UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS

ECUACIONES DIOFANTINAS

Y

PROBLEMA DECIMO DE HILBERT

T E S I S

QUE PARA OBTENER EL TITULO

DE

M A T E M A T I C O

SUSTENTA

ENRIQUE MARTINEZ TELLEZ

México, D. F.

1992

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INDICE

INTRODUCCION

David Hilbert al dirigirse a las personas que asistieron al Segundo Congreso Internacional de Matemáticas en Paris el 8 de agosto de 1900, propuso un a lista de 23 problemas que han mantenido en constante trabajo a varias generaciones de matemáticos, los cuales han contribuido a la generación de nuevas teorías matemáticas. Uno de los problemas recientemente conquistado fue el resuelto en 1970 por el matemático ruso de 22 años Yuri Matyasevich.

David Hilbert nació en Konisberg en 1862 y fue profesor en la Universidad de Gottingen desde 1895 hasta su muerte en 1943. Después de la muerte de Henri Poincaré en 1912 fue considerado como el matemático más destacado de su tiempo, Hilbert hizo contribuciones fundamentales en varios campos pero es tal vez más recordado por su desarrollo de los métodos abstractos como herramienta poderosísima en las matemáticas.

El problema diez de Hilbert se describe fácilmente. Tiene que ver con la más simple y la más básica actividad matemática: resolver ecuaciones.

Las ecuaciones a resolver son ecuaciones polinomiales, es decir, ecuaciones tales como $X^2-3XY=5$, las cuales se forman sumando y multiplicando variables y constantes, usando exponentes enteros. Además Hilbert especificó que las ecuaciones deben tener y usar enteros, es decir, números enteros positivos (y o) negativos.

No se permiten números irracionales en la formación de las ecuaciones o de sus soluciones. Los problemas de éste tipo se llaman Ecuaciones Diofantinas que derivan su nombre de Diofanto de Alejandría, quién escribió un libro sobre éste tema en el siglo tres.

El problema diez de Hilbert es el siguiente: Dar un procedimiento mecánico mediante el cual se pueda probar cualquier Ecuación Diofantina y checar si existe solución para la ecuación elegida. Pero dejemos a Hilbert que lo exprese por si mismo: "Dada una Ecuación Diofantina con número arbitrario de incógnitas y con coeficientes numéricos racionales enteros: encuéntrese un proceso el cual pueda determinar mediante un número finito de operaciones si la ecuación dada se puede resolver en enteros racionales". Hilbert no pide un proceso para encontrar las soluciones sino un proceso para determinar si la ecuación tiene soluciones. El proceso deberá ser un proceso formal bien definido que pueda ser programado en una computadora y que se pueda garantizar que trabaje en todos los casos, tal proceso recibe el nombre de algoritmo.

Si el problema de Hilbert se enuncia fácilmente, la solución de Matyasevich sin embargo se enuncia todavía en forma más simple: No se puede crear tal proceso, tal algoritmo no existe. Puesto en cierta forma la respuesta parece negativa. El resultado de Matyasevich sin embargo constituye una adición importante y útil para entender las propiedades de

El trabajo de Matyasevich utilizó una serie de trabajos por tres americanos: Martin Davis, Julia Robinson y Hilary Putnam.

El trabajo de estos tres americanos a su ves está basado en las investigaciones hechas por diferentes fundadores de la Lógica Moderna y de la Teoría de la Computación; Alan Turing, Emil Port, Alonzo Church, Stephen Kleene y el mismo Kurt Goedel siendo éste último famoso por su trabajo sobre la Consistencia de Sistemas Axiomáticos (El Problema 2 de Hilbert) y sobre la Hipótesis del Continuo de Cantor (Problema 1 de Hilbert).

Comencemos a tratar el problema diez de Hilbert considerando unas cuantas ecuaciones Diofantinas.

El término Ecuaciones Diofantinas, es un poco errado, porque no es la naturaleza de las ecuaciones lo que es crucial en la naturaleza de las soluciones admisibles.

Por ejemplo, la ecuación $X^2+Y^2-2=0$ tiene una infinidad de soluciones si uno no piensa en ella como una Ecuación Diofantina.

Las soluciones están representadas por la gráfica de la ecuación, que es un circulo en el plano formado por los ejes X, Y.

El centro del circulo se encuentra en el punto de coordenadas $X=0$, $Y=0$.

Este punto recibe el nombre de origen y se abrevia con el símbolo ya conocido de $(0,0)$.

El radio del circulo es $\sqrt{2}$. Las coordenadas de cualquier punto en el circulo satisfacen la ecuación y existe un número infinito de tales puntos.

Si se consideran el problema como una Ecuación Diofantina; existen solamente cuatro soluciones:

(1) $X=1, Y=1$

(2) $X=-1, Y=1$

(3) $X=1, Y=-1$

(4) $X=-1, Y=-1$.

Cambiemos ahora de ecuación a $X^2+Y^2-3=0$. Existe un número infinito de soluciones si ésta ecuación es considerada como una ecuación ordinaria, pero no tiene soluciones si se considera como una Ecuación Diofantina. La razón es que ahora la gráfica es un circulo con radio igual a $\sqrt{3}$, y no hay puntos en ésta curva que tenga ambas coordenadas simultáneamente igual a números enteros.

Una familia famosa de Ecuaciones Diofantinas tiene la forma $X^n+Y^n=Z^n$, en la cual n puede ser igual a $2,3,4$ o cualquier entero mayor si $n=2$ la ecuación se satisface por las longitudes de los lados de cualquier triángulo rectángulo y recibe el nombre de Teorema de Pitágoras.

Una solución es el conjunto de números $X=3$, $Y=4$, $Z=5$. Si n es igual o mayor que 3, la ecuación recibe el nombre de Ecuación de Fermat. El matemático del siglo XVII de nacionalidad francesa Pierre de Fermat pensaba que él habia probado que estas ecuaciones no tienen soluciones positivas enteras. En el margen de una copia del libro de Diofanto el escribió que

había encontrado una prueba maravillosa, pero que infortunadamente era muy larga para ser escrita en ese espacio. La prueba (si en realidad la hubiera encontrado Fermat) nunca ha sido encontrada.

Conocido como el último Teorema de Fermat es probablemente el más antiguo y el más famoso problema al que no se le ha encontrado solución aun.

Estos ejemplos demuestran que las Ecuaciones Diofantinas son fáciles de escribir pero difíciles de resolver. Son difíciles de resolver porque se es muy exclusivo en relación a la clase de números que se aceptan como soluciones.

En relación a las ecuaciones de primer grado, es decir, ecuaciones en las cuales las incógnitas no se satisfacen entre si y todos los exponentes son iguales a uno como $7X+4Y-3Z-99t-13u-10=0$, la existencia de las soluciones se puede determinar por una técnica de división conocida desde tiempos antiguos que recibe el nombre de Algoritmo de Euclides. En relación a las ecuaciones de segundo grado en dos incógnitas tales como $3X^2-5Y^2+7=0$ o $X^2-XY-Y^2=1$, se desarrolló un teoría a principios del siglo diecinueve por el gran Karl Friedrich Gauss la cual permite determinar si existen soluciones. Algunos trabajos desarrollados por el joven matemático británico Alan Bolwer ha arrojado considerable luz en ecuaciones de grado mayor que dos que poseen dos incógnitas. Para las ecuaciones de grado mayor que uno que tiene más de dos incógnitas existen solo casos

especiales que pueden ser manejados por trucos especiales y existe un gran mar de ignorancia.

¿Porque es tan difícil encontrar un proceso tal como lo pedía Hilbert?

El enfoque más directo sería simplemente probar todos los posibles conjuntos de valores de las incógnitas, uno tras otro hasta que se encuentre una solución.

Por ejemplo, si la ecuación tiene dos incógnitas se puede hacer una lista de todos los posibles enteros. Entonces simplemente se recorrería la lista probando uno por tras de otro para ver si satisface la ecuación.

Ciertamente esto es un procedimiento claramente mecánico que bien puede realizar una maquina. ¿Cual sería entonces el resultado?.

Si la ecuación es la primera que mencionamos $X^2+Y^2-2=0$, se debería probar $(0,0)$, $(0,1)$, $(1,0)$, $(0,-1)$, $(-1,0)$ y por supuesto rechazar estos pares. El siguiente candidato $(1,1)$ es una solución, tuvimos suerte: solamente se consideraron seis pares. Si por otra parte la ecuación fuera $X^2+Y^2=20000$ se deberían probar miles de pares de números enteros antes de que se encontrara una solución. Es claro que si existiera una solución, ésta sería encontrada en un número finito de pasos.

Por otro lado, hablando de la otra ecuación $X^2+Y^2-3=0$, se puede probar pares de enteros desde ahora hasta la eternidad, y lo único que se sabrá es que aun no se encuentra una solución. No sería posible saber si el siguiente par de números sería una solución.

En éste ejemplo particular es posible probar que no existen soluciones. Pero la prueba requiere una idea nueva; ésta no se puede obtener solamente por substituciones sucesivas de enteros dentro de la ecuación.

El medio que lleva a cabo el proceso de la clase sugerida por Hilbert debería aceptar como elemento de entrada los coeficientes de una Ecuación Diofantina arbitraria. Como elemento de salida debería encender una luz verde si la ecuación tiene solución y una luz roja si no hay solución. Tal maquina podría ser llamada Máquina de Hilbert. En contraste un medio que simplemente busque soluciones por pruebas sucesivas *ad infinitum* puede ser descrito como una Máquina de Luz verde, si la ecuación tiene solución la luz verde se prende Después de un número finito de pasos. Si la ecuación no tiene solución el cálculo se continúa por siempre simplemente; a diferencia de la Máquina de Hilbert, la Máquina de Luz verde no tiene forma de saber cuando parar. Es fácil construir una maquina de luz verde para las Ecuaciones Diofantinas. La pregunta es, podemos mejorar la situación y construir una Máquina de Hilbert es decir, una Máquina de Luz verde, luz roja que se detenga siempre Después de un número finito de pasos y dar una respuesta de si o no definida. Lo que probó Matyasevich es que esto no puede ser llevado a cabo jamás. Aun si permitimos que la máquina tenga una memoria ilimitada y tiempo de cálculo ilimitado, no se puede escribir un programa y no se puede construir una

máquina que haga lo que Hilbert pedía. No existe tal máquina de Hilbert.

Finalmente recuerdese que problema diez de Hilbert fue resuelto independientemente y con diferencia de tres días por G. V. Chudnoskii otro matemático ruso que en el año 1970 tenía 18 años y que aun ahora sigue activo, pero cuyo trabajo matemático quizá es mas importante que el de Matyasevich.

También quiero hacer notar que casi todo problema matemático tiene su análogo en el lenguaje de las Ecuaciones Diofantinas, por ejemplo la conjetura de Poincaré que dice que toda variedad de tres dimensiones cerrada y conectada simplemente es homeomorfa a una esfera de tres dimensiones, debe tener su análogo en el reino de las Ecuaciones Diofantinas. En los capítulos siguientes de este trabajo solamente se trata a fondo la parte de teoría de números. Las funciones recursivas no se mencionan por merecer un trabajo muy extenso y profundo.

CAPITULO I

CONJUNTOS DIOFANTINOS

Una Ecuación Diofantina es una ecuación polinomial $P(a_1,\ldots,a_m,x_1,\ldots x_m)=0$ en varias variables con coeficientes enteros. Las variables se dividen en parámetros $a_1,a_2,\ldots a_m$ e incógnitas $x_1,x_2,\ldots x_m$ todas las variables, parámetros e incógnitas, toman valores en los enteros no negativos $1,2,\ldots$ En la teoria clásica de Ecuaciones Diofantinas, se comienza teniendo la ecuación y se pregunta por los valores de los parámetros para los cuales existe solución, en este trabajo se dará otra versión al procedimiento. Se comenzará teniendo la solución y se buscará la ecuación.

Se comenzará con la relación $A(a_1,a_2,\ldots a_m)$ y se busca un polinomio $P(a_1,\ldots a_m,x_1,\ldots x_m)$ definido en el sentido de 1.1

DEFINICION 1.1

La relación $A(a_1,a_2,\ldots,a_m)$ es diofantina si existe un polinomio $P(a_1,..a_m,x_1,\ldots x_m)$ tal que para todos los valores de $a_1,a_2,\ldots a_m$ (los parámetros)

1.1 $A(a_1,a_2,\ldots a_m)\Leftrightarrow(\acute{E}x_1,x_2,\ldots,x_m)[P(a_1,\ldots a_m,x_1,\ldots x_m)=0]$

Se deduce que una función es diofantina cuando su gráfica es diofantina. A continuación tenemos ejemplos de relaciones diofantinas, la mayoria se utilizará en la prueba. En estos ejemplos se incluye las relaciones de orden $\leq$ divisibilidad $a|b$ y congruencia $a\equiv b(mod\ c)$.

1.2 $a\leq b\Leftrightarrow(\acute{E}x)[a+x=b]$

1.3 $a/b\Leftrightarrow(\acute{E}x)[ax=b]$

1.4 $a\equiv b(mod\ c)\Leftrightarrow(\acute{e}x)[(a=b+cx)\ o\ (a=b-cx)]$

Los "y"s, "o"s se manejan usando:

1.5 $A=0$ o $B=0 \Leftrightarrow AB=0$ $A=0$ o $B=0 \Leftrightarrow A^2+B^2=0$

En el caso de "y" es necesario renombrar variables que aparecen en A y B.

$\acute{e}xA(x)=0$ y $\acute{e}x\ B(x)=0$ es equivalente a $\acute{e}x\acute{e}y[A(x)=0$ y $B(y)=0]$.

A partir de 1.5 se deduce que "y"s y "o"s de relaciones diofantinas son diofantinas.

Procediendo de esta manera se puede probar que gran cantidad de relaciones son diofantinas.

Un buen ejemplo es la relación de primos relativos o sea a primo relativo con b $(a,b)=1$ que se escribirá como $a\perp b$: Se puede ver que esta relación es diofantina usando (1.5) junto con (1.6) $a\perp b\Leftrightarrow\acute{e}(x,y)[ax-by=1$ o $ax-by=1]$ otros ejemplos de funciones diofantinas son $r=rem(a,b)$, $q=quo(a,b)$

1.7 $r=rem(a,b)\Leftrightarrow r\equiv a(a\ mod\ b)$ y $r\leq b$

1.8 $q=quo(a,b)\Leftrightarrow 0\leq a-qb<b$

Procediendo de otra forma definiendo nueva relación en base a lo anterior usando (1.5) repetidamente se puede demostrar que muchas relaciones son diofantinas. La herramienta más importante en éste proceso será la sucesión de soluciones de la Ecuación de Pell.

CAPITULO II

ECUACION DE PELL

Es un hecho conocido que cuando $m\in Z-\{0\}$ el dominio $Z(m)$ con el conjunto $\{x+y\sqrt{m}, x,y\in Z\}$ con las operaciones:

$$(x+y\sqrt{m})+(a+b\sqrt{m})=(x+a)+(y+b)\sqrt{m}$$

$$(x+y\sqrt{m})(a+b\sqrt{m})=(xa+ybm)+(xb+ya)\sqrt{m},$$

forman un anillo en el cual la representación de los elementos de la forma $x+y\sqrt{m}$ con m no-cuadrática es única:

$$(E)\ x+y\sqrt{m}=a+b\sqrt{m} \text{ implica } x=a,\ y=b \ \forall\ x,y,a,b$$

El subdominio $N(m)=\{x+y\sqrt{m}, x,y\in N\}$ es cerrado con las condiciones anteriores de suma y producto, en tal forma que para $a<1$ arbitrario y n existe exactamente una solución $(X(n,a),Y(n,a))$ en N para la ecuación

$$x+y\sqrt{(a^2-1)}=(a+\sqrt{(a^2-1)})^n.$$

Estas soluciones son exactamente las soluciones en enteros no-negativos de la Ecuación de Pell en a:

$$x^2-(a^2-1)y^2=1$$

Recuerde que la Ecuación General de Pell es una ecuación de la forma

$x^2-dy^2=1$ (d es no-cuadrática)

cuando d es constante y x,y son las incógnitas cuando d es cuadrática, la Ecuación de Pell posee la solución trivial $(1,0)$.

Como x^2-dy^2 se puede factorizar en los reales, $x^2-dy^2=(x+y\sqrt{d})(x-y\sqrt{dt})$ es natural trabajar en el dominio entero $Z[\sqrt{d}]$, formado por los números reales de la forma $a=x+y\sqrt{d}$ $x,y\in Z$ la Ecuación de

Pell con $d=a^2-1$, $x^2-(a^2-1)y^2=1$ tiene como solución fundamental a $(x,y)=(a,1)$

LEMA 1.

$(\forall a>1)$: $\{(X(n,a), Y(n,a); n\in N)=\{(x,y); x,y\in N, x^2-(a^2-1)y^2=1\}$

$X(n,a)$, $Y(n,a)$ se llaman la solución n-ésima de x,y de la Ecuación de Pell para a. Existen relaciones de divisibilidad entre los números de la solución y las soluciones de la Ecuación de Pell para a, así como propiedades de crecimiento de la sucesión de soluciones que admiten una descripción diofantina $x=y^n$ por medio de $x=X(n,a)$. Se dará una descripción de exponenciación y posteriormente de "x es la n-ésima solución de la Ecuación de Pell en a". Para completar el cuadro también se probarán propiedades simples de teoria de números de la Ecuación de Pell que utilizaremos.
Para evitar distinción de casos molestos de $z=0$ o $y=0$, entenderemos a lo largo de esta sección cuando se utiliza el término número, números naturales positivos y usaremos variables y cuantificadores normalmente a menos que se indique lo contrario.

PROPOSICION.

Descripción diofantina de exponenciación por medio de $x=X(k,a)$. Para m,n,k positivos $m=n^k$ tiene validez exactamente cuando el sistema (G1)-(G5) definido adelante y que relaciona igualdades y desigualdades diofantinas tiene solución para parámetros m,n,k con $y\in N$ y a,x,b,z positivas.

PRUEBA.

Se desarrollará (G1)-(G5) para encontrar suficientes condiciones diofantinas para $m=n^k$. $m=n^k$ se concluye fácilmente cuando m, y n^k son congruentes módulo para una cierta r y son menores que r. Por un lema de J. Robinson de 1952 $2an-n^2-1$ cuando $1<a$ se presenta con el módulo apropiado.

LEMA 2.

$(\forall\ a>1\ \forall\ k,n):$

$[X(k,a)-Y(k,a)(a-n)\equiv n^k\ mod(2an-n^2-1)]$

En base a éste lema las condiciones de congruencia pueden ser formuladas por el requerimiento diofantino de que m es congruente $mod(2an-n^2-1)$ con el número $x-y(a-n)$ con la solución (x,y) de la Ecuación Pell de a, y de que esta solución tiene índice k:

(G1) $x^2-(a^2-1)y^2=1,\ x=X(k,a)$

(G2) $x-y(a-n)\equiv m\ mod(2an-n^2-1)$

(G3) $m<2an-n^2-1$

La estimación $n^k<2an-n^2-1$ se concluye de $n^k<a$ para $n=1$ observándose que $a>1$ (compare con G4) y para $1<n$ se tiene que $a\leq na-1$. Entonces para la hipótesis $n\leq n^k<a$ se tiene que

$$a<(na-1)+n(a-n)=2an-n^2-1.$$

Se puede dar una condición diofantina para $n^k<a$ mediante el uso del lema siguiente.

LEMA 3.

Propiedades de crecimiento de las soluciones de la Ecuación de Pell. Para toda $a>1$ y $n\in N$:

$a^n \leq X(n,a) \leq (2a)^n$

$n \leq Y(n,a)$

$X(n,a) < X(n+1,a)$

$Y(n,a) < Y(n+1,a)$

Por el lema 3 se puede describir a a como la solución x de una Ecuación de Pell con índice suficientemente grande i, a saber $a=X(i,b)$ cuando $1<b$ y $n,k, \leq b-1<i$ así que debido a la tasa de crecimiento:

$$n^k < b^k \leq b^{b-1} \leq X(b-1,b) \leq X(i,b) = a$$

Por tanto se requiere que

(G4) $1<a,b$ y $n,k<b$.

Queda encontrar una expresión diofantina para la solución $a=X(i,b)$ para tener un número i suficientemente grande $(b-1 \leq i)$:

LEMA 4.

Relación por congruencia entre la Y-solución de una Ecuación de Pell y su número solución. Para toda $1<b$ y para toda i:

$$Y(i,b) \equiv i \mod (b-1).$$

Como i, siendo el número solución de a, no puede ser el número 0 de la solución trivial $X(0,b)=1$ debido a que $1<a$, $b-1 \leq i$ se concluye de la congruencia de i y 0 módulo $(b-1)$ y esto por el lema 4 de la divisibilidad de la Y-solución y perteneciendo a la X-solución a por $b-1$:

(G5) $a^2-(b^2-1)((b-1)(z-1))^2=1$.

Por tanto si (G1)-(G5) se satisfacen para los números positivos a,x,b,z,m,n,k y $y\in N$, entonces el lema 1, $x=X(k,a)$ y $y=Y(k,a)$ y por tanto por las consideraciones anteriores $m=n^k$. Reciprocamente si $m=n^k$ escoger b arbitrariamente por (G4) y hágase que $a=X(b-1,b)$, entonces por (G4) y por el lema 3

$$1\leq n^k<b^k\leq b^{b-1}\leq X(b-1,b)=a$$

Entonces $m=n^k<2an-n^2-1$ y por tanto tiene validez (G3). Como $1<a$ $x=X(k,a)$ y $y=Y(k,a)$ están bien definidas. Con esto se satisface (G1) y $0<x$ por el lema 1 y con la hipótesis $m=n^k$, por el lema 2 también se satisface (G2). Debido a que

$$Y(b-1,b)\equiv b-1\equiv 0 \mod(b-1)$$

por el lema 4, existe una z positiva con $Y(b-1,b)=(b-1)(z-1)$ en tal forma que con esta z (G5) se satisface.

Resta dar la prueba de los lemas (1-4) y proporcionar una descripción diofantina de $x=X(k,a)$.

PRUEBA DEL LEMA 1.

Tómese $a>1$ arbitraria, definase a

$$\alpha=\sqrt{(a^2-1)}.$$

"<=" La afirmación:

$(\forall n)$: $X(n,a)+Y(n,a)\alpha\in\{x+y\alpha;x,y\in N$ y $x^2-(a^2-1)y^2=1\}$

se concluye de la definición de $X(n,a)$ y $Y(n,a)$ mediante inducción completa sobre n, y la cerradura de éste conjunto bajo el producto (en particular con $a+\alpha$ en el dominio $Z(a^2-1)$ que pertenece a (a^2-1) y la solución de la Ecuación de Pell de a por $(X(n,a),\ Y(n,a))=(1,0)$. Lo último es trivial,

mientras que la propiedad de cerradura se puede establecer fácilmente.

Se tiene: $X(1,a)=Y(1,a)=(a,1)$.

$$(x+ya)(u+va)=(xu+yv(a^2-1))+(xv+yu)a$$

$$(x-ya)(u-va)=(xu+yv(a^2-1))-(xv+yu)a.$$

Entonces:

$$(xu+yv(a^2-1))^2-(a^2-1)(xv+yv)^2$$

$$=((xu+yv(a^2-1))+(xv+yu)a)(xu+yv(a^2-1))-(xv+yu)a)$$

$$=(x+ya)(u+va)(x-ya)(u-va)$$

$$=(x^2-(a^2-1)y^2)(u^2-(a^2-1)v^2)$$

$=1$ cuando $x^2-(a^2-1)y^2=1$ y $u^2-(a^2-1)v^2=1$

para $x,y,u,v\in Z$.

"$\Rightarrow$" si (x,y) es una solución de la Ecuación de Pell para a y $x,y\in N$, entonces debido a que $n(a+a)^n$ es monótona para alguna n $(x+ya)$ se puede estimar por:

$$X(n,a)+Y(n,a)a=(a+a)^n\leq(x+ya)<(a+a)^{n+1}$$

Entonces para tal n tiene validez

$$1\leq(x+ya)(a+a)^{-n}=(x+ya)(a-a)^n<(a+a)^{(n+1)}(a-a)^n=a+a.$$

De aquí se concluye que $1=(x+ya)(a-a)^n$, porque por la propiedad de cerradura mostrada anteriormente la Ecuación de Pell en a produce las soluciones (x,y), $(a,-1)$ otra produce las soluciones $(x+ya)(a-a)^n$, y cuyas componentes son no negativas porque $1\leq(x+ya)(a-a)^n$; pero $(a,-1)$ es la solución positiva más pequeña de la Ecuación de Pell en a (es decir con la primer componente más pequeña). De la última ecuación se deduce que:

$$(x+ya)=(a-a)^{-n}=(a+a)^n.$$

Para los lemas 2-4, se usarán las siguientes fórmulas (para $a\geq 2, m,n\in N$);

Fórmula de suma:

$$Y(m\pm n,a)=X(n,a)Y(m,a)\pm X(m,a)Y(n,a)$$

$$X(m\pm n,a)=X(m,a)X(n,a)\pm(a^2-1)Y(m,a)Y(n,a)$$

Fórmulas de recursión:

$$X(n+2,a)=2aX(n+1,a)-X(n,a)$$

$$Y(n+2,a)=2aY(n+1,a)-Y(n,a)$$

PRUEBA DEL LEMA 2.

Por inducción

Base:

$$X(0,a)-Y(0,a)(a-n)=1$$

$$X(1,a)-Y(1,a)(a-n)=n.$$

Paso inductivo:

$$X(k+2,a)-Y(k+2,a)(a-n)$$

$$=2aX(k+1,a)-X(k,a)-(2aY(k+1,a)-Y(k,a))(a-n)$$

$$=2a(X(k+1,a)-Y(k+1,a)(a-n)-(X(k,a)-Y(k,a)(a-n))$$

$$\equiv 2an^{k+1}-n^k \bmod (2an-n^2+1)=n^k(2an-1)$$

por hipótesis inductiva

$$=n^k(2an-1)\equiv n^k n^2(2an-n^2-1)=n^{k+2}.$$

PRUEBA DEL LEMA 3.

La propiedad de monotonia se deduce de las fórmulas de suma ($m=1$) con $2\leq a$. La estimación se muestra por medio de inducción;

Base:

$a^0=1=X(0,a)$, $a^1=X(1,a)$, $0=Y(0,a)$, $1=Y(1,a)$.

Paso inductivo:

$a^{n+2} \leq aX(n+1,a)$ hipótesis inductiva para $n+1$

$\leq X(n+2,a)$ fórmula de suma

$\leq 2aX(n+1,a)$ fórmula de recursión

$\leq (2a)(2a)^{n+1}$ hipótesis inductiva.

De

$$n+1 \leq Y(n+1,a) < Y(n+2,a)$$

se concluye que $n+2 \leq Y(n+2,a)$.

PRUEBA DEL LEMA 4.

Por inducción sobre i para $b>1$ arbitraria:

Base:

$Y(0,b)=0$, $Y(1,b)=1$.

Paso inductivo:

$Y(i+2,b)=2bY(i+1,b)-Y(i,b)$ por las fórmulas de recursión

$\equiv 2(i+1)-i \mod(b-1)$ por hipótesis de inducción.

PRUEBA DE LAS FORMULAS DE SUMA.

Por la propiedad de unicidad (E):

$X(m+n,a)+Y(m+n,a)\alpha=(a+\alpha)^{m+n}$

$=(X(m,a)+Y(m,a)\alpha)(X(n,a)+Y(n,a)\alpha)$

$=(X(m,a)X(n,a)+(a^2-1)Y(m,a)Y(n,a))$

$+(X(m,a)Y(n,a)+X(n,a)Y(m,a))\alpha$.

Análogamente:

$X(m-n,a)+Y(m-n,a)\alpha$

$=(X(m-n,a)+Y(m-n,a)\alpha)(X(n,a)+Y(n,a)\alpha)(X(n,a)-Y(n,a)\alpha)$

$=(a+\alpha)^{m-n}(a+\alpha)^n(X(n,a)-Y(n,a)\alpha)$

$=(X(m,a)+Y(m,a)\alpha)(X(n,a)-Y(n,a)\alpha)$

$=(X(m,a)X(n,a)-Y(m,a)Y(n,a)(a^2-1)$

$+(X(n,a)Y(m,a)-X(m,a)Y(n,a))a.$

PRUEBA DE LAS FORMULAS DE RECURSION.

De las fórmulas de suma se deduce:

$X(n+2,a)=aX(n+1,a)+(a^2-1)Y(n+1,a)$ ya que

$a=X(1,a)$ y $1=Y(1,a)$

$X((n+1)-1,a)=aX(n+1,a)-(a^2-1)Y(n+1,a).$

Entonces,

$$X(n+2,a)+X(n,a)=2aX(n+1,a)$$

Análogamente para $Y(n+2,a)$.

Finalmente queda la descripción diofantina de $x=X(k,a)$: para $2\leq a$, $x=X(k,a)$ exactamente cuando el sistema de ecuaciones diofantinas y desigualdades (G1-G7) definidas más adelante son soluciones para los parámetros x,k,a con $y,t,v\in N$ y b,s,u positivos.

PRUEBA.

Se desarrollará (G1)-(G7) encontrando suficientes condiciones diofantinas para $x=X(k,a)$:

(G1) (x,y) resuelve la Ecuación de Pell en a.

Se busca la propiedad de que el número solución i de $x=X(i,a)$ deberá ser igual a k al imponer condiciones en las soluciones:

LEMA 5.

Para toda a,i,j,n con $1<a$, $0<i\leq n$ tiene validez

$X(j,a)\equiv X(i,a) \bmod X(n,a) \Rightarrow$

$$j\equiv i \bmod 4n \quad \text{o} \quad j\equiv -i \bmod 4n.$$

$i=k$ se deduce de su congruencia con respecto a algún módulo y de la condición de que i,k se encuentran conectadas en un sistema de clases residuales con respecto a éste módulo, las condiciones de congruencia se obtienen usando el lema 4 al través de la siguiente cadena de congruencias: k es congruente a una solución $t=Y(j,b)$ de la Ecuación de Pell módulo $4Y(i,a)$:

(G2) $k=t \bmod 4y$, (s,t) resuelven la Ecuación de Pell en b.

Por el lema 4, $Y(j,b)\equiv j \bmod (b-1)$, entonces también $\bmod 4Y(i,a)$, cuando $b-1$ es un múltiplo de $4Y(i,a)$:

(G3) $4y \mid (b-1)$ y $1<b-1$.

Por el lema 5, $j\equiv i \bmod 4Y(i,a)$ cuando para alguna solución x, $u=X(n,a)$ tiene validez:

$$0<i\leq n,\ X(j,a)\equiv X(i,a) \bmod X(n,a),\ Y(i,a)\mid n.$$

(G4) (u,v) resuelve la Ecuación de Pell de a.

Como las soluciones y son monótonas, $i\leq n$ se deduce de $y=Y(i,a)\leq Y(n,a)=v$.

LEMA 6.

$(\forall\ i,n,1<a)$: $Y(i,a)^2 \mid Y(n,a) \Rightarrow Y(i,a)\mid n$.

Por el lema 6, la solución $Y(i,a)\mid n$ se puede imponer por $y^2\mid v$

(G5) $y\leq v$, $y^2\mid v$

Por el lema 7 y $s=X(j,b)$,

$x=X(i,a)\equiv X(j,a) \bmod X(n,a)=u$

se deduce de:

(G6) $x \equiv s \bmod u$ y $b \equiv a \bmod u$

LEMA 7.

Para toda $c, 1<a, b$:

$a \equiv b \bmod c$ implica $(\forall n)\ X(n,a) \equiv X(n,b) \bmod c$.

La estimación de tamaño $i, k \leq Y(k,a)$ se deduce del lema 3 y:

(G7) $k \leq y$.

De los lemas 5-7 se concluye que una solución (G1)-(G7) ya implica $x = X(k,a)$, inversamente sea $x = X(k,a)$ con $a \geq 2$ dado. El par $(X(k,a), Y(k,a))$ satisface (G1).

Con $n = 2kY(k,a)$ el par $(X(k,a), Y(k,a))$ satisface la condición (G4). (G5) tiene la validez para esta elección de u, v, porque por las dos condiciones de divisibilidad siguientes

T1: $\forall\ c>1\ \forall\ n,k:\ Y(n,c) \mid Y(k,c) <=> n \mid k$

T2: $\forall\ a>1\ \forall\ k\ :\ Y(k,a)^2 \mid Y(kY(k,a),a)$

por una tenemos $Y(k,a)^2 \mid Y(kY(k,a),a)$ y por la otra $Y(kY(k,a),a) \mid Y(2kY(k,a),a)$. Por tanto $Y(k,a)^2 \mid Y(n,a)$ por la definición de n y entonces $Y(k,a) \leq Y(n,a)$ ya que $1 \leq k => 0 < Y(k,a)$.

Por el Teorema Chino del residuo existe $b>1$ tal que $b \equiv a \bmod u$ y $b \equiv 1 \bmod 4y$ (G3,G6) porque $4y$, u son primos relativos.

PRUEBA POR

LEMA 8.

(∀ a>1,n): n par *<=> Y(n,a)* par,

se tiene que *v=Y(2kY(k,a),a)* es par y por tanto como

$u^2-(a^2-1)v^2=1$, *u* es impar por

LEMA 9.

(∀ a>1,n): Y(n,a) y *X(n,a)* son primos relativos.

u y *v* son primos relativos, por tanto *u* y *4y* también; para un factor común de *u* y *4y*, como *u* es impar, deberia dividir a *y*, por tanto también *v* ya que $y \mid v$ por (G5).

(s,t)=(X(k,b),Y(k,b)) resuelve la Ecuación de Pell en *b* tal como se pide en la segunda parte de G2 Por tanto $x \equiv s \bmod u$ a partir de (G6), por la congruencia de $b \equiv a \bmod u$, por la congruencia establecida en G6 se concluye por el lema 7

$$s=X(k,b) \equiv X(k,a)=x \bmod u.$$

También $k \equiv t \bmod 4y$ por el lema 4

$$t=Y(k,b) \equiv k \bmod (b-1)$$

y por tanto $\bmod 4y$ ya que por G3 b-1 es múltiplo de *4y*. La condición $K \leq Y(k,a)=y$ de G7 se deduce por el lema 3.

PRUEBA DEL LEMA 9.

De $t \mid X(n,a)$ y $t \mid Y(n,a)$ se deduce $t \mid 1$ de acuerdo con

$$X(n,a)^2-(a^2-1)Y(n,a)^2=1.$$

PRUEBA DE T1.

Demostraremos $Y(n,c)|Y(ni,c)$ por inducción en i: cuando $Y(n,c)|Y(ni,c)$ se tiene también que $Y(n,c)|Y(n(i+1),c)$ por la fórmula de suma

$$Y(n(i+1),c)=X(n,c)Y(ni,c)+X(ni,c)Y(n,c).$$

Supóngase nuevamente $Y(n,a)|Y(k,a)$ y n no divide a k

Para $k=ni+r$ con $0<r<n$ y $0\leq i$ se deduce $Y(n,a)|X(ni,a)Y(r,a)$ porque por la fórmula de suma

$$Y(k,a)=X(r,a)Y(ni,a)+X(ni,a)Y(r,a)$$

y por hipótesis $Y(n,a)|Y(k,a)$ y $Y(n,a)|Y(ni,a)$. Como $Y(n,a)$ y $X(ni,a)$ son primos relativos y cada uno divisor de $Y(n,a)$ también divide a $Y(ni,a)$ por el caso 1, el cual por el lema 9 es primo relativo a $X(ni,a)$ y se deduce $Y(n,a)|Y(r,a)$ contradiciendo a $Y(r,a)<Y(n,a)$ ya que $r<n$.

PRUEBA DEL LEMA 6.

A partir de $Y(i,a)^2|Y(n,a)$ se deduce $i|n$ por T1, entonces $n=ik$ para alguna k.

PROPOSICION.

$(\forall\ 1<a)(\forall\ i,k)$: $Y(ik,a)\equiv kX(i,a)^{(k-1)}Y(i,a)\ mod\ Y(i,a)^3$

De la proposición se deduce

$$Y(i,a)^2|kX(i,a)^{(k-1)}Y(i,a).$$

de $c^2|d$ y $d\equiv e\ mod\ c^3$ se deduce $c^2|e$ y

$$Y(i,a)|kX(i,a)^{k-1}.$$

Entonces $Y(i,a)|k$ ya que $Y(i,a)$ y $X(i,a)$ son primos relativos y por tanto se tiene $Y(i,a)|n$.

La proposición se deduce de la representación única(E) de los elementos de un dominio cuadrático: de

$$X(ik,a)+Y(ik,a)\alpha=(a+\alpha)^{ik}=(X(i,a)+Y(i,a)\alpha)^{k}$$

$$=\sum_{j=0}^{k}\begin{bmatrix}k\\j\end{bmatrix}X(i,a)^{(k-j)}Y(i,a)^{j}(a^2-1)^{j/2} \qquad \text{(Teorema del Binomio)}$$

$$=\sum_{j=0}^{k}\begin{bmatrix}k\\j\end{bmatrix}X(i,a)^{(k-j)}Y(i,a)^{j}(a^2-1)^{j/2} \quad + \quad j \text{ par } \in N$$

$$\sum_{j=0}^{k}\begin{bmatrix}k\\j\end{bmatrix}X(i,a)^{(k-j)}Y(i,a)^{j}\,(a^2-1)^{j/2} \qquad j \text{ impar}$$

se deduce:

$$Y(ik,a)=\sum_{j=0}^{k} v_j \begin{bmatrix}k\\j\end{bmatrix}X(i,a)^{(k-j)}Y(i,a)^{j} \qquad j \text{ impar}$$

$$\equiv\begin{bmatrix}k\\1\end{bmatrix}X(i,a)^{(k-1)}Y(i,a) \bmod Y(i,a)^3$$

donde $v_j=(a^2-1)^{(j-1)/2}$.

PRUEBA DE T2.

Es un caso especial de la proposición con $k=Y(i,a)$. (de $u\equiv v^2w \bmod v^3$ se deduce $v^2|u$.)

PRUEBA DEL LEMA 8.

Debido a la fórmula de recursión

$$Y(n+2,a)=2aY(n+1,a)-Y(n,a)\equiv Y(n,a) \bmod 2$$

se tiene que:

$$Y(2n,a)\equiv Y(0,a)=0 \bmod 2$$

$$Y(2n+1,a)\equiv Y(1,a)=1 \bmod 2.$$

PRUEBA DEL LEMA 7.

Por inducción sobre n, de las fórmulas de recursión:

$X(0,a)=1=X(0,b)$, $X(1,a)=a\equiv X(1,b)$ y

$X(n+2,a)=2aX(n+1,a)-X(n,a)$

$\equiv 2bX(n+1,b)-X(n,b) \bmod c$ (por paso de inducción ya que $a\equiv b \bmod c$)

$=X(n+2,b)$

Llegamos ahora a la investigación de la periodicidad de las propiedades de la sucesión $X(k,a)$ de soluciones de la Ecuación de Pell en a, con idea a la prueba del lema 5, primero se obtiene la fórmula de adición la propiedad de periodicidad:

P1: $X(2n\pm j,a)\equiv -X(j,a) \bmod X(n,a)$ para toda $a>1$ $j,n\in N$

$X(4n\pm j,a)\equiv -X(j,a) \bmod X(n,a)$ para toda $a>1$ $j,n\in N$

Porque

$X(n+(n\pm j),a)$

$=X(n,a)X(n\pm j,a)+(a^2-1)Y(n,a)Y(n\pm j,a)$

$\equiv (a^2-1)Y(n,a)(X(j,a)Y(n,a)\pm X(n,a)Y(j,a)) \bmod X(n,a)$

$\equiv (a^2-1)Y(n,a)^2X(j,a) \bmod X(n,a)$

$=(X(n,a)^2-1)X(j,a)$ como $X(n,a)^2-(a^2-1)Y(n,a)^2=1$

$\equiv -X(j,a) \bmod X(n,a)$

y de esto

$$X(2n+(2n\pm j),a)\equiv -X(2n\pm j,a)\equiv X(j,a) \bmod X(n,a).$$

Con la condición de periodicidad

P2: para toda $a>1$, todo $n>0$ y todo i,j

$X(i,a)\equiv X(j,a) \bmod X(n,a)$ y $0<i\leq n$ y $0\leq j<4n$

implica $j=i$ o $j=4n-i$

se obtiene la

PRUEBA DEL LEMA 5.

Sea $X(i,a)\equiv X(j,a) \bmod X(n,a)$, $0<1\leq n$

y $j=4nq+r$ con $0\leq r<4n$, la aplicación *q-veces* de la condición de periodicidad P1 proporciona

$$X(4nq+r,a)\equiv X(r,a) \bmod X(n,a),$$

y por tanto con la hipótesis $X(i,a)\equiv X(j,a) \bmod X(n,a)$ y $j=4nq+v$ se obtiene la congruencia

$$X(i,a)\equiv X(r,a) \bmod X(n,a)$$

de la cual por la propiedad de periodicidad P2, se deduce: $i=r$ o $i=4n-r$. Entonces

$$i=r \bmod 4n \quad \text{o} \quad -i\equiv r \bmod 4n.$$

Como $j=4nq+r\equiv r \bmod 4n$ tenemos el buscado.

$$i\equiv j \bmod 4n \quad \text{o} \quad -i\equiv j \bmod 4n.$$

Para la prueba de P2 se establece ahora la siguiente afirmación:

P2a: para toda a,n,i,j si

$1<a$ y $0<n$ y $1\leq j\leq 2n$ y $no-(a=2$ y $n=1$ y $i=0$ y $j=2)$

entonces

$i=j$ se deduce de $X(i,a)\equiv X(j,a) \bmod X(n,a)$.

PRUEBA DE P2A. HAY DOS CASOS.

CASO 1. $X(n,a)$ es impar.

Sea $q=(X(n,a)-1)/2$. Se demostrará que los miembros de la sucesión

$$X(0,a),X(1,a),\ldots,X(n-1,a)$$ son primos relativos.

Por la condición de periodicidad P1 los miembros de la sucesión $X(n+1,a),X(n+2,a),\ldots,X(2n-1,a),X(2n,a)$ son congruentes módulo $X(n,a)$ respectivamente a

$$-X(n-1,a),-X(n-2,a),\ldots,-X(1,a),-X(0,a)$$

y por,

$$-q\leq -X(n-1,a)<-X(n-2,a)<\ldots<-X(0,a)<X(0,a)<\ldots<X(n-1,a)\leq q$$

todos estos números $X(i,a),-X(i,a)$ se encuentran en el sistema completo de representantes $-q,-q+1,\ldots,0,..,q$ de clases residuales módulo $X(n,a)$. Por eso $X(0,a),X(1,a),\ldots,X(2n,a)$ son primos relativos módulo $X(n,a)$. Por tanto la hipótesis módulo $X(n,a)$ congruente a los números $X(i,a)$ y $X(j,a)$ tienen indice igual, porque $0\leq i,\ j\leq 2n$. Que $X(0,a),\ldots,X(n-1,a)$ son primos relativos y $X(n-1,a)\leq q$ descansa en lo siguiente: por las fórmulas de suma ($0<n$), cuando $2\leq a$

$$X(n-1,a)\leq X(n-1,a)+(a^2-a)Y(n-1,a)/a$$

$$=X(n,a)/a\leq X(n,a)/2.$$

Entonces $X(n-1,a)\leq (X(n,a)-1)/2=q$, porque debido a la hipótesis $X(n,a)$ es impar. Por tanto la sucesión monótona creciente $X(0,a),X(1,a),\ldots,X(n-1,a)$ se encuentra entre 1 y q y por tanto sus miembros son primos relativos.

CASO 2. $X(n,a)$ es par.

Sea $q=X(n,a)/2$. Como anteriormente $X(n-1,a)\leq q$ porque $-q\equiv q \bmod X(n,a)$, la sucesión

$$-q+1,\ldots,0,\ldots,q-1,q$$

es un sistema completo de representantes de clases residuales módulo $X(n,a)$ y la afirmación se deduce como en el primer caso si

$$no-(X(n-1,a)=q=X(n,a)/2).$$

Pero esto significa que $X(n,a)=2X(n-1,a)$. En consecuencia por las fórmulas de suma ($1<a$),

$$2X(n-1,a)=X(n,a)=aX(n-1,a)+(a^2-1)Y(n-1,a)$$

y por tanto $a=2$ y $Y(n-1,a)=0$. Entonces $n-1=0$ y $i=0$. Debido a que

$$j\leq 2 \text{ y } X(0,a)\equiv X(j,a) \bmod X(n,a)$$

pero

$$X(0,a)=1\neq 2=Y(1,a) \bmod X(1,a) \text{ y } j\neq 2,$$

se tiene $j=0$.

PRUEBA DE P2 USANDO P2A.

CASO 1. $j \leq 2n$.

Como $i \leq n$ entonces

$$no-(a=2,\ n=1,\ i=2) \text{ y } 0<i.$$

La hipótesis de la condición de periodicidad P2A se satisface y de acuerdo a esto se deduce $i=j$.

CASO 2. $2n<j$.

Por la hipótesis $j<4n$ se tiene que $0<4n-j<2n$ y por la condición de periodicidad P1,

$$X(4n-j,a) \equiv X(j,a) \bmod X(n,a).$$

Entonces de la hipótesis $X(j,a) \equiv X(i,a) \bmod X(n,a)$, también

$$X(4n-j,a) \equiv X(i,a) \bmod X(n,a).$$

Como $0<4n-j,i$ la hipótesis de la propiedad de periodicidad P2A se satisface, asi que se deduce que $i=4n-j$.

CAPITULO III
COEFICIENTE BINOMIAL

El coeficiente binomial es una relación diofantina. La idea básica en la prueba es que los coeficientes binomiales son los digitos en base u de la descomposición de $(1+u)^n$, cuando u es suficientemente grande.

Probemos un lema antes que nada.

I) Para $0\leq k,n$ y $u>2^n$, $\begin{bmatrix} n \\ k \end{bmatrix} = res\left(\left[\frac{(u+1)^n}{u^k}\right], u\right)$.

PRUEBA.

Descomponiendo a $(1+u)^n$ por medio del Teorema del Binomio y dividiendo entre u^k, se obtiene

a) $$\frac{(u+1)^n}{u^k} = \sum_{i=k+1}^{n} \begin{bmatrix} n \\ i \end{bmatrix} u^{i-k} + \begin{bmatrix} n \\ k \end{bmatrix} + \sum_{i=0}^{k-1} \begin{bmatrix} n \\ i \end{bmatrix} u^{i-k}.$$

De a) junto con la desigualdad $u^{i-k} \leq \frac{1}{u}$ que es válida para $i\leq k-1$, se deduce:

$$\sum_{i=0}^{k-1} \begin{bmatrix} n \\ i \end{bmatrix} u^{i-k} \leq \sum_{i=0}^{k-1} \begin{bmatrix} n \\ i \end{bmatrix} \frac{1}{u} \leq \frac{1}{u} \sum_{i=0}^{n} \begin{bmatrix} n \\ i \end{bmatrix} = \frac{2^n}{u} < 1.$$

Por tanto $\left[\frac{(u+1)^n}{u^k}\right] \equiv \begin{bmatrix} n \\ k \end{bmatrix} \mod u$ asi que el lema

I) Se deduce de $\begin{bmatrix} n \\ k \end{bmatrix} \leq 2^n < u$.

Por el lema 2, a), 1.7, 1.8, se deduce que el coeficiente

binomial es diofantino. Se tiene que:

$m=\begin{bmatrix} n \\ K \end{bmatrix}$ si y solo si existen u,x,y tales que

$(u+1)^n=yu^{k+1}+mu^k+x$, $2^n<u$, $x<u^k$ y $m<u$

CAPITULO IV

TEOREMA DE LUCAS

Antes de demostrar el Teorema de Lucas se propone una técnica de conteo básica. Como notación en este capítulo se utiliza a X como un conjunto finito, y p un número primo.

Para $A \subseteq X$, con $|A|$ se representa el número de elementos de A.

TEOREMA.

Sea $f: X \to X$ con $f^p = I$ (mapeo idéntico). Sea $X_o = \{x \in X \mid f(x) = x\}$

Entonces $|X| \equiv |X_o| \mod p$.

PRUEBA.

Para toda $x \in X$, definimos la órbita $\overline{x}$ de x como el conjunto $(x, f(x), \ldots, f^{p-1}(x))$.

Claramente si $|\overline{x}| = 1 \iff x = f(x)$, es decir, si $x \in X_o$ ahora si $|\overline{x}| > 1$, entonces $|\overline{x}| = p$. Porque si tuviéramos una duplicación de $\overline{x}$, entonces $f^i(x) = f^j(x)$ para alguna i, j $0 \le i < j < p$, asi que $f^{j-i}(x) = x$. Como $f^p(x) = x$ y $(j-i, p) = 1$, se deduce que $f(x) = x$ y por tanto $|\overline{x}| = 1$.

Finalmente como hay $|X_o|$ órbitas de longitud 1 y las demás órbitas n, tienen longitud p, se tiene $|X| = X_o + np$ esto nos da la buscada congruencia.

APLICACION 1. Teorema de Fermat $n^p \equiv n \mod p$

PRUEBA.

Tomar el conjunto X de puntos $(x_1, \ldots x_p)$ con $1 \le x_i \le n$ y sea $f(x_1, \ldots, x_p) = (x_2, \ldots, x_p, x_1)$. Claramente $f^p = I$ y $|X| = n^p$, $|X_o| = n$ y el Teorema 1 da el resultado buscado.

APLICACION 2. Teorema de Lucas (1875)

Suponga que

$$n=n_o+n_1p+\ldots+n_kp^k;\ r=r_o+r_1p+\ldots+r_kp^k,$$

con $0\le n_i,r_i<p$. Entonces

$$\begin{bmatrix} n \\ r \end{bmatrix} \equiv \begin{bmatrix} n_o \\ r_o \end{bmatrix} \begin{bmatrix} n_1 \\ r_1 \end{bmatrix} \cdots \begin{bmatrix} n_k \\ r_k \end{bmatrix} \mod p.$$

PRUEBA.

Si escribimos $n=Np+n_o$, $r=Rp+r_o$, donde $0\le n_o$, $r_o<p$ es suficiente probar que

$$\begin{bmatrix} n \\ r \end{bmatrix} \equiv \begin{bmatrix} N \\ R \end{bmatrix} \begin{bmatrix} n_o \\ r_o \end{bmatrix} \mod p.$$

DEFINICION.

$A_i=\{(i,1),\ldots,(i,N)\}$ para $i=1,\ldots,p$ y

$B=\{(0,1),\ldots,(0,n_o)\}$. Entonces haciendo

$$A=A_1U\ldots UA_pUB$$

se tiene que $|A|=N_p+n_o=n$. Definase $f:A\to A$ moviendo ciclicamente los A_i's y manteniendo B fijo:

$$f(i,x)=(i+1,x) \qquad 1\le i\le p-1$$

$$f(p,x)=(1,x)$$

$$f(0,x)=(0,x)$$

Entonces

$$f(A_i)=A_{i+1}\ (1\le i\le p-1),\ f(A_p)=A_1,\ f(B)=B.$$

Claramente $f^p=I$.

Se toma a X como la colección de subconjuntos $C\subseteq A$ con $|C|=r$.

Como $f:A\to A$, f actúa naturalmente en subconjuntos de

$A:f(C)=\{f(x)\mid x\in C\}$. Como f es $1-1$ $|f(C)|=|C|$, asi que $f:X\to X$, con $f^p=I$, Claramente

$$|X|=\begin{bmatrix}n\\r\end{bmatrix}$$

Encontremos ahora $|X_o|$, cualquier subconjuntos C de A se puede escribir en forma única como

$$C=C_1U\ldots C_pUC_o$$

donde $C_i\subseteq A_i$, $C_o\subseteq B$, como f manda las A_i, ciclicamente y B se mantiene fijo, se observa que $f(C)=C$ si y solo si

$$Ci=f^{i-1}\ (C1)\quad i=1,..,p.$$

Para $C\in X$, se tiene que $|C|=r$ y si $C\in X_o$ se tiene $|C|=p|C_1|+|C_o|=r=Rp+r_o$. Note que $0\le|C_o|$, $r_o<p$. Entonces la restricción de cardinalidad en C se satisface si y solo si $|C_1|=R$,

$|C_o|=r_o$. Pero hay $\begin{bmatrix}N\\R\end{bmatrix}$ elecciones para C_1 y $\begin{bmatrix}n_o\\r_o\end{bmatrix}$ elecciones independientes para C_o. Entonces

$$|X_o|=\begin{bmatrix}N\\R\end{bmatrix}\ \begin{bmatrix}n_o\\r_o\end{bmatrix}.$$

Se tiene el teorema aplicando el Teorema 1.

CAPITULO V

TEOREMA DE LAGRANGE

El problema diez de Hilbert puede ser formulado en términos de existencia de soluciones en números naturales. Estas dos formas del problema diez de Hilbert son equivalentes. Una ecuación $P(x_1,x_2,..x_n)=0$ tiene solución en enteros si $\Leftrightarrow$ $\pi P(\pm x_1,\pm x_2,...,\pm x_n)=0$ tiene solución en números naturales. En base al Teorema de Lagrange de los cuatro cuadrados (1770) $P(x_1,x_2,..,x_n)=0$ tiene solución en números naturales $\Leftrightarrow$ $P(x_1^2+y_1^2+u_1^2+v_1^2+,x_2^2+y_2^2+u_2^2+v_2^2,...,x_n^2+y_n^2+u_n^2+v_n^2)=0$ tiene solución en enteros.

Antes de demostrar el Teorema de Lagrange (1770) es necesario mostrar un lema y un teorema debido a Euler.

LEMA (Euler 1748).

Para toda $x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4\in Z$ se tiene que:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2$$
$$+(x_1y_2-x_2y_1-x_3y_4+x_4y_3)^2$$
$$+(x_1y_3+x_2y_4-x_3y_1+x_4y_2)^2$$
$$+(x_1y_4-x_2y_3+x_3y_2-x_4y_1)^2$$

TEOREMA (Euler 1751).

Sea p un primo impar, entonces existen enteros x,y además un entero m tales que $0<m<p$ y $mp=x^2+y^2+1$.

PRUEBA.

Sea S el conjunto de todos los cuadrados x^2 donde $0\le x\le(p-1)/2$. Como con x_1^2,x_2^2 en S la congruencia $x_1^2\equiv x_2^2 (mod\ p)$ implica $x_1=x_2$, S contiene $(p-1)/2+1$ enteros

incongruentes módulo p.

En forma similar, el conjunto T de $(p-1)/2+1$ enteros $-1-y^2$, donde $0\leq y\leq (p-1)/2$ está formado por números que son incongruentes por pares módulo p.

Como cada sistema de residuos completo módulo p tiene exactamente p-elementos, deducimos que debe existir x^2 en S y $-1-y^2$ en T tales que $x^2\equiv -1-y^2 \pmod p$. Esto es, $x^2+y^2+1=mp$ para alguna $m\in Z$. Finalmente como $0\leq x,y\leq (p-1)/2$ se tiene

$$0<x^2+y^2+1<(p/2)^2+(p/2)^2+1= p^2/2+1<p^2.$$

Entonces se deduce que $m<p$.

Finalmente trabajemos ahora la prueba del Teorema de Lagrange.

PRUEBA.

Por el lema de Euler (1748) y la igualdad $2=1^2+1^2+0^2+0^2$, se muestra que solamente necesitamos probar el teorema para primos impares. Sea p tal primo. Por el Teorema de Euler (1751) algún múltiplo de p es una suma de tres y por tanto, cuatro cuadrados. Sea kp el mínimo múltiplo de p que se pueda expresar como una suma de cuatro cuadrados. $kp=a^2+b^2+c^2+d^2$. Por el Teorema de Euler (1751) sabemos que $k<p$. Se debiera demostrar ahora que $k=1$, por tanto supongamos que no lo es. Ahora si k es par, entonces de las a,b,c,d:

i(todas son pares) o

ii(todas son impares) o

iii(dos son pares y dos son impares)

En el caso iii supóngase sin perder generalidad que a,b son pares, entonces en todos los tres casos

$$\frac{k}{2}\,p=\left[\frac{a+b}{2}\right]^2+\left[\frac{a-b}{2}\right]^2+\left[\frac{c+d}{2}\right]^2+\left[\frac{c-d}{2}\right]^2$$

contradiciendo asi la elección de k. Por tanto k es impar. No todas las a,b,c,d son divisibles entre k, o de lo contrario $k\mid p$, lo que sería contrario a $1<k<p$. Se encontrarán enteros A,B,C,D que se encuentran entre $-k/2$ y $k/2$ tales que $a\equiv A,\ b\equiv B,\ c\equiv C,\ d\equiv D\ (mod\ k)$. Además al menos una de las A,B,C,D es diferente de cero. Por tanto

$$0<A^2+B^2+C^2+D^2<4(k/2)^2=k^2.$$

Por otro lado si hacemos que $S=A^2+B^2+C^2+D^2$ y $S=a^2+b^2+c^2+d^2$, se tiene que $S\equiv s\equiv 0(mod\ k)$.

Por tanto supongamos que $S=mk$, donde necesariamente $m<k$. Examinando

$$k^2mp=kpmk=sS=X^2+Y^2+Z^2+T^2. \qquad (*)$$

donde X,Y,Z,T corresponden a los cuatro sumandos a la derecha de la igualdad en el lema de Euler (1748). En consecuencia:

$$X=aA+bB+cC+dD\equiv aa+bb+cc+dd\equiv 0\ (mod\ k)$$

$$Y=aB-bA-cD+dC\equiv ab-ba-cd+dc\equiv 0\ (mod\ k)$$

y de la misma forma $Z\equiv T\equiv 0\ (mod\ k)$. En consecuencia $X=kx$, $Y=ky$, $Z=kz$, $T=kt$, *para* $x,y,z,t\in Z$. Pero (*) muestra que $mp=x^2+y^2+z^2+t^2$ contradiciendo asi la elección (mínima) de k, por tanto k debe ser igual a 1 tal como se prueba.

BIBLIOGRAFIA

(1930) D.H. Lehmer

An extended theory of Lucas' functions.

Annals of Math 31 pp 419-448.

(1970) G.V. Chudnovskii

Diophantine predicates.

Uspekhi Matematicheskikh Nauk 25 pp 185-186.

(1976) M. D. Davis, Y. v. Matyasevich, J. Robinson

Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution.

American Mathematical Society, Symposia in Pure Mathematics, 28, pp 323-378.