también es irracional. c) Existe un número natural, n, tal que la milésima cifra decimal de $n\beta$ es un 7.

4) Sabiendo que el grupo de clases de $\mathbb{Z}[\sqrt{-17}]$ es isomorfo a $\mathbb{Z}_4$ y que está generado por $(3, 1+\sqrt{-17})$, hallar el número de soluciones enteras de $x^2 + 17y^2 = 9^{1999}$.

5) Sea la curva elíptica $E : y^2 = x^3 + 8$ y sean $P = (2, 4)$ y $Q = (1, 3)$. Calcular $1999P + 1999Q$.

6) Calcular la suma $\sum_{d|n} d^{-1}\phi(d)$ para $n = 100^{100}$.

7) Hallar una fórmula para las soluciones racionales de $x^2 + 2xy + 2y^2 = 5$. ¿Cuántas de ellas son enteras?

8) a) Si $p > 2$ es primo, ¿con qué es congruente $(p^4 - 1)!$ módulo p^4? b) Si $n \in \mathbb{Z}$, demostrar que $(n+6)(n+7)(n-4)/6 \in \mathbb{Z}$. c) ¿Qué número representa $[2, 3, 3, 3, \ldots]$?

9) Considérese el punto $P = (1, 2)$ de la curva elíptica $E : y^2 = x^3 + 3$. Hallar razonadamente otro punto racional, $Q = (x_0, y_0)$, en E con $y_0 > 0$ y demostrar que P no tiene orden 4. (Indicación: No es necesario calcular $3P$).

10) Sabiendo que $\mathbb{Z}[\sqrt{-5}]$ tiene número de clases dos, hallar el número de soluciones enteras de $x^2 + 5y^2 = 231^2$. (Nota: $231 = 3 \cdot 7 \cdot 11$).

11) Sabiendo que el número de clases de $\mathbb{Z}[\sqrt{-5}]$ es dos, hallar el número de soluciones enteras de $x^2 + 5y^2 = 1089^{1999}$.

12) Hallar una fórmula que dé todas soluciones racionales de $x^2 + xy + 3y^2 - 5 = 0$. ¿Cuántas de ellas son enteras?

13) Contestar breve pero razonadamente a las tres preguntas siguientes: a) ¿Qué número representa la fracción continua $[2, 4, 4, 4, 4, \ldots]$? b) Si p es un primo impar, ¿con qué es congruente $(p^2-1)!$ módulo p^2? c) Sea p es un primo impar, si p tiene 4 representaciones como suma de dos cuadrados, ¿cuántas puede tener $p + 2$?

14) Sabiendo que 103 es primo, hallar cuántas soluciones tiene $x^5 - x^4 - 10x^3 + 10x^2 + 21x - 21 \equiv 0 \ (103^2)$.

15) Dadas la curvas elípticas $E_a : y^2 = x^3 + a$ con $a \in \mathbb{Z}^+$, hallar todos los valores de a para los que E_a tiene algún punto de orden dos. De entre estos valores, encontrar alguno mayor que dos de manera que el grupo de Mordell-Weil no sea $\mathbb{Z}_2$.