Álgebra moderna

e introducción al álgebra geométrica

Róbinson Castro Puche

ECOE EDICIONES

ÁLGEBRA MODERNA
e introducción al álgebra geométrica

RÓBINSON CASTRO PUCHE

Catalogación en la publicación – Biblioteca Nacional de Colombia

Castro Puche, Róbinson
Álgebra moderna e introducción al álgebra geométrica / Róbinson Castro Puche – 1ª. ed. – Bogotá : Ecoe Ediciones, 2013
326 p. – (Ciencias exactas. Matemáticas)

ISBN 978-958-648-850-1

1. Aritmética 2. Álgebra 3. Geometría algebraica I. Título II. Serie

CDD: 512 ed. 20 CO-BoBN– a834338

Álgebra moderna
e introducción al álgebra geométrica

Copyright © Róbinson Castro Puche. Es propiedad intelectual del autor. Todos los derechos reservados. Prohibida la reproducción total o parcial, por cualquier medio o con cualquier propósito, sin autorización escrita del autor. Montería – Colombia

robinson_casto_p@hotmail.com

ISBN: 978-958-648-850-1

Primera edición: 2013
Reimpresión: Bogotá, octubre de 2013

Diagramación: En LaTeX realizada por Róbinson Castro Puche
Diseño de Carátula: Wilson Marulanda
Impreso por Multi-impresos SAS

E-mail: correo@ecoeediciones.com
www.ecoeediciones.com
Carrera 19 No 63C-32, Pbx: 2481449, fax. 346 1741
Coordinación editorial: Andrea del Pilar Sierra
Impreso en Colombia
Depósito legal: Hecho.

A Olga, la esposa; Milton, Tania, Jaime y Glenna, los hijos;
Alejandro, Andrea, Paula, Valery, Daniel y Sara, los nietos.

Índice general

EL AUTOR

RÓBINSON CASTRO PUCHE
Licenciado en Matemáticas, Universidad Nacional de Colombia, Bogotá.
Master of Arts Mathematics Education, Ball State University, Muncie, Indiana, USA.
En la Universidad de Córdoba, en Montería, ejerció las funciones de secretario académico de la Facultad de Ciencias, director de la Oficina de Registro y Admisiones, director del Departamento de Matemáticas y profesor titular. También fue rector del Colegio El Carmen de Cotorra, Córdoba y entre diciembre de 1993 y noviembre de 1994, fue docente adscrito a la Universidad Nacional de Colombia.

PRESENTACIÓN

Álgebra moderna e introducción al álgebra geométrica es un texto cuyo objetivo es promover una actitud matemática positiva entre los estudiantes de una asignatura reconocida tradicionalmente como una disciplina abstracta, en la que se estudian entes aparentemente distantes de la realidad concreta y de la experiencia tangible.

¿Qué se persigue con la enseñanza del álgebra moderna en las instituciones de educación superior? Ciertamente no es hacer conocer al futuro matemático una serie de teoremas y ejercicios ingeniosos relacionados con las estructuras algebraicas, sino enseñarle a ordenar el pensamiento con arreglo al método axiomático, para desarrollar el rigor del juicio lógico, indispensable en la labor del matemático.

En ese aspecto, el autor presenta un trabajo prolijo que será de gran ayuda a los estudiantes que se inician en el conocimiento del álgebra moderna. El texto está agradablemente redactado y en algunos aspectos presenta originalidad en la exposición y concatenación lógica de los temas, cosa difícil de lograr con un material que hoy es completamente estándar. De acuerdo con mi criterio, esto último representa un aspecto muy valioso del libro.

Conociendo las cualidades pedagógicas del profesor Róbinson Castro, veo en la presente obra la continuación de su convicción de poner en práctica las teorías de la enseñanza de las matemáticas desarrolladas por Piaget; por esta razón puedo afirmar que estamos, sin duda, frente a un material valioso para los interesados en conocer de cerca los fundamentos del álgebra moderna.

RAFAEL OBREGÓN, Msc.
Los Ángeles, California, USA. enero de 2013.

PREFACIO

Si nos ubicamos en la posición del maestro, de enseñar la teoría o en la del epistemólogo, que tiene que ver con la naturaleza de los entes matemáticos; el problema consiste en saber si las conexiones matemáticas son engendradas por la inteligencia o si esta las descubre como una relidad exterior.

Jean Piaget en su disertación, con motivo del Coloquio de la Rochette de Melun en 1952, refiriéndose a las estructuras matemáticas; expresó: *Un grupo es un sistema operatorio; la cuestión estriba en saber si los elementos de diversa naturaleza a los que se aplica la estructura existen previamente a esta, o si, por el contrario, es la acción de la estructura la que confiere a los elementos sus propiedades esenciales. El problema sicológico consiste en establecer si los entes que sirven de elementos a las estructuras son el resultado de las operaciones que los engendran o si preexisten a aquellas operaciones que se aplican a ellos.*

Para dar respuesta al dilema, continuó diciendo: *En vez de definir los elementos aisladamente por convenio, la definición estructural consiste en carcterizarlos por las relaciones operatorias que mantienen entre sí, en función del sistema. Y la definición estructural de un elemento hará las veces de demostración de la necesidad de este elemento, en cuanto está concebido como perteneciente a un sistema cuyas partes son interdependientes.*

Teniendo en cuenta el criterio de Piaget, el objetivo principal de este trabajo es poner a la consideración de la comunidad matemática un texto que proporcione a los estudiantes las bases teóricas del álgebra moderna que les permita abordar con éxito una disciplina con un alto grado de abstracción. Dominar las ideas expuestas en el texto constituye un paso fundamental para el estudio de teorías más avanzadas relacionadas con el desarrollo axiomático de las matemáticas.

En concordancia con lo anterior, el texto está diseñado para usarlo como guia para un primer curso de álgebra moderna. Se encuentra dividido

en seis capítulos. En el primero se estudian los aspectos más relevantes de la aritmética elemental, comenzando con la caracterización de los números naturales tomando como fundamento los postulados de Peano. A partir del concepto de divisibilidad se estudian las congruencias, concluyendo con una presentación suscinta de los sistemas de numerción de base diferente a la decimal.

Los capítulos segundo y tercero están dedicados al desarrollo de los grupos. El material consignado es el que tradicionalmente se estudia, pero he considerado que desde el punto de vista didáctico los subgrupos normales se introduzcan a través de los automorfismos internos.

Los capítulos cuarto y quinto están dedicados a los anillos. El cuarto se inicia con una descripción detallado de los enteros módulo n, se extiende el estudio de la divisibilidad a los anillos en general y se desarrolla la teoría correspondiente a las estructuras algebraicas hasta la noción de campo. El quinto correponde al anillo de los polinomios.

El álgebra geométrica es un tópico que en la actualidad no cuenta con una amplia difusión como herramienta matemática aplicada a la solución de algunos problemas de la ingeniería; donde el análisis vectorial estándar, en dos y tres dimensiones, y el álgebra matricial son las ayudas ampliamente usadas. Pero lo cierto es que cada día aumenta el número de investigadores convencidos de la utilidad de esta rama descubierta por Günther Grassmann.

Presentar las bases mínimas de esta teoría, tiene como propósito invitar a los interesados a profundizar en su estudio e investigar acerca de la importancia de esta herrmienta en la reformulación de algunos conceptos de la física.

El autor.
Montería, enero de 2013.

ÁLGEBRA MODERNA
e introducción al álgebra geométrica

Capítulo 1

TEORÍA DE LA ARITMÉTICA

Introducción

El punto de partida es aceptar que los enteros y sus operaciones aritméticas han sido objeto de análisis. El interés primario será estudiar los fundamentos de la aritmética elemental. Se supone conocido el desarrollo axiomático de los naturales propuesto por G. Peano en 1889 que permite concebirlos como la colección $\{0, 1, 2, \ldots, n, \ldots\}$ y una operación unaria, la función siguiente o sucesor que verifica los postulados de Peano:

1. Cero es un número.
2. El sucesor de un número es único.
3. Cero no es el sucesor de ningún número.
4. Si $Sig(n) = Sig(m)$, entonces $n = m$.
5. El principio de inducción completa: Dado un conjunto M de números naturales con las dos propiedades siguientes:

   a) Cero pertenece a M.

   b) Si n pertenece a M implica que $Sig(n)$ también pertenece a M;

   entonces M contiene a todos los números naturales.

Partiendo de estos fundamentos se define la adición mediante las fórmulas:

$$Sig(n) = n + 1$$
$$Sig[Sig(n)] = n + 2$$

y así sucesivamente,

$$n + Sig(m) = Sig(n + m)$$

llamadas fórmulas de recurrencia.

La multiplicación se expresa en términos de la adición por:

$$nm = \underbrace{m + m + \cdots + m}_{n \text{ veces}}$$

indicando que el número m se ha sumado n veces.

Los enteros serán el resultado de reunir los naturales con sus respectivos inversos aditivos, o sea:

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Más tarde se estudiarán como ejemplos de sistemas numéricos específicos objeto del álgebra moderna.

La representación polinómica de los enteros será igualmente asumida, dándose por cierto que para todo entero $t > 1$, cada uno de los enteros $a > 0$ puede representarse en forma única como

$$a = c_0 + c_1 t + \cdots + c_{n-1} t^{n-1} + c_n t^n = \sum_{i=0}^{n} c_i t^i$$

donde c_n es positivo y $0 \leq c_i < t$, para $0 \leq i \leq n$. Esta proposición garantiza que cada entero mayor que 1 puede servir como base para un sistema de numeración.

Las precisiones expuestas servirán para movernos con libertad suficiente en el desarrollo de algunos tópicos cuya construcción está por fuera de los objetivos planteados.

Construir triángulos rectángulos con lados enteros fue objeto de investigación por parte de los babilonios 1600 años antes de Cristo. No solamente le dieron solución a este problema sino que lo aplicaron a la trigonometría

construyendo tablas. Euclides en el décimo libro de los Elementos escribió un análisis detallado al plantear la solución en los enteros de la ecuación:

$$x^2 + y^2 = z^2$$

conocida como ecuación pitagórica, debido a la creencia que fue Pitágoras quien la planteó por primera vez en el año 550 antes de Cristo. Las soluciones más simples están conformadas por $3, 4, 5$ y $5, 12, 13$ y múltiplos de estos, por ejemplo $6, 8, 10$ que es el doble de la primera y $25, 60, 65$ que es cinco veces la segunda. Tal vez se piense que no haya otras, pero efectivamente las hay. En los triángulos de lados $3, 4, 5$ y $5, 12, 13$ la hipotenusa es una unidad mayor que uno de los catetos. Si a y b son los catetos y la hipotenusa es $b + 1$, de acuerdo con el teorema de Pitágoras

$$a^2 + b^2 = (b + 1)^2.$$

Realizando las operaciones pertinentes se llega a la igualdad

$$a^2 = 2b + 1$$

de donde se concluye que a^2 es impar y por lo tanto a también lo es. Tomando

$$a = 2n + 1,$$

reemplazando en la igualdad anterior se observa que

$$b = 2n^2 + 2n$$

lo que lleva a deducir que $(2n+1)$, $(2n^2+2n)$, $(2n^2+2n+1)$ son los lados de un triángulo rectángulo, donde la última expresión corresponde a la hipotenusa. Pero los anteriores distan de ser todos, estos se encuentran a través de la solución de la ecuación

$$x^2 + y^2 = z^2$$

ecuación que tiene infinitas soluciones si x, y, z son primos relativos; y es par positivo; x, z ambos impares positivos. Las soluciones vienen dadas por

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2$$

donde u, v son enteros que satisfacen las condiciones $u > v > 0$, son primos relativos y uno de los dos es par. Si $u = 2$, $v = 1$ se tiene la solución $3, 4, 5$. Si $u = 3$, $v = 2$, la solución es $5, 12, 13$.

La mejor contribución de Euclides a la aritmética fue el desarrollo de las demostraciones del algoritmo euclidiano, la existencia de un número infinito de primos y el teorema fundamental de la aritmética que establece que todo entero distinto de cero se puede expresar como el producto de un número finito de factores primos, conceptos que tienen su fundamento en la relación de divisibilidad.

Fermat estudió la ecuación

$$x^n + y^n = z^n$$

para enteros $n \geq 3$. Afirmó tener una solución asegurando que, excepto para el caso en que $n = 2$, no había solución diferente a $0, 0, 0$. Desafortunadamente no la dio a conocer siendo este uno de los tres problemas insolubles más famosos. Este hecho se nombra en la historia como el último teorema de Fermat o el teorema grande de Fermat, en contraposición al conocido como el teorema menor de Fermat, cuyo enunciado establece que si p es primo, entonces para todo a,

$$a^p \equiv a \bmod p.$$

Y si p no divide a a,

$$a^p - 1 \equiv 1 \bmod p.$$

Lo de menor tal vez fue para resaltar la importancia del primero. Un caso especial del teorema menor de Fermat establece que si p es primo, entonces

$$p|(2^p - 2).$$

Los chinos creyeron por mucho tiempo que el recíproco también era cierto y lo verificaron hasta 300. Consideraron durante más de 23 siglos que era una regla infalible para decidir primalidad, pero falla para $341 = 11 \times 31$.

Debido a que $2^{341} - 2$ consta de 103 cifras comprobarlo se pospone hasta cuando haya la teoría suficiente.

1.1. Divisibilidad

Definición 1.1.1. *Considérense los enteros a, b con $a \neq 0$. Si existe un entero c tal que $b = ac$, se dice que a divide a b y se escribe $a|b$. Si a no divide a b, se escribe $a \nmid b$.*

Como $8 = 2 \times 3 + 2$, se deduce que $3 \nmid 8$. Otros ejemplos son:

$$5|15,\ 1|4,\ (-2)|6,\ 2|(-8),\ 5 \nmid 14.$$

La relación de divisibilidad no es una equivalencia debido a que no es simétrica, por ejemplo $3|6$, pero $6 \nmid 3$.

Es fácil verificar que es reflexiva y transitiva.

Para todo entero a diferente de cero, existe el entero 1, tal que $a = a \times 1$ y de acuerdo con la definición $a|a$ indicando que es reflexiva.

Sean a, b, c tres enteros donde a y b son ambos diferentes de cero tales que $a|b$ y $b|c$ entonces existen enteros d, e que satisfacen las igualdades

$$b = ad, \qquad c = be.$$

Si el valor de b en la primera igualdad lo reemplazamos en la segunda se obtiene

$$c = (ad)e = a(de)$$

y como de es un entero se concluye que $a|c$, infiriéndose que es una relación transitiva.

Las siguientes proposiciones son otras propiedades de la divisibilidad que se pueden deducir usando la definición. Como es tradicional las letras se usarán para representar enteros. Para evitar confusiones las cifras enteras se escriben sin usar los puntos correspondientes a la escritura formal. El punto y el signo $\times$ se usan para expresar producto, por ejemplo, $23 \cdot 45$ y 23×45 significan «23 por 45», mientras que 2345 debe leerse «dos mil trescientos cuarenta y cinco».

1. Si $a|b$ y $b|a$, entonces $a = b$ o $a = -b$.

2. Si $a|b$ y $a|c$, entonces $a|(bx \pm cy)$ para toda pareja x, y. En particular $a|(b \pm c)$. Si $a|b$, entonces $a|bx$, para todo x.

3. Si $a|b$ y $b > 0$, entonces $a \leq b$.

4. Para todo $a \neq 0$ y para todo b, $a|0$ y $\pm 1|b$.

5. Sean a, b, k con $a \neq 0$, $k \neq 0$, entonces $a|b$ si y solo si $ak|bk$.

6. Si $a|b$ y $b \neq 0$, entonces $|\,a\,| \leq |\,b\,|$.

Note que el orden en que aparecen las anteriores proposiciones no es importante, por ejemplo la proposición (3) se puede considerar como una consecuencia de (6) pero es posible hacer una demostración directa de (3) sin usar (6).

Definición 1.1.2. *Dos enteros a, b ambos diferentes de cero tales que $a|b$ y $b|a$ se dice que son asociados.*

De acuerdo con (1) los únicos asociados de un entero a son a y $-a$.

Para demostrar la propiedad (1) se deben tomar dos asociados y concluir que son iguales o que solo difieren en el signo. Para el efecto tómense los asociados a, b. Por definición existen c y d tales que

$$b = ac, \qquad a = bd.$$

Si el valor de a, en la igualdad de la derecha, lo reemplazamos en la de la izquierda se obtiene

$$b = (bd)c = b(dc)$$

y de esta última se deduce que $dc = 1$, pero debido a que d y c son enteros, únicamente se pueden tener dos posibilidades, $d = c = 1$ o $d = c = -1$. Si ocurre la primera posibilidad, reemplazando a c se concluye de la primera igualdad que $b = a$. Si ocurre la segunda se obtiene $b = -a$.

Para demostrar la propiedad (2) se supone que $a|b$ y $a|c$, luego existen enteros m, n tales que

$$b = am$$

$$c = an.$$

Multiplicando ambos miembros de la primera igualdad por x y los de la segunda por y, sumando miembro a miembro y factorizando a, se tiene

$$bx + cy = a(mx + ny).$$

Por la selección de m, x, n, y, $(mx+ny)$ es un entero, t lo que permite concluir que

$$bx + cy = at$$

de donde se puede afirmar que $a|(bx + cy)$. Haciendo $x = y = 1$, obtenemos $a|(b + c)$. Si reemplazamos a x por 1, a y por -1 entonces $a|(b - c)$. Si se iguala c con cero se concluye que $a|bx$.

Hay dos hechos importantes de la aritmética que usaremos a lo largo del texto. El primero afirma que cualquier conjunto de enteros positivos que contenga al menos un elemento contiene un elemento mínimo, y es conocido como el principio de la buena ordenación. El segundo es una consecuencia del primero y se ha mencionado con anterioridad, es el algoritmo de Euclides o algoritmo de la división. Se denomina algoritmo porque proporciona un método mediante el cual se pueden hallar cocientes y residuos al momento de dividir.

Definición 1.1.3. *Un entero p es primo si siendo distinto de cero y de ± 1 es divisible solamente por ± 1 y $\pm p$.*

Definición 1.1.4. *Un natural $n \neq 1$ se dice compuesto si no es primo, esto es, si existen naturales d_1 y d_2 tales que $1 < d_1 < n$, $1 < d_2 < n$ con $n = d_1 d_2$.*

Teorema 1.1.1 (El algoritmo de la división). *Si a es un número natural y b es un entero, existen enteros únicos q, r tales que $b = aq + r$, con $0 \leq r < a$.*

Demostración. De la igualdad $b = at + r$, se obtiene $r = b - at$. Tómese el conjunto

$$S = \{b - at,\ t \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Consideremos $b \geq 0$, como t recorre el conjunto de los enteros, sea $t = 0$. En este caso $b - at \geq 0$.

Supongamos que $b < 0$ por idéntica razón hagamos $t = b$. En dicho caso,

$$b - at = b - ab = b(1 - a).$$

Pero, $1 \leq a$ entonces, $b(1-a) \geq 0$ es decir, $b - at \geq 0$, lo que permite afirmar que el conjunto S posee elementos no negativos. Sea $D \subseteq S$ formado por los elementos no negativos de S. Por el principio de la buena ordenación, D tiene un elemento mínimo. Tomando r como este número y a q como el mayor entero que satisface la condición $b - aq \geq 0$, se deduce que, $r = b - aq \geq 0$. Restando a a ambos miembros y factorizando,

$$r - a = b - aq - a = b - a(q + 1).$$

Pero, $q + 1 > q$ y por la selección de q debe tenerse que

$$b - a(q + 1) < 0$$

o sea,

$$r - a < 0$$

de donde se concluye que $r < a$ lo que permite escribir

$$0 \leq r < a.$$

Para demostrar la unicidad supongamos que q y r no son únicos. Sean q_1 y r_1 enteros tales que $b = aq_1 + r_1$, con $0 \leq r_1 < a$. Por la propiedad transitiva de la igualdad,

$$aq_1 + r_1 = aq + r.$$

Supongamos que $r > r_1$, entonces $r - r_1 > 0$. Trasponiendo términos y factorizando,

$$0 < r - r_1 = a(q_1 - q)$$

de donde se tiene que $a|(r - r_1)$.

Pero $0 \leq r_1 < a$, implica que $-a < -r_1 \leq 0$ y como $0 \leq r < a$ se pueden sumar miembro a miembro estas desigualdades dando como resultado

$$-a < (r - r_1) < a$$

o sea,

$$(r - r_1) < a.$$

De acuerdo con la propiedad (3) de divisibilidad, como $a|(r - r_1)$, necesariamente $a < (r - r_1)$; lo cual es una contradicción. Por lo tanto, r no es mayor que r_1. Suponer que r_1 es mayor que r conduce a una contradicción similar, de donde se deduce que r_1 no es mayor que r, quedando como única posibilidad, $r = r_1$.

De la expresión $r - r_1 = a(q_1 - q)$ observamos que $0 = a(q_1 - q)$ y como a es diferente de cero se concluye que $(q_1 - q) = 0$ y por lo tanto, $q = q_1$. En síntesis la unicidad del cociente y el residuo quedan demostradas. □

El quinto axioma de Peano es el principio de inducción, este enunciado establece que dada una proposición $P(n)$. Si $P(0)$ es verdadera y para cualquier k, la veracidad de $P(k)$ implica la de $P(k + 1)$, entonces $P(n)$ es verdadera para todo natural n. De este principio se conocen cinco formas, la tercera tiene relación con el buen orden y es la clave para demostrar que todo subconjunto S de los naturales que contenga a *cero* y contenga a $n + 1$, siempre que contenga a n, contiene también a todos los naturales. La quinta forma nos permite realizar inducción a partir de un determinado natural k.

Para ilustrar el método de inducción matemática realizamos el siguiente ejercicio.

Ejemplo 1.1.1. *Para todo natural s,* $11|(10^{2s+1}+1)$.

Demostración. Por inducción.

$$\begin{aligned} 10^{2+1}+1 &= 10^3+1 \\ &= 1001 \\ &= 11\times 91. \end{aligned}$$

De las igualdades se ve que la proposición es válida para $s=1$.

Supongamos que es válida para s, esto es,

$$10^{2s+1}+1 = 11k.$$

Multiplicando ambos miembros de esta igualdad por 100,

$$10^{2s+3}+100 = 100\times 11k.$$

Descomponiendo y factorizando el exponente y transponiendo términos,

$$10^{2(s+1)+1} = 100\times 11k - 100.$$

Sumando 1 a ambos miembros,

$$\begin{aligned} 10^{2(s+1)+1}+1 &= 100\times 11k - 99 \\ &= 100\times 11k - 11\times 9 \\ &= 11(100k-9). \end{aligned}$$

Lo anterior permite inferir que la proposición es válida para $s+1$, luego debe serlo también para todo natural. □

Con respecto a los primos surgen algunas inquietudes referentes a su número, a la existencia de una regla para calcular su secuencia, fórmulas para determinarlos y muchos otros interrogantes estudiados por los matemáticos de todos los tiempos entre los que se pueden mencionar, Euclides, Fermat, Euler, Pòlya. En 1914 D. N. Lehmer calculó la lista de los primos desde el primero hasta el que ocupa el 664999-ésimo lugar, este último resultó ser 10006721.

El siguiente enunciado sirve para establecer primalidad en un solo sentido

Ejemplo 1.1.2. *Si $2^n - 1$ es primo, entonces n es primo, para $n \geq 2$.*

Solución. Para demostrarlo supongamos que n es compuesto, es decir, existen naturales a, b tales que, $1 < a < n$, $1 < b < n$, con $n = ab$, entonces

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1 \\ &= c^b - 1 \\ &= (c-1)(c^{b-1} + c^{b-2} + \cdots + c + 1) \end{aligned}$$

donde $c \geq 4$. En consecuencia, $2^n - 1$ es el producto de un entero mayor o igual a 3, por un entero mayor o igual a 5, contradiciendo la hipótesis, luego la proposición se sigue. □

El recíproco no es cierto, ya que para 11, $2^{11} - 1 = 2047$ que es compuesto.

Ejemplo 1.1.3. *La suma de los cuadrados de dos números impares no puede ser un cuadrado perfecto*

Solución. Para un entero cualquiera k, los posibles residuos al dividir por 4 son $0, 1, 2, 3$, lo que significa que k es de una de las formas $4t$, $4t+1$, $4t+2$, $4t+3$, y por consiguiente k^2 se puede escribir como $16t^2$, $4(4t^2+2t)+1$, $4(4t^2+4t+1)$, $4(4t^2+6t+2)+1$. Por lo visto el residuo de dividir k^2 por 4 es 0 o 1.

Tomemos los impares $x = 2n+1$, $y = 2m+1$, elevándolos al cuadrado y sumando

$$\begin{aligned} x^2 + y^2 &= (4n^2 + 4n + 1) + (4m^2 + 4m + 1) \\ &= 4(n^2 + m^2 + n + m) + 2 \end{aligned}$$

lo que lleva a concluir que al dividir $x^2 + y^2$ por 4 el residuo es 2. En mejores palabras $x^2 + y^2$ no es un cuadrado perfecto. □

Teorema 1.1.2. *El menor divisor positivo mayor que 1, de un entero $n > 1$ es un primo.*

Demostración. Sea $n \in \mathbb{N} - \{1\}$, $m > 1$ el menor divisor positivo de n. Por definición $m|n$. Si n es primo, $n = m$ luego m es primo.
Sea n compuesto y suponga que m no es primo. Como $m > 1$, debe ser compuesto, esto es, existe un natural d tal que $1 < d < m$ y $d|m$, pero por hipótesis $m|n$. Por la propiedad transitiva de la divisibilidad, $d|n$ contradiciendo la minimalidad de m. Por consiguiente m debe ser primo. □

Teorema 1.1.3. *Todo compuesto es el producto de un número finito de factores primos.*

Demostración. Supongamos que existen compuestos que son el producto de un infinito número de factores primos. Por el principio de la buena ordenación existe m el menor compuesto que puede expresarse como un número infinito de factores primos. Por el teorema 1.1.2, existe un primo p, $1 < p < m$ además $p|m$, entonces

$$\frac{1}{p} < 1 < \frac{m}{p}.$$

Multiplicando por m la primera desigualdad tenemos, $\frac{m}{p} < m$, luego

$$1 < \frac{m}{p} < m.$$

Como $\frac{m}{p}$ es un natural, entonces

$$\frac{m}{p} = p_1 p_2 \cdots p_r$$

con p_i un primo, para $1 \leq i \leq r$, r es un número fijo. Dicho en otras palabras $\frac{m}{p}$ debe ser el producto de un número finito de factores primos ya que es menor que m y como es sabido, m es el menor compuesto que puede escribirse como el producto de un infinito número de factores primos. Pero,

$$m = p(\frac{m}{p}) = p(p_1 p_2 \cdots p_r)$$

indicando que m es el producto de un número finito de factores primos, contradiciendo el supuesto. En conclusión, todo compuesto es el producto de un número finito de factores primos. □

Teorema 1.1.4 (Teorema fundamental de la aritmética). *Todo entero distinto de cero puede expresarse como el producto de* (± 1) *por un número finito de factores primos. Esta expresión es única salvo el orden en que los factores se consideren.*

Demostración. Si n es primo el teorema es inmediato. Si es compuesto basta aplicar el teorema 1.1.3 teniendo en cuenta el signo y asunto concluido.

Unicidad. Dado $n > 1$ suponga que se puede escribir en dos formas diferentes como producto de primos

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$