--- Página 1 ---  
  
. TEMAS DE MATEMATICAS ELEMENTALES (1)  
  
v  
  
Saulo Rada Aranda  
  
CENAMEC  
  
CENTRO NACIONAL PARA EL MEJORAMIENTO DE LA ENSEÑANZA DE LA CIENCIA  
" CARACAS/VENEZUELA '  
1992  
  
Scanned by CamScanner  
  
N á  
  
  
--- Página 2 ---  
  
Comité Ejecutivo del CENAMEC  
  
Dr. Enrique Planchart  
  
Dr. Rubén Caro  
  
Dra. Maritza Dorta  
  
Dra. Isbelia Martín  
  
Dra. María de Lourdes Vargas  
Prof. Mercedes Urbaneja  
  
Dr. Hugo Groening --  
  
Dr. Claudio Bifano  
  
Personal Directivo  
  
Director: Dr. Enrique Planchart \_  
qudírectora: Prof. Dalia Diez de Tancredi  
  
—  
  
Ediciones CENAMEC. 1995 -  
ISBN: 980-218-039-4 —  
ISNN: 0798-3247 .  
  
12 Edición a cargo de Ligia de Lima de Bianchi  
  
Portada: Felix Nakamura  
  
Impreso en Venezuela por: Gráficas Colson, C.A. Av Panteón l  
Armadas, San Miguel a San Narciso, Sótano Edificio Tamara, C$f¿?%5?.e?ás— 1838  
  
CENAMEC/Sede Central: Edif. Sociedad Venezolana de Ciencias Naturales, Av. Arichuna  
  
c/Calle Cumaco, El Marqués, Caracas [070- . \_  
228779 - 225246 - 227819 - Fax (02) 22507:¿5/.Vem.=,zuela. Tlefs: 219133 - 222467 - 229511  
  
Scanned by CamScanner  
  
  
--- Página 3 ---  
  
CONTENIDO  
  
p.p.  
INTRODUCCION . ... .. 1i  
SECCIONES  
1. EL PRINCIPIO DE INDUCCION MATEMATICA . .. ... 1  
2. EL ALGORITMO DE LA DIVISION . . ., a a a . « B  
3. EL MAXIMO COMUN DIVISOR . . ... .,, 11  
4. LA ECUACION ax + by =c . ..... .., a. s ed7  
5. EL MINIMO COMUN MULTIPLO -............—...21  
6. NUMEROS PRIMOS . .. ... . ... aa .. 23  
7. LA FUNCION PARTE ENTERA . . ... . .. .....929  
S. CONGRUENCIAS ENZ .. a \_34  
9. LA ECUACION x?+y?=2? . a ... 42  
10. LAS CONGRUENCIAS DE EULER, FERMAT Y WILSON .45  
11. RESOLUCION DE CONGRUENCIAS .. . ..... . . Ol  
12. EL INDICADOR DE EULER ... ' . . 56  
SOLUCIONES A LOS PROBI.EMAS PROPUESTOS  
Sección 1 ... . ... . ... E eeago. re aa ea 61  
Sección 2 . .aa a 67  
Sección 3 . . ... ... aaa FE 73  
Sección 4 . . .. N 76  
Sección 3 . . . .a 84  
Sección 6 .. . aaa 85  
Sección T .. aa 94  
Sección 8 . ... ... 101  
Sección 9 .. .. .. 107 -  
Sección 10 . . . .. 112  
Sección 11 . . . . 118  
Sección 12 . . . . .aa 121  
  
Scanned by CamScanner  
  
  
--- Página 4 ---  
  
Ía de números, en las cuales participaron estudiantes del  
Ciclo Diversificado y último año de Educación Básica con un rendimiento destacado en  
la matemática escolar, muchos de ellos ganadores de las Olimpíadas Matemáticas Vene-  
zolanas. . -  
Las sesiones formaron parte del programa de entrenamiento que debían cumplir dichos  
Jóvenes antes de someterse a las pruebas de selección para conformar el equipo que re-  
  
realizó en Córdoba, Argentina, en el mes de septiembre de 1991,  
  
En este tipo de competencias internacionales se plantean problemas enmarcados en un  
temario que, en la mayoría de los países, forman parte de la matemática preuniversitaria.  
Sin embargo, generalmente los problemas exigen considerable ingenio, creatividad y mucha  
soltura en el empleo de técnicas matemáticas básicas. \_ . o  
  
Dado que la educación matemática que reciben los jóvenes en nuestro país (y en mu--  
chos otros) en los niveles básicos está lejos de proporcionar tales habilidades, es necesario  
  
El programa de entrenamiento comprende temas como f1¿ncíones, desigualdades, teoría  
de ecuáciones, combinatoria, teoría de números y geometría. Es de hacer notar que los- .  
dos últimos señalados son casi totalmente ignorados en nuestros programas escolares pese  
al extraordinario valor formativo que tienen por cuanto permiten plantear problemas con  
Muy diversos niveles de complejidad a partir de pocos conocimientos previos, se encuentran  
en muchas situaciones vinculadas a la vida cotidiana (tangibles y familiares) y apelan a  
la curiosidad natural del joven. En estos temas, el entrenamiento prácticamente comieriza  
desde cero. " T  
  
La experiencia de los profesores que han participado en las sesiones de entrenamiento  
en resolución de problemas con estos estudiantes ha resultado verdaderamente gratificante.  
Es sorprendente ver el entusiasmo con que los jóvenes ejercitan la imaginación y se dedican  
al trabajo creativo.  
  
Obviamente, el CENAMEC tiene limitaciones para extender estas experiencias a nivel  
masivo en forma directa, por lo cual se ha propuesto publicar diversas monografías sobre  
temas complementarios de matemática escolar que, a la vez de proporcionar a los docentes  
materiales apropiados para la experimentación, sean útiles para los estudiantes atraídos  
Por el estudio de esta ciencia.  
  
En particular, el presente trabajo contiene los conocimientos básicos que debe poseer  
el estudiante que aspire a abordar los problemas que, sobre teoría de núrmeros, se pueden  
Proponer en competencias matemáticas internacionales. Al final de las diferentes secciones  
se plantean conjuntos de problemas, los cuales constituyen la parte más importante del  
entrenamiento. Algunos son bastante sencillos, aplicaciones más o menos rutinarias de la  
teoría, pero la mayoría se han tomado de olimpíadas matemáticas realizadas en diversos  
Países así como de competencias iberoamericanas e internacionales, y es posible que el  
  
ii  
  
Scanned by CamScanner  
  
  
--- Página 5 ---  
  
- s —  
  
.\_——v.uv'¡c:º£:\_—%&ws'ww,¿y…n ENEO Nn o  
  
lector se desconcierte un poco cuando se enfrente por primera vez con alguno de los enun-  
ciados. Aún cuando en la segunda parte del trabajo se presentan los problemas resueltos,  
la recomendación es no acudir a las soluciones sino como última instancia. No se debe  
olvidar que cuando se intenta resolver un problema, el esfuerzo realizado deja huellas sub-  
conscientes útiles para la formación del estudiante, aún cuando no se llegue a una solución  
  
completa.  
  
Saulo Rada Aranda  
  
Caracas, Noviembre de 1991.  
  
Scanned by CamScanner  
  
  
--- Página 6 ---  
  
SECCION 1  
  
EL PRINCIPIO DE INDUCCION MATEMATICA -\*  
  
Las reglas aritméticas de los números enteros:  
  
(....—8,-2,—1,0,1,2,3,,..)  
  
(al menos de los enteros positivos, también llamados números naturales) están entre los  
logros más antiguos e importantes de la civilización. Hace más de 5000 años los chinos  
y los egipcios usaban la aritmética en su vida cotidiana; no obstante, fueron los griegos,  
principalmente los pitagóricos, quienes dieron inicio formal al estudio de la aritmética  
superior o teoría de números como la conocemos actualmente.  
  
Álgunos ejemplos de problemas planteados y resueltos por los griegos son los siguientes:  
  
\* Demostrar que /2 no es un número racional (es decir, no puede expresarse como el  
. a |  
cociente de dos números enteros -b-)  
  
Esto equivale a demostrar que no existen enteros a, b, donde b £ 0, tales que a?—2b =  
  
o Hallar todos los triángulos rectángulos tales que las medidas de sus lados son números  
enteros. — -  
  
Si las medidas de los catetos de un triángulo rectángulo son a, b y la medida de la  
hipotenusa es c, de acuerdo con el teorema de Pitágoras se tiene:  
  
ard=c?,  
El problema consiste en hallar todas las ternas (a,b,c) de números enteros que\_'é\_á't'is— -  
facen esta ecuación. Tales ternas, por ejemplo (3,4,5), (5,12,13), ... se denominan triples  
pitagóricos.  
  
e Si a, b, c son tres enteros dados, hallar todos los enteros 7, y tales que az + by =0.  
  
Los tres problemas anteriores conducen a casos de las denominadas ecuaciones diofán—  
ticas, llamadas así en honor al matemático griego Diofanto, de Alejandría. En general, una  
ecuación diofántica es una ecuación con cualquier número de incógnitas en la cual se deben  
determinar sus soluciones enteras, .  
  
Quien se inicia en el estudio de la teoría de números debe tener presente que, para  
la mayoría de los problemas que se presentan, no existen métodos generales de resolución.  
Asimismo, debe estar consciente de la dificultad considerable de muchos de estos problemas,  
los cuales, a veces, tienen una apariencia bastante sencilla pero requieren una buena dosis  
de ingenio para abordarlos satisfactoriamente.  
  
A continuación damos dos ejemplos de famosos problemas que, hasta ahora, no han  
sido resueltos:  
  
Scanned by CamScanner  
  
  
--- Página 7 ---  
  
e La conjetura de Goldbach (ruso); establece que todo número par mayor que 2 puede  
escribirse como la suma de dos números primos. (Un entero positivo p, mayor que 1, es  
primo si no tiene divisores positivos diferentes de 1 y de p).  
  
— En efecto, si consideramos los primeros números pares mayores que 2 observamos que:  
  
4=2+2;6=3+3;8=3+5:10=34+7=5+5;  
12=5+7;14=3+11=7+7:16=3+13=5+11;  
18=5+13=7+11;20=3+17=7+193;  
22=3+19=5+17=9+13=11+115etc.  
  
— “Así pues, parece que la conjetura fuera cierta, pero aún no se ha encontrado una de-  
mostración general, así como tampoco un caso en el cual no se cumpla. '  
  
Es preciso aclarar que si se quiere probar que una proposición es verdadera, la prueba  
tiene que ser general, es decir, abarcar todos los casos posibles. Ahora bien, si se quiere  
probar que la proposición es falsa, basta hallar un caso particular en el cual no se cumpla.  
Esto es lo que se llama un contraejemplo. Si quisiéramos demostrar que la conjetura de  
Goldbach es falsa deberíamos buscar un número entero par, mayor que 2, que no se pueda  
expresar como la suma de dos números primos. |  
  
\* La ecuación pitagórica generalizada:  
  
TIT+y"=z", —  
donde n > 3, no tiene soluciones en enteros r, y, z (salvo el caso trivial en que alguno de”  
estos sea igual a cero). - \_  
  
Este problema, planteado por Fermat (francés) hace más de 300 años se conoce como  
el “Ultimo Teorema de Fermat" y ha desafiado el talento de numerosos matemáticos desde  
entonces; se ha podido demostrar para muchos valores particulares de n, pero no se ha  
encontrado una prueba g-:ieral. Lr llamativo e:: que Fern:ai afirmó I:ber demostrado el  
teorema, pero nunca publicó tal den-»stración. Aciialmente. la mayoría de los matemáticos  
piensa que la prueba de Fermat tenía algún error. En todo caso, el problema continúa  
vigente.  
  
Al iniciar nuestro estudio de la teoría de números, convendremos en usar (salvo que  
se exprese lo contrario) a las letras del alfabeto latino: a, b,c, d, ... para designar números  
enteros. Además, asumiremos-dos principios básicos, que serán útiles para demostrar  
muchas propiedades. Estos son:  
  
1.1. El Principio de Buena Ordenación. Todo subconjunto no vacío de números  
enteros positivos tiene un menor elemento. Es decir, si A C £\*+ y A £ é entonces existe  
un entero m € A tal que m < z7 para todo r E A. -  
  
1.2. El Principio de Inducción Matemática. Supongamos que para todo número  
entero positivo n se da una proposición P(n). Supongamos que P(1) es cierta y que,  
siempre que P(n) es cierta también lo es P(n + 1). Entonces P(n) es cierta para todo  
entero positivo n, '  
  
O  
  
Scanned by CamScanner  
  
  
--- Página 8 ---  
  
P  
750f/ de ,e  
ff'  
  
1.3. ElO MA puede defstrárte,a partir del principio de buena orde-  
  
nación.  
En efecto, supongamos que A es un conjunto de enteros positivos que contiene al 1 y  
  
que, siempre que n € A entonces también (n + 1) E A. Para probar que A=Z + bastará  
demostrar que el conjunto A', formado por todos los enteros positivos que no pertenecen  
a A, es'vacío. Daremos una prueba indirecta (reducción al absurdo), que consiste en negar  
la tesis que se pretende demostrar y, a partir de allí, llegar a un resultado contradictorio.  
Supongamos que A' $ d; entonces, de acuerdo con el principio de buena ordenación, A'  
contendrá un menor elemento m. Como 1 E A, necesariamente m > 1 y, en consecuencia,  
— 1 es positivo. Como además m — 1 < m 'y m es el menor elemento de A', se tiene  
que (m — 1) E A. Pero entonces, por hipótesis, (m-1)+1=m E A. Esta contra…d1ccxon  
proviene de haber supuesto que A' £ d. Esto concluye la prueba.  
Las pruebas indirectas se usarán con bastante frecuencia en la demostración de toere-  
mas y resolución de problemas sobre divisibilidad. \_  
A continuación daremos un par de ejemplos sobre cómo se procede para demostrar  
  
algunas propiedades usando el pnnc1p10 de inducción.  
  
e Probar que para todo entero positivo n se tiene:  
  
1+2+3+...+n "(n9+) (1)  
  
-  
  
La prueba por inducción requ1ere en pnmer lugar, la demostración para n = l. En  
este caso es inmediata, por cuanto:  
  
— 1(1+1)  
=.  
  
En segundo lugar supongamos la igualdad (1) válida para un cierto valor de n: (esfa.  
es la llamada thate.m de inducción ), e intentemos demostarla para n +1. +  
Se tiene, por la propiedad asociativa de la adición:  
  
1+2+3+...+n+(n+1)=(1+2+3+...+n)+(n+1)  
y, de acuerdo con la hipótesis de inducción:  
  
14243+..+0+(0+1) =D 4 (141)=  
  
= An+1)+2(n+1) \_  
  
2  
- (n+1)(n+2)  
— S —  
  
Pero esta es, precisamente, la ¡gua.ldad (1) para n + 1 sumandos, con lo cual completamos  
la demostracxon  
  
Scanned by CamScanner  
  
  
--- Página 9 ---  
  
—  
  
—  
  
=. — — -  
  
+m7wrammf&-mmmfuw…i…,— o  
  
¿Ad EO d Ó  
  
»  
  
Nota. Usualmente, cuando se presentan expresiones como 1+2+3+...+n resulta  
conveniente abreviarlas mediante el uso del símbolo de sumatoria, que se representa por  
  
la letra griega sigma mayúscula (3;). En este ejemplo se escribe:  
n  
  
»  
=1  
y se lee suma (o sumatoria) de : donde : va desde 1 hasta n, lo cual indica que el primer  
sumando se obtiene asignando a í el valor que aparece debajo de la letra $>; (en este caso  
1), para los siguientes sumandos se asignan a ? los valores 2,3,4, ... hasta llegar al valor  
  
colocado en la parte superior de la letra 3$\* . Otros ejemplos serían:  
  
Y B=13+23+33+...+7,  
  
i=1  
  
n  
  
Y i(1+i)=12+23+34+...+n(n+1),  
i=1  
  
n-1 - -  
S (2:+1)=1+3+5+7+...+(2n-1).  
  
1=0  
  
e Probar que para todo entero positivo n se tiene:  
  
. 1  
; (2:—12:+1) -+ 1“'\_  
  
Esto es, probar que:  
1 1 1 1 n  
—7 E- +H+==- +H...+=—————— = — 1  
13 35 57 '+'(2n —1D(2n+1) 2n-1 C  
Si n = 1 se obtiene inmediatamente: \_ M  
1 1  
  
13 21+1  
(1) es nuestra hipótesis de inducción.  
  
Supongamos la propiedad cierta para n sumandos.  
  
Para n + 1 sumandos debemos llegar a la igualdad:  
  
1 1 1 1 1 n+l  
  
Tatizzt757 t--+79 e .= — ——s= ——.  
  
13 3557 (2n-D2n+1) \* (2n+D2n+3) - 2n+3  
  
En gfecto, si sumamos Zn + D(2n+3) al primer miembro de (1), usando la hipótesis  
de inducción se tiene:  
  
1 1 + 1 \_  
(2n +1)(2n+3)  
  
1 1  
(ñ+ñ+ñ+"'+(2n—1)(2n+1)  
n(2n+3)+1 \_  
  
n 1  
- MmI1\* (27 +1)(2n+3) (2n+1(2n+3) .  
\_ \_2n?+3n+1 \_ 2n+3n+1) n+1  
(27 +1)(2n+3) (2n+1)(2n+3)” 2n+3'  
  
4  
Scanned by CamScanner  
  
-  
  
  
--- Página 10 ---  
  
Problemas.  
Demostrar, - usando el método de inducción:  
  
\_n(n+ 1(2n + 1)  
==——6 —  
  
1.4. Í (i+1)= %—n(n + 1(n +2).  
  
1.5. Z(3: 2) = "(3" D  
  
1.6. 2n? > (n+ 1)2 para todo entero n > 3.  
1.7. 2" > n? para todo entero n > 4.  
  
1.8. El número de diagonales de un poligono de n lados es:  
  
”)  
  
1.9. La suma de los a.ngulos interiores de un polígono de n la.dos es (n — 297 (o bien,  
(n — 2).180\* en grados sexagesimales).  
  
1.10.  
  
i=0  
  
Nota. Todas estas propiedades se aplican con frecuencia, por tanto, es conveniente me-  
morizarlas.  
  
donde  
  
Scanned by CamScanner  
  
  
--- Página 11 ---  
  
SECCION 2  
  
EL ALGORITMO DE LA DIVISION  
  
Dados dos números enteros a, b, coñ a \* 0, se dice que a divide a bsi existe un entero  
z tal que b = az.  
  
Si a divide a b se usa la notación: a|b. Por cjemplo, 4 | 20, 7 | 98, 11 | 242.  
Si a no divide a b se escribe: a /b. Por ejemplo, 4 / 10, 5 /24, 12 / 15.  
Si a divide a b, también se dice que a es un divisor de b, o que a es un factor de , o  
que b es divisible por a, o que b es múltiplo de a.  
  
| Propiedades Básicas.  
  
A continuación se presentan algunas propiedades básicas de la relación de divisibilidad  
entre dos enteros. '  
  
2.1. Si a|b entonces albc para todo entero c.  
2.2. Si alb y b|c entonces alc.  
  
2.3. Si a|b y alc entonces al(bz + cy) pára.\_ todo par de enteros 7, y.  
2.4. Si alb y b|a entonces a = +b.  
  
2.5. Si alb, a > 0,5 > 0, enf.onces a<b.  
  
Las demostraciones de estas propiedades resultan inmediatas a partir de la definición  
  
de divisibilidad. En efecto:  
2.1. Si a|b entonces existe un entero z tal que —  
  
b=ar  
  
y rnúltiplicando ambos miembros por c:  
  
be= (a.1;)c = a(zc),  
  
de donde:  
albc.  
  
2.2. Si alb y b|c entonces existen enteros r,y tales que:  
  
, b=ar,c = by,  
de donde:  
e = (az)y = a(zy),  
  
6  
  
Scanned by CamScanner  
  
  
--- Página 12 ---  
  
deiians 166 D  
u—y A RD S  
p  
  
. —  
  
oeo e  
  
alc.  
  
2.3. Si alb y alc, de acuerdo con 2.1. ajbz y alcy, luego existen enteros m;n- talg?f que: -  
  
bz = am,  
  
ey = an.  
  
Sumando miembro a miembro ambas desigualdades se tiene:  
  
bz + cy = a(m+n7);  
luego »  
al(bz + cy). . |  
Nota. Obsérvese que si, en parti¿ular, to;ñamóá' z =y =1, se tíene: e .  
al(b+c). - — '  
Similarmente, si tomamos z = 1, y = —l1, nos queda: — »  
ál(b—c). Y  
Por tanto, si un entero divide a otros dos divide también a su suma y a su diferencia.  
El lector podrá generalizar este resultado por inducción para n enteros. Es decir, si  
a|b1,alb,,...,alb,, entonces - e  
n  
- a Z b¡:l:¡  
i=l  
  
para cualquier conjunto de n enteros zy 1y Z2y ... , a.  
  
2.4. Si alb y bla, entonces existen enteros z, y tales que:  
  
b=azr, a=by,  
de donde:  
  
b = (by)7 = b(yz)  
  
y por consiguiente yz = 1. Ahora bien, como z, y son enteros, se tiene necesariamente que .. e  
T=y= lóz=y=—l,demaneraque a,= +b.  
  
2.5. Si alb, entonces b = ar para algún entero . Como a > 0 y b > 0,z necesariamente  
debe ser positivo; es decir, 7 > 1 y, en consecuencia, a < b.  
  
=7  
  
+  
  
Scanned by CamScanner  
  
  
  
--- Página 13 ---  
  
Cuando dividimos un entero entre otro, de la manera usual, se obtighe un cociente ly  
  
“ un resto (este último a veces es nulo, cuando el primer entero es divisible por el segundo).  
  
A continuación vamos a probar que este procedimiento siempre es posible. Este resultado  
es conocido como el . - .  
  
2.6. Algoritmo de la División. Dados dos enteros a y b, con a > 0, existen enteros q,r  
ta.lesqueb=qa+r,donde0\_<\_r<a. .  
Para demostrar la proposición, observemos la progresión aritmetica  
  
\_[....,b\_\_—\_—2a,b—q,b,b+a,b+ 2a,...).  
En esta progresión hay números positivos y negativos y, eventualmente; está el cero  
en caso de que b sea divisible por a. De acuerdo con el principio de buena ordenación,  
existe un menor entero no negativo en la progresión. Si llamamos r a este entero, 7 tiene  
la forma:  
r =b- a,  
  
de donde: v - -  
b=ga+r. ' (1)  
  
Obsérvese que q toma alguno de los-valores del conjunto (...,—2,—1,0,1,2,.. .)  
Falta comprobar que r < a. Supongamos lo contrario (reducción del absurdo). En-  
tonces tendríamos T 2a yY -  
  
r=a +r1, donde r¡ 2-0.  
  
Reemplazando en (1) se tiene: -  
  
b=\_q'a+(a+rl),  
  
Pero esto indica que 7j es un elemento .- la progresión aritmética considerada, no A  
negativo y menor que, lo que contradice la deíinición de r. Esto completa la demostración.  
q se denomina cociente y r resto de la división. \_ —  
  
De acuerdo con este resultado, al dividir cualquier entero por ?, los restos posibles  
son 0 y 1; al dividirlo por 3,'los restos posibles son 0,1 y 2; al dividirlo por 4, los restos  
posibles son 0, 1, 2 y 3, y así sucesivamente. o  
  
Se dice que un entero n es de la forma ak + b si existe un entero k tal quen = ak+6.  
En virtud de lo expuesto anteriormente, todo entero es de la forma 2k ó 2k +1 (par o  
impar); de la forma 3k,3k + 1 ó 3k +?; de la forma 4k,4k + 1,4k +2 6 4k+3, etc. En  
cada caso, k es el cociente que resulta al dividir el entero entre 2, 3 ó 4 respectivamente.  
  
Esta Fonsidcración resulta útil para resolver diversos problemas de divisibilidad. Veamos  
dos e\_1euxxplog\_ .  
  
O.P\_rc\_>ba.r que n? —n es divisible por 2 para todo entero n. Probar además que n? —n e$  
divisible por 3. -  
  
Scanned by CamScanner  
  
  
--- Página 14 ---  
  
En primer término, tenemos que probar que n?—n es de la forma 2k para todo entero n.  
  
Ahora bien, se tiene que n? —n = n(n— 1). Si n = 2k, entonces n? —n = 2k(2k — 1) = 2k,,  
donde k¡ = k(2k — 1). Si n = 2k +1, entonces n? —n = (2k + 1).2k = 2k,, donde  
k = k(2k + 1). Luego, en cualquier caso n? —n es divisible por 2. Obsérvese que esto nos  
dice que el producto de dos enteros consecutivos siempre es un número par.  
  
Consideremos ahora el entero n? — n. Debemos probar que es de la forma 3k. -Ahora  
bien  
  
n-—n= n(nº— 1) = (n- 1n(n +1).  
  
Veamos los casos posibles. Si n = 3k, entonces n? — n = (3k — 1)3k(3k + 1) = 3k,,  
donde k = k(3k+1)(3k+2). Siri = 3k+2; entonces n? —n = (3k+1)(3E+2)(3k+3) = 3k;,  
donde kz = (3k + 1)(3k + 2)(k + 1). Por consiguiente, en cualquier caso n? —n es divisible  
por 3. Esto nos dice que el producto de tres enteros consecutivos siempre es múltiplo de 3.-  
  
\* Si n es impar, entonces n? — 1 es divisible por 8. Debemos probar que n? — 1 es Ide la |  
forma 8k. Ahora bien, - \_ :  
  
n -1=(n+D(n-1). |  
Si n es impar, entonces n es de la forma 4k + 1ó 4k +3. Consíderémos ambos casos.  
Sin=4k-1, entonces n? — 1 = (4k +2).4k = 8k¡, donde ky = k(2k +1). Sin = 4k +3,  
  
entonces n? — 1 = (4k + 4)(4k +2) = 8k;, donde k = (k + 1)(2k + 1). Luego, en ambos  
casos n? — | es divisible por 8. . . \_-  
  
Problemas.  
  
-2.1. Dos enteros son de la misma paridad si son- ambos pares o ambos impares. Dados\_\_dos  
  
enteros cualesquiera, su suma y su diferencia tienen la misma paridad. e  
  
2.2. Si aclbc, entonces alb.  
  
-2.3. Si alb y cld, entonces aclbd.  
  
É GZ>4 n? + 2 para ningún entero n.  
“ 2.5. Sin 2 2 y k es positivo, entonces (n — DI(n\* — 1).  
  
. +2.6. Sin > 2 y kes positivo, entonces  
  
(n—1)\*(n\* — 1) si y sólo si (n — 1)|k.  
Xa. Ún'cuadrado perfecto (es decir, un número entero elevado al cuadrado), no es de la  
  
forma 3k +2.  
  
9  
  
Scanned by CamScanner  
  
  
--- Página 15 ---  
  
Además, por la propiedad 2.3., cualquier divisor común de a y b divide también a  
d = azo + dyo, Y PO la propiedad 2.5., cualquier divisor común será menor o igual que d,  
luego d = (a, b)- \_ .;  
  
De acuerdo con esto último se observa que el máximo común divisor de a y b puede  
caracterizarse como el divisor común positivo de a y b que es múltiplo de cualquier divisor  
común de a y b.  
  
Si (a,b) = 1, el teorema demostrado nos garantiza que existen enteros Z, y tales que  
az + by = 1. Este resultado se conoce como Relación de Bezout. —  
  
Nota. Si (a,b) =1 se dice que a y b son primos entre sí (o coprimos ). En general, si  
(a1,a2,...,An) =1se di<\_:\_é que los n enteros a1,a2,...,Gn son primos entre sí.  
  
Ahora bien, si en un conjunto de n enteros, cada par de ellos son primos entre sí, se  
dice que los números son primos dos a dos.. Por ejemplo, los números 4, 11, 35, 39 son  
primos dos a dos. Lógicamente, si varios números son primos dos a dos entonces serán  
primos entre sí, pero no necesariamente a la inversa; por ejemplo, (3,7,14) = 1, pero 3,7 y  
14 no son primos dos a dos ya que (7, 14)=7. —  
  
El razonamiento empleado en la demostración del teorema anterior es generalizable  
para cualquier número n de enteros por inducción (el lector puede hacerlo como ejercicio).  
Es decir, si d = (a1, Q2, .., a.) entonces existen enteros T1,72.....7n tales que:  
  
d= a1 + 0272 + ... + anTn.  
  
— Esto pone de manifiesto que el máximo común divisor de varios números enteros  
puede expresarse como combinación lineal entera de dichos números. En particular; es  
fácil ver que a1, a2,...,On son- primos entre sí, si y sólo si 1 es combinación lineal entera  
  
de a¡, a2, - .., Qn- . \_  
A continuación vamos a explicar un procedimiento que permite calcular el maximo  
común divisor de dos números enteros. Este es conocido como el:  
  
3.2. Algoritmo de Euclides. Dados dos en:eros, 1 y b. siendo a > 0, =: aplicamos  
reiteradamente el algoritmo de la división obtenemos una secuencia de ecuac:-nes:  
  
=\_q1(1+7'1, O<ri <a,  
a = 271 +72, O<ra<Ti,  
r1 = 372 +73, 'O<r3 <2,  
  
rn-2=ann—l+rn. 0 < n< "n-1:  
  
y como la sucesión de los restos es estrictamente decreciente y todos ellos son no negativos, -  
alguno de ellos, digamos 7Tn, será el último resto no nulo en la cadena de igualdades.  
  
Eptónces, . -  
Tn-1 = In+iTn. /  
Qn+iTn Z  
  
Ahora bien, probaremos que ra = (a,b).  
  
12  
  
Scanned by CamScanner  
  
  
--- Página 16 ---  
  
“Para demostrar esto, basta recorrer la secuencia de ecuaciones de abajo hacia arriba  
e inversamente, de arriba hacia abajo.  
  
En efecto, de la última ecuación se desprende que r |r ,1, pero subiendo a la prece-  
dente se observa que, como rn|"n y Tn| n+1, entonces necesariamente ra|"n+2. Continuando  
el proceso (esto se puede formalizar fácilmente por inducción), llegamos a que rn|r3 y r, r2,  
luego rn|r1; de allí concluimos que, como rr y rn|r1, entonces Tn|a, y finalmente si r, |r1  
y "n|a entonces rn|b. Por tanto, r, es un divisor común de a y de b.  
  
Por otra parte, partiendo de la primera ecuación se ve que todo divisor común de a  
y b lo es también de r¡; todo divisor común de a y r1 lo es también de r2; todo divisor  
común de r y r lo es también de r3; y así sucesivamente todo divisor común de r,\_7 y  
  
Tn—1 lo es también de r. Por consiguiente, r, es justamente el máximo común divisor de  
  
a y 5. :  
El siguiente ejemplo ilustra la utilización del algoritmo en un cálculo numérico.  
  
e Calcular (440,252). -  
  
Al efectuar las divisiones en la forma usual, se obtienen las siguientes igualdades:  
  
440 =1.252+188,-. --  
252 = 1.188 + 64,  
  
188 = 2.64 + 60,  
64=1.60+4, \_  
  
60 =15.4. - ,  
  
El último resto no nulo en la secuencia es 4, luego (440,252) = 4. Ahora, si queremos  
expresar 4 como combinación lineal entera de 440 y 252, podemos eliminar los restos 60,  
64 y 188 de la manera siguiente:  
  
4=64-60=  
= 64 — (188 — 2.64) = —  
= —188 + 3.64 =  
= —188 + 3.(252 — 188) =  
= 3.252-4.188 =  
  
= 3.252 — 4.(440 — 252) =  
= (—4).440 + 7.252.  
  
El método puede ser útil también en la resolución de algunos problemas. Por ejemplo:  
  
21 4 . ,  
\* Demostrar que la fracción -14—Z-+— es irreducible para todo entero n.  
$e quiere probar que, para todo n, (21n +4) y (14n+3) son Prímos entre sí. Al dividir  
Sucesivamente se tiene:  
  
21n+4=1.(14n+3)+(7n+1),  
lMn+3=2(7n+1)+1.  
  
13  
  
Scanned by CamScanner  
  
  
--- Página 17 ---  
  
Luego,  
(21n+4,14n +3) =1.  
  
Concluimos esta sección demostrando algunas propiedades ¡mportant  
  
es del máximo  
común divisor.  
  
Prop1edades  
Sea d = (a,b). Se tiene:  
  
a b -  
.3. —7 )=.  
S (d' d)  
3.4. Sialbc y d=1 entonces alc.  
  
a  
3.5. Si albc entonces -  
  
d  
  
C.  
  
3.6. Si m > 0 entonces (ma, mb) m(a, b). |  
  
En efecto: —  
3.3. Si (a,b) = d, entonces existen enteros 7, y tales que  
az + by = d,  
luego,  
de + y=1  
de a  
  
y, en consecuencia  
  
<¿2 "  
d'd) - \_  
  
3.4. Sid=1, entonces existen enteros , y tales que:  
  
az+by =1.  
  
Multiplicando ambos miembros por c se tiene:  
  
arc+ byc =c.  
  
Como ala y albc se concluye que alc.  
  
5. s , . a|b b |  
3.5. Si albc entonces es inmediato que il De acuerdo con 3.3., <-3—, 3) = 1, luego, por  
3.4., \*  
  
14  
  
Scanned by CamScanner  
  
  
--- Página 18 ---  
  
3.6. Es inmediato que md es un divisor común de ma y de mb. Supongamos que d' es otro  
divisor común. Debemos probar que d' Imd. En efecto, sabemos que existen enteros  
z, y tales que \_  
  
a.1:+by=d.  
  
Multiplicando ambos miembros por m se tiene:  
maz + mby = md,  
luego, si d'|Ima y d'Imb entonces d'Imd; por tanto  
  
. A(ma, mb) = md = m(a, 5).  
  
Problemas.  
  
- 3.1. Probar que si (a,b) =1, alc y blc entonces ablc.  
  
-3.2. n55nes divísiblé\_porí30. o .. '. e  
  
3.3. El ¡\_J-roduct\_o de cuatro enteros consecutivos es divisible por 24.  
3.4. Probar que ((a, 6), c) = (a, (8,c)).  
.3.5. No existén enteros r,y tales que  
| 7+y=100; (z7,y)=3.  
3.6. Existen inñ¿itos pares deáenterés Z,y tales que -  
7+y=100; (zr,y)=5.  
3.7. Si (a,4) =2 y (b,4) =? entonces (a+b,4) =4.  
  
- 3.8. Dados dos enteros impares, a y b, a? — d? es divisible por 2" si y sólo si a—bes divisible  
por 27,  
  
3.9. Se define la sucesión de Fibonacci de la siguiente manera:  
  
ay = aj =,  
  
a2=ag+a,=1+1=2,  
a3 =aj +a,z=1+2=3,  
ay =A7 +a07 =2+3=5,  
  
An+2 = An + An+i.  
  
15  
  
Scanned by CamScanner  
  
  
--- Página 19 ---  
  
<a) Probar que dos términos consecutivos cualesquiera de la sucesión de Fibonacci son  
primos entre si. 4  
  
b) Probar que, si n > 1, entonces  
  
x 3.10. Sean d = (a,b), d' = (a',b'). Probar que  
| | ¿¿4 = (aa',ab', ba', bb').  
3.11. Sean los enteros a, b, c,\_d primos ;:on m, donde:  
m = ad — ij  
  
Probar que las expresiones az +by y cz+ dy son múltiplos de m para el mismo  
conjunto de números enteros r, y. -  
  
:3.12. Sean a y b dos enteros positivos tales que (  
  
a, b) = d. Probar que exactamente d de los  
números: :  
  
— a,2a,3a,...,(b— 1)a, hr  
  
son divisibles por b.  
  
16  
  
Scanned by CamScanner  
  
  
--- Página 20 ---  
  
A |  
. N  
  
A a é  
4 rZ 2ñ p  
  
- E .  
AE CAA ANE REN ? Se RÁeN e CEA  
iac ECQ A s A TA  
  
SECCION 4  
LA ECUACION ax+by=c  
  
Con las propiedades básicas que hemos estudiado hasta ahora sobre divisibilidad, es  
posible resolver algunas ecuaciones diofán9ica.s, es decir, ecuaciones en las cuales se procura  
hallar soluciones en números enteros. :  
  
Los tipos de ecuaciones diofánticas que se pueden presentar són prácticamente ¡li-  
mitados, y no existen, usualmente, métodos generales de solución. En la presente sección  
vamos a resolver el caso más sencillo: la ecuación lineal en dos variables. Al final de la  
sección se presentan diversos problemas diofánticos, en los cuales se requiere plantear o  
resolver ecuaciones de otros tipos.  
  
Toda ecuación lineal en dos variables con coeficientes enteros, puede escribirse en la  
forma: . \_  
aT + by =. ' (1)  
  
Sia=06b=0, el problema es inmediato pues se reduce a ver si la solución de una  
ecuación de primer grado con una incógnita es un número entero. Supongamos entonces  
que a £ 0 y b55 0. Sea d = (a,b). Probaremos el siguiente resultado. o  
  
4.1. La ecuación ar + by -= c tiene solución en enteros si y sólo si d|c. Además, si (Zo, y0)  
es una solución particular, la solución general tiene la forma:  
  
- T=T0+-k y=yo—3k donde kEeZ.  
  
En efecto, si (a,b) = d entonces di(az + by) para todo par de enteros z, y; luego, si  
d fc entonces la ecuación az + by = c no tiene solución en enteros.  
Supongamos que d|c. Sabemos que existen enteros 7', y' tales que  
  
az' + by =d - = -(2)  
(recordemos que estos valores 7',y' pueden obtenerse aplicando apropiadamente el algo-  
  
ritmo de Euclides). c  
Multiplicando ambos miembros de (2) por j\* tiene:  
  
- L c C .7 . .\_  
por consiguiente: ) = 7'-, yo = y'2 es una solución particular de la ecuación (1).  
  
Á fin de encontrar todas las soluciones, supongamos que (7, y) es una solución arbi-  
traria de (1). Entonces se tiene:  
  
az + by = azo + byo,  
a(7 — 0) = d yo —y),  
  
17  
  
Scanned by CamScanner  
  
  
--- Página 21 ---  
  
O a nca s a i n an  
  
de donde,  
  
bla(r — z0)  
y en consecuencia,  
a  
ad  
- º — 1, se concluye: -  
y, como a= cluye:  
, 2' (I — :L'o).  
  
Es decir, 7 — 70 = -c-i-k para algún entero k, luego  
  
= —k.  
T =TI0+ j  
  
Sustitúyendo este valor de z en (1) y despejando y se obtiene:  
  
b  
  
luego  
b = c-aro-a=k=  
y =c — aro—az  
= byo — bk  
a  
  
y entonces  
= 1 — Ek  
Y = Yu d  
  
Por tanto, toda solución entera de la ecuación (1) puede escribirse en la forma  
  
b V a  
LE=m+gh vSW-gh  
  
Además, si reemplazamos estas expresiones en (1), se ve inmediatamente que se verifica  
  
“ la igualdad, luego efectivamente hemos hallado la solución general.  
Veamos a continuación un par de ejemplos.  
  
e Resolver en enteros 327 + 60y = 30.  
Observemos que (32,60) = 4 y 4 /30, por consiguiente la ecuación  
tiene soluciones en enteros.  
  
327 + 60y = 30 no  
  
e Resolver en enteros 4407 — 252y = 12.  
  
18  
  
Scanned by CamScanner  
  
  
  
--- Página 22 ---  
  
a iii rai U d  
raj vi a = AE  
A Ta eal \_,¡»———-\_¡\_\_.…¿\_-—'““'¡\_' TA TiO NENCA antiiee e oee  
  
Aplicando el algoritmo de Euclides, en la sección 3 determinamos que (440,252) =  
4. Como 4|12, la ecuación tiene soluciones enteras. Más aún, determinamos que 4 puede  
  
\_ escribirse como combinación lineal entera de 440 y 252 de la siguiente manera:  
  
(-4).440 + 7.252 = 4,  
  
luego —  
(—4).440 - (-7).252 =4  
  
y de acuerdo con la notación que hemos usado se tiene  
T= —4\_: y,\_= \_'71  
  
12 12  
I= (—4)? = '\*º12, Yo = (—7)? = -'21,  
  
. de donde x9 = —12, y, = —21 es una solución particular.  
  
.4.  
  
-4  
  
4  
  
- La solución general viene dada por:  
  
252 D. 440,. .  
=-12- k - y=-21= k  
=27 y=1=7 |  
  
7=-12-63k, y =-21-110k, dondeke Z. --  
  
Problemas. \_- - - \_  
  
,  
  
1. Siar+by =ctiene dos soluciones (Zo, y0) y (21,y1) tales que 71 = 1 + 70 y (a,b) =1,  
entonces b = +1. \_  
  
.2. Hallar una condición necesaria y suficiente para que el sistema de ecuaciones diofán—  
  
ticas  
ar + b1y +C¡Z = d1,  
az + by + c2z =do,  
  
donde b $ b,, tenga al menos una solución.  
-3. Probar que el sistema de ecuaciones diofánticas  
  
7 +6y+z=2,  
47 + 10y + 2z = 3,  
  
no tiene soluciones.  
  
-4.4. Resolver el sistema de ecuaciones diofánticas  
  
7 +2y+3z =4,  
  
27—-z=-—]1,  
  
19  
  
Scanned by CamScanner  
  
  
--- Página 23 ---  
  
+ 4.5.  
  
x4.6.  
  
Xx4.7.  
  
4.11.  
  
x4.12.  
  
4.13.  
  
-4.14.  
  
4.15.  
  
4.16.  
  
- 4.170  
  
Resolver en enteros el sis¿ema |  
| — T+Yy—-—2=-1,  
— y +7 = 1,  
-DIipIir=-L  
  
La ecuación z\* + 57 + 9 = 0 no tiene soluciones enteras.  
  
El producto de dos números que son sumas de dos cuadrados puede también expresarse  
como la suma de dos cuadrados  
  
Dados tres enteros consecutwos, el cubo del mayor no puede ser igual a la suma de  
los cubos de los otros dos,  
  
El producto de cuatro enteros p051t1vos consecutivos no puede ser un cuadrado per-  
fecto.  
  
Si la suma de los cuadrados de tres números enteros se multiplica por tres, el resultado  
puede expresarse como la suma de cuatro cuadrados perfectos.  
  
Si 2n se puede expresar como la suma de cuatro cuadrados perfectos, entonces n  
también puede expresarse como la suma de cuatro cuadrados perfectos.. -  
  
No existen números enteros T,y que satisfagan la ecuación  
  
n 157\* — y? =9.  
  
Dado un entero n, existen enteros z, y tales que 7? —y? = nsi y sólosin es el producto  
de dos enteros de la mismá paridad.  
  
Si p, q son enteros positivos tales que 2? + 1 = q?, entonces p = q =3.  
  
Dados los enteros a, b,c, d, demostrar que  
z2+am+b=yº.+cy+d  
  
tiene infinitas soluciones enteras (7, y) si y sólo si  
  
2\_ 4b= \_c2 — 4d.  
Hallar las soluciones enteras de la ecuación  
T+15" =2.  
  
-Dados los enteros positivos n, p, hallar condiciones necesarias y suficientes para que el  
  
sistema de ecuaciones  
' , T +py =n,  
  
T+y =p",  
  
tenga solución (7,y, z) de enteros pos¡t1vos Demostrar además, que a lo sumo hay  
  
una tal solución.  
  
20  
  
Scanned by CamScanner  
  
  
--- Página 24 ---  
  
SECCION 5  
EL MINIMO COMUN MULTIPLO  
  
Si a, b son dos enteros no nulos, se dice que c es un múltiplo común de a y de b si alc  
y b|c. Por ejemplo, 24 es un múltiplo común de 4 y de 6 ya que 4|24 y 6|24.  
  
Es evidente que todo par de enteros no nulos, a y b, tienen múltiplos comunes; por  
ejemplo, ab es un múltiplo común de a y de b, así como todos los múltiplos de ab. El  
principio de buena ordenación garantiza que existe un menor múltiplo común positivo de .  
a y b. A éste se le llama mínimo común múltiplo de a y b y se le denota por a, b).  
  
En general, dados n enteros no nulos, a¡,az,...,dn, su mínimo común múltiplo se \_-  
  
denota por [a1,a2,. ..\_,a,;].. EO  
Propiedades.  
  
5.1. Si c es un múltiplo comun de a y b, entonces [a, dlc.  
  
En general, si c es un múltiplo común de a1,a2,...,an, entonces [21,a2,...,an]|c.  
Luego, el mínimo común múltiplo de varios enteros puede caracterizarse como el múltiplo — -  
  
común positivo que es divisor de cua.lquíex\_º múltiplo común.. \*  
5.2.- Si m > 0 entonces [ma,mb| =mía, b).  
  
5.3. Sia > 0 y b > 0 entonces [a, b](a, b) = ab. En general, [a, b](a, ) = |ab].  
En efecto: ' . — -  
5.1. Sea m = [a, b|. De acuerdo con el algoritmo de la división, existen enteros q y r tales  
  
que  
e=0gm+r y O<r<m.  
  
Debemos probar que r = 0. Ahora bien, si fuese r > 0, como alc, a|m, dlc, b|m,  
tendríamos que a y b serían divisiones de c — qm =, esto es, r sería un múltiplo común  
de a y b, contradiciendo la definición de mínimo común múltiplo por cuanto r <- m.  
La contradicción proviene de haber supuesto que m fe; por tanto, queda demostrada la  
  
propiedad. \_ v  
Obsérvese que el mismo razonamiento se puede generalizar, inmediatamente, para el  
caso de n enteros a¡, a, ...,dn. — : .  
  
5.2. Como ma|[ma, mb] se tiene que m|[ma, mbl, luego [ma, mb| = mz¡ para algún entero  
  
positivo z1. \_  
Sea [a,b] = 77. Entonces a|z y b|z2, luego  
  
ma|lmz, y — mb|ma,,  
es decir, mz7 es un múltiplo común de ma y mb, y por tanto  
[ma, mb||mzz,  
  
21  
  
Scanned by CamScanner  
  
  
--- Página 25 ---  
  
luego,  
  
m:c¡lng,  
$1l121  
  
T| < Ta. (1)  
  
Po£ otra parte, se tiene que  
ma|mz: y mb|mzií,  
luego,  
alz: y blz:,  
| zaz Ne  
De (1) y (2) se concluye que 71 = 2; luego, [ma,mb] = mla, b].  
  
5.3. Supongamos primero que (a,b) = 1. [a,b] es múltiplo de a, luego la, b] = ar para  
algún entero positivo z. Pero además blaz, y como (a,b) = 1 entonces necesariamente blz,  
luego b < 7 y ab <ar. Ahora bien, como ab es un múltiplo común positivo de a y de b, no  
puede ser menor que su mínimo común múltiplo, por lo cual concluimos que [a, b) = ab.  
Consideremos ahora el caso: general. en el cual (a,b) = d > 1. Entonces 7 y  
  
d -  
  
son  
  
y  
  
al o  
  
ab "  
enteros tales que (-— —) = 1, luego podemos escribir:  
  
d'd  
a b|(fady\_90  
ral d9) £  
  
Multiplicando ambos miembros por d? y tomando en cuenta las propiedades 5.2. :  
3.6. nos queda: — \_  
  
[d, b(a,b) = ab.  
  
Obsérvese que [a, b) = [a, —8) y (a) = (a,—b). lego en general, si a 0 b son nega£ivos,  
se cumple: '  
  
[a, bl(a, b) = labl.  
Problemas. |  
- 5.1. Sines un entero positivo,'evaluar (n,n+1) y (1, +1]-  
-5.2. Si ay b son enteros positivos tales que alb, hallar los valores de (a,b) y [a, 0)-  
- .5.3. Hallar todos los enteros positivos a y b tales que  
  
(a05)=10 y (ab| =100.  
  
5.4. Dados los enteros positivos d y m; probar que existen enteros 7, y tales que ( iH y) =d,  
[r,y] = msi y sólo si d|m.  
  
Scanned by CamScanner  
  
  
--- Página 26 ---  
  
E A AA  
  
17 AG 0  
  
0 a TNA r tz de , ,  
  
o  
  
SECCION 6  
  
NUMEROS PRIMOS  
  
En el conjunto de los números enteros positivos, se observa que el número 1 tiene un  
único divisor: el propio 1.  
  
En este sentido, el 1 constituye un caso particular. Cualquier entero positivo n > 1  
admite, por lo menos, dos divisores: 1 y n.  
  
Se dice que un entero positivo P > 1esun número primo si únicamente admite dos  
divisores positivos: 1 y p. Por ejemplo, 2, 3, 5, 7, 11, 13, ... son números primos. Si un  
entero positivo tiene más de dos divisores positivos diferentes, es un número compuesto.  
El número 1 no es ni primo ni compuesto. . - -  
  
El resultado fundamental de esta sección establece que todo entero positivo, mayor  
que 1, puede ser expresado en forma única como un producto de factores primos (si el  
entero es un número primo, puede considerarse como producto de un solo factor). Para  
demostrar esto, necesitamos usar dos propiedades previas. Una propiedad que se prueba  
para usarla en la demostración de otra, más importante o general, recibe el nombre de  
lema. — . - E  
  
6.1. Lema. Sin es un entero mayor que 1, entonces n es un producto de =núuietos primos.  
  
Para demostrarlo procederemos por vía indirecta; es decir, supondremos que existen  
enteros positivos mayores que 1 que no son productos de factores primos. De acuerdo  
con el principio de buena ordenación, existe un menor eñtero positivo que satisface tal  
condición. Llamemos m a este número. e \_  
  
m no es un número primo (de lo contrario sería el producto de un factor primo). Por  
consiguiente, existe un entero positivo a, diferente.de 1 y de m, tal que a|m. Luego, m = ar  
para algún entero positivo z. . \_  
  
Ahora bien. de acuerdo con la propiedad 2.5., se tiene que a < m y T <m, por t\_'a.nt\_o  
a y 7 pueden expresarse como productos de números primos. Sean D  
  
a= pi1P2...p;,  
7 = q192...Q;,  
  
donde p,,... "PirQ1,...,4j denotan números primos. Entonces  
  
m=p¡...p¡q1...q¡-  
  
es también un producto de factores primos, lo cual contradice la forma como hemos definido  
m. Por consiguiente, concluimos que todo entero mayor que 1 es un producto de factores  
primos.  
  
6.2. Lema. Si p es un número primo y plab, entonces pla ó plb. —  
  
Este hecho es una consecuencia directa de la propiedad 3.4. En efecto, si p /a, como  
P €s primo se tiene necesariamente que (a, ) =1, luego plb.  
  
23  
  
Scanned by CamScanner  
  
  
--- Página 27 ---  
  
De iN MN PRC 0 N  
  
Nota Es fácil generalizar, por inducción, este resultado para un producto de n factores  
Es decir, si pla102 -- n» entonces pla; para algún ? = 1,2,...,n.  
Ahora estamos en condiciones de probar el:  
  
mental de la Aritmética. Todo entero positivo > 1 puede  
  
6.3. Teorema funda  
ma única (salvo el orden en que  
  
expresarse como UN producto de factores primos en for  
  
aparezcan los factores).  
De nuevo, procederemos por reducción al absurdo. El lema 6.1. nos dice que todo  
  
entero mayor que 1 puede expresarse como producto de números primos. Admitamos  
que hay enteros que tienen más de una descomposición en factores primos y supongamos  
(de acuerdo con el principio de buena ordenación) que m es el menor entero positivo que  
  
satisface tal condición. Entonces  
m = piP2 ---Pi = 9192 ---Ji  
  
primos (evidentemente, diferentes de m). Entonces  
  
divide a alguno de los factores del pro-  
ctores si es necesario) que pilgi-  
= q y entonces, simplificando  
  
donde pi,---.Pi:91----9; SON  
- P1lg192 - -- 4j Y, de acuerdo con el lema 6.2., P1  
  
ducto q192 -- - qj- Podemos suponer (reordenando los fa  
Como pi y 41 Son primos, se tiene que necesariamente P1  
  
por pi = q1 en la expresión (1) sé tiene  
  
P1 . ,  
piedad 2.5.,.M1 < m. Pero  
  
Como p¡|m, — es un entero mi y de acuerdo con la pro  
1 1 1J .  
  
entonces, la expresión (2) muestra que 771 €s UN entero menor que m que tiene más de una  
descomposición en factores primos. Esta contradicción demuestra el teorema. .  
Usualmente, cuando se aplica el teorema fundamental de la aritmética, un entero  
  
n > 1 se escribe en la forma:  
— nA ay . Ak  
n—pllp2 p¡; 1  
  
donde p1,P2,-.-.Pk SON primos diferentes y C1,02, ... ,Q SOn enteros positivos. Esta es  
  
la llamada forma conónico del entero n. Por ejemplo,  
1960 = 22.5.7?; 1188 =2?.3%.11.  
ac ligeramente cliferente de la forina canónica, cuando  
  
es sean nulos. Por ejemplo, si queremos EXpresar el  
ltiplo de dos enteros a y b, en términos de  
  
A veces es útil usar una modalid  
se permite que algunos de los exponent  
máximo común divisor y el mínimo común mú  
sus factores primos, podemos escribir  
  
a= p?'tpgz \_\_.pz¡,  
- 24  
  
Scanned by CamScanner  
  
  
--- Página 28 ---  
  
donde los exponentes a1, ...Qk,91,-..,.x son enteros no negativos. De las definiciones de  
máximo común divisor y mínimo común múltiplo se deduce inmediatamente que  
  
mín(ar, í ,  
(a, b) = pl (a )p;mn(a:.hl\_\_ .pímn(º"º'),  
  
donde min(a;, 6;) denota al menor entre los enteros a; y 6i, y máx(a;, P;) al mayor entre  
a; y 6;. Por ejemplo, si queremos calcular (1960,1188) y [1960,1188] se tiene:  
  
- 1960=2?,39,51.72,11",  
  
. 1188=22,3% 5070 111,  
(1960,1188) = 2?.39%.5%.79 119 — 4,  
[1960,1188] = 2\*.33.51.72.111 = 582120.  
  
A continuación, comprobaremos algunos hechos básicos sobre los números primos.  
  
6.4. (Euclides). Existen infinitos números primos.  
  
Se procede por vía indirecta. Supongamos que la sucesión de números primos  
P1,P2,--. ,P4 es finita y consideremos el número n = pip,...Pk + 1. Sin es primo, es -  
diferente de cada uno de los pi, p>....,Pk. Si n es compuesto, n admite un divisor primo  
p. Ahora bien, necesariamente p es distinto de cada uno de los P1,P2,...,Pk Ya que de lós -  
contrario tendríamos que p|p1p2 ... P+ y, como p|n, entonces también p|1. En ambos casos  
se llega a una contradicción, la cual proviene de haber supuesto que la sucesión de números  
  
primos es finita.  
  
Nota. Usando argumentos similares se puede demostrar que existen infinitos primos de  
las formas 3k + 1, 3k +2, 4k + 1, 4k +3, 5k+1, 5k +2, 5k + 3, 5k + 4, etc. Estos son  
casos particulares del siguiente teorema, debido a Dirichlet, que enunciamos aún cuando  
no lo demostraremos. >  
  
6.5. Toda progresión aritmética de la forma a, a +b, a + 2b,a + 3b,... donde (a,b) =1  
contiene infinitos números primos. .  
  
6.6. Para todo número entero positivo k, existen k números compuestos consecultivos.  
En efecto, consideremos los números  
  
(E+1)!+2,(k+1)!+3(k+1)!+4,..., (E +1)!+(k+1).  
En general, si ?2 <n < k+1, entonces (k + 1)! + es divisible por n y es diferente de  
; por tanto, es un número compuesto. ,  
Esto nos dice que en el conjunto de los números enteros positivos es posible hallar  
  
[ . . , , s  
lagunas”, tan grandes como se quiera, en las cuales no aparezca ningún número primo.  
  
25  
  
Scanned by CamScanner  
  
  
--- Página 29 ---  
  
405 I 7 AZ PAO  
  
1a  
  
Es conveniente tener “encuenta' que no existe ningún patrón o ley de formación de'los -  
-. números primos.  
  
(' \_.4¿—?¡\_.¡ e.  
  
6.7. Sin es un numero compuesto entonces existe un primo p ta.l que pRyP< f  
En efecto,'si n es un numero compuesto entonces existen enteros positivos 7, y tales  
..—…'í'-'“\*".n = zy, . con- 2 <r<y<n.  
  
Sir<y entonces E ¡—< a:y\_\_:—,(n, de donde 7 < Vn. Si p es un primo tal que p|a: entonces  
p < z y se concluye que p < f  
De acuerdo:con este. resultado se tiene que para verificar si un número dado n.> 1 es  
pnmo o no, es s suñc1ente ver si es dmsxble 'o'“no por a.lguno de los pnmos PE < Í 51 no lo, \_'  
es, entonces n es pnmo :  
Por e¿emplo, si querémos ver si e1 número 191 es primo v no, calculamos J1T y  
obsewamo= que p  
  
—  
  
13<x/19 <14  
  
= luego basta dividir 191 entre todos los primos menores o 1º'uales que 13 (esto es, entre 2,  
3,5,7 y 13). Al hacer\_e\_s\_to, se ve que 191 es primo. | EA  
  
Esta idea sugiere un metodo sencillo para formar la tabla de los números primos que .  
  
no excedan a un cierto “entero positivo n. Tal método se conoce como criba de Eratóstenes  
  
y consta de los siguientes. pasos:  
  
e Se escriben los nú\_\_r\_nerov\_s;1\_,\_2¿ 3,4,... ,1.  
  
e El 2esel p;rimer(jnurríero¿f:¡')ri:no;; Se tachan de la lista el -1;y todos los múltiplofs\_¿de'2  
(excepto el\_mismo 2) , .  
  
o El 3esel s¡guxe.xte'numero primo (no esta tachado porque no es múltiplo de 2)\_ :"Se.tachan\_  
  
todos los múltiplos de.3; ex" Lpto el mism:: “, que no hayan sido tachados antenormente  
por ser tamb1en mu1trplos dc 2.  
  
Te El s¡guxente número no tachado es e1 5. Se tachan los mult1plos de 5, con excepc1on de el  
mismo. Obsérvese que. el primero en ser tachado será 25 = 5? ya que los múltiplos menores  
\_de5 ya ha.n s1do tachados por serlo tamb1en de 26 de 3.  
  
dN  
  
.  
  
a  
  
e Se cont1nua. con: e1 1msmo proced1rmento, observando que a1 tachar los mult1plos de un  
primo p se comxenza s¡empre por p. .  
  
r . AE  
I':-' . A  
  
e El método termina cuando se han tachado los números compuestos que son múltiplos de  
los números primos menores o iguales que /n. e  
  
EE  
  
= - Problemas. |  
  
x6.1. - Sean a > 2,n >:2.3Sita”.— 1 es primo, entonces a = 2 y n es primo.  
  
26  
  
Scanned by CamScanner  
  
  
--- Página 30 ---  
  
©¡Sx 2 — 1 es primo y n > 2, entonces 2" + 1 es compuesto.  
  
6.4.  
  
763  
C  
  
6.7.  
  
x6.10.  
  
6.11.  
  
6.12.  
  
6 13. 3Ensten infinitos pr1mos de la forma 4k + 3; de la forma 6k — 5.  
  
6.14.  
6.15.  
  
6.16.  
  
Para ningún entero positivo n,2" + 1 es un cubo.  
  
La suma de cuatro enteros consecutivos no puede ser un cuadrado perfecto.  
  
Existe un único primo p tal que 2p + 1 es un cubo.  
Si 2" 1 1 es primo, con n > 0, entonces n debe ser potencia de 2.  
  
Si los términos de una progresión aritmética infinita de enteros p051t1vos no son todos  
iguales, entonc&s no todos pueden ser primos. - :  
  
Sean pí, p, primos tales que p; = p; + 2, con Di > 3. Probar que 12/(p¡ + p2).  
  
Sea n = p1 'D;?...Pk\* escrito en su forma canónica. Entonces el número de divisores  
  
de n es (1 +a1)(1 + a2)...(1 +a¿)  
  
Sea n = 2p—1(2º — 1) y sea 2? — 1 un número pnmo “Probar que la. suma de todos los  
divisores po<ztnos de n, sin incluir a n, es exactamente . .  
  
Si n es un entero positivo y k la cantidad de primos distintos que dividen a-n, probar  
  
-  
  
que  
  
logn > klog?.-  
  
Si p es un primo, entonces (p — 1)! +1 es potencia de p si y sólo sip =2,365.  
  
Sea an = 111...1 el número cuya expresión decimal está formada por n unos. Proba.r  
que, si Gn es primo entonces n es primo.  
  
¿Cuántos cuadrados perfectos existen entre 40000 y 640000 que son múltiplos, si-  
multáneamente, de 3,2 y 5?  
  
Del conjunto (1,2, 3,...,360) escogemos 8 números compuestos Demostrar que por  
lo menos 2 de los números escogidos no son primos entre sí.  
  
¿Cuántas ternas ordenadas de números enteros positivos (a, b, c) verifican que:  
  
[a, b] = 1000, (b, c] = 2000, (c, a] = 2000?  
  
Probar que  
[a, b, e? (a,b, c)2  
  
[a, bJ(b, cl[c, aj (a bY(b, c)(c, a)  
27  
  
Scanned by CamScanner  
  
  
--- Página 31 ---  
  
HE .":"'fv"'í$:¡…€'-;f'¡" r - ,  
  
6.19. Sean d, b,c,d,u enteros tales que cada uno de los números  
ac, be + ad, bd  
  
es múltiplo de u. Probar que bc y ad son múltiplos de u. -  
  
, /Áxx  
  
“ 6.20./ Si n es un entero mayor que 1, entonces 4" + n1 no es primo.  
  
6.21. Sea k el número de factores primos distintos de n. Probar  
  
que existe no tal que, si  
n > no entonces  
  
1  
1991'  
  
|  
  
<  
  
6.22. Sean a, b,c, d números enteros posxtnos tales que a5 = b%, 3 = d? c- a= 19. Hallar  
d—b. —  
  
6.23. Probar que, para todo entero positivo n, el número —  
  
An = 2903" — 803 — 464" + 261"  
  
es divisible por 1897.  
  
28  
  
Scanned by CamScanner  
  
  
--- Página 32 ---  
  
º¡.  
"\*  
  
SECCION 7  
  
LA FUNCION PARTE ENTERA  
  
Si 7 es un número real, el símbolo [7] denota al mayor entero que es menor o igual  
que 7. Por ejemplo,  
  
[g] = h[r]=3,(0,7]=0,-0,7)]=—1.  
  
La función que a cada número real z le hace corresponder [z], se denomina función  
parte entera y juega un papel importante en la teoría de números. -  
  
A continuación vamos a probar algunas de las propiedades básicas de la función 'pa.rte  
entera. . - | '  
  
Propiedades. -  
Consideremos dos números reales Z, y. Se tiene:  
  
7.1. 7—1<f[r]<z,[r]<r< [2]+1,0<z — [7 <1.  
7.2. Sin esun én\_tero, [ +n]=f[7)]+n.  
  
7.3. (2]+[y] <f +y] <fr]+f]+1.  
  
0 si 7 es un entero  
7-4o I T \_I] = í : ,  
[z] + [—2] —1 si7 noes un entero.  
  
7.5. [MJ = [í] si m es un entero positivo.  
m m  
  
7.6. —[—z] es el menor entero mayor o igual que z.  
  
En efecto:  
  
7.1. 7-1<f[r]<zry[r] << [7] + 1 se desprenden inmediatamente de la definición  
de parte entera de z. Si a los tres miembros de la segunda desigualdad se les resta [f], se  
tiene: O <z — [r] <1.  
  
Nota. Al número z — [z] se le denomina parte fraccionaria de z y usualmente se le denota  
por (z). -  
  
7.2. La igualdad [7 +n]=[z]+n, si n es un entero, es evidente por la definición de [z].  
  
7.3. Escribamos z = n +a,y=  
  
m + $, donde n y m son enteros y a y 6 son dos números  
reales tales que -  
  
O<a<1, O< A<1.  
  
U  
  
29  
  
Scanned by CamScanner  
  
  
--- Página 33 ---  
  
Se tiene:  
  
[z)+[y]=n+m<[n+a+m+AP]=n+m+[a+p)|<  
<n+m+1=f[r)+[y)+1.  
  
7.4. Siz=n+a, donde n es un entero y 0 <a < 1, entonces  
  
—-T=-n-a=-—n-1+1-a,  
O<l-a<1.  
  
En consecuencia,  
— fel+[=2)=ñ+[-n-1+1-a)=  
0 sia=0  
=n-n-1+f-a]=(0 sie=0,  
¿ + 1 —al —l sia>0.  
7.5. Escribamos nu…ente I= + a, donde 0 < a < 1. Se tiene, n = gm +r,.donde  
q,7 son enteros y 0 <r <m — 1. Por consiguiente, como 0 <r +a<m, nos queda:  
  
Por otra parte  
  
luego  
  
7.6. Si en la desigualdad r — 1 < [r] < 7 se reemplaza r por —r se tiene  
—r—l<[-r <—r,  
y multiplicando por -1 nos queda  
| a:\_<¡\_—[—á:]<:z:+l.  
  
El siguiente teorema proporciona un resultado que es bastante útil para la resolución  
de algunos problemas. ' |  
  
7.7. Consideremos un entero n y un primo p. El mayor exponente £ para el cual p\*|n! es  
[n  
E  
"=1  
  
Obsérvese qué en realidad la suma es finita ya que a partir de un cierto 2, digamos 15,  
  
se tiene que p' > n para todo ¿ > i y, en consecuencia, los términos correspondientes se  
anulan.  
  
. 30  
  
Scanned by CamScanner  
  
  
--- Página 34 ---  
  
,  
  
;  
Para la demostración proce¿ieremos por inducción sobre n. Si n = 1'la igualdad se  
verifica inmediatamente. Supongamos que la propiedad es cierta paran! y sea j el mayor  
  
exponente tal que p)|(n + 1). Como (n + 1)! = (n + 1)n! debemos probar que  
  
i=1 i=1  
  
Ahora bien, esta igualdad se desprende inmediatamente del hecho:  
  
E- 10 A  
  
A continuación veremos algunos ejemplos en \_losº.'¿:\_úa\_\_.1\_es se aplica esta propiedad.  
  
e ¿Cuál es la ma.y¿r potehciá de 7 queldívide a 100!?  
  
/  
  
luego 715/100! pero 717 7100!. \_Obsér\_Vese que si 7 > 3 entonces [l77]= .  
  
—  
  
. ¿En cuántos ceros termina 1000!?  
Es preciso determinar cuántas veces aparece el factor 10 = 2.5 en el producto 1.2....  
  
...1000. Como hay menos múltiplos de 5 que múltiplos de 2 en este producto, basta -  
determinar la mayor potencia de 5 que divide a 1000!. Esta es: -  
  
1000 , [10001 , [10001 , [10001 \_ 00 , 40 84 1—249,  
5 ? 5 5 |  
  
5  
luego 1000! termina con 249 ceros.  
  
e ¿Cuál es la descomposición canónica de 20!?  
Los números primos menores o iguales que 20 son  
  
2,3,5,7,11,13,17 y 19,  
  
luego, se requiere hallar las máximas potencias de ellos que dividen a 20!.  
  
201 [20] [20] 20 |  
— — — — I= 2 —  
[2J+[22]+[23]+[24] 10+5+2+1=18,  
  
2  
=—|+ -º]=6+2=8,  
  
Scanned by CamScanner  
  
  
--- Página 35 ---  
  
Por consiguiente, 20! = 218.3º.54.7º.'11.13.17.19.  
  
e Demostrar que'a si aj, az,..., 2k son enteros no negativos tales que aj +a,+... +az =n,  
n!  
entonces —— — es un entero.  
ajla,!...a;!  
  
Es necesario probar que todo primo que divide al denominador divide también al  
numerador, elevado a un Exponente mayor o igual. Es decir, \*  
  
Ahora bien, como a 1+02+...+ 2k = N, usando reíteradaménte la propiedad 7.3. se  
  
tiene - .  
P P LD' P  
para todo z. Sumando sobre ¿ se llega al resultado Propuesto.  
Problemas.  
\*7.1. Determinar el menor entero n para que 30'n sea un cuadrado perfecto.\_\_\_  
7.2 Si z, y son números reales, entonces \_  
) +[y]+[7+y] <(27) 1 [2y].  
  
N 7.3. Siz es un número real, entonces  
  
B- \_  
  
7.4. Hallar fórmulas para el mayo: “xponente k del primo P tal que p\* divide a:  
a) 2.4.6.., (2n),  
b) 1.3.5... (27 — 1).  
  
7.5. Sin es un entero positivo, entonces W €S UN Número par,  
n!  
  
n ,  
7.6. Demostrar que H(a + K) es divisible por n!.  
k=1  
  
7.7. Demostrar que, para todo entero positivo n,  
  
E  
N E  
  
Scanned by CamScanner  
  
"Ie aa q ...  
  
\* .  
  
  
--- Página 36 ---  
  
7'8 Si m y n son enteros no negativos, probar que  
  
(2m)!(2n)!  
n | —y €sentero.  
min!(m +n)!  
  
7.9. Probar que para todo par de enteros a, ,  
| m es entero.  
7 10 ¿Cúá¿to$ áe los priiñ¿ros IOÓ vnú.meros enteros positivos pueden expresarse en la forma  
7.11. Demostrar que la ecugqión\_  
| [7] + [27] + [47] + [8] + [167] + [327] = 12345  
  
no tiene solución real, - - -  
  
LA . . “ . . . k .  
7.12. Sea p un número primo y k un entero positivo. Si p es divisor de ) para todo z,  
?  
  
1 S 1< k—1, entonces existe un entero positivo m tal que k = p”".  
  
7.13. Si 2"-1 |n! entonces n = 2 para algún entero positivo k. a  
  
33  
  
Scanned by CamScanner  
  
  
--- Página 37 ---  
  
SECCION 8  
  
CONGRUENCIAS EN Z  
  
Consideremos un entero posi£ivo m. Se dice que a es congruente con b módulo m, y  
se escribe a = b (mód. m), si a — b es divisible por m.  
  
Por ejemplo, 7 = 2 (mód. 5) ya que 5|(7 — 2),3 = —5 (mód. 4), -31 = -4 (mód. 27),  
etc.  
  
Si a — b no es divisible por m, entonces se dice que a no es congruente con b módulo  
m y se escribe a % b (mód. m).  
  
— 8.1. a es congruente con b módulo m si y sólo si a y b dejan el mismo resto al ser divididos  
  
por m.  
  
En efecto, si .  
a=qim+rí1, donde O<ri<m,  
  
b= g2 +72, donde O <r, <m,  
  
entonces a — b = (q1 — q2)m + (11 —r72), y simi(a — b) entonces necesariamente mi(r1—r72),  
y como |r¡ — r,| < m se tiene que r¡ —r2 =0, luego r = r2. Recíprocamente, si  
  
a=q9m+r y  
b = q2m+r donde 0 <r<m,  
entonces a — b = (q1 — 92)m, de donde m[(¿z —b)y a= b(rñód. m).  
Por consiguiente, cualquier entero es congruente módulo m con uno y sólo uno de los  
enteros 0, 1,2,...,m— 1. Por ejemplo, si m = 2, los enteros quedan divididos en dos clases:  
...,—6,—4,—2,0,2,4,6,...=0 (mód. 2),  
-5,-3,-1,1,3,5,...=1 (mód. 2).  
  
Si m = 3 se tienen tres clases:  
  
...,—9,-6,—3,0,3,6,...=0 (mód. 3),  
...,—8,-8,-2,1,4,7,...=1 (mód. 3),  
...,—7,-4,—1,2,5,8,...=2 (mód. 3).  
  
En general, habrá m clases:  
  
..,—3m,-2m,-m,0,m,2m,3m,...=0 (mód. m),  
  
.-2m+1,-m+1,1,m+1,2n+1,...=E1 (mód. m),  
  
e. -2m+2,-m +2,2,m+2,2m +2,...=2 (mód. m),  
  
.,-2m — 1,-m — 1,-1m-—1,2m—1,...2m—1 (mód. m).  
s 34  
  
Scanned by CamScanner  
  
  
--- Página 38 ---  
  
Por otra parte, decir que a = b (mód. m) es equivalente a la posibilidad de expresar  
a en la forma mk + b, donde b es un entero; decir que a = O(mód. m) es decir que mla,  
luego el concepto de congruencia que hemos introducido es otra manera de expresar las  
  
nociones de divisibilidad.  
Ahora bien, la notación que se emplea es muy ventajosa por cuanto muchas de las  
  
propiedades de las congruencias son semejantes a las propiedades de las igualdades y es  
fácil operar con ellas, como veremos a continuación.  
  
Propiedades. \_  
Sean a, b, c, d números enteros. Para todo m > 0 se tiene:  
  
8.2. a=a (mód.m).-.  
8.3. Sia=b (mód. m), entonces b=a (mód. m).  
8.4. Si a = b (mód. m) y b = c(mód. m), entonces a=c (mód. m)  
  
8.5. Si a = b (mód. m) y c= d (mód. m), entonces a+c = b+d (mód: m) y a- c=b-d  
  
8.6. Si a = b (mód. m) y c= d (mód. m), ént-onces ac = bd (fnód. m).  
Las dem¿>straciones son inmediatas. En efecto,  
8.2. mj(a —a).  
8.3. Si 'm.|(a — b), entonces m|(b —'a).  
8.4. Si m|(a — b) y m|(b — c), entonces mi[(a — b) + (5— 0)), luego mi(a —c).  
  
8.5. Si ml(a — 5) y ml(c—d), entonces mil(a — b) + (c—d)] y mi[(a — b) — (c—d)], luego  
mil(a + €) — (6+ )) y mi[(a — c) - (5-d)]. |  
  
8.6. Si ml(a — 5), entonces m|e(a — b), luego m|(ac — de). (1)  
Si ml(c — d), entonces mib(c — d), luego m|(dc — bd). (2)  
De (1) y (2) se concluye que mi[(ac — de) + (bc — ba)], luego mi(ac— da).  
  
Nota. Cuando se tienen varias congruencias como a = b (mód. m), b =c (mód. m),  
c = d (mód. m), esto usualmente se abrevia escribiendo:  
  
a=b=c=d (mód. m).  
  
Li%s propiedades 8.5. y 8.6. se pueden generalizar fácilmente por inducción, para  
cualquier número finito de congruencias, Así se tiene que, si  
  
A =bi (mód. M), a7 =b, (mód. m),...,an = ba (mód. m),  
  
35  
  
—  
  
Scanned by CamScanner  
  
  
--- Página 39 ---  
  
entonces  
  
a +az+...an=b1+b2+...ba (mód. m)  
  
En particular, si a = b (mód. m), para todo entero positivo n se tiene:  
a"=b" (mód. m).  
  
Toma.ndo en cuenta estos hechos es fácil demostrar el teorema s¡gu1ente  
  
8.7. Sea f un pohnormo de coeñcxentes enteros. 81 a=  
= f(b(mód. m).  
En efecto, supongamos z) = aT + aj7 AE +an-17 + an, donde los a; son  
  
enteros para 1 = 1,2,...,n. De acuerdo con las prop1edade38 5. y 8.6. generahzadas se  
tiene -  
  
b (mód. m) entonces f(a) =  
  
aga" = agb" (mód. m),  
  
aja" ! = a1b"-!(mód. m),  
  
An-10 = An-. ¡V(MÓd. M),  
  
II  
  
an = an(MÓd. M)..  
  
Por consiguiente,  
aga" +aja" ! +...+an-\_10 +a, = aob" + a1b"v\_1 +...+ a¡.\_1b + ay(mód. m).  
  
Veamos 2 continuación algunas ap::caciones p- :-ticas de esras proniedar!e=.  
  
e ¿Cuál es la última cifra de 34007 — \_  
Basta observar que todo entero r escrito en el sistema decimal: 7 = a0.10" +...+  
+an—1.10 + an, es congruente con su última cifra módulo 10. Entonces:  
. 3 =3 (mód. 10),  
=9 (mod 10),  
3 =27=7 (mód. 10),  
3 =1=1l (mód. 10).  
  
De esta última congruencia se deduce:  
  
(3)'\* = 1100 (mód, 10),  
3%=1 (mód. 10).  
  
Luego, la última cifra de 310 es 1,  
  
36  
  
3  
  
Scanned by CamScanner  
  
  
--- Página 40 ---  
  
\_ \_—]  
  
nN  
  
s a aA A E  
  
e Si f(z) == - 5r + 6z? — 37 +2, ¿cuál es el resto al dividir f(1991) entre 4?  
Obsérvese que 1991 = 3 (mód. 4); por consiguiente, 19914 — 5.19913 + 6.19912—  
\_3.1991+ 2=3 -5.3?+6.3?-3.3+2=81-135+54-9+2=-7=1 (mód. 4)  
  
Por tanto, el resto es 1.  
  
e Expresando los números enteros en el sistema decimal de numeración, deducir el criterio  
  
de divisibilidad por 3.  
Sea 7 = ag.10" + aj.10" ! +...+an-1.10 + an. Obsérvese que  
  
ñori ¡:aúto; para t'o.do ?ntef¿'posítiíúo' n:, -  
  
107 =1"=1 (mód. 3).  
Luego, 7 = aq + a +...+an—1 +n (mód. 3),es decir, 7 es divisible por 3 si y sólo 'si'  
la suma de sus cifras es un múltiplq\_dg3. o - - , A  
L, Expresa.ndo los áúmeros enteros en ellsis£ema. decimal de numéración, deducir el criterio  
  
de divisibilidad por 11.  
Sea y7 = ao.10"\* + a,.10" ! +...—an—1.10 +an. Obsérvese que  
  
10=-1 (mód. 11),  
  
. 10 = (-1)" (mód.11).  
Por consiguiente, 7 = ag.(—1)"+a¡.(—-1)"1+...+an-\_1(—1)+a, = (an+ant2+An-4+.:-:.  
...) — (an-1 + An-3 + An-5+...) (mód. 11), por tanto r es divisible por 11 si y sólo si  
la diferencia entre la suma de las cifras que ocupan lugares impares (contando desde las  
  
unidades) y la suma de las cifras que ocupan lugares pares, es un múltiplo de 11..  
Seguidamente haremos un par de observaciones que puede ser útil tener en cuenta  
  
para resolver algunos problemas.  
  
e Todo cuadrado perfecto es de la forma 4k ó de la forma 4k + 1; asimismo, es de una de  
las formas 8k, 8k + 1,8k +4. Escrito en términos de congruencias:  
  
= 0 (mo:d. 4) in es par,  
1 (mód. 4) <inesimpar.  
0 (mód. 8) <sin=0 (móád. 4),  
n?=4 (mód. 8) sin=2 (mód. 4),  
1 (mód. 8) si n es impar.  
  
\* Si consideramos una ecuación diofántica en dos variables, f(z, y) = 0, como 0 es divisible  
por cualquier entero m, para todo m > 0 se tiene que f(zx, y) = 0 (mód. m). Luego, si no  
a7  
Scanned by CamScanner  
  
  
--- Página 41 ---  
  
—  
— …...]=u-º..—%£.—,——;—-—-—.. \* -  
  
(mód. m) para todo m > 0, la ecuación diofántica  
  
y tales que f(z,y)= 0  
no tiene soluciones. (  
  
deremos la ecuación diofántica  
  
existen enteros %  
  
f(z,y) =0  
  
Por ejemplo, consi  
r? —8y? =3  
  
y probemos que no tiene soluciones. Tomemos m = 8: Entonces la congruencia x£? — 8y —  
\_3 = 0 (mód. 8) no tiene soluciones. En efecto, de lo contrario se tendría  
  
— AE=y-3=-355 0649  
  
y hemos visto que x? siempre es congruente con 0,1 64 módulo 8.  
- Otras propiedades importantes de las congruencias son las siguientes.  
  
8.8. ar = ay (mód. m) si y sólo si T.= y<mód.-—ín——- .  
- (a,m)  
  
8.9. Si ar = ay (mód. m) y (d,m)' =1, entonceé T= (mód\_ m)-  
\_,mk, éntonces 7 =Y (mód. m1), T = Y-  
  
8.10. Dados los enteros positivos m1,mg,;..  
.., kl  
  
(mód. ma), -- =I (mód. m¿) si y sólo si7 =y (mód. Im1-72--  
En efecto: \_  
  
8.8. ar = Y (mód. m) si y sólo si mi(az — ay): esto es, si y sólo si existe un entero 7 tal  
  
que mz = a(7 — y), lo cual ocurre.si y sólo si  
  
—  
  
(a,m)  
  
v  
  
I  
  
T-  
|  
  
=  
  
es decir, .  
  
y como <m, \_('fn\_1\_)' =1 (prop¡edad 3.3.), esto último sucede si Y sólo si \_(E% (,)  
  
o sea .  
. M  
v T =y(mod(a'm)>.  
  
Nota. A diferencia de otras pmpíedades de las congruencias qu  
nótese que ésta difiere de la que correspondería en las '1gua.ldades. No siempre $€ puede  
  
cancelar un factor común en ambos miembros de una congruencia. Por ejemplo, 37 =  
2 (mód. 3): 37 = 6 (mód. 8)  
  
e hemos demostrado,  
  
—  
  
(mód. 9) no es equivalente 2 7 = 2 (mód. 9):sí loesa7=  
es equivalente a 7 =2 (mód. 8)-  
  
8.9. Este es un caso particular de 8.8., cuando (a,m) = 1. Se usa con bastante frecuencia-  
  
28  
  
Scanned by CamScanner  
  
  
--- Página 42 ---  
  
8.10. Siz = y (mód. m;) para todo ¡ = 1,2,...,k, entonces r —y es un múltiplo común de  
  
M , M2,...,Mk y, de acuerdo con la propiedad 5.1., mi,ma,... »"JI(T — Y), luego z = y  
(mód. [m¡,m2,...,m¿]). ' |  
Reciprocamente, si 7 = y(mod.[m¡,mg,...,mk]), entonces [m, ma,...me]I(z — y), y  
  
comocada mil[m,, m2, .., 7+], de acuerdo con la propiedad 2.2. se tiene 7 = y (mód, m;)  
  
para ?=1,2,...k  
Ál principio de esta sección mencionamos que cualquier número entero es congruente  
  
con uno y sólo uno de los números 0,1,2,....m—1 módulo m. Siy =r (mód. m) se dice  
Que y es un resto de 7 módulo m, En general, se dice que un conjunto C = (71,72,.. -Zm)  
  
único entero 7 € C tal que y = 7; (mód. m). .  
Obviamente, (0,1,2,..., m— 1) esun sistema completo de restos módulo m y cualquier  
  
conjunto que se forme tomando un elemento de cada una de las m clases en las cuales  
  
quedan divididos los enteros al considerar los restos que se obtienen al realizar la división .  
  
Por m, es también un sistema completo de restos módulo m. 4  
Ejemplos de sistemas completos de restos módulo 7 son los siguientes:  
  
-(0,1,2,3,4,5,6),  
  
(7,8,9,10,11,12,13),  
— 17,15,22,3, \_3 5,13),  
| (—¿3,—2,—1,0,1,2,3).  
  
ejemplo, sj queremos saber cuál es el resto que resulta al dividir 737 entre 17, podemos  
»—2,—1,0,1,2, 3,4,5,6,7, 8) y proceder de.  
  
7 =(—1)= l(mód. 17),  
7 = 73 4 — 4(mód. 17),  
TT=7 7=47= 28 = 1(mód. 17),  
  
Y POr tanto, el resto buscado es 11,  
Ántes de introducir un Nuevo concepto, vamos a demosrar el siguiente teorema.  
  
8.11. Siz=y (mód. m), entonces (7,m) = (y, m).  
  
En efecto, si y = Y (mód. m), entonces mi(z — Y), luego existe un entero z  
7 —y = mz. Ahora bien, de esta igualdad se desprende que (7, m)|y, luego (7,m)I(y, m) y  
En Consecuencia (z, M) < (y,m). De la misma manera (Y,mM)I7, por tanto (y,m)l(::,m) y  
se tiene (y, m) < (7,m). Por consiguiente, (7,m) = (y, m).  
  
tal que  
  
39  
  
Scanned by CamScanner  
  
  
--- Página 43 ---  
  
Ahora definimos un sistema reducido de restos módulo m como un conjunto R =  
= (1 22-..T ) tal que para cualquier número entero y primo con m existe un único  
entero 7; E R tal que Y = 7i (mód. m).  
  
De acuerdo con el teorema anterior, un sistema reducido de restos módulo m puede  
obtenerse a partir de un sistema completo de restos módulo m, eliminando de este último  
aquellos enteros que no son primos con m. Por ejemplo, un sistema reducido de restos  
  
“ módulo 8 es: (1,3,5,7). Ótro sería: (—-3,—1,1,3).  
  
Además, si se tienen dos sistemas reducidos de restos módulo m, R y R', cada elemento  
de R es congruente módulo m con un único elemento de R', y viceversa. Por consiguiente,  
todos los sistemas reducidos de restos módulo m tienen el mismo número de elementos. -A  
este número se le llama Indicador de Euler y se le denota por é(m).  
  
Dado que los elementos de un sistema reducido de restos módulo m pueden obtenerse a  
partir del sistema completo de restos módulo m formado por los números 1,2,..., m—1,m,  
é(m) indica el número de enteros positivos menores o iguales que m que son primos con m.  
Por ejemplo, $(7) = 6, 6(8) = 4, $(10) = 4. En particular, nótese que si m es un número  
primo entonces é(m) = M — 1. Más adelante regresaremos con el indicador de Euler.  
  
Para finalizar esta sección, demostraremos el siguiente resultado.  
  
8.12. Si XY = [I¡,12,...,xk)\_es un sistema completo (reducido) de restos módulo m y  
(a,m) = 1, entonces aX = fazr1,0T2,...,0T k) es también un sistema completo (reducido)  
de restos de módulo m. - » '  
  
En efecto, como X y aX tienen el mismo número de elementos, bastará demostrar  
que ar; £ ar; (mód. m)sii 75j para todo par de elementos de aX. Pero como (a,m) =1,  
esto se desprende inmediatamente de la propiedad 8.9. \_  
  
Problemas.  
  
:8.1. Escribir una congruencia que sea equivalente al par de congruencias  
  
M  
  
U  
  
1(mái. 4), T 2(mód.3).  
  
8.2. Expresando los números enteros en el sistema de numeración de base 100, dedúcif el  
criterio de divisibilidad por 101.  
  
8.3. Exprésando los números enteros en el sistema de numeración de base 1000, deducir  
los criterios de divisibilidad por 7, 13, 37.  
  
8.4. Demostrar que, si m > , entonces (12,2?,...,m?) no es un sistema completo de  
restos módulo m.  
  
= 8.5. Sean a, b, c, d cuatro enteros. Probar que el producto de las seis diferencias  
b—a,c—a,d—a,d—-c,d—b,c—-b,  
es divisible por 12.  
  
40  
  
Scanned by CamScanner  
  
  
--- Página 44 ---  
  
ZE N NZ  
  
8.6. Si p es un primo tal que p = 22+y =0+ bz donde z, y, a, b son números primos  
  
tales que 7 > y,0> b, demostrar que z =a,y=b.  
  
7 8.7. Si a1, a, ... , An SON enteros y p es un número primo, entonces  
  
(a1 + a7 +...+a1) = af+a;+...af,(mód. p)-  
y 8.8. Demostrar que para todo entero positivo n,  
z:—-1)|[a: (:z:—)—1]  
  
8.9. Sea d un entero posxt1vo d15tmto de 2 36 13 Demostra.r que pueden ha.lla.rse dos  
.. números diferentes a y b pertenecientes al conjunto [2 5,13, d) tales que áb — 1 no es  
un cuadrado perfecto. |  
  
8.10. Si S(n) es la suma de las cifras del entero n escrito en base decimal, entonces  
S(48917) — S(1984n)  
- -- es siempre múltiplo de 9. \_A  
  
8.11. Si a,m,n son enteros positivos, con m % n, entonces  
si a es par,  
  
(cºm—!-l,a2-n+l)=íl' a ,  
2 si a es Impar.  
  
7  
  
8.12. Las longitudes de los ca:et0s y de la hipotenusa de un triángulo rectángulo son a, b,c  
respectivamente. a,b y c son números enteros y c no es divisible por 5. Demostrar  
que el érea del triángu:o es múltiplo de 10.  
  
8.13. Dados los 2k números  
  
donde k > 1, demostrar <::e al menos uno de estos números es múltiplo de 2k +1.  
  
8.14. Tomemos la sucesión de los cuadrados perfectos y sumemos 100 a cada término para  
formar la sucesión '  
  
101,104,109,116,125,136, 149,.  
  
Sea d, el máximo común divisor del n-simo término y del (n + 1)—es¡mo término de  
esta sucesión. ¿Cuál es el mayor valor que puede tener dn?  
  
41  
  
Scanned by CamScanner  
  
  
--- Página 45 ---  
  
SECCION 9  
  
— LA ECUACION x?+y?=z2  
  
Antes de proseguir con nuestro estudio de las congruencias, vamos a resolver uno de  
los problemas más antiguos de la teoría de números, que ya mencionamos al inicio de estas  
notas: hallar todos los triángulos rectángulos cuyos lados son enteros. Esto es, hallar todas  
las soluciones enteras de la ecuación:  
  
T+y=2  
  
Haremos algunos comentarios previos. ' . ..  
  
Se dice que un conjunto de tres enteros (7,y, z) tales que 77 + y? = 2?, es un triple  
pitagórico. Vamos a obviar el caso trivial en donde 7 = y =2 = 0. Además, si (7, y, z) es un  
triple pitagórico, también lo son todas las ternas (+7, +y, +z), luego podemos concretarnos  
a estudiar el caso en que z, y, 7 son enteros positivos.  
  
Por otra parte, si (7,y,z) es un triple pitagórico, para cualquier entero k se tiene  
que (zk, yk, zk) estambién un triple pitágórico, luego para resolver la ecuación podemos  
limitarnos a encontrar todos los triples pitagóricos (, Y, 2) que sean primos entre sí (más  
aún, serán primos .dos a dos ya que si d es un divisor común de dos de los enteros T, y, z,  
de la igualdad 7? + y? — 2? se desprende que lo será también del tercero). Una solución  
de la ecuación 7? + y? = 2? en la cual z, y, z son primos dos a dos es llamada una solución  
primitiva y el triángulo rectángulo correspondiente es un-triángulo primitivo. Por ejemplo,  
  
(3,4,5)  
  
es una solución primitiva de la ecuación por cuanto 3, 4 y 5 son primos dos a dos y 3?+4? —  
= 5?. Para cualquier entero £, (3k,4k,5k) es también una solución de 1? + y = 2?. Por  
ejemplo, (6,8,10),(9.12,15),(12,16.20), (15, 20, 25), ... son soluciones que se desprenden  
de la solución primitiva (3,4,5). \_ — v  
  
Además, observemos que en la ecuación r? + y? = 2\*, r,y no pueden tener la misma  
paridad. En efecto, si (7, y) = 1, entonces no pueden ser ambos pares. Por otra parte, si  
suponemos que ambos son impares se tiene:  
  
7 = 1(mód. 4),  
y = 1(mód. 4),  
  
de donde resulta que z? = 2(mód. 4), lo cual sabemos no es posible. Supondremos, sin  
pérdida de generalidad, que 7 es impar e y es par.  
  
Hechas estas consideraciones, pocedamos a hallar todas las soluciones primitivas de  
T +y=2? Se tiene:  
  
y2 = 22 — 121  
de donde  
y =(2+ rT (z — z)  
42  
  
Scanned by CamScanner  
  
  
--- Página 46 ---  
  
Dividiendo ambos miembros por 4 se tiene,  
  
y 2\_ Z+r Z2—r  
2/ l3 2  
(obsérvese que z + z y z — z son pares). Además,  
  
(z+z z—z)lz+z 2—T  
  
— )— +  
  
22 2 2  
  
=z,  
  
=,  
  
Z+T 2— Z+r z—\*a:'  
279 \_  
  
2 .2  
  
\_pór tanto se concluye que  
  
Z+I 2—r \_i |  
  
y como el producto ( z ; :z:> - ( z ; z) es un cuadrádó\_\_ perfé¿to, cada uno de estos dos  
  
factores debe ser un cuadrado perfecto. Escribamos: - 1-  
que m > n > 0; además (m,n) =1 y, al resolver el sistema  
  
z Z—r —  
= m?, 5= n?. Observemos  
  
Z+z 2  
  
()  
  
)  
  
se tiene que 7 = m? — nz=m?2+n?, Reemplazando en Y = 2? — 2? nos queda . Ñ  
2 2 22 2\_ 212  
y = (m+%)\* — (m? - n?)2,  
  
y2 — 4m2n2,  
  
Finalmente, observemos que si m y n fuesen de la misma paridad, de las igualdades  
T=m?-—n?, 2=m? in?se tendría que z,z son ambos pares, contradiciendo el hecho  
que (7,z) = 1, -  
  
Recíprocamente, es fácil verificar que los tres números 7 = m? — n?, y = 2mn,  
z2=m?+n? satisfacen la ecuación pitagórica 7? + y =z?, por tanto, tenemos el siguiente  
resultado.  
  
9.1. Todas las soluciones primitivas positivas de la ecuación r? + y? = 2?, donde z es  
"mMpar e y es par, vienen dadas por:  
  
I= mº—nº,  
y = 2mn,  
43 \_  
  
Scanned by CamScanner  
  
  
--- Página 47 ---  
  
»-=\*¡º¡¡“¿.»  
ME  
  
donde m y n son enteros arb1tranos que satisfacen las tres condiciones s¡g…entes  
  
a)m>n> 0,  
b)(m,n) =1,  
C) M y n tienen d13tmta paridad.  
  
Veamos algunos ejemplos:  
  
\* Sim=2yn=1, se tiene  
7=2 \_77 3,  
y =\_2.2.1¿ = 4,  
luego m =2 y n =1 dan origen a la solpción Apr1mítiyva (3,4,5).  
  
\*Sim=3yn=2, entonces  
  
m=Iiyn=2 danorigen a la solución primitiva (5,12,13).  
  
\*Sim=4yn= 1, entonces  
  
T=4?-12=15, -  
y=2.4.1=8,  
=4?412-— 17  
  
m=4yn=1 dan origen a la solución primitiva (15,8 17)  
  
Problemas.  
  
.9.1. Hallar todos los triples pitaguricos cuyos términos forman una progresión aritmética.  
  
. 1 1 1  
9.2. Si z,y, z son enteros tales que —7 \* 7 = —, entonces (7,y) > 1.  
z y 2?  
  
9.3. Siz,y, z son enteros tales que 7? + y? — ?, entonces Tyz es múltiplo de 60.  
9.4. Si a > 3 entonces existe un triángulo pitagórico cuyo cateto mide a.  
9.5. Hallar todos los triángulos p1tagoncos cuyo perímetro mide 60.  
  
9.6. Resolver la ecuación diofántica  
  
5z? + 10zy + 10y? = ? +2z+1.  
  
9.7. Hallar todos los triángulos pitagóricos cuya área es igual a 120.  
  
44  
  
Scanned by CamScanner  
  
  
--- Página 48 ---  
  
SECCION 10  
  
LAS CONGRUENCIAS DE EULER, FERMAT Y WILSON  
  
En esta sección estableceremos tres congruencias que, además de tener interés histó—  
rico, son bastante útiles para resolver diversos problemas en teoría de números. Comen-  
  
zaremos probando el:  
  
10.1. Teorema de Euler. Si (a,m) = 1, entonces a(”) = 1 (mód. m), donde 4(m) es  
el indicador de Euler. — . — v " -  
\_ En efecto, consideremos un sistema reducido de restos módulo m : R = [71,27,...  
... Zó(m)). Entonces, como (a,m) = 1, el conjunto aR = [ar¡,azz,...... y AZ ¿(m)) es  
también un sistema reducido de restos módulo m (propiedad 8.12.). Por consiguiente, a  
cada z; € R le corresponde un y sólo un az ¿ € aR tal que  
  
T¡;=ar; (mód. m).  
  
Además, a elementos diferentes de R les corresponderán elementos diferentes de aR, -- -  
por tanto ar¡,az»,...,aT¿(m) son congruentes con Z1,T2,...,Tó(m) Módulo m (no nece- ...  
sariamente en ese orden). 'Luego,  
  
(az1)(az72)...(azo(m)) = 7172...Z4(m) \_(mód. m),  
  
y como (7172... Zó(m), M) = 1, de acuerdo con la propiedad 8.9. se tiene:  
  
a) =1 (mód. m),  
  
conforme se quería demostrar. N  
Dado que, si m es primo entonces é$(m) = m — 1, el siguiente resultado se desprende  
  
inmediatamene como un corolario del teorema de Euler.  
10.2. Teorema de Fermat. Si p es un primo tal que p a, entonces  
al=1 - (mód. p).  
  
Á veces, éste se llama “pequeño teorema de F ermat”, para diferenciarlo del “último teorema  
  
de Fermat”,  
Una aplicación típica del teorema de Fermat es la siguiente.  
  
\* Calcular el resto que resulta al dividir 2199! entre 11.  
Como 11 es un primo y 11 1? se tiene: ,  
  
2'%E1 (mód. 11).  
  
45  
  
Scanned by CamScanner  
  
  
--- Página 49 ---  
  
Ahora bien, 1991 = 10.199 +1, luego  
. 21991 = (210)199.2 = 1199¡2 =2 (mód 11),  
  
por consiguiente, el resto buscado es 2. |  
  
Al teorema de Fermat se le puede dar otra forma, multiplicando ambos miembros de  
la congruencia a?-1 =1 (mód. p) por a. Se tiene entonces la congruencia:  
  
a?=a (mód. p),  
la cual se cumple para todos los valores enteros de a, por cuanto también es cierta si pla.  
  
Del teorema de Euler se deduce también el siguiente resultado.  
  
Si (a,m) = 1, entonces la congruencia az = b (mód. m) tiene una solución 7 = r 1.  
En efecto, basta tomar  
TI = aó('")\_1b.  
  
Además, si 7 es la solución general de az = b (mód. m), se tiene:  
ar—ar¡ =b-—b (mód. m),  
a(z—7,)=0 (mód. m)  
y como (a,m) = 1, - - |  
T=Tj, (mód. m),  
  
por consiguiente, 7 = T1 + km donde k es un entero. Además, la propiedad 8.7. garantiza -  
  
que, para todo entero k, 7 = 71 + km es-una solución de la congruencia az = b (mód. m).  
En conclusión:  
  
10.3. Si (a,m) = 1, entonces az = b (mód. m) tiene una solución \* = rj. Todas las  
soluciones de la congruencia vienen dadas por T = T1 + \*m, donci-= L E S. -  
Veamos un ejemplo.  
  
e Resolver la congruencia 57 =2 (mód. 7). -  
Como (5,7) = 1, la congruencia tiene una solución particular T| = 597)-1,2 = 552 y  
  
la solución general viene dada por z = 55.2 + 7k donde k € Z. -  
Usualmente resulta más práctico, cuando el módulo 'es un número pequeño, hallar la  
  
solución particular por simple inspección. En el ejemplo anterior, si tomamos el siguiente  
sistema completo de restos módulo 7: —  
  
, — (-3,-2,-1,0,1,2,3),  
  
se verifica fácilmente que r = —1 es una- solución particular.  
A continuación vamos a probar el:  
  
10.4. Teorema de Wilson. Si p es un primo, entonces  
(P-1)!=-1 (mód. ).  
46  
  
Scanned by CamScanner  
  
  
--- Página 50 ---  
  
Sip=2óp=3, entonces la congruencia se verifica inmediatamente. Supongamos  
  
que p > 5.  
Antes de hacer la demostración formal, vamos a dar un ejemplo que ilustra la idea en  
  
la cual se apoya aquella. Tomemos p = 11 y procuremos agrupar los números 2,3, 4, 5,  
6, 7, 8 y 9 en parejas de manera que el producto de los dos elementos de cada pareja sea  
congruente con 1 módulo 11. Se tiene:  
  
26=1" (mód. 11),  
34=1 (mód. 11),  
59=1 (mód. 11),  
  
— T8=1 (méd.11), ...  
  
y ademá$,  
110=-1 (mód. 11).  
  
Multiplicá.ndo miembro a míez\_nbró estas congruencias nos queda  
10!=—1 (mod 11)  
  
Ahora bien, si-en general j es un entero tal que 1<j < P— 1 entonces (, p) = 1  
y por consiguiente, según 10.3., la congruencia 2 =1 (mód. p) t1ene solución y existe  
exactamente una solución z tal que O< 1r <p—1. Eudentemente ? = 0, luego teremos  
l<r:<p—1. - -  
  
S1 a cada j le asignamos el ¿ correspondiente, como ij =ji =1 (mód. p) podemos' .  
obser\*—ar que j es el entero asociado con 1. Observamo: además que -  
  
l1=1 (mód. p),  
(P—-1)\*=1 (mód. p),  
  
luego 1 y p — 1 se asocian con ellos mismos. Consideremos los casos en que 2 < j <p—2.  
  
Para estos enteros se tiene ,  
— 17)=1 y  
  
(7+1,7)=1,  
por consiguiente (? — 1,p) = 1 y entonces  
Él (mód.p).  
  
Luego, todo j tal que 2 < j < p — 2 está asociado con un tal quei Xj y 2<1<  
< p—2. Por tanto, los enteros 2,3,...,p — 2 pueden ser asociados en parejas (1,7) tales ...  
que jP=1 (mód. p). Multiplicando miembro a miembro estas congruencias nos queda  
  
2.3...(P—-2)=1 (mód. p)  
  
y como  
l(p—-1)=-1 (mód.p)  
  
47  
  
4l  
  
Scanned by CamScanner  
  
  
--- Página 51 ---  
  
se deduce ' '  
(p-I)!'=-1 (mód. p).  
Los teoremas de Wilson y Fermat puéden usarse para resolver un tipo particular de  
congruericias cuadráticas, como veremos en el siguiente resultado.  
10.5. Si p es un primo, la congruencia z2=-1 (mód. p) tiene soluciones si y 'sólo si  
p-1 |  
2  
  
p=26p=1 (mód. 4).Sip=1 (mód. 4), entonces y =( ! es una solución.  
  
En efecto, si p = 2 se tiene la solución 7 = 1. Supongamos que p es un primo impar y  
supongamos además que. '  
  
2=—1 (mód. p) para algún TEZ.  
  
Entonces,  
5= (.'1:2)L;—l = (—1)%1 (mód. p).  
Por otra parte, de acuerdo con el teorema de Fermat,  
  
T7 1=1 (mód. p)  
  
ya que p /z. Luego,  
  
1=(-1)7" (mód.p),  
[1'— (-1)L5¿].  
  
, p—1 . P— .  
Sil—(-1) 7 0, entonces necesariamente 1 — (—1) 7 =?, lo que contradice el hecho  
. de ser p impar. Por tanto, |  
  
P  
  
1-(-1)7 =,  
  
P—l  
  
2 NL  
  
41(7— 1),  
  
pEl (mód. 4).  
  
Recíprocamente, supongamos que p =1 (mód. 4). Se tiene  
  
(P-D)1=12... ... (p-2p-1)  
1  
  
=1.2...p;1.(p—1)(p—-2)...p  
  
+  
  
|l0  
  
1  
  
\_=\_1.2...p;1.(-1).(—2)...<\_P  
  
1e  
D  
  
(mód. p)-  
  
48  
  
Scanned by CamScanner  
  
  
--- Página 52 ---  
  
Luego, |  
\_ \_ 2  
(p-1)!=(- 1)'1' 12,2?., ( 2 1) E(l.2. .. p\_2\_1\_> (mód. P),  
  
yaquep=1 (mod. 4).  
Por otra parte, el teorema de Wilson garantiza que  
  
(p-1)!= \_,-1 (mód¿ P),  
  
por tanto, si tomamos T=1.2... PT T)' se tiene  
  
T=l (mód. p).  
  
Este resultado puede ser útil en algunos ejercicios, como en el 51gmente ejemplo  
  
E Probar que la ecuación d10fant1ca z72+1= 23y no t1ene soluc1ones  
— Siz?+1= 23y, enitonces oe  
  
23/(2? +1),  
luego,  
pero 23 es un primo de la forma dE + 3 luego no existe ningún entero 7 tal que 2? =  
=—1 (mód. 23). | '  
Problemas.  
  
-10.1. Probar que n!? — a? es divisible por 91 si (n,91) = (a,91) =1.  
\* 10.2. Probar que, para todo entero n, n" —n es divisible por 42.  
-10.3. Probar que 19 Má4n? + 4) para ningún entero n. |  
10.4. Probar que un entero m > 1 es primo si y sólo si  
mil(m — 1)! + 1).  
  
\* 1  
10.5. Probar que, para todo entero n, 3n5 + 51-n3 + 1—75-n es entero.  
  
10.6. Probar que, si p es un primo, entonces  
  
(P-1)!=p-1 (móád. 1+2+...+[p—1)).  
  
49  
  
Scanned by CamScanner  
  
  
--- Página 53 ---  
  
10.7. Si p es un primo impar, entonces: -  
a) 22.42.0%...(p— 1? =(-1)F" (mód. p).  
b) 1237...(p-2)?=(-1)F (mód.).  
  
10.8. Si p es un primo diferente de 2 y de 5, entonces p divide a infinitos enteros de la forma. ;  
  
9, 99, 999, 9999, . Asimismo, p divide a infinitos enteros de la forma 1, 11, 111,  
1111,  
  
- 10.9. Sean a, b,c enteros consecut1vos donde b es un cubo perfecto. Demostrar que abc es  
dnns1ble por 504 — .  
  
- 10.10. Para cualquier entero positivo n,  
1\*+2721+3"44"  
es divisible por 5 si y sólo si n no es divisible por 4.  
  
10.11. Hallar todas las sóluciones de la ecuación  
  
31¡\_5m=4  
  
e  
  
para n,m enteros positivos.  
  
/  
  
10.12. Demostrar que, para todo srimo p, existen infinitos enteros positivos n tales que 2? —n  
es divisiLie por p. -  
  
10.13. Demostrar que el productu de los primeros n enteros positivos, n > 1, es divisible por \*  
su suma si y sólo si n + 1 no es primo.  
  
50  
  
Scanned by CamScanner  
  
  
--- Página 54 ---  
  
SECCION 11  
  
RESOLUCION DE CONGRUENCIAS  
Supongamos que se tiene un polinomio de coeficientes enteros:  
r) =aor" +a,r" 11, + an\_ 1T + an.  
  
Si Zo es un número entero tal que, dado un entero positivo m, f(70) =0 (mód. m),  
entonces se dice que zj es una solución de la congruencia f(7) =0 (mód¿ m). . .  
  
Recordemos que si a, b son dos enteros tales que a = b (mód. m), entonces -  
Sa) = f(b) (mód. m) (propiedad 8.7.), lúego si a es una solución de la congruencia  
S(z) = 0 (mód.- m); entonces b también lo es. De acuerdo con esto, si la congruencia  
S(z)=0 (mód. m) admite una solución 70, entonces admite infinitas soluciones (todos  
los enteros congruentes con 70 módulo m). No obstante, se considera que dos soluciones  
son distintas si y sólo si no son congruentes entre sí módulo m. Esta consideración per-  
mite definir el número de soluciones de la congruencia f(7)-= 0 (mód. m) como el  
- número de enteros de un sistema completo de restos módulo m : [71,T2,.: -,Tm) tales que  
  
Por ejemplo:  
  
\* Resolver la congruencia 75 +7+1=0 (mód. 7). \_  
' Si tomamos el sistema completo de restos módulo E—  
  
(-3,—2,—1,0,1,2,3),  
  
observamos que los enteros -3 y ? satisfacen la congruencia y sólo ellos. Luego, la con-—  
gruencia tiene dos soluciones, a saber: 7 = 3 (mód. Józ =2 (mód. 7). .  
  
Por otra parte, obsérvese que si 70 es una solución de la congruencia f(7) = 0 (mód.  
m) y si d es un entero positivo tal que dim, entonces z) es también una solución de la  
congruencia f(z) =0 (mód. d). En efecto, si  
  
entonces «  
  
mffy($º)  
  
y como dim se tiene:  
  
dlf($o)  
  
de donde se concluye que fz0)=0 (mód. d).  
  
Si f(z) = agr" + arreit,..+ An-17 + An, Y a É O (mód. m), se dice n es el  
grado de la congruencia S(z) =0 (mód. m). Ahora bien, si ao = 0 (mód. m) y k es  
el menor entero positivo tal que a £ 0 (mód. m), entonces el grado de la congruencia  
S(z)=0 (mód. m) es n — k. Si todos los a;(?=0,1,...,7) son múltiplos de m, entonces  
no se le asigna grado a la congruencia. -  
  
ól  
  
Scanned by CamScanner  
  
  
--- Página 55 ---  
  
De acuerdo con esta definición, nótese que el grado de la congruencia f(7) = 0 (mód. -  
m) no necesariamente coincide con el grado de la ecuación f(z) = 0.:De hecho, el grado  
de la congruencia depende del módulo. Por ejemplo:  
  
87 +3r+1=0 (mód. 4) tiene grado 1;  
87 +37+1=0 (mód. 5) tiene grado 3.  
  
Para congruencias de grado mayor que 1, no se conocen métodos generales de re-  
solución. En esta sección nos limitaremos al estudio de congruencias de primer grado.  
  
11.1. Congruencias de Primer Grado. Toda congruencia de grado 1 puede ser escrita  
en la forma az =b (mód. m), dondea 20 (mód. m). Podemos considerar dos casos:  
  
a) (a, m) = 1. En este caso ya hemos visto, como consecuencia del teorema de Euler,  
que la congruencia az =b (mód. m) tiene una solución única módulo m; ésta es:  
  
7 =a")-15 (mód. m):  
  
b) (a,m) = d > 1. Si 20 es una solución de az = b (mód. m), se tiene que 7 es  
también una solución de az = b (mód. d), luego azo = b (mód. d) y, como azo = 0 (mód.  
d), entonces necesariamente b = 0 (mód. d). Por consiguiente, si d b se puede garantizar  
que la congruencia ar = b (mód. m) no tiene soluciones.  
  
Supongamos que d|b. Entonces existe un entero zo-tal que azo = b (mód. m) si y sólo  
  
. a , m . .. , . , m — 2 m  
la congruencia = mód. T tiene solución única módulo T Sea 7 = T1 | mód. F  
C  
  
tal solución. Entonces, las soluciones de ar = b(mód. m) son aquellos enteros 7q tales que  
  
d .  
  
Si asignamos a K los valores 0,1,...,d — 1, entonces .-; toma d valores que no son  
congruentes entre sí, dos a dos, módulo m. Además, si se le asigna a k cualquier otro valor  
entero, el 70 resultante será congruente módulo m con alguno de los d anteriores, luego la  
- congruencia a7 = b (mód. m) tiene exactamente d soluciones.  
  
Veamos dos ejemplos.  
  
a m . . m .-  
T0 =T1 (mod. ——); es decir, .. =7| +« T dede kEeZz.  
  
o Resolver la congruencia 167 = 10 (mód. 4).  
Se tiene (16,4) = 4. Como 4 /10, la congruencia no tiene soluciones.  
  
\* Resolver la congruencia 167 = 10 (mód. 10).  
  
(16,10 ) = 2. Como 2|4, la congruencia tiene dos soluciones.  
Debemos resolver: 87 = 2 (mód. 5).  
  
Por inspección en un sistema completo de restos módulo 5 se observa que esta última -  
congruencia tiene la solución:  
  
T=4 (mód. 5),  
  
52  
  
Scanned by CamScanner  
  
  
--- Página 56 ---  
  
ITO ia si auraic ia N  
“ PA EE ei  
  
AE  
  
luego las soluciones de 167 = 4 (mód. 10) vienen dadas por los enteros: 70 = 4+5k. Dam?o  
a k los valores 0 y 1 (por cuanto d = 2) se tiene que las dos soluciones de la congruencia  
son 7 =4 (mód. 10) y 7 = 9 (mód. 10). ,  
  
Cuando el módulo es pequeño, es fácil encontrar la solución de la congruencia, como  
en el ejemplo anterior. Si el valor de m es grande, este proced.ímien¡to puede no fegultax  
práctico; en este caso obsérvese que resolver la congruencia az = b (mód. rn) es equa.lente'  
a resolver la ecuación diofántica az — b = my, y restringir nuestra atención a lo? vlalo\_res:  
de z. En el ejemplo anterior, si resolvemos por el método usual la ecuación diofántica  
87 — 5y = 2, obtendremos los mismos valores para z.  
  
Si el módulo m es un número compuesto, m = PI'p?...pe", de a.;\_:uerd9\_ cc\_nfi la '  
propiedad 8.10. resolver la congruencia az = b (mód. “m) es equíyz\_¡.ler\_1\_t; g::ggplyez:-,g12\_ .  
  
- sistema de congruencias: -  
  
ar=b (mód. p?\*),  
  
az=b (mód. p;\*),  
donde los números py', p2?,..., p£”. son menores que m y, por tanto, los cálculos se. pueden  
facilitar. Hay varias formas de resolver un sistema como el anterior. El siguiente resul-  
- tado nos garantiza que, efectivamente, un sistema de congruencias como el anterior tiene  
soluciones comunes y nos brinda un método para hallarlas. \_  
  
11.2. Teorema Chino del Resto. Consideremos E enteros positivos m1,M2,...,Mí  
  
primos dos a dos. Las congruencias -  
  
z =ay (mód.m;),  
7=ax (mód.m.),  
  
tienen soluciones comunes. Dos soluciones cualesquiera son congruentes entre sí módulo  
  
m¡mg...m¡,. ,  
En efecto, si j = 1,2 k "- m  
AJ T5 Y M = MiMz...m,, entonces — es un entero tal que  
j  
  
(m—¡'m = 1. Por consiguiente, la congruencia —7 =1 (mód. m;) tiene una solución  
m:  
Además, si i £ j entonces m; £, luego,  
mj  
a AP  
m—¡' j = 1 (mod m¡),  
AA , o  
m—j,—=0 (mód. m;)si7 A j.  
  
53  
  
Scanned by CamScanner  
  
  
--- Página 57 ---  
  
EAO NEÉ  
  
Consideremos:  
  
m m m  
0= — b10 + — 1a7 +...+ — braks.  
M moz Mk  
m , . . .  
Entonces, 70 = ——bia; (mód. m;) para todo ¡ = 1,...,k, es decir, Zg es una solución  
— v  
  
común del sistema de congruencias. Además, la propiedad 8.10. garantiza que si zj es  
otra solución común de las congruencias, entonces z0 = z1 (mód. mim2...mx).  
  
Veamos a continuación dos e jemplos.  
— e Hallar todos los enteros que dejan restos 1,2,3 cuando se dividen por 3,4 y 5 respecti-  
  
— vamente.. ... - o  
Se requiere resolver el sistema:  
  
T=l (mód. 3),  
T=2 (mód. 4),  
T=3 (mód. 5).  
  
-De acuerdo con la notación que se ha utilizado, se tiene:  
aj = 1,a2 =2,a3 = 3,  
  
m =3,m7 = 4,m; = 5,m = 60,  
  
m - m . m  
— =20, — =15, — =12.  
M1 mz2 3  
  
En las expresiones ;b,— =1 (mód. m;) determinamos valores particulares para b;, b, y  
  
b; : .  
2001 =1 (mód. 3) — di = —1,  
1557 =1 (mód. 4) — 6, = —1,  
12b3 =1 (mód. 5) — b, = —2.  
Por tanto,  
  
70 = 20.(—1).1+15.(—1).2+12.(-2).3 = -20 - 30- 72 = —122 = —2 (mód. 60).  
  
7 = —2(mód. 60).  
\* Hallar todos los enteros que dejan restos 2 ó 3 cuando se dividen por 4,567.  
Se trata de hallar todos los enteros z tales que, simultáneamente:  
íz52 ()mód. 4) í2:52 (mód. 5) í:c52 (mód. 7)  
) 5 ()  
  
o)  
7=3 (mód.4), [ 7=3 (mód. 5), |r=3 (mód. 7).  
  
54  
Scanned by CamScanner  
  
  
--- Página 58 ---  
  
r  
k  
  
Entonces: m¡ = 4, m7 = 5,m3  
  
mi  
  
— =35, " =28, 7 =20,  
maz2 m  
  
3  
  
— 356 =1 (mód. 4) — b = —1,  
28¿2 =l (mód 5) = bg = 2,  
2007 =1 (mód. 7) — b; = —1.  
rT = —dda; + 56a, — 20a;  
  
Como a1, az, a; pueden tomar los valores 263, se presenta.n ocho casos, los cua.les se  
  
resumen en la s1gmente tabla.  
  
aj a  
  
Problemas.  
  
11.1. ¿Para cuáles valores de r es (57 + 1(37 +?) divisible por 13?  
  
(mód. 140).  
  
az T(mód. 140)  
  
2 2 .2 2  
2 2. 3 18  
23 2 58  
2-3 3 38  
3 2 3 —53  
3 32 23  
3 3 3 3  
  
- —  
  
11.2. Hallar todos los enteros que dejan restos 1 ó 2 cuando se dividen por 3,4165.  
  
11.3. Resolver la congruencia z? -1 =0 (mód. 56).  
  
11.4. Resolver la congruencia 1'1:z: +1=0 (mód. 210).  
  
11.5. Resolver la congruencia 57? + 77 - 3 =0 (mód. 35).  
  
11.6. Si k > 0, entonces existen k enteros consecutivos,  
  
por un cuadrado mayor que 1,  
  
cada uno de los cuales es divisible  
  
Scanned by CamScanner  
  
  
--- Página 59 ---  
  
SECCION 12  
EL INDICADOR DE EULER  
  
- En la sección 8 hemos definido al indicador de Euler, $(m), como el número de ele-  
mentos de un sistema reducido de restos módulo m, y hemos visto que éste es el número  
de enteros positivos menores o iguales que m que son primos con m. -  
  
En la presente sección, con el auxilio del teorema chino del resto, deduciremos una  
fórmula que nos permitirá calcular directamente el valor de é(m). Para esto, establecemos  
el siguiente resultado previo.  
  
12.1. Sean m, ñ dos enteros positivos tales que (m,n) = 1. Entonces, é(mn) = Amáln).  
  
Nota. Toda función f : Z+ — C, donde C es el conjunto de los números complejos, se  
llama función aritmética. Se dice que una función aritmética es multiplicativa si, siempre  
que (m,n) = 1 se tiene f(mn) = f(m)f(n). 12.1 establece que la función que a cada  
m EZ le asigna é(m), es multiplicativa. |  
  
Para probar 12.1., supongamos que R = fr1,72,...,74(m)) es un sistema reducido de  
-restos módulo m y S = (s1,82, .. ., S6[n)) UN sistema reducido de restos módulo n. Si 7 es  
un entero que pertenece a un sistema reducido de restos módulo mn entonces (z,mn) =1  
y, por consiguiente, (7,m) = (7,n) = 1. Por tanto, existen r; € R y s; E S tales que  
  
=r (mód. m),  
7 =sj (mód. n).  
  
Por otra parte, de acuerdo con el teorema chino del resto, cada par (ri,s;¡) determina  
un único z módulo mn y, evidentemente, diferentes pares (7;,s;) determinan diferentes  
r mádulo mn. Ahora bien, hay exactamente ¿(m)ó(n) de tales pares, luego un sistema  
red:cido de resto: módulo m: «ontiene ól : “A(n) ele=: ntos, y se tiene: -  
  
élmn) = elms(n), —  
  
conforme se quería demostrar. |  
Es inmediato generalizar, por inducción, este resultado para cualquier número finito  
  
de enteros; es decir, si m1,M2, ...,M son enteros positivos primos dos a dos, se tiene:  
é(mim2...ma) = Almi)A(M2) ... BlMa).  
Por ejemplo, si queremos calcular 6(210) basta observar que 210 = 2.3.5.7. Entonces.  
  
e(210) = A(2)6(3)6(5)6(7) = 1.2.4.6 = 4S.  
  
Nótese que esta propiedad es válida sólo si los m; son primos dos a dos. Por ejemplo  
se tiene:  
  
d9)=6,  
  
56  
  
-  
7  
  
Scanned by CamScanner  
  
  
--- Página 60 ---  
  
pero  
- 6(3)8(3) =2.2 =4  
  
Evidentemente, ¿é(1) =  
  
1. Si n es un entero mayor que 1, entonces se verifica el  
siguiente resultado. :  
  
12.2. Sin = pr'p3?...py", entonces:  
  
é(n) = n(1— p—11) (1-¡%>( \_"i> T  
  
-En efecto, si n = prpg ; PR", como los P? son primos dos a dos se puede aplicar  
. el teorema 12.1., y se tiene:  
  
— An) = dlore(ps:)... A(per).  
  
Entonces, el problema se reduce a calc  
primo 'y a un entero  
positivos que son men  
los enteros menores oj  
Luego, entre 1 y p\* h  
  
ular. el valor de ¿(5  
positivo. .Para esto, notamos que- é( p"  
ores o iguales que p\*  
guales que p” exceptu  
ay exactamente p\*—1  
  
), donde p es un número \_  
) es el número de enteros .  
  
y, a la vez, primos con p”. Estos son todos - \*  
ando los múltiplos de P:P,2p,3p,..., p 1p,  
múltiplos de p y, en consecuencia:  
() =pE \_ na-1\_ .a \_l  
  
é) =p"-p=1=>p (1 p>-  
  
Por consiguiente,  
  
1N 1 1  
ó(n)=pº\*(l——)pºº(l——>... º\*(1\_\_>=  
' P1/” P? e, Dk  
a \_a a ' 1 1 \_  
=P lP z'--P h(l\_\_) (1——)(1—— =  
1 P? k AN D  
(-D6-D-(-)  
Pi P? DRJ  
  
conforme se quería demostrar,  
  
Por ejemplo, si queremos calcular 45(3600),r  
  
jen en primer lugar escribimos 3600 en su  
forma canónica. Se tiene:  
  
3600 = 232 52  
  
é(3600) = 3600./(1 - %) . (1 - 33) . (1 - 53)=  
  
Entonces,  
  
Scanned by CamScanner  
  
  
--- Página 61 ---  
  
e ANENO yeN y—  
  
Nota Frecuenteménte se usa la notación H para indicar el producto sobre todos los  
  
pIn  
primos que dividen a n. Si n, escrito ken su forma canónica, es n = porp? ...p\*, entonces  
Hp = pip? -- -PH S decir Hp = Hp¡. Utilizando esta notación en el teorema 12.2., se  
p| pÍn =1  
tiene:  
| 1  
  
pln  
  
“ También es corriente encontrar la not\_ación\_2 para indicar la suma sobre todos los divi-  
  
sores de n (sean estos primos o no). Por ejemplo,  
  
Zd=1+2+;+4+s+s+12+\_24='sd.  
  
Esta notación resultará útil en el siguiente teorema.  
  
12.3. S¡ n > 1, entonces Z A(d) =. \_ —  
din.  
Haremos la demostración por 1nducc1on sobre el número de factores primos de n. Si  
  
n = p” se tiene:  
  
Y. él a) = 6(1) + élp) + 617\*) +... + 615") =  
  
din  
=1+(p-1)+(9? -p)+...+(9 —p\*') =  
=pa —  
  
Supongamos que la propiedad es cierta para todos los enteros que tienen k o menos  
factores primos diferentes en su descomposición canónica y consideremos un entero m con  
k + 1 factores primos diferentes. Entonces  
  
m =np",  
  
donde p“ icl \_  
E P\* es uno de\_los factores que aparecen en la descomposición canónica de m, n tiene  
actores primos diferentes y (n, p”) =1.  
  
Obsérvese i yi  
ue 2 .\_.  
que si d es un divisor de n, entonces d, pd, p“d, ... , p“d son divisores de m;  
  
58  
  
Scanned by CamScanner  
  
  
--- Página 62 ---  
  
- por consiguiente, se puede escribir:  
  
Y\_ e(a) = Y d(d) + Y. lra) + Y> élr\*d) +... + Y> élp"d) =  
  
dim din d|n d|n din  
=2 () + rAA + Y Ao\*)b(a) +... + >|j MA =  
d|n din din din  
=Y A d)l1 + 9(p) + élp?) +... + dl =  
d|n  
= Z¿(d)[1 +(p— 1)+ (p —p)+ + (9% -P = |  
p =m.  
  
Por tanto, la propiedad es cierta para todo entero positivo n. Por ejemplo, los divisores  
positivos de 24 son: '  
- 1,2,3,4,6,8,12y 24  
  
y se tiene:  
ó(1) + é(2) + ó(3) + $(4) + 45(6) + é(8) + ó(lº) + ó(24)  
+1+2+2+2+41+4+8=24.  
  
Problemas.  
  
-12.1, Halla.r el número de enteros positivos menores o iguales que 3600 que tienen un factor  
comun con 3600.  
  
12.2. Si p es un número primo y n un entero positivo, entonces  
  
— | Pá(n) si p|n.  
np) = f(P — lé(n) sip .  
  
12.3. Si n|m, entonces é(nm) = nó(m).  
12.4. ¡¿Para cuáles valores de n es $() impar?  
  
12.5. ¿Para cuáles valores de n es  
2) 6(2n) = é(n),  
b) é(27) > é(n)?  
  
12.6. Probar que existen infinitos enteros n tales que  
  
3 7A(n).  
  
12.7. Hallar el número de ent  
  
200 eros positivos menores o iguales que 25200 que son primos con  
0.  
  
59  
  
+l  
  
Scanned by CamScanner  
  
  
--- Página 63 ---  
  
\* NN E  
NAN ENO ANE NAA -  
  
probar que el número de enteros positivos menores o  
  
k son enteros pqsi\_tivqs,  
que mk que son primos con m es ké(mM)-  
  
a. La función f definida por f(7) = N - (d)  
d|n  
  
12.8. Si my  
iguales  
  
12.9. Sea 9 una función aritmética multiplicativ  
  
para todo entero positivo , es también multiplicativa.  
  
12.10. Sea n > 1.Sin = pripy?...pe' en s forma canónica, entonces la suma de los  
  
divisores de n es: "  
p<11¡+1\_1 pgz+1\_l pt:¡.l\_1  
=l P—l pr—-1  
60  
  
Scanned by CamScanner  
  
  
--- Página 64 ---  
  
A PP E A c NO ,  
  
SOLUCIONES A LÓS PROBLEMAS PROPUESTOS  
  
Sección l1.  
  
11 .Z"!\_2 \_ n(n+ 1)6(2n + 1)\_  
  
Si n =1 se tiene: .  
12- 1.(1+1).(2.1+ 1),  
6  
lo cual obviamente es cierto.  
. Supongamos ahora que:  
  
lº+2º+3º+...\_3\_hº=”("+1)6(2n+1). | | (1)  
  
Debemos probar que: \_  
12422437177 +04 12 - CD +2)(ºn +3  
  
Sumando (n+1)? al primer nruembro de (1) y usando la hipótesis de 1nducc10n  
  
(1º+2º+...+nº')+(n+1)2 …+( n+1)?=  
  
= + 20 +1)+60+1 \_ (n+(2n+1) +6(1 + 1)  
=T AEA E en 1) + 60041  
  
\_ (n +1)(2n? + ?n + 6) (n+1)2(n+2)(n+ 2) (n+ 1)(n+º)(ºn+3)  
6 6 6  
  
12. z [n<n+l)]  
  
I=1  
  
Sin =1 se verifica:  
  
1= 1(1\_+1.). 2\_  
2  
Supongamos que:  
  
2  
| 1º+2º+33+...+n3=[w] .  
  
- (1)  
  
Debemos probar que:  
1+2+34...+(n+1) =[“("+1)("+º)]2  
> .  
  
61  
  
Scanned by CamScanner  
  
  
--- Página 65 ---  
  
Suma.ndó (n + 1)% a ambos miembros de (1) se tiene: \*  
  
2  
nn+1  
(1º+2º+33+...+n3)+(n+1)3=[—(-—2—2] +(n+1)\* =  
  
n2(n+1)?+4(n+1% \_ (n+ 1)2(n? +4n+4) \_ (n+1(n+2)? \_  
á 4 4  
  
=[(n+1)2(n+2)]º\_  
  
1.3. Í(2i =1) .  
  
1=1  
  
Si n = 1 se verifica:  
2-1=1?:  
  
Supongamos que:  
- 1+34+5+7+...+(2n-1)=7. (1)  
  
Debemos probar que:  
ad d+ 54 7+...+(2n—1)+(2n+1)=(n+1).  
Sumando (2n + 1) a ambos miembros de (1) se tiene:  
  
[1+3+5+7+...+(2n—1)]+(2n+1)=nº+(2n+1)=(n+1)'—'.  
  
1.4. Zn:i(i\_ +1)= %n(ñ + 1(n+2).  
  
i=1  
  
Si n = | se verifica:  
  
1  
12=-.1.2.3.  
3  
Supongamos que:  
1  
1.2+2.3+34+...+n(n+1)= -3-n(n+1)(n+2). (1)  
Debemos probar que:  
12+23+34+...+n(n+1)+(n+1)n+2)= %(n+1)(n+2)(n+3).  
62  
  
Scanned by CamScanner  
  
  
--- Página 66 ---  
  
Sumando (n + 1)(n + 2) a ambos miembros de (1) se tiene:  
  
[12+2.3+3.4+...+n(n+1)]+(n+1)(n+2)=  
  
= ¿nn +1)(0+2)+(n+1)0+2) =  
(n+1)(n+2)( n+1) =(n+1)(n+2)("—¿º) =  
  
= %(n + 1)(n + 2)(n +3). |  
  
Z(3 )= "6.  
  
Si n =1 se verifica: -  
  
. — 1(3-1)  
Súpoúgamos que: — — \_ “ : —  
| 1+4+7+10+.. +(3n 2) ¿(\_n2\_\_) |  
  
Debemos probar que:  
  
- (n + 1)(3n + º)  
  
1+4-7+10+...+(3n—2)+(3n+1)= 5  
  
Sumando (3n + 1) a ambos miembros de (1) se tiene:  
  
[1-1—4+7+.10+...+(3n—2)]+(3n+1)¿ n(3n2— 1)  
  
= — = =  
  
\_ n +D(n+3) \_ (n+1)(3n+2)  
2 2 -  
1.6. 2? > (n+1)? para todo entero n '> 3.  
Sin=3 'se verifica:  
2.37 > (3+1)?, por cuanto 18 > 16.  
Supongamos que, para un n > 3 se tiene:  
2n? > (n+1).  
  
63  
  
+n+1=  
  
(1)  
  
(1)  
  
Scanned by CamScanner  
  
  
--- Página 67 ---  
  
Debemos probar que: - o  
$ 2(n+1)?> (n+2Y. -  
En efecto: '  
2(n+1)? =2(n? +2n + 1) =2n?+4n+2,  
  
y tomando en cuenta (1):  
  
2An+1)> (n+1) +4n+2=n?2+2n+1+4n+2=  
n?+4n+4+2n-1=  
  
(n+2) +2n-1> (n+2).  
  
1,7. 2" > n? para todo entero n > 4.  
Si n = 5 se verifica: - .  
25 > 5? por cuanto 32 > 25.  
  
Supongamos que, para un n > 4 se tiene:  
n 2 s . . |  
2 >n (1)  
Debemos probar Qúe:  
De acuerdo con (1), y dado que 2"+1 = 2.2", se tiene:  
  
2n+l > 277.2,  
  
luego, bastará probar que:  
2n? > (n+1).  
  
En efecto, como n > 4 se tiene:  
  
de dónde:  
\_ n? > 2n+1,  
  
l2nº>nº+2n+l,  
2n? > (n+1).-  
  
1.8. El número de diagonales de un polígono de n lados es:  
  
n(n—3)'  
  
-  
  
Iniciemos la inducción con n = 3 (no hay polígonos con menor número de lados). En  
este caso:  
n(n —3) \_ 3.(3—3)  
2 2  
y efectivamente, un triángulo no tiene ninguna diagonal.  
  
=0,  
  
64  
  
Scanned by CamScanner  
  
  
--- Página 68 ---  
  
\* — Consideremos un polígono de n lados, ABCDEF ... , como se muestra en la figura,  
en donde la línea punteada representa los n — 5 lados restantes. Supongamos que este  
  
. \_ \_n(n—3) |  
polígono tiene 2  
  
lados.  
  
Si le añadimos un lado, como cuando formamos el polígono A\_PBCDEF , el mí1evo  
polígono tiene las diagonales del polígono anterior,. más el lado AB que ha pasado a ser -  
una nueva diagonal, más n — 2 diagonales que se origirian al unir el punto P con losn —2 \*  
vértices no adyacentes; por tanto, el polígono de n + 1 lados tiene: “. \* —  
  
n(n — 3) En-1= n(n—3)+2(n—l)'=  
  
2 2 .  
2\_\_9 — 2  
  
1.9. La suma de los ángulos interiores de un polígono de n lados es (n — 2)7.  
  
Al igual que en el problema 1.8., iniciamos la inducción con n = 3. En este caso, la  
suma de los ángulos interiores de un triángulo es justamente (3—2)7 = . Consideremos la  
misma figura utilizada en el problema 1.8. Si la suma de los ángulos interiores del polígono  
ABCDEF ... mide (n — 2)r, al formar el polígono APBCDEF ... agregamos la suma de  
los ángulos interiores del triángulo ABP, luego la suma de los ángulos interiores del nuevo  
  
polígono mide:  
(n-2)7 +7 =(n-2+1)r =(n-1)r.  
  
= (n " n n  
1.10. — n—1h1 —  
(a+6b) ;(z>a b', donde (2) —l  
Si n =0, entonces (a + b)" = (a +b) =1 y, además,  
= (n 7 0  
Z (')ºn\_'b' = ( )aºbº =1.  
. ! 0  
1=0  
Supongamos la propiedad cierta para n, esto es:  
n\_ = (n n-ipi  
(a+b) —; (i>a D.  
  
65  
  
Scanned by CamScanner  
  
  
--- Página 69 ---  
  
Al multiplicar ambos miembros por (a + b) se tiene:  
  
(q.+ = Í (?)ºn+l\_íbí+-Í (';> an-ipit,  
  
i=0 .. i=0  
  
Obsérvese que, en general, al multiplicar el término  
  
n n-i-1pi+1  
  
| (i+1)º |  
n. n—-iLi+1 ' 1  
<i + 1)º , (1)  
  
mientras que al multiplicar el término  
<n) a-  
z.v  
  
<Í> aive - .(2)  
  
y al sumar los dos términos semejantes (1) y (2) nos queda:  
  
por a, result\_a.  
  
por b, resulta  
  
n N (AV on-ipiht - (2 + an-ipit  
i+1 1 t+1 '  
  
ya que la suma de dos números combinatorios del mismo numerador y órdenes consecutivos,  
  
es otro número combinatorio cuyo numerador es una unidad mayor y tuyo orden es el del -  
sumando de mayor orden. :  
  
Por tanto, nos queda: ' —  
  
+ (" + 1) a?b!+ (" + 1) ab" + <") b+1,  
\_ n—l1 n n  
". y como <n i n - ("+1 se puede escribir:  
! ' 0/ 0 /7 u +1 »P '  
  
. n+l  
¡ (a+ b)n+l = Z <n 'Í' 1)a"+l\_ibi,  
1 : . i=0 -  
  
conforme queríamos demostrar.  
  
66  
  
Scanned by CamScanner  
  
  
--- Página 70 ---  
  
Sección 2.  
  
2.1. Dados dos enteros, a y b, se pueden presentar tres casos: ambos son pares, ambos  
son impares, o uno de ellos es par y el otro impar. Consideremos cada uno de estos casos,  
  
a) Si a = 2k y b = 2k>, entonces a + b = 2(k¡ + ky) y a - b = 2(k1 — k2), luego a+b  
y a — b son ambos pares. ' ,  
  
b) Si a = 2ky +1 y b=2k, +1, entoncesa+b=2(k¡+k2+1)ya—b=2(k1\_k2),  
por tanto, en este caso a + b y a — b son también ambos pares.  
  
c) Si a = 2k¡ y b= 2k, +1, entonces a+b=2(k¡+kz)-i\_-l y a-b=2(k: Ákg)¿1;Í -  
de manera que ambos son impares. El mismo resultado se obtiene si a es impar y b es par,  
  
luego la suma y la diferencia de dos enteros siempre tienen la misma paridad.  
  
2.2. Si aclbc entonces existe un entero z tal que:  
  
be = (acz,  
de donde: — - C . o  
b = az, . - '  
luego: l -  
alb.  
  
2.3. Si a|b entonces existe un entero 7 tal que  
b=ar. . . (1)  
Similarmente, si c|d entonces existe un entero y taí qúe |  
d=cy O  
  
| Multiplicando miembro a miembro (1) y ( 2) se tiene:  
  
,  
  
bd = (az)(cy),  
bd = (ac)(zy),  
  
luego:  
aclbd.  
  
2.4. Sin = 2k entonces n? +2= 4k? +2. 4k? es múltiplo de 4, luego si 4k? + 2 fuese  
divisible por 4, también lo sería 4k?+2—4k? =. Por tanto, si n es par entonces 4 /n?+2.  
  
Sin = 2k+1 entonces n?+2=4k?+4k1+1+2= 4(k? + k) +3. Con un razonamiento  
similar al anterior se concluye que, como 4 /3, entonces 4 n? + 2 si n es impar.  
  
67  
  
p  
  
Scanned by CamScanner  
  
  
--- Página 71 ---  
  
2.5. Basta factorizar:  
| nf -1=(n- 10014042 4...An+1).  
Nota. Conviene recordar las identidades: | |  
a" — b" = (a —b)(a"'+ "2a 24 b rab"? i b"—1),  
para todo entero n, y, si n es impar: l  
a"+b" = (a+b(a" ! —a"?b5+a"-35? —... + a26"3 — ab" ? + b"=1),  
  
2.6. Escriba.rríos:  
n= [(n — 1) + 1]k.  
  
Entonces se tiene:  
n\*%()(n—1)\*+Kl)(n—1\* +.. (kfl)(n—\_1)+<z),  
  
-1 = (n- 1? [(g>(n - í)\*'“º + (Í>(n — 1 3+...+ (k \* 2>]+k(n — 1)  
  
por ¿onsigíi¿rite¡ (n—1)\*|(n\* — 1) si y sólo si (n — 1)?|k(n — 1), esto es, si y sólo si existe  
un entero z tal que  
  
| k(n — 1)= (n-1)\*,  
\_ k = (n — Dr,  
luego, (n — 1)|(n\* — 1) si y sólo si (n — D|£.  
  
2.7. Se pueder1 presentar tres casos: |  
a) Si n = “k, entenices n? = 9k? = :':1, donde —»=3kº.  
b) Sin —3k+1 entoncesn —9k2 +6k +1 = 3k2+1 donde k7 = 3/c2 + 2k.  
c) Sin = 3k + 2 entonces n? = 9k? + 12k + 4 3k3 + 1, donde k3 = 3k? + 4k +1.  
Por consiguiente, todo cuadrado perfecto es de la forma 3K o de la forma 3k +1.  
2.8. Sin=6k+5, entonces:  
n = 6k+6-1=3(2k+2)-1=3k; — l dondek¡ = 2k +2.  
  
El recíproco no es cierto. Por ejemplo, 2 = 3.1 — 1 es de la forma 3k — 1 pero no es de l:  
  
forma 6% + 5 (de hecho, es de la forma 6k + 2, tomando k = 0). Nótese que todo númerc  
de la forma 3k — 1 es de la forma 34 +2.  
  
68  
  
Scanned by CamScanner  
  
  
--- Página 72 ---  
  
2.9. Sin = 5k+1, entonces  
n? = 25k +10k+1=5(5k? + 2£) + 1= 5k +1,  
donde k1 = 5k? + 2k.  
  
2.10. Sean m = 2k + 1,n = 2k, +1.  
  
") m?\* —n? = (m+n)(m —n) = (2k; + 2k7 + 2(2k; — 2kº) \_  
  
= +R T D(B-k) =0 1  
  
Ahora b1en, como k — k y k1 +k2 tienen la m15ma paridad, el número ( k1 +kz +1Y%: —k2)  
es de la forma 2k, luego 8/(m? —n?).  
  
4 mº+n4-?-2=m4—2m2n2+n4+2m2r3'\_25= .  
| = (=) +Q(min?=1).-  
En (a.) hemos visto que 8|(m? —n ) luego ba.sta. probar que 4|(m n — 1), e\_s dec1r que.. -  
? es de la forma 4k+1. En efecto:'- PA '  
  
m?n? = (4k?+ 4k1 + 1462 + 4k, 3r 1)=  
= (4k3 + 1)(464 + 1) = .\_\_  
  
donde hemos hecho: k; = k? + Ey, ky = k2 + ky, ks = 4ksk; + kz - =¡c4  
  
2.11. De acuerdo con el algoritmo de la d.1v1sxon, si se divide a entre n entonces existen  
enteros qo, ag tales que  
  
a-qon+ao, O <ay <n.  
  
Si a) = O hemos temunado De lo contrario, se aplica nueva.mente el algoritmo y se  
tiene una secuencia de igualdades:  
  
d0 = 91 + a1, 0<01 <n,  
91 =9N+az, O<ar<n,  
  
Qk-3 = Qk-21 + Ak-2, O< ar-7 <n,  
Jk-2 = Qk-11 + Ak-1, O<ax-1 <n,  
  
en la cual los qi  
  
. van decreciendo estrictamente basta que uno de ellos será menor que n, y  
se tiene:  
  
Jk-1 = ak.  
s RQ  
  
Scanned by CamScanner  
  
  
--- Página 73 ---  
  
En esta secuencia, podemos despejar a de la siguiente manera:  
  
Qk-2 = AN + Ck—1,  
  
2  
Qk-3 = G1 + ar-1N + ak-2,  
  
k—2 k-3  
q1 = an + ak-1N +...+azn +az3,  
k— k 2  
  
q0 = ag N 1+a;c\_¡n +...+azn +ayn + a,  
  
a= aknk + a¡<\_¡nk"1 +...+ a2n2 + ay + do.  
Nota. Sin = 10, esta es la representación de a en el sistema decimal de numeración (ba  
10). Se escribe: | :  
  
a= arAk—1 ...7j a.  
  
(Generalmente el contexto evita que haya confusión con la notación de la multiplicació:  
Sin=?, le base se llama binaria.'Si n = 16, la base se llama hexadecimal. Por ejempl  
  
3510 = 1.25 +0.21+0.27+0.22+12+1=1000119=2.16+3=2316-  
2.,12. Para n = l se tiene: .  
— A =5+2.39+1=5.  
  
An  
  
Supongamos que 8  
  
51 4+23"+1,  
  
An+1 —  
Ana — An =5"H14+23"+1-5"-23" —1=  
= 5".(5— 1) +371.(6-2) =4(5" +3"7).  
Como 5" y 3-1 sor: mpares, su “:mMa rs par, ::::50 Sil An+1— .5. y CO 8|A , entor  
  
SlAn-1-  
2.i3. Si en la identidad:  
a" - b" =(a—b)(0" + a"-?2b+...+ab"?+b"1),  
hacemos a =2 y b=-1, se tiene:  
2 - (-1)" = ((2-(-D)]E =36,  
donde k es un entero. Por consiguiente,  
2+1=2"-(-1)" +(-1)" +1=3k+1+(-D"  
  
Por tanto, si n es impar entonces 2" +1 es de la forma 3k, pero si n es par entonces?"  
es de la forma 3k +?2. Por ende, 2" + 1 es divisible por 3 si y sólo si n es impar.  
  
70  
  
Scanned by CamScanner  
  
  
--- Página 74 ---  
  
2.14. Se tiene:  
= (3+1)",  
  
Luego 4 es un entero de la forma 3K + 1 y 4" + 1 es de la forma 3k + 2. Por tanto,  
3 14 + 1).  
  
de donde,  
  
2.15. Se tiene:  
n? +100=n? + 1000 900 = (n+ 10)(n — l0n + 100) 900  
  
Luego si (n + 10)|(n? + 100) entonces (n + 10)/900.  
  
El mayor divisor de 900 es 900, luego el mayor valor para n + 10 es 900 y el mayor: .  
valor que puede tomar n es 890. D.  
  
. .)  
  
2.16. Si n fuese impar, entonces a, az, . an tendrían que ser todos impares; pero la.  
suma de un número 1mpa.r de números impares es impar y, por lo tanto, diferente de 0.  
Por consiguiente, n es par y en consecuencia alguño de los a; tamb1en lo es.  
  
Sea ay el terrmno par. Entonces, '  
  
a1+az+.--+ak—1+ak+l+--—+an=\_\_a¡=' . —  
  
Como en el primer miembro hay un número 1mpa.r de términos que sumados dan un- número -  
par, alguno de ellos debe ser par. Si aj es el otro término par, en el producto  
  
aj a... ¿ln —=Rn  
hay dos factores pares, a, y aj; por.tanto ? es divisible por 4. - \_ -  
2.17. Si n es impar se tiene:  
  
a, =(7-1)" +(7+i)º,  
  
)7,.-2+\_\_ (n—3) +(n—l)]  
  
01991 = 49k + 14.1991 = 49k + 27874.  
Al dividir 27874 entre 49, el resto es 42,  
  
I  
t M  
—  
  
Sin= 1991 se tiene:  
  
Scanned by CamScanner  
  
  
--- Página 75 ---  
  
2.18. Es necesario probar que al menos uno de los factores es par.  
Si n es impar, entonces n €es de la forma 2k +1, luego el producto tiene 2k +1 factores  
Además, entre los números 1,2,3,...,7 hay exactamente k + 1 impares ya que:  
  
1=2.1-1,  
3=2.2-—1,  
5=2.3-1,  
  
2X+1=2(k+1)-1.  
  
Luego, en los a; hay también k + 1 números impares y entre los 2n números 1,2,...  
... ,, 01, 02,---,Ón, habrá 2(k+1) =2k+2=n+ 1 números impares. Pero sólo hay n  
factores, luego al menos uno de los factores contiene dos números impares, cuya diferencia  
es un número par.- '  
  
Nota. En el razonamiento anterior hemos empleado, tácitamente, un argumento ex-  
tremadamente simple y útil que se conoce como Principio de las Casillas; éste. establece  
que, si se colocan n +1 objetos en n casillas, entonces al menos una de estas casillas debe  
contener más de un objeto. :  
  
| 2.19. C.omo n es par, n es de la forma 6k 66k+-266k+4. Ahora bien, para todo k > 1,6  
es abundante pues entre sus divisores diferentes se encuentran:  
cuya suma es mayor que 2.6k. Luego, si n = 6k y k > 4 se tiene:  
| n =6k=62+6(£-  
  
donde cada término es ab::adante. 4  
Si n = 6k+2 y k > . se tiene: .  
  
— 6k+2=6.3+6(k-3)+2=20+6(k-3)  
  
donde 20 y 6(£ — 3) son abundantes.  
Si n = 6k+4 y k >8, se tiene:  
  
n =6k+4=6.6+6(k-6)+4=40+6(k—6)  
donde 40 y 6(k — 6) son abundantes. Esto completa la prueba.  
2.20.  
  
1  
+1).(57.2'—1) =  
1)= '  
  
3  
?  
  
-  
-  
l  
  
225 41=22211=21.228+1=(641 -51).2\*  
— 641.228 — (51.22 - 1) = 641.2%.(5”  
= 641.2?8 — (5?.214 + 1).(5.27 + 1).(5-  
= 641.[2?8 — (52.214 +1).(5.27 — D-  
  
+  
  
H  
-  
T2  
  
Scanned by CamScanner  
  
  
--- Página 76 ---  
  
2.21. El entero m no es divisible por 5, ya que de lo contrario:  
amº+bmº+cm+d=m(amº+bm+c) +d  
  
sería divisible por 5 sólo si d fuese divisible por 5, en contra de nuestra hipótesis. Por  
consiguiente m es de la forma 5k + r, donde r es un entero positivo menor que 5.  
  
Sean:  
A = am? +bm? +cm+i,  
  
B = dn' +cn? + n+a.  
  
Eliminando d de estas expresiones, se tiene:  
  
An — B =a(m"n\*-—1)+bn(m\*n? — 1) + en?(mn — 1)=  
  
= (mn — 1)fa(m?n? + mn + 1)+bn(mn +1) + en].  
  
Ahora bien, si m = 5k +r es un entero tal que 5/A, y si podemos seleccionar n de manera  
que el último miembro de la igualdad anterior sea divisible por 5, entonces B será d1V151ble  
  
por $.  
  
Tomemos, para cada entero m que no sea divisible por 5 un entero n de manera que  
el factor (mn — 1) sea divisible por 5.  
  
Como m = 5k +r, mn = Skn +rn, luego mn — | es divisible por 5 si rn = 5k +1.  
Por tanto, si 7 = 1, podemos tomar n = l; si r = 2, podemos tomar n = 3; si7 = 3,  
podemos tomar n = 2 y, si r = 4, podemos tomar n =4. De esta manera, para cada m,  
hemos hallado un n tal que mn — 1 es divisible por 5 y, por consiguiente, la expresión 3  
es divisible por 5.  
  
Sección 3.  
3.1. Si a|c entonces existe un número entero r tal que  
c =ar. | (1)  
Si b|c, como (a,b) = 1, necesariamente b|z, luego existe un entero y tal que  
7 = by. (2)  
  
De (1) y (2) se deduce:  
c = a(by),  
  
c = (ab)y,  
ablc.  
  
3.2. Tenemos que:  
  
n-—n= n(n\*—1)=n(n? - 1yn?+1) = (n-1Dn(n +1)(7?+1).  
  
73  
  
Scanned by CamScanner  
  
  
--- Página 77 ---  
  
Como en la descompos¡c¡on en factores de n5 —n aparecen tres enteros consecutnos  
sabemos que n\* — n es divisible por 2 y por 3. Veamos que alguno de los cuatro factores:  
(n — 1),n,(n+1) ó (n? + 1) es divisible por 5. Se presentan cinco casos posibles  
  
a) Si n = 5k, hemos terminado. |  
b) Si n = 5k +1, entonces n —1 = 5k.  
c) Si n = 5k +2, entonces  
  
n? +1=25k? +20k+4+1=5(5k? + 4k+1) = 5ki,  
donde kj = 5k? + 4k +1.  
  
d) Si n = 5% +3, entonces  
  
n +1—95kº+30k+9+1\_5(5kº+6k+2)\_ob,  
donde k, = 5k? J-6k+º  
  
e) Si n = 5k +4, entonces n+1=5k+5 a S(k + 1)= 5ks, donde k3 = k +1.  
  
En cualquiera de los casos 5|(n5 — n). Como 2, 3 y 5 son primos dos a dos, en virtud  
del problema 3.1. se tiene que 15 —n es divisible por 2.3.5 = 30.  
  
3.3. Consideremos el producto P = n(n + 1)(n + 2)(n + 3). Hemos visto que el mismo es  
  
divisible por 3, luego bastará probar que es divisible por 8. En efecto, consideremos los  
cuatro casos posibles:  
  
a)Siñ=4k,entoncesn—í:—4k-Lºxn(n+2)-—: k +2) = EX(2k +1).  
  
b) Sin = 4L+1, entonces n+1 =4k+ " yn+3=4k+14, portanto (n +1)(n+3: =  
= (4k + 2)(4k + 4) = 8(2k + 1(k + 1). ' '  
  
c) Si n = 4k +2, entonces n + 2 = 4k + 4, luego n(n + 2) = (4k + 2Y(4k + 1) =  
= 8(2€ + 1)(k +1). —  
  
d) Sin = 4k+3, entonces n+1=4k+4yn+3=d4k+6, de donde (n +1)(n +3) =  
= (4k +4)(4k + 6) = 8(k +1)(2k +3).  
  
Por consiguiente, 8|P en todos los casos posibles.  
  
3.4. Sean d = ((a,b),c) y d' = (a, (b, 0)).  
  
Si di(a,b) y dic, entonces dla, d|b y dlc, luego dja y di(b,c), de donde di(a, (b,c)), o sea  
d|d' y por consiguiente d < d' (1).  
  
Scanned by CamScanner  
  
  
--- Página 78 ---  
  
- a.. .Por un razonamientó análogo se've que d'.Z'd  
, 1 EE IT “ Te e s a .  
3.5. Si (2,y) =3, entonces YZ + 1) porianto =Ly 7 100  
  
u  
  
TE .  
  
3.6. Una solución inmediata es z = 5,y0 = ¿95%Sl tomamos y =5 Fi00k;y — 95<  
100k, para cada valor entero de k se tiene un'p\_a.r\_\_'¿c¡!j£ere\_p\_f:e\_..dg¡\_entetbs que satisfacen las —  
condiciones. s Y . o -  
  
3.7. Si (a,4) =2 y (b,4) =?, entonces a y b son pares. Además, son de la forma 4k +7  
  
ya que, de lo contrario, sería (a, 4) = 4 ó (b,4) = 4. Luego, si a = 4k,+2y b=4k, +2, se  
tiene: . . :  
  
a+b=4(k1+k7+1),  
4/(a+b), . |  
\_ (a+kQ¿Áf?4  
  
S  
  
3.8.  
  
.A  
  
P  
  
- luego, si a — b es divisiblez'zp6"rf2\_'¡,—”tá£i5íé;i¿ esa 'Además, .como a y b son imipares, =  
  
a?+ab+ d? es impar y (2",Oº+ ab +\_' bº)=1, luegº “Í(a3 — $) sólo si 2"|(a—b) -'  
  
3.9. a) Procedemos por inducción sobre n. Si n = 0,8ntonces (Lzo, aj ) = (1,1) =1.  
  
Supongamos que (an, an41) =1. Entonces, si (ag';1,an+2) =d  
  
, se tiene que d|(an.. .—  
—An+1), luego dla,, y como djan+1 entonces dil, luego d =1. \_ —  
  
b) Sin =1 se tiene: a, = (1;1 =(g =41.  
  
Supongamos que la propiedad es cierta hasta n. — D  
n—?2 n—g3 n—4 v - - \_  
- (2-=1 , /n-2) (/n-3 /n- 4y —  
  
Como (n \_ 1) = (n> y como (a " 1) + (a - 1) = (a) sumand¿ miembro a miembro  
0 0 b-—1 b AUA :  
(1) y (2) se tiene: - -  
  
principio de inducción equivalente a la que se planteó  
s que para cada entero positivo n se da una propiedad  
  
Nota. Se ha usado una vérsión del  
en la sección 1. Esta es: Supongamo  
  
T5  
  
Scanned by CamScanner  
  
  
--- Página 79 ---  
  
P(n). supongamos que P(1) es cierta. Supongamos además que siempre que; P(m):e  
cierta para todos los enteros positivos m < n, entonces P(m+1) es cierta. Entonces P(n  
es cierta para todos los enteros positivos n. . .  
  
3.10. Sean d = (a b),d' = (a', b'). Se tiene:  
  
(aa ab', ba', bb') = ((aa', ab'), (ba',bb')),  
(aa',ab') = a(a', b') = ad',  
(ba', 58') = ba',b') = bd ,  
(aa' áb' ba', bb'Y = (ad', bd') = d'(a, ) = dd'.  
3.11. Sea.n u= -ar + by,v =c + dy. Entonces  
  
du — by = (ad — bc)z = mr  
  
by = du — me.  
  
Si z, y son enteros tales que U es mult1plo de m, entonces bu tamb1en es mu1t1plo de  
  
"m y, como (b,m)'=1;'se tiene que. m|v  
  
En m -  
  
E1 rmsmo razonam1ento muestra que si v eg mult1plo de m, ta.mb1en lo es de u.  
  
3. 12 Se t1ene a= d:z: b\_ dy, donde T, y son enteros y (r, y) =1.  
  
Si se d1v1den a, 2a7¿;3a,.'.. ,(5 — l)a, ba por b, se obtienen los cocientes  
rT 2r (b—1)z br  
yy " y "y  
  
Como (7, y) = 1 los únicos números enteros entre las fracciones anteriores son aquellos  
1 los cuales el coeñc1ente de 7 en el numerado: es un múltin!o de y. C omo b = dy, esto  
sucede d veces, cx…ndo los coeñc1entes toman los valores y, 2y, .., dy. -  
  
Sección 4. A  
  
4.1. Si (a,b) = 1y ('zº;¡y"¿',), (z¡;\*y¡) son soluciones de la ecuación az + by =, enton—ces- '  
.'L'o + bkj = 71 + bkz,  
para dos enteros k; y k2 Como 7| = 1 + , se tiene  
  
T0 + dk1 = (1 + 20) + bkz,  
  
blky — k) =1,  
b=+1.  
  
"  
  
76  
  
Scanned by CamScanner  
  
  
--- Página 80 ---  
  
e 3;.!\_ '“…'5 4  
  
l."[l u  
  
4.2. Restando miembro a miembró las écuaciónes del sistema  
ar + b¡y+ C7 = d¡,  
a + b2y + c2z = do,  
  
se tiene  
  
(b¡ - bz)y + (C¡ — 62)Z = d — da.  
Esta última ecuación tiene soluciones enteras si y sólo si  
(b1 — d2,01 — ºz)|(d1 — d2)  
  
lo cual nos garantiza que las dos ecuac1ones t1enen al menos una soluc1on s¡multanea… (para  
z =0).  
  
4.3. Multiplicando ambos miembros de la primera ecuación por 4 y ambos m1embros de .  
  
la segunda ecuación por 3, se tiene:  
Obsérvese que (24— 304 —6) =2 y 2 18-—9); luego, de acuerdo con el resultado obtenido”  
  
en el problema 4.2., el sistema no tiene soluciones enteras.  
  
4.4. Si en el sistema — -  
z7+2y+3z=4, . ' (1)  
  
27—-z=-l1, — (2)  
  
se multiplican los dos miembros de la ecuación (2) por 3 y se suma miembro a mxembro  
con (1), nos queda -  
77 +2y =1. |  
  
Esta ecuación tiene una solución particular: 70 = 1,y0 = —3 (se puede hallar por ins—  
pección), luego la solución general de 77 + 2y = 1 es  
  
T=1+ 2k,y =—d—-17k, donde k recorre Z.  
Reemplazando estas expresiones en (1) se tiene  
  
1+2k+2.(-3 — 7k) +3: =  
1+2k-6- 14k+3z=4,  
32 =9+12k,  
  
z2=3+4k.  
  
Por tanto, la solución general del sistema es:  
z =1+2k,y=-3-Tk,z=3+4k, donde ke Z.  
  
TT  
  
Scanned by CamScanner  
  
  
--- Página 81 ---  
  
4.5. T+y-2=—1,  
  
T- y2 +:?= 1,  
  
-—a:º+yº+zº=—l.'  
  
De la primera ecuación del sistema se desprende:  
T+y=2z-—1. | (1  
De la segunda ecuación se desprende: |  
(5 +y7 — y) +(2+1)(2 - 1) =0,  
  
por tanto .  
(z—1)(z—y)+(z+l)(z—l)=0, |  
(2-1)(2-y+2+1)=0, (2;  
por consiguiente, 2 -1 — 0ó x— Y +2+1=0. Analicemos ambos casos.  
a) Siz—1=0, entonces z =1 y de (1) se concluye que y = —y. Reemplazando en la  
tercera ecuación del sistema nos queda:  
  
3  
-E — =-—1-1,  
  
—27% =2  
T= 1,  
T=l1, -  
y en consecuencia y = —l1, luego una solución es: \*  
(1,—1,1).  
b)Siz-y+z+1= 0, entonces  
T-Y=—2—1.  
  
Sumando miembro a miembro esta última ecuación con (1) se tiene:  
  
27 =—2,  
  
T=-—l,  
y además z = y, Reemplazando en la tercera ecuación del sistema, nos queda  
  
\_(—1)3 +2y3 = \_11  
  
2y3=—2.'  
y3 h \_11  
Yy=—l.  
  
78  
  
r  
  
Scanned by CamScanner  
  
  
--- Página 82 ---  
  
. .setiene .  
  
Entonces, la otra solución del sistema es:  
  
(-1,—1,-1).  
4.6. Si z = 2k entonces 73 + 57 + 9 = 8k\* + 10k+9= 2k +1, donde k¡ = 4k? + k +4.  
Si 7 = 2k + 1 entonces 7\* + 57 + 9 = 8k3 + 1242 + 16k + 15 = 2k7 + 1, donde  
  
ky = 4k3 + 6k? + 8k +7.  
  
Luego, 7\* + 57 + 9 siempre es un número impar y, por tanto, no puede ser igual a0.  
  
4.7. Basta verificar la identidad:  
| (a? + 5%Y(e? + d?) = (ac — ba)? + (ad+ be)”.  
  
4.8. Sean n — 1,n,n + 1 los tres números. Entonces, si  
  
(n+1) =(n-1)+7",  
  
n? - 6n?-2=0, |  
n\*(n — 6) =2.  
  
El primer miembro es positivo sólo si n > 6, y en ese caso n\*(n — 6) > 36, luego  
  
n?(n—6) 2.  
  
4.9. Si7 =n(n+1)(n +2)(n + 3) se tiene:  
  
2 = [n(n+3))l(n + D(n +2)) = (? + 3n)(n? + 30 +2) =  
= (17 + 3n[(n\* + 3n) + 2] = (n? +31)\* + 2? + 31) =  
= [(n\* + 31)? +2(? + 3n) +1)-1=(n?+3n+1)? —1.  
  
Luego, (n? + 3n)? < 1 < (n?+3n+1)\* y, en consecuencia, 7 no es un cuadrado perfecto.  
  
4.10. De las identidades:  
  
(a—b)? = a? — 2ab +??,  
  
(a—-c) = a? - 2ac+\*,  
  
(b-c)? = b - 2bc +?,  
  
(a+b+0)? =a?+b + ? + 2ab + 2ac + e,  
sumando miembro a miembro se tiene:  
Nd + b +ct)=(a-b)? +(a—c)?+(b-e)? +(a+b+0)7.  
79  
  
Scanned by CamScanner  
  
  
--- Página 83 ---  
  
4 11 Supongamos¿q  
1 i1 X ..”'é' .- "  
.1 Q 5$“3N19' .  
  
Como la su1>'rna de:losfcuadra.dos de a b c, ,des pa.r hay tres casos posibles:  
  
TA TA  
  
e a.) Los' cuatro son pares.v  
b) Los' Cuatro s0 % \_r;1pares…¿¡  
c) Hay dos pa.res y -dos 1mpares  
  
En cualqu1era de los “Casos hay dos parejas de números con la misma pand.  
manera que su suma “y\_su dxferenc1a son pares. Supongamos que las pare\_]as de nu  
(a,b) y (c, d] t1er31en la nnsma. panda.d “Entonces: — eS  
  
4. 12 Observe<e que-la: c  
0,1,4, 5 6 09 Entonces  
  
4.13. S¡ r? l = 'n, entonces (:c + y)(:c — y)  
pa.ndad (problema,3 1'L), luego s¡ I+ y=01-y= b, entonces n = ab, con a  
  
Scanned by CamScanner  
  
  
--- Página 84 ---  
  
4.14. Si 2?+1=q? se tiene 27 = (4+1)(9—1), por consiguiente q es impar. Si q = 2k+1,  
  
entonces  
2? = 4k(k+1).  
Como k y k +1 son dos enteros consecutivos, k(k + 1).es una potencia de 2 sólo si  
  
k = 1, luego  
2? =8,  
  
de donde  
p=3 y q=3.  
  
4.15. La ecuación ? +ar+b= y? + cy + d puede escribirse en la forma:  
+ 6-2 =ly+10-5  
2 4 2 a.  
  
Si a? — 4b = c? — 4d, la ecuación es equivalente a:  
  
luego  
  
axtc  
  
2 " . . - . \_  
  
I=y -  
  
— Como a? — e? = 4(b-d), entonces 4(a + c)(a — c). Sabemos que a + c y a —c tienen la  
c  
son números  
  
. : .. . a  
misma paridad, por consiguiente ambos son pares y, en consecuencia,  
  
enteros. Luego, para cada número entero y habrá un entero z que satisfaga la ecuación.  
Reciprocamente, supongamos que la ecuación 1? + ar+b= y? + cy + d tiene infinitas  
soluciones enteras. De la ecuación  
  
a a? e?  
+ b-== \_E  
(z 2) \* <y+ 2> -7  
  
2 2 2 2  
a c a (a)  
(++5) -(1+5) ---£+a  
  
(27 + a)\* — (2y + c)? = a? - 4b - ? + 4d,  
(27 +2y +a+c)(27-2y +a—-c)=a?-4b-c\*+4d  
  
se tiene  
  
21  
  
Scanned by CamScanner  
  
  
--- Página 85 ---  
  
g.'—.  
N  
  
Si suponemos aº,—>4b — ?+4d + 0, este número tendrá un núm<\_aro finito de dIWSZ  
luego (27 + 2y + a + c) y (27 - 2y + a —c) tendrán un número finito de valores par  
infinitos enteros z, y que satisfacen la ecuación. Ahora bien, para que 27 +2y+a+cto  
un número finito de valores, es preciso que 27 + 2y = 0, es decir, 7 = —y, y en ese ci  
27—-2y+a—c=4r+a-c tomará infinitos valores. Esta contradicción implica c  
'aº—4b—cº+4d=0,luegoaº—4b=cº—4d. - '  
  
4.16. Consideraremos tres casos según que a sea menor, igual o mayor que 0.  
  
b i5la] \_  
a-)SÍ(1<0entonces;z;º=2'º\_.\_l \_ 215 l  
  
= — — luego z nunca será entero y  
15lal l5lal  
  
ecuación no tiene soluciones enteras,  
  
b) Si a = 0 entonces 2? = 2 \_ 1. Para que haya solución entera es necesario qr  
sea b > 0. Si b = 0 entonces ry = Oysib=1 entonces 7 = +1. Si b > 2 entonces 42  
luego 4/(7? + 1), lo cual es imposible ya que para todo entero r se tienc que 2? = 4l  
? =4k+1. Por tanto, en este caso las únicas soluciones son:  
  
c) Si a > 0, de 154 = 2\_ 7 se desprende que 3|(25 — 1?). Ahora bien, 2? — (3—1)>—  
3k+(—1)?, luego 3/[(—1)\* —z\*], de donde 3[2\*—(—1)\*]. Si bes impar, esta relación implica  
  
. 7  
  
que 31(7?+1), lo cual es imposible porque 7\* es de la forma 34 ó 3£ + 1. Por consiguiente  
  
Nótese que si r es una solución d la ecuaición. —r también - es, luego podemos  
suponer z > 0. (Ei :aso 7 = 0 ya ha sido analizado en (b)). - \_  
  
Ahora bien, 3[15\* y 5/15a, luego 3 y 5 dividen a (2—mz)(2 +2). Pero 2- z y 2 + no  
pueden ser ambos divisibles por 3 ya que, en ese caso, también lo sería la suma de ambos,  
esto es, 3|2\*+1, lo cual es falso. Similarmente se comprueba que 2 — y y 2 + no son  
ambos divisibles por 5. Las posibilidades que quedan son las siguientes:  
  
1)2-—7=1y2+7=15.  
Sumando ambas igualdades se tiene:  
  
2 =15" +1,  
  
y debe ser c > 3. Sic = 3, entonces 21 = 15 + 1 y hay las soluciones:  
  
a=1,b=  
  
6,7 =7,  
  
a=1,0=6,r=-7,  
82  
  
Scanned by CamScanner  
  
  
--- Página 86 ---  
  
32|(15\* + 1). Pero 152 = 225 = 32.71— 1,  
entonces 15“ es  
  
Si c > 3 entonces 32|2\*\*! y, por consiguiente, '  
32k+1 y si a es impar,  
  
luego si a es par se verifica que 15\* es de la forma  
de la forma 32k + 15; por tanto, en ningún caso 32|(15” + 1).  
  
)2 -—2=3" y 2+r=5".  
  
Sumando ambas igualdades se tiene:  
  
241 =3"+5".  
  
y debe ser c > 2. Si c =2, 2?=3+5 y hay las soluciones:  
a=1;b=4,7=1,  
  
a=1,b=4,7=-1.  
  
Si c > 2 se tiene que 16|2\*\*! y, por consiguiente, 16)(3\* + 5). Ahora bien, 3" + =  
= (4-1)\*+(4+1)\* y, desarrollando por el binomio de Newton se llega a que 3\* +5\* es  
de la forma 16k + 8 si a es impar y 16k +2 si a es par. Por tanto, 16 1(3\* + 5").  
  
En total la ecuación tiene siete soluciones.  
  
4.17. ' . - ' - :  
T +py =n, (1) -  
  
T+y =p". (2)  
  
En la ecuación (2) se observa que para que el sistema tenga solución (7,y,7) de enteros .  
positivos, debe ser.p > |, luego p-1>0. . ,  
Despejando y en (2) y reemplazando en (1) se tiene:  
  
T+p(P5 —1)=n,  
T+pt!-—pr=n, —  
  
z(1-p)+p\*!=n,  
  
y como pÉ l,  
z\_pt+l\_n \_p=+1\_1\_(n\_1)  
p-1 — p—1 '  
TI1 n—l  
Ul (3)  
p—1 p-1  
De la ecuación (2) se tiene:  
y=p=—z,  
  
z+1  
; Pl ml  
— - — + —,  
y=P p—1 p—1  
  
prri-p-p++l+n-—1  
  
y=  
Pp-1 '  
n— z  
y=—\_p\_,  
p—-1  
a  
  
Scanned by CamScanner  
  
  
--- Página 87 ---  
  
n—l \_ pr=—1 (4)  
p-1 p-1'  
Como (p—1)I(p\*—1) para todo entero positivo z, los valores de 7, y dados en las í%ualdades  
(3) y (4) son enteros si y sólo si (p—1)|(n—1). Además, z es positivo si y sólosip\* —n > 0,  
es decir p\*\*! > n, mientras que y es positivo si y sólo si n — p? > 0, luego n > p\*. Se tiene  
entonces N  
  
p: <n< Pl+l' (5)  
  
y=  
  
Por consiguiente, las condiciones que deben satisfacerse para que el sistema tenga soluciones  
(7, y, z) de enteros positivos son: ,  
  
a) p>1, .  
b) (p — Di(n — 1),  
c) p .  
  
Obsérvese que la desigualdad (5) determina z en forma única. Una vez hallado el valor  
de z, las ecuaciones (1) y (2) determinan, también en forma única, los valores de z, y.  
  
Sección 5.  
  
5.1.n+1l=1ln-+1, luego, por el a1goriffno de Euclides, (n,n + 1) =1. Por otra parte,  
  
[n,n+1] ='?£í+—1) =n(n+1).  
\_ ab  
5.2. Si alb entonces (a.b) = a y [a,b) = — =.  
| a  
  
5.3. Si (a, b) = 10 y (a,b] = 100, entonces ab = 1000.  
Como a y b son ambos múltiplos de 10, las soluciones posibles son:  
  
-  
  
a = 10,5= 100,  
a = 20,5=50,  
a = 100,5=10,  
a = 50,b = 20.  
  
5.4. Si dlm basta tomar y = d, y = m y entonces se satisfacen las condiciones (7, y) =d,  
[? y] = m (problema 5.2.).  
  
un di or ºtáº parte, si existen enteros r, y que satisfacren ambas condiciones, entonces d es  
ivisor . .  
eTey. Comoasuvez re y son divisores de m, entonces necesariamente dim.  
  
a  
  
Scanned by CamScanner  
  
  
--- Página 88 ---  
  
Sección 6.  
6.1. En la identidad  
a"-1=(a-1)(a"!+0"7+...+a+1)  
  
se observa que  
(a—1)I(a" —1),  
  
luego si a" — 1 es primo entonces necesariamente a — 1 = 1, de donde a = 2. Además, si  
n fuese compuesto tendríamos n = zy, con z,y enteros tales que 1 < 7,y < n, y de la  
  
identidad:  
  
2"-1=2"7-1=(25)" -1=(27 - 1)(270-1 +97(7-2) + ,,, +27+1)  
se concluye que 2” — 1 no es primo. Por consiguiente, n debe ser primo.  
Nota. Los primos de esta forma son llamados primos de Mersenne (fra.nc&s)  
  
6.2. Dados los tres zúmeros consecutivos  
  
uno ce ellos es de la forma 3k. Como 2" — 1 es primo y 3 (2", entonces necesariamente  
3/(2” + 1). Además, si n > 2 entonces 2” + 1 > 3, luego 2" + 1 es compuesto.  
  
6.3. Si suponemos 2" 11 =7\*, se tiene  
  
2"=7>—1,  
  
2"=(7-1(7?+2+1),  
  
pero el factor 7? +7 +1 es impar, y como z > 1 (de lo contrario sería 7 — 1<0),7?2+7+1  
no puede ser un factor de 2" (teorema fundamental de la aritmética).  
  
6.4. Consideremos los enteros: n — 1,n,n + 1,n +2. Se liene:  
(N-1)+n+(n+1)+(n+2)=4n+2=2.(2n+1).  
  
, A'h.ora. bien, como (2,2n + 1) = 1, de acuerdo con el teorema fundamental de la  
aritmética 2 tendría que ser un cuadrado para que 2.(2n + 1) fuese un cuadrado perfecto.  
  
6.5. SiI2p+1=", entonces 2p=(7-1)(7?+7+1).  
  
teoreAhºí\_a Zlen, como 7\* +7+1 siempre es impar, necesariamente, de acuerdo con el  
ia tuncamental de la aritmética se tiene z — 1 = ?; lueggo 7 = 3 y p=13.  
  
85  
Scanned by CamScanner  
  
  
--- Página 89 ---  
  
6.6. Si n no es potencia de 2, podemos escribir n = 2\*.:, donde £ > 0 c ? es un enterc  
  
impar mayor 0 igual que 3. Entonces:  
9ni1=22i+1=(2)'+1=(27 +1)(2?6-1 \_ 929 4 \_27 +1).  
  
Como cada uno de los dos factores del último miembro de la igualdad es un entero mayor  
que 1, 2" + 1 sería compuesto.  
  
Nota. Los números primos de la forma 2? + 1 se llaman primos de Fermat. Los cinco  
primeros primos de Fermat son: 2 11= 3, 2 1= 5, 27 11= 17, 22 11= 257,224+1 =  
  
Fermat conjeturó que todos los números de la forma 2? +1 eran primos, aún cuando  
no realizó los cálculos para números mayores que los cinco anteriores. Posteriormente, el  
matemático suizo Euler comprobó que el siguiente número de Fermat, 2? +1, no es primo  
(ver Problema 2.20). De hecho, se ignora si existen más primos de Fermat.  
  
Los números de Fermat aparecen en un problema completamente diferente, la cons—  
trucción de poligonos regulares con regla y compás. Se sabe que un polígono regular de n  
lados, con n primo impar, es constructible con regla y compás si y sólo si n es primo de  
Fermat. - - -  
  
6.7. Sea d la razón de la probgresión. Entonces  
Aan+1 = An + d Y On+k=Ant kd  
  
Sea k = an y consideremos el k-ésimo término después de an. Entonces an.x = k + kd=-  
= k(1 + d) y, por consiguiente, no es primo.  
  
6.8. S1 p, = pi + 2 entonces, necesariamente p¡ es de la forma 34 + ? y p, de la forma  
  
3k + 1, lueen pi + p: es divisible por 3. . s  
Además, comc p¡ y p2 di-:cren en -:7s unidades, uno de ellos es de la forma 4k +1 y  
  
el otro es de la forma 4k + 3, luego p -+ p, es divisible por d. '  
Por consiguiente, 12|(p + p2).  
  
6.9. Sin = pr'p?? ...py\* y d es un divisor de n, entonces d = pf'pfº ... P? donde los 6;  
son enteros tales que 0 < ; < a;; luego, cada $; puede tomar 1 + a; valores: 0, 1,...,;,  
que al combinarlos con los valores que pueden tomar los k — 1 exponentes restantes dan  
un total de  
  
(1+a1)(1+01)...(1+01)  
  
divisores.  
  
6'10P— ?l n =2P-1(27—1) y 2? -1 es un número primo, los divisores de n son los divisores  
de 2 y los divisores de 2?-1 multiplicados por ?? — 1. Estos son: -  
  
1,2,2? ,,, 297-? 9P-1 (1)  
  
Scanned by CamScanner  
  
  
--- Página 90 ---  
  
27 — 1,2.(2?—1),27.(2? —1),...,27-?.(97 — 1), (2)  
  
sin incluir al propio n.  
La suma de la progresión geométrica (1) es  
  
La suma de la progresión geométrica (2) es  
27-2.(27 — 1).2-— (27 —1  
E- DD (1) - (7 -1)= (7 -1)(2-1-1)  
Por consiguiente, la suma deseada es  
  
?— 1+(27—1).(221-—1)= (27 -1).(14271 1) =2=1 (9 - 1) =n.  
  
Nota. Si un entero positivo n coincide con la suma de todos sus divisores positivos menores  
que n, se llama un número perfecto . El problema anterior proporciona un método para  
hallar números perfectos pares, a p\_a…rt1r de los primos de Mersenne. 'Más aún, se puede -  
probar que todos los números perfectos pares son de esa forma. Todavía no se sabe  
si existen infinitos números perfectos páres, ni tampoco si existe algún número perfecto  
  
impar.  
  
6.11. Si n = l se tiene que k = 0 y logn = klog? = 0. Súpongamos quen > 1l y  
expresémoslo en su forma canónica - y  
  
— nA 02 a  
n-p1 p2 ...pk'  
  
donde pí,p2,...,Pk son primos diferentes y a1, 07,...,Q; son enteros positivos. Como.  
cada uno de los factores primos es mayor o igual que ?, se tiene  
  
n>201,2%,,,9% — 9014024504 > 96  
  
por cuanto a; > 1 para todo : = 1,...,k. Por consiguiente,  
  
logn > klog2.  
  
6.12. Sip=2,3 65 se verifica inmediatamente que (p 1)!+]1 es potencia de p.  
. luego (p — 1)' es divisible por  
  
Si p > 5, (p — 1)! tiene como factores 2,p — 1 y  
  
(P — 1)”; es decir, existe un entero z lal que (p—1)!' = :( - 1.  
Si (p — 1)! + 1 es potencia de p, se tiene que  
  
(P—-1)'=p"-1 donde n>1, (1)  
  
luego  
P-l=a(p-1)  
  
87  
  
Scanned by CamScanner  
  
  
--- Página 91 ---  
  
y n  
(p— 1 1(p" — 1).  
  
Ahora bien, esto se verifica si y sólo si (p—1)|n (problema 2.6. ), en cuyo caso sería n > p—1  
de donde  
  
P>Pl,  
Ppr-1>p!-1,  
P=-1> (p-1)!  
lo cual contradice a la igualdad (1).  
6.13. Supongamos que P1,P2,...,Pj son todos los primos de la forma 4k + 3 y con-  
  
sideremos el número  
n =4pip; ...p; — 1.  
  
n es de la forma. 4k + 3. Si n es primo, hemos terminado, por cuanto es diferente de  
cada uno de los p;, 1= 1,...,j.Sin es cnmpt.esto entonces n admite un divisor primo de  
la forma 4k +3, ya que el producto de números de la forma 4£ + 1 es también de la formz  
4k +1. Tal divisor es diferente de cada uno de los p; ya que, de lo contrario, dividiría a 1.  
  
Similarmente, como los números primos mayores que 3 son de la forma 6k+1 ó 6k+5  
y como el producto de números de la forma 61 + 1 es de la misma forma, si pi, P2io.aD:  
son números primos de la forma 6% + 5 entonces el número  
  
es de la forma 6k + 3 y tiene un divisor primo que no coincide con ninguno de los  
P1,P2, ... ,Pj.  
  
6.14. Supongamos n = £y con 1< ;y <n. Entonces se tiene:  
  
\_ 107 1 ¿0971 (105 -1D)1070-D 1 1074 ..T 107 !  
  
an — = \_\_\_ = EEEoo———];]—]]———]——]—]——————————— ];»————Ú—]——]];———————————————— —  
  
\_ 9 9  
L"—1(1oz(y—l) + 10702 4 ...+107+1),  
  
y, en consecuencia, a, no sería primo.  
  
6.15. Se requiere hallar el número de enteros n que satisfacen las condiciones:  
  
40000 < n? < 640000 (1  
y  
3n,2|n y |n. (2  
La condición (1) es equivalente a ,  
200 < n < 800 (3  
88  
  
Scanned by CamScanner  
  
  
--- Página 92 ---  
  
y la condición (2) es equivalente a  
  
30|n, (4)  
  
luego, es fácil ver que los números que satisfacen (3) y (4) son  
30.7,30.8,30.9,...,30.26.  
En total, 20 enteros.  
  
6.16. Supongamos que hay 8 números compuestos, a1, az,... , a3, Menores que 360 y que  
son primos dos a dos. Como y360 < 19, cada uno de estos números debe tener un factor  
primo menor que 19. Ahora bien, los números primos menores que 19 son  
  
2,3,5,7,11,13,17,  
  
en total 7, por consiguiente, de acuerdo con el principio de las casillas, por lo menos dos  
de los ocho números escogidos tienen un factor primo común.  
  
6.17 Se pide hallar todas las ternas ordenadas de números enteros positivos (a, b, c) tales  
que: - '  
[a, b) = 1000, [b, c] = 2000, (c, a = 2000.  
  
Como 1000 y 2000 son de la forma 2\*.59, entonces a, b y c deben ser de la misma forma.  
Luego: '  
a=2"1,5% =9 5% c — 20 593  
  
donde los a; y los 9; son enteros no negalivos para ¿ = 1,2,3. Además, como [a, b] = 23.33,  
[b,c] =2\*.3\*, [c,a] = 21.33, debe tenerse que:  
  
máx(a,02) =3,máx(02,03) = 4, máx(a¡, q;) =4, (1)  
má.x(;3¡,62] “ 3.máx[52,53] = 3,máx(\_51,\_63] =3. . (2)  
  
Para satisfacer (1) se tiene que 3 = 4 y además a ó Q7 es igual a 3, mientras que el otro  
puede tomar cualquiera de los valores 0, 1,2 ó 3. Hay siete ternas ordenadas que satisfacen  
estas condiciones:  
  
(3,0,4),(3,1,4), (3,2,4),(3,3,4), (0,3,4), (1,3,4), (2,3,4).  
  
Para satisfacer (2), dos de los B¡ son iguales a 3, mientras que el otro puede tomar cualquiera  
de los valores 0, 1,2 ó 3. Hay diez ternas ordenadas que saltisfacen estas condiciones:  
  
(3.3,1),(3,3,2),(3,0,3),(3, 1, 3),(3,2, 3).  
  
Como la elección de los a; es independiente de la de los 8;, se puede escoger un total de  
7.10 = 70 maneras diferentes, Esto corresponde al número de ternas ordenadas (a, b,c).  
  
89  
  
Scanned by CamScanner  
  
  
--- Página 93 ---  
  
be + ad = p:.'¡y, ) (2)  
b =pf"z (3)  
para tres enteros z, y, 7. Por consiguiente, de (1) y (3) se tiene  
(be)(ad) = p?"zz.  
  
Esta relación se cumple si y sólo si p; aparece elevado a un exponente mayor o igual —  
que a; en de o en ad, pero entonces la ecuación (2) muestra que p; aparece elevado a un  
exponente mayor o igual que a; en bc y en ad; por tanto bc y ad son múltiplos de p;'.  
  
El mismo razonamiento se aplica a todos los factores que aparecen en la expresión  
  
canónica de u.  
  
6.20. Si n fuese un número par, entonces 4" + n\* sería un número par mayor que 2 y, en  
  
consecuencia, sería compuesto.  
Supongamos que n es impar y procuremos escribir 4" + n1 como un producto de dos  
  
factores. Para ello, hacemos uso de la identidad  
+y =(7 +y + V20y(7? + y? — V27y).  
  
Sin=2k+1, entonces 4" = 4?5+1 — 44 — (/2.25)\*, luego 4 + n\* = (/2.25Y +n\*=  
  
= (2 +n? + 25+1n)(2" + n? — 25+In).  
Para finalizar la prueba, debemos ver que ambos factores son diferentes de 1. De  
  
hecho, basta probar que el menor de ellos es mayor que 1. En efecto,  
  
2 +n?- 261 — 926H1 1 (2 41)? - 2HBE11)="  
225225 (26+1)+(2k+1)?=  
[2 — (2k+1)?+2\* >5,  
  
ya que k > 0.  
  
6.21. Supongamos que n = pj 'p??...p7\*. como p; > 2 para todo i = 1,...,k, podemos |  
  
escribir  
n> 201902 9%% >9k  
  
Ahora bien, todo entero positivo está comprendido entre dos potencias consecutivas de 2;  
por consiguiente  
  
2m—1 S n< 9m  
para algún entero positivo m, y se tiene  
  
1  
< 9m—1"  
  
3|  
  
k<m y  
  
Multiplicando miembro a miembro ambas desigualdades:  
  
k m  
< (1)  
  
n - m  
  
91  
  
Scanned by CamScanner  
  
  
--- Página 94 ---  
  
Por otra parte, si m > 6 se verifica que  
  
m? <2-1  
  
(esta desigualdad puede demostrarse por inducción), luego  
  
m 1  
2m-T < m  
  
y reemplazando en (1) se tiene "  
  
— < —,  
  
n m  
l < á equivale a m > 1991; luego si tomamos no = 2191, bara todo n > n se tiene  
m  
k < 1  
n — 1991  
  
6.22. Como c —a = 19, se tiene que c=a+19ya=c-9. Por consiguiente, c > 19 :  
c >a.  
Como ¿\* = d? e y d? contienen los mismos factores primos en sus expresione:  
canónicas; luego si  
— m%1 02 k  
C =P 'P??...pR\*,  
— »O - 8 )  
d=py'p>'...D",  
  
30¡ 303 30g — 2,¡31 252 2;3¡ . . .  
entonces p¡ 'p) ... p — P Py\*... D yº se tiene que todos los exponentes de los  
primos en la descomposición canónica de ¿? ó d? son divisibles por 2 y por 3 (es decir, por  
6). -  
  
Con el mismo razonamiento podemos concluir que todos los exponentes de los primos  
que aparecen en la descomposición canónica de a5 ó b4 son divisibles por 5 y por 4 (es  
decir, por 20). Tenemos entonces que el valor, más pequeño que podría tomar a5 ó b\* sería  
920 .  
  
. , ?  
Ahc: bien, si a5 = b\* = 2% se -:ne  
  
a = 16,  
luego  
c=16+19=35,  
C=5.7,  
=5.7,  
  
y estos exponentes no son divisibles por 6.  
El segundo valor que se puede tomar para a5 ó b' es 320 En este caso se tiene  
  
a =3 =81,  
c =81+19=100,  
cC= 22\_52'  
C3 = 26\_56  
92  
  
Scanned by CamScanner  
  
  
--- Página 95 ---  
  
exponentes que sí son divisibles por 6. Entonces tenemos:  
a? =b',  
815 =b",  
3 =  
b=35=243.  
Por otra parte  
  
d =,  
  
d' = (10)",  
  
d? =105,  
  
d =10\* = 1000.  
  
Por consiguiente, '  
d— b= 1000 — 243 = 737.  
  
6.23. Tomando en cuenta la identidad:  
  
a"—b" =(a—b(a" ! +a”20+...+ab?+b"—1)  
  
en el número  
  
an = (2903" — 4647) - (803" —261") —  
  
observamos que 2903” — 464"” es divisible por  
2903 — 464 = 2439 — 9.271  
mientras que 803" — 261" es divisible por  
  
803 — 261 = 542 =2.271,  
  
luego an es divisible por 271; es decir, a, = 271b, donde D, es un entero.  
Pero a, también es igual a:  
  
(2903” — 803”) — (464" — 261")  
donde 2903" — 803" es divisible por  
2903 — 803 = 2100 = 7.300  
y 4647 — 261 es divisible por  
| 464 — 261 = 203 = 7,29,  
luego an es también divisible por 7.  
93  
  
Scanned by CamScanner  
  
  
--- Página 96 ---  
  
Como 7 /271,an = 271b, es divisible por 7 sólo si bn = TCn para algún entero c; por  
  
iguiente, - |  
consigu an = 271.7c, = 1897cn.  
  
Sección 7.  
7.1. Es preciso hallar la descomposición canónica del número 30!. Los números primos  
  
menores o iguales que 30 son  
2,3,5,7,11,17,19,23 y 29.  
  
Procedamos a determinar las máximas potencias de estos primos que dividen a 30!.  
  
3 a 0  
  
+[º]=10+3+1=14,  
  
+  
  
+  
— 1  
[ E O ]  
  
8 —l|% ór  
  
=l  
E—  
oo  
\_  
r—ll00  
o  
....—.  
lI  
1  
  
—  
»-AI(.0  
-1|O H  
E—  
  
II  
  
Por consiguiente, 30! = 2?6.3''.57.7\*.11?.13?.17.19.23.29. Entonces el m<:.or entero n  
de manera que 30'n sea un cuadrado perfecto es:  
  
n =5.17.19.23.29 = 1077205. \*  
  
7.2. Sean r =n+a,y = m+, donde m,n son enteros y a, 3 números reales tales que  
0 <a, f < 1. Entonces  
  
[z + [y) + [7 -+y)=m+n+m+n+[a+29)=2m+n)+[a+58),  
[27] + [2y] = 2m + [2a] + 2n + [26] = 2(m +n) + ([2a] + [23])-  
Por consiguiente, bastará probar que (a +2] < [2a]+([28). Si a+8 < 1 entonces [4+6] =0  
  
y se cumple la desigualdad. Si 2 + $ > 1, entonces a > = óB> l y se tiene [a +8] =1  
y [2a] + (28) >1. E , |  
  
94  
  
Scanned by CamScanner  
  
  
--- Página 97 ---  
  
2  
  
7.3. Se tiene: [IJ+[Í+1J=[Lg]+[[z;1]]=[%J+[[\_º\_lítl]\_  
  
2  
  
Si [r] es par, entonces  
  
Si [r] es impar, entonces  
  
2 2  
En ambos casos la suma es igual a [z].  
7.4. a) 2.4.6...(2n) = 2".n!.  
  
La mayor potencia k de un primo p que divide a n! es Z [ —¿-J , por consiguiente  
- . — Edl  
  
- i= -  
  
e —  
Z [—¡J si p es impar,  
=1 1P 1. '  
  
k= r  
n+ Z [9—] sip=2.  
  
i=1 57  
, 2n)' 2n)! ;  
b) 1.3.5...(2n — 1) = $)9n) “ '()ní31; por tanto, para calcular la mayor  
  
potencia de p que divide a 1.3.5...(2n — 1) bastará restar la mayor potencia de p que  
divide a 2".n! a la mayor potencia de p que divide a (2n)!. Esto es: -  
  
/ 2  
0 sip=2.  
  
7.5. Hay que demostrar que la mayor potencia de 2 que divide a (2n)! es mayor que la  
mayor potencia de 2 que divide a (n!)?, es decir:  
= [2n =f  
2,|77)> 2[5 1).  
1=1 i=1  
2n n ".  
º—] > 2[2—¡J Además, si j  
  
Ahora bien, en virtud de la propiedad 7.3. siempre se verifica [ 7  
<n  
  
es el mayor entero tal que 23 < 2+1 <2 se tiene'| — |= 5+1  
q < n, entonces 2 < 2n y se tiene E| O< ENE De  
  
aquí se concluye (1).  
  
Scanned by CamScanner  
  
  
  
--- Página 98 ---  
  
7.6. Multiplicando y di.vidien'do H(a + k) por a! se tiene:  
k=1  
  
-  
  
a+n)  
  
H( + k) =  
  
E a+n)!  
H(a + k) por cuanto ( a'n?) = (a 1- n) es entero.  
  
k=1  
  
y !  
  
7.7. En la identidad |  
T z+1|  
[z]\_[5H 2 ]  
  
(problema 7.3.), hacemos sucesivamente z igual a n, — 2 77 Se tiene  
  
2  
  
donde h es tal que 2\*> <n <\*\*1; por consiguiente,  
n | n  
Sumando miembro a miembro estas igualdades se tiene que  
00 k  
n+2  
k=0" "  
7.8. Para cualquier primo p, el mayor exponente a tal que p\*|(2m)!(2n)! es  
(.)  
  
E-EA-20-5)  
  
1=1 i=1  
96  
  
Scanned by CamScanner  
  
  
--- Página 99 ---  
  
mientras que el mayor exponente b tal que p” |mIn!(m + n)! es  
  
PE ra  
  
1=1 l-'l !-—l  
  
— EGPEE)  
  
i=l  
  
Basta demostrar que b < a; es decir, para todo 1,  
  
Pero esto se desprende de la identidad  
  
[z) + [y] + [7 + y] < [27] + [?y],  
planteada en el problema 7.2.  
7.9. Se debe probar que,v para todo .primo P,  
  
1=1 5 =1  
  
Denotemos por j y k a los enteros tales que p? < a < py p S.b < p\*T!. Se tiene:  
  
k  
  
.  
  
i=1  
I=j+k+1  
  
E  
  
[  
  
= [  
(  
  
»  
  
i=1  
  
Por cuanto, aplicando reiteradamente la propiedad 7.3. se tiene  
  
97  
  
Scanned by CamScanner  
  
  
--- Página 100 ---  
  
7.10. Denotemos F(z) = [27] + [4z] + (6z] + (8z].  
  
Si n es un entero positivo, entonces  
  
Sa + 1) = f(z) + 20n,  
  
luego si un entero k puede expresarse como f(T0) para algún número real z0, entonces para  
n = 1,2,3,... podemos expresar k + 20n de manera similar, ya que k + 20n = f(x0 + n).  
Por consiguiente, basta determinar cuáles de los primeros 20 enteros positivos pueden ser  
generados por f(z) cuando z recorre el intervalo semiabierto (0, 1).  
  
Obsérvese que cuando z se incrementa, el valor de S(Z) cambia únicamene si alguno  
de los números 2z, 4r, 6, 87 sobrepasa un valor entero. En el intervalo (0, 1) estos cambios  
  
m .  
ocurren cuando z es de la forma —, donde 1 <m<nyn=2,4,6u8. Existen 12 de  
  
estas fracciones, que escritas en forma creciente son  
  
Por consiguiente, sólo 12 de los primeros 20 enteros positivos pueden ser representados  
en la forma deseada, y en consecuencia 12.5 = 60 de los primeros 100 enteros positivos  
pueden representarse así. -  
  
7.11. Supongamos que existe una solución T. Podemos escribir  
  
- . La 1 .  
donde n es un entero, a, b, c, d, e son Igualesa Oóa1, YO< f< 35 De la ecuación dada  
  
se desprende que: .  
63n + 31a +15b+ T+ i+e= 12345;  
  
se tiene además que:  
63n < 12345 < G4n,  
  
donde n = 195, 63n = 12285 — 12345 — 60, y por tanto  
dMa+15b+7c+3d+e— 60.  
Pero'como a, b, c. d, e toman únicamente los valores 06 1, el valor máximo que puede tomar  
el primer miembro de la igualdad anterior es 57 y, por consiguiente, la ecuación original  
no tiene solución real. |  
7.12. El número k está ubicado entre dos potencias consecutivas de D. esto es  
P<k <p"+  
  
98  
  
Scanned by CamScanner  
  
  
--- Página 101 ---  
  
y por consiguiente, p” es uno de los valores que puede tomar ¿. Entonces p es un divisor  
  
de  
<pk") - W.!—p")!'  
  
Sean p“,p\* y p\* las mayores potencias de p que dividen a kl, (p")! y (k — p")! respectiva-  
mente. Entonces  
  
La mayor potencia de p que divide a (p ) es p -\*—", es decir, p[r"k\*[ 1. Como k <p"tl  
  
el e: a Slo si k = "11 v | ó iy |  
xponente [ n+l] es no nulo sólo si k = p"+1 y sólo en este caso será p un divisor de  
  
()  
  
7.13. El mayor exponente al cual se puede elevar 2 para que divida a n! es  
  
Escribamos n en base ?, es decir  
N \_ .  
n = ao.2 +a¡.2" 1+...+a¿.\_¡.2+a¡  
donde aj + O y, para todo ? tal que O < ¿ < k se tiene a;= 06ó a; =1. En este caso,  
  
k —  
[E]\_[Go.º +a1.2'º 1+...+ak\_¡.2+a¿  
=| — 1 TA  
2 2 !  
  
-  
-  
  
99  
  
Scanned by CamScanner  
  
  
--- Página 102 ---  
  
Como as <2, se tiene  
  
[;—]= (10.2k-l + a¡.2"'2 +...+Aadk—1,  
  
%] = a9.2? £ a,.23+...+ar-2,  
  
n  
| o2ra.  
  
n .  
?; = ap.  
Sumando miembro a miembro estas igualdades, se tiene que la mayor potencia de 2 que  
  
divide a n! es " E2  
ao.2 .+a,.2 \*+...+ak-1+  
  
— k3 , c  
+ao.2k 2+(11.2 3T...+ak\_2—¡—  
  
+ao-2 + a1+  
. \_ +ao.  
Por consiguiente, la mayor potencia de 2 que divide a n! es  
a0-(25—1) +a1.(251 — 1) + a2.(25? — 1) + ... + ax-1.(2—1).  
  
Sumando y restando ax,  
  
a9.(25 — 1) +a1.(21-—1)+a,.(21—1)+...+ax-1.(2-1) +ax.(1—1) =  
  
= aq.2 + a,.251 + a,. 24 ag 124 —(a0 + ap+ar+...+ar\_1+0s)=  
  
=n-(ao+a,+a7+...+ax-1 +ar). -  
Pero como ay £ O y a;= 06 a;=1 para todo 1, entonces  
  
n — (ay +aj +a7+...+ax-1+ax) <n—1.  
  
Si 2"—1 divide a n! se sigue que la mayor potencia de 2 que divide a n! es 2"-1. Ahora  
bien, si - '  
n— (ay +ar +az+...+ax-1 +ax) =n-—1,  
entonces necesariamente  
ay =07 =...=0k-1 =0.=0  
  
ya que ag = 1, por tanto  
  
n=254+0.25-1+02524 . +0.2+0,  
  
n=9k  
  
-  
  
100  
  
Scanned by CamScanner  
  
  
--- Página 103 ---  
  
Sección 8.  
  
8.1. De acuerdo con la propiedad 8. 8., la congruencia 7 = 1 (mód. 4) es equivalente a  
37 =3 (mód. 12) (1), y la congruencia 7 =2 (mód. 3) es equivalente a 47 = 8 (mód. 12)  
  
(2). Restando miembro a miembro (2) menos (1) se tiene:  
  
z = 5(mód. 12)  
  
que es la congruencia buscada.  
  
8.2. Sea 7 = aj.100" + a¡.100"-1+.. +an e 100+a,. Como 100 —1 (mód. 101), para  
  
todo entero positivo n se tiene:  
  
100" = (-1)"(mód. 101),  
  
luego,  
T = ao.(-1)" +a.(-1)" 1 + ... + An-1-(—1) +an(-mód. 101),  
I= (an + An-2 T An-4 +-. ) — (an.—1 + An-3 + An-5 +.. )(mód 101)  
  
Por tanto, 7 es divisible por 101 si y sólo si la diferencia entre la- suma de las cifras que  
ocupan lugares impares (contando desde la derecha) y la sumía de las cifras que ocupan  
lugares pares, escrito el número en base 100, es un múltiplo de 101.  
  
8.3. Sea 7 = aog.1000” +a;. 1000" 1+...+an—\_1.1000 + ax. Como 1000 = —1 (mód. 7.13)  
  
se tiene  
1000” = (—1)"(mód. 7.13),  
  
para todo entero positivo n. Luego,  
  
ao.(—1)" + a1.(-1) ! +...+an-1.(—1) + an(mód. 7.13),  
Y(mód. 7.13).  
  
.T  
z = (aAn + An-2 + An-4 +.'..)—(a,,\_1 + an\_3 + An-5 +...  
  
Por tanto, z es divisible par 7 ó por 13 si y sólo si la diferencia entre la suma de las cifras  
que ocupan lugares impares (contando desde la derecha) y la suma de las cifras que ocupan  
lugares pares, escrito el número en basc 1000, es un múltiplo de 7 ó de 13 respectivamente.  
  
Por otra parte se tiene  
' 1000 = 1(mód. 37),  
  
de donde  
1000" = 1(mód. 37)  
  
para todo entero positivo n. Luego,  
T ==ag +ai+...+an-1+ar(mád. 37).  
  
101  
  
Scanned by CamScanner  
  
  
--- Página 104 ---  
  
. ACE EE EE AA -  
  
Por tanto, 7 es divisible por 37 si y sólo si la suma de sus cifras, escnto el número en  
  
base 1000, es un múltiplo de 37.  
8.4. Obsérvese que para todo k tal que 1 < k <m, se tiene  
= (m — k) (mód. m),  
  
luego, si m > 2 entonces (1?, 2?,...,m?) no es un sistema completo de restos módulo m.  
  
8.5. Dados los enteros a, b, c, d, al menos dos de ellos son congruentes entre sí módulo 3,  
luego el producto de las seis diferencias es divisible por 3. Además, si no hay dos de esos  
enteros que sean congruentes entre sí módulo 4, entonces necesariamente dos de ellos son  
pares y los otros dos son impares; por consiguiente, el producto de las seis diferencias es  
  
divisible por 4.  
  
8.6. 2? + y” es congruente con 0,1 ó 2 móduio á, y si p es primo, entonces necesariamente  
P =1 (mód. 4). Por consiguiente 7? ó y? es congruente con 0 módulo 4 y al ser z, y primos  
  
y 7 > Y, se deduce que y =2.  
Similarmente se puede ver que b = 2, y de  
  
T +4=0+4  
se deduce que 7 = a.  
8.7. SiIn =2 se tiene:  
(a1 +02) =aj + ©a'f“1az +...+ <Pp 1)a1ao + a  
= al + a?(mód. n)  
Supongamos que se verifica:  
(a1 +a7+...+a,Y =a?+ab+...+a? (mód. p).  
Entonces tenemos  
  
(ar+a2+...+an+ans Y = ((a, +a2+...+a1)+an-1)? =  
(a1 +a2+...+an) +ah;, =  
  
por consiguiente la congruencia es cierta para todo entero positivo n.  
  
8.8.  
$n“"(-"—""1)—1=(ír—l)(a:"'l-l—a:"'º+...+:z:+l)—n(-'x'-1)=  
  
= (72-1("1+27"724.. . +7+1-n).  
  
102  
  
Scanned by CamScanner  
  
  
--- Página 105 ---  
  
Por consiguiente, basta probar que (7 — 1)|(2"-1 + 724 1, +1—n). En efecto,  
  
observese que  
T\_ ?= O(mód. z —1),  
  
277 \_99"3= O(mód. z-1),  
  
379 \_= O(mód. — 1),  
  
(n-1)7-(n-1)= O(mód. — 1).  
  
Sumando miembro a miembro las congruencias anteriores se llega a  
;] +z"'º+x"\_3+....+z+(l —n)50(mód. z—]1),  
conforme se quería demostrar.  
  
8.9. Sean a,b E (2,5,13, d), con a + b, y supongamos que el número ab—1 es un cuadrado  
perfecto. En particular tenemos:  
  
— 2d—1=?, — | - (1)  
d—-1=y?, (2)  
13d—-1=z?, (3)  
  
para algunos enteros y, y, . De la igualdad (1) se deduce que 7 es impar, luego 2d = z?+1=  
= 2 (mód. 8). Por consiguiente, d = 1 (mód. 4); luego d es impar y, en consecuencia, de  
acuerdo con (2) y (3), y, z son pares. Sean y = 2y1,2 = 2z1. Como 2? — y? = 8d, se tiene  
que  
  
4:f — 4ylº = 8d,  
  
de donde  
(21 — y(21 + y1) = 2d,  
  
y en consecuencia  
z1 = y1(mód. 2),  
  
luego  
(21— y)(71 + y1) = 2d = 0(mód. 4),  
  
por tanto, resulta que d es par, lo cual es una contradicción.  
  
8.10. Vamos a demostrar que si a = b (mód. 9) entonces S(an) = S(bn) (mód. 9)  
donde S(z) es la suma de las cifras del número z. Ahora bien, sia =b (mó'd.- 9) entonces  
an = bn (mód. 9), es decir, 9|(an — bn) y, de acuerdo con el criterio de divisibilidad por 9,  
9|S(an — óm).  
  
Faltaría probar que  
  
S(an — bn) = S(an) — S(bn)(mód. 9).  
  
103  
  
Scanned by CamScanner  
  
  
--- Página 106 ---  
  
Sean T =aº.10h+a¡.10\*'¡+-...+ak\_¡.10+ak.  
  
agregando, si es necesario, algunos ceros a la izquierda de manerz que ,y $E escriban con  
  
el mismo número de cifras.  
Entonces,  
  
1—y55(f—y)5(ao—bo)+(al—bl)+.--+(ak-bk)(mód- 9),  
  
pero  
S(7) =ao +a1 +...+ak,  
  
de donde  
  
Sx) — Sty) = (ao — bo) + (a1 — d1) + ... + (04 — de) = S(7 — vI(mód. 9).  
  
En el caso dado, 4891 — 1984 = 2907 y 9|2907, luego S(48911) — S(1984n) es un múltiplo  
de 9. ' . "  
  
.\_. s m n “ T.  
S.11. Sea p un divisor común de a?" 11 ya\* +1. Supongamos que N > M. De la  
  
congruencia  
a?” = —1 (mád. p),  
  
elevando ambos miembros a la 2— se tiene  
  
(a?”) (-1)? ” (mód. p).  
  
2m,9"—”  
  
II  
  
a? =1(mód. p).  
  
Por otra parte .  
a? = —1(mód. p),  
  
luego  
2=0(mód. p),  
  
de donde p|2, por consiguiente, si a es par se tiene (a?” +1,a? +1) =1 ysi a es impar.  
entonces (a?” +1,0?" +1) =2.  
8.12. Los enteros a, b, c satisfacen la igualdad a\* + b? = e?. Si c no es múltiplo de 5, hay  
ab  
7  
  
En primer lugar probemos que 5|ab. Se tiene  
5. y por consiguiente c? es congruente con 1 ó 4 módul  
¡y se tiene que a? y 6? son congruentes con 1 ó 4 mó  
congruente con 0,2 ó 3 módulo 5, lo que contradice el hecho  
4 módulo 5. Por consiguiente, 5/ab.  
  
que probar que 10  
que c es congruente con 1,2,364 módulo  
o 5. Si 5 fab, entonces 5 fa y 5 P.  
  
2 1 .2  
dulo 5, de manera que a + 07 ES -  
que c? es congruente con 1ó  
  
104  
  
Scanned by CamScanner  
  
  
--- Página 107 ---  
  
Veamos ahora que 4|ab. Como c? es congrúente con 0 ó 1 módulo 4, se presentan dos  
casos: - -  
  
a) ? = 0 (mód. 4). En este caso a? = 0 (mód. 4) y b? = 0 (mód. 4), por tanto a y b  
son pares y 4|ab. '  
  
b) <? = 1 (mód. 4). Como c? = a? + ?? se tiene:  
  
(a+b)º = a? +Qab+bº =? + 2ab,  
  
luego  
(a+b? -c  
  
2 L  
\_ (a+b+ca+b-e)  
=y — -  
  
Además, a? = 0 (mód. 4) y 5? =1 (mód. 4), o bien a? = 1 (mód. 4) y 5? = 0 (mód.  
4). Entonces se presentan las siguientes posibilidades. .  
  
ab =  
  
ab  
  
1)a=1 (mód. 4) ó a =3 (mód. 4) y b=0 (mód. 4) ó b =? (mód. 4),  
2) a= 0 (mód. 4) ó a =? (mód. 4) y b=1 (mód. 4) 6ó b =3 (mód. 4) .  
En total, hay ocho casos posibles. Analicemos el primero de ellos.  
  
Sia = 1 (mód. 4) y b = 0 (mód. 4), entonces c = 1 (mód. 4), y se tiene que  
a+b+c=2 (mód. 4) y a+b-c=0 (mód. 4), por tanto, existen enteros ky y kz tale-  
que  
  
c >b—c=4k>.  
  
Entonces,  
  
4k, +2).4k  
ab = (——-\*w = 4k,.(2k1 +1),  
  
-  
  
luego 4|ab. Entonces, como 2  
  
ab ab ab  
7y 5Ií se concluye que 10 7  
  
Para los casos restantes se hace un análisis similar.  
8.13. Sea A=(21-1,2?—1,2—1,...,226—1).  
  
Si ningún elemento de Á es divisible por 2k + 1, cada uno de los elementos de A debe  
ser congruente módulo 2k + 1 con alguno de los siguientes números:  
  
Se presentan dos casos:  
  
105  
  
Scanned by CamScanner  
  
  
  
--- Página 108 ---  
  
j  
  
a) Existen dos elementos de A,2" — 1 y 2'-1.conr> t, tales que  
  
2 —1=2-1(mód. 2k+1),  
  
de donde : —  
  
| 2" -? = 0 (mód. 2k+1),  
212 1) = O (mód. 2k + 1),  
  
(2k+1)1(27-"-1),  
  
y se llega a una contradicción por cuanto 2"-t \_ 1 es un elemento de A.  
b) No existen dos elementos de A con  
alguno de los elementos de A de  
  
un entero r, 1 <r < 2k, tal que  
  
gruentes entre sí módulo 2k + 1. En este caso  
be ser congruente con 2k módulo 2£ + 1, es decir, exist  
  
e  
  
27 —1=2k(mód. 26£ +1),  
2 =2k+1(mód. 2k+1),  
  
y entonces 2k + 1 divide a 27, con lo cual también se llega a un  
  
a contradicción. Por  
consiguiente, alguno de los elementos de A es divisible por 2k+1.  
  
8.14. Sea d, = (100+ n? 100+ (n+1)”). Entonces,  
  
dn = (100 + 1?,2n + 1).  
  
Como 2n + 1 es impar, d, es impar. Supongamos que dn =2k+1. Entonces se tiene:  
  
2n+1=0(mód. 2£+1). (1)  
  
100 +n\* = 0 (mód. 2k+1). (2)  
De (1) se deduce: \_  
n= k(mód. 2k +1),  
  
| (3)  
De (2) se tiene: n? = —100 (mód. 2k +1), luego  
  
n\*=-100+(2t+ 1).100 (mód. 2 +1),  
n\* = 200k (mód. 2k + 1),  
y por (3), |  
  
n\* = k? (mód. 24 + 1),  
luego  
  
k = 200 (mód. 2k + 1).  
106  
  
Scanned by CamScanner  
  
  
--- Página 109 ---  
  
Como (k, 2k + 1) = 1 para todo entero k, se puede simplificar:  
k = 200 (mód. 2k +1),  
  
luego  
2k+1=400+1(mód. 2£+1),  
  
2k +1=401(mód. 2k +1).  
  
Como 401 es primo, entonces 2k + 1 = 401 es el máximo valor que pude tomar da.  
  
Falta ver que efectivamente d, alcanza ese valor. Si  
  
n = 200 (mód. 2k +1),  
  
entonces .  
n? = 301 (mód. 2€+1),  
luego ' .  
100 +n\* = 401 (mód. 2k +1),  
y dado que ... |  
2n+1=0(mód. 2k +1),  
se tiene ' | —  
100 + (n+1)? = 401 (mód. 2£+1).  
  
Sección 9.  
9.1. Si (7,y,2) es un triple pitagórico primitivo, entonces se tiene:  
  
2 2  
  
z=m—n”,  
y = 2mn,  
z=mº+nº,  
  
donde m > n > 0,(m,n) = 1 y m y n tienen diferente paridad. Si z,y,z están en  
progresión aritmética, entonces  
y-1=2-3,  
luego  
, 2mn - m? +n? = m? + n? — 2mn,  
4mn = 2m?,  
m = 2n.  
  
Como n|m y (m,n) = 1, se tiene necesariamente n = 1, luego m = 2 y el único triple  
pitagórico primitivo cuyos términos forman una progresión aritmética es (3,4,5). Todos  
los triples que satisfacen la condición son de la forma (3k, 4k,5k), con k E Z.  
  
107  
  
Scanned by CamScanner  
  
  
--- Página 110 ---  
  
- 1 1 1  
9.2. De la igualdad 7 + y——2- = — se desprende  
  
!€  
  
y2? +722? =7?7, . (1)  
  
luego  
yz = 22y7 —7 = zº(yº \_ ?2),  
  
y si (7,y) = 1, entonces  
  
T?7, (2)  
Similarmente, de 2?z? = 2?y? — yº¿º = y?(1? — z?) se tiene que  
yZ\*. (3)  
  
Como hemos supuesto (7, y) = 1, de (2) y (3) se tiene  
2? |:?  
  
y, dividiendo por z?y\* ambos miembros de (1), nos queda  
. \_ 7 - —  
T, y \_  
  
92.3. Si 77 + y? = 2? entonces 7 Ó y es par. Si y es par, es de la forma 2mn, con m y n de  
diferente paridad, luego  
  
lo cual no es posible.  
  
y = 0 (mód. 4). )  
  
Sir= 16-1 (mód. 3) e y =1 6-1 (mód. 3), entonces :I:2 = y? =1 (mód. 3), luego  
z? =2 (mód. 3), lo cual no es posible y por tanto  
  
. | z =0(mód. 3) óy = 0 (mód. 3). : (2)  
  
Por otra parte, si n es un entero se tiene  
  
0 (mód. 5) si n = 0 (mód. 5),  
n= 1(mod 5)sin=lón=4 (mód. 5),  
1 (mód. 5) sin=2ón=3 (mád. 5)  
  
Se presentan los siguientes casos:  
  
2 2  
  
a) 7?=y? =1 (mód. 5), luego z? = 2 (mód. 5) (imposible).  
  
b) 772 = y? = —1 (mód. 5), luego 2? = —2 (mód. 5) (imposible).  
108  
  
Scanned by CamScanner  
  
  
--- Página 111 ---  
  
- —  
  
=  
A  
  
c) 2? =1 (mód. 5) e y? = -1 (mód. 5), o bien ? = -1 (mód. 5) e y? =1 (mód. 5).  
  
Entonces z? = 0 (mód. 5), luego  
  
2 =0 (mód. 5).  
  
De (1), (2) y (3) se concluye que zyz = 0 (mód. 4.3.5), luego 60|7yz.  
  
9.4. Consideremos dos casos:  
  
a) a impar. De la igualdad  
+y =2?  
  
se desprende -  
a?=22- y,  
a= (z+y)(2—3).  
  
Haciendo -  
Z+y= (12,  
\_ - 2—y =l,..-.  
se obtienen los valores \_ - \_ |  
2-1  
a  
y . 9 7  
a?+1  
  
que satisfacen la igualdad (1).  
  
b) a par. De la igualdád  
  
iao=  
se tiene  
  
a?=z?- a:º,  
a =(2+9):—-).  
  
Como a? = 4k, con k > 1, podemos hacer  
  
Z2+r=2k,  
  
2-TI=2,  
  
de donde , .  
22=2k+2=2(k+1)¡  
2=k+1,  
  
y  
27 =2k-2=k-1),  
T=k-1,  
  
(3)  
  
(1)  
  
Scanned by CamScanner  
  
  
--- Página 112 ---  
  
con lo cual queda resuelto el problema.  
  
9.5. En todo triángulo pitagórico primitivo de catetos ,y e hipotenusa z, se tiene T+y —  
= z\*, donde 7 = m? +n?, y = 2mn, z = m? — n? cam>n> 0,(M,7) =1 y m,n de  
diferente paridad. Entonces, el perímetro 2p del triángulo es: .  
  
2=T+y+z=  
= m? + n? + 2mn+m?-n?=—  
  
= 2m? + 2mn = 2m(m+n).  
  
Si 60 = 2m(m +n), entonces 30 = m(m +n). Ahora bien, 30 se puede escribir como  
un producto de dos factores positivos de las siguientes maneras:  
  
30 = 1.30,  
— 30=2.15,  
  
30 =3.10,  
  
30=5.6.  
  
Es inmediato verificar que para ninguna de estas descomposiciones se pueden hallar  
valores de m y n que satisfagan las tres condiciones: requeridas. Esto indica que no hay  
triángulos pitagóricos primitivos de perímetro 60. No obstante, esto no excluye la posibi—  
  
lidad de hallar soluciones no primitivas.  
  
Los divisores propios de 30 son: 1, 2, 3, 5, 6, 10 y 15. De éstos, los únicos que se pueden  
expresar como producto de dos factores m(m + n) donde m y n satisfagan las condiciones  
“requeridas son: 6 = 2.3y 15 =3.5. Sim =2 y n =1, esto conduce al triángulo pitagórico  
primitivo (3,4,5), cuyo perímetro es 12, ysim=3yn=2 se tiene el triángulo pitagórico  
primitivo (5,12,13),. cuyo perímetro es 30. Luego, los únicos triángulos pitagóricos cuyo  
perímetro mide 60 son: - D '  
  
(15,20,25) y (10,24, 26)..  
  
5r + 10ry + 10y = 47? + 127y + 9%? + 2? — 27y + y? =  
= (27 + 3y)\* + (7 — yy,  
  
92.6.  
  
luego, la ecuación original puede escribirse como:  
(27 +3y) + (7 — y) = (2+1)?.  
  
Si denotamos a = 27 + 3y,b=r-y,c=2+1, entonces las soluciones primitivas de  
  
a? + d? = son:  
a=m?-n?,  
  
b = 2nmn,  
  
7  
c=m" —nº,  
  
110  
  
Scanned by CamScanner  
  
  
--- Página 113 ---  
  
donde m y n son dos enteros arbitrarios, de diferente paridad, tales que (m,n) = 1 y  
  
m>n>0.  
Despejando z, y, z en términos de m y n, se obtienen las soluciones:  
m? — n? + 6mn  
1==—E — (1  
m?-—n?-4mn  
— 0)  
z=m"+n\*-1. (3)  
  
Por tanto, hay que agregar a m y n la condición adicional que sean tales que m?-—  
  
—n? + 6mn =mº—nº—4mn 0 (mód. 5). Como m? — n? + 6mn = m? — n? —4mn=  
= m? —n? + mn =0 (mód. 5), esto equivale a estudiar cuándo se verifica que  
  
m? —n? +mn = 0(mód. 5),  
  
es decir,  
= n(n — m) (mod 5).  
Áhora bien, si m =0 (rnod 5) entonces n=0 (mod a) p051b1hdad que se descarta  
  
porque en este caso (m,n) 1.  
Sim = 1 (mód. 5), entonces n = 3 (mód. 5); si m =2 (mód. 5), entonces 7 =1  
  
(mód. 5); si m =3 (mód. 5), entonces n = 4 (mód. 5); si m =4 (mód. 5), entonces n=2:  
(mód. 5).  
  
Con estas restricciones pará m y n, (1), (º) y (3) dan las soluciones de la ecuación.  
9.7. El área de un triángulo pitagórico primitivo viene dada por:  
1 .  
1= 5= ma(m —n)(m +1n).  
  
Como m y n tienen diferente paridad, tres de los cuatro factores son impares. Además,  
  
es fácil ver que son primos dos a dos.  
La única descomposición de 120 en 4 factores que cumplan con tales condiciones es:  
  
120 = 1.3.5.8  
  
(nótese que dos factores podrían ser iguales a 1 sólo en el caso de.ser m = 2,n = 1, luego  
  
no es aplicable aquí).  
  
Si m+n = 8, entonces m = 5 y n = 3 que son de la misma paridad y, por consi-  
guiente, no-hay Sóluciones primitivas. Esto no excluye la posibilidad de hallar soluciones  
no primitivas. Si los lados del triángulo son dz, dy, dz, entonces el área es:  
  
111  
  
Scanned by CamScanner  
  
  
--- Página 114 ---  
  
1  
A= Ed:cdy = d\*mn(m —n)(m+1n)  
  
y - puede ser el área de un triángulo primitivo. En su descomposición canónica,  
d? v  
  
contiene un cuadrado perfecto (2?), luego  
  
A  
  
5= 30,  
y como  
30=1.2.3.5,  
haciendo m + n = 5,m = 3,n=2, se tiene:  
z0 =9-4=5,  
yo = 12,  
zo=9+4=13,  
T =270 =10, - -  
y = 2y0 = 24,  
  
z = 2z0 = 6.  
  
El triángulo pitagórico de lados 10, 24 y 26 tiene por área 120.  
  
Sección 10.  
  
10.1. Como 91 =7.13, se tiene (n, 7) = (a,7) = (n, 13) = (a, 13) =1.  
De acuerdo con el teorema de Fermat  
  
nS = 1(mód. 7) y a“ = 1 (mód. 7),  
de donde, elevándo al cuadrado: -  
n1? =1 (mód. 7) y al? =1 (mód. 7).  
  
Además, \_  
n'\* =1 (mód. 13) y a?? = 1 (mód. 13).  
  
Como (7,13) = 1, de (1) y (2) se concluye  
n? = 1(mód. 91) y a'? = 1 (mód. 91),  
  
luego  
n1? = a\* (mód. 91),  
  
91|(n1? — a?).  
112  
  
Scanned by CamScanner  
  
  
--- Página 115 ---  
  
10.2. De la igualdad:  
n-n=n(n\*-1)=n(n\* - 1(1 +1) =  
= n(n— 1(n+ 1)(n2 +n+ 1)(n2 —n+1),  
  
se concluye que n' —n es divisible por 6, ya que en el último miembro aparece el producto  
de 3 enteros consecutivos. Además, de acuerdo con el teorema de Fermat se tiene:  
  
n =n(mód. 7),  
luego 7|(n7 — n). Como (6,7) =x1,\_.se tiene:  
— 42|(n' —n).  
10.3. Si 19|(4n? +4) entonces, como (19,4) = 1, necesariamente 19|(n? + 1), es decir:  
= —l (mód. 193, |  
  
pero hemos visto que esta congruencia no tiene solución cuando el módulo es un pnmo de — -  
la forma 4k +3, luego 19 J(4n? +4).  
  
10.4. Si m es primo, entonces la parte directa del problema no es más que el teorema de  
  
Wilson. —  
— Supongamos que (m — 1)! = —1 (mód. m). Si m es compuesto, entonces m= ab  
  
— donde a,b son enteros tales que 1 <a <b<m—1.  
  
Se pueden presentar los siguientes casos:  
  
a) a 7 b. Entonces ab|(m — 1)!; luego (m — 1)! =0 (mód. m).  
b) a =b=?. Se verifica inmediatamente que 3! £ —1 (mód. 4).  
c) a =b5?. Entonces 2a = 25 < m — 1 y-también abl(m — 1).  
En conclusión, si m es compuesto, (m — 1)! 5 —1 (mód. m).  
  
Nota. Obsérvese que hemos probado además, que si m es un número compuesto mayor  
que 4, entonces (m — 1)! = 0 (mód. m).  
  
10.5. Se tiene:  
  
3" y 3" T 75 W x  
De acuerdo con el teorema de Fermat, para todo entero positivo n se cumple:  
n\* =n(mód. 5), luego 3n? = 3n (mód. 15), (1)  
- n\*=n(mód. 3), luego 5n? = 5n (mód. 15), (2)  
113  
  
Scanned by CamScanner  
  
  
--- Página 116 ---  
  
y además se tiene:  
Tn = Tn (mód. 15). (3)  
  
Sumando miembro a miembro (1), (2) y (3) nos queda:  
3n5 + 5n\* + 7n = 15n (mód. 15),  
  
luego  
15/(3n5 + 5n? + 7n).  
  
10.6. Sabemos que  
1+2+--.+(p—1)=-p(pº—\_l).  
  
—l  
Como (p, p\_2\_> = 1, basta probar que  
  
P— =p-1(méd. »), (1)  
  
(p—1)!5p—l(mód. P5—1> | - (2)  
Ahora bien, (1) se deduce inmediatamente del teorema de Wilson y (2) también se  
p—1  
2  
  
verifica por cuanto  
  
—l  
(p—1)'y pT)(p — 1). Esto completa la prueba.  
  
10.7. a) Se tiene:  
  
27.4\*.6%...(p—1)\* =[2.4.6...(p— 1) =  
  
| NO  
[2'\*?£ (1.2.3 pT—1)J = 2P—1.(p—;l>2!.  
  
- Abora bien, como p es impar, el teorema de Fermat garantiza que  
271 =1(mód. p). | (1)  
  
Por otra parte, como consecuencia del teorema de Wilson hemos probado que  
-1 s(-.1)Lí-\*.(PT“1)!(mód. p),  
de donde, multiplicando ambos miembros por (—1)Lí\_l se tiene:  
P— 1 ? ;1 -  
(21) 1=(-1) (más. ») (2  
114  
  
Scanned by CamScanner  
  
  
--- Página 117 ---  
  
Multiplicando miembro a miembro (1) y (2):  
  
-1 (P-1Y\* '  
27 1.(p7) l=(-1) (mód. p),  
luego ' -  
2?.4?.6...(p-1)? = (-1)E (mód. p).  
  
b) De acuerdo con el teorema de Wilson:  
(7 — 1)! = -1 (mód. p),  
— (P—1)? = 1(mód. p),  
1%.32.5%...(p—2)?.22.4?.6?...(p— 1) =1(mód. p).  
Tomando en cuenta la parte (a) nos queda:  
12.32.5?...(p—2)?.(-1) =1(mód. p),  
  
y multiplicando ambos miembros por (—1)2';—1:  
— 123252...(p-2)?=(-1) (mód. p)- 7 -  
10.8. Si p es un primo diferente de ? y de 5, entonces p [10. De acuerdo con el teorema —  
de Fermat se tiene:  
  
10?-1 = 1 (mód. p),  
  
luego  
PIIOP — 1), — —  
  
y 107-1 — 1 es un número de la forma 999...999. Para todo entero positivo k Use—'1:i'<e—r'ie  
104(-1) = 1 (mód. p), de donde p|(10\*6-1) — 1), por consiguiente, p divide a infinitos  
  
números de esa forma. .  
Además, si p \* 3 entonces (p,9) = 1, y como un número de la forma 999...999 es  
  
igual a 9.(111...111),p divide también a infinitos números de la forme 111...111. Si por  
el contrario, p = 3, entonces p divide a todos los números de la forma 111...111 que tienen  
  
un número de cifras múltiplo de 3.  
10.9. Sean a =n,b=.n+1,c=n+2.Sin+1=£k\*, entonces  
a=kº—1,b\_=k3,c=kº+l.  
  
Debemos probar que (k\*—1)k\*(k3+1) = 0 (mód. 504). Abora bien, como 504 = 7.8.9,  
debemos demostrar que el primer miembro de la congruencia es divisible por 7, por 8 y  
  
por 9.  
115 -  
  
Scanned by CamScanner  
  
  
--- Página 118 ---  
  
a) Obsérvese que |  
(K — )RR +1)=K -6 = K(7 - £),  
y ¿e acuerdo con el teorema de Fermat, k” = k (mód. 7), luego  
(X — 1)X%E3 +1) = 0 (mód. 7).  
b) Si k es par, en¿onces k = 2k:, luego  
(k\* — 1)(26)%(4? + 1) = 0O (mód. 8).  
  
Si k es impar, entonces k? — 1 y k3 + 1 son pares y, además, alguno de los dos es  
congruente con 0 módulo 4, luego  
  
m (K — 1)1%(k3 +1) = 0 (mód. 8).  
c) Falta demostrar que k — k=0 (mod : 9) Tenemos:  
  
k - = k3(k\* 1).  
  
Si 3|k, entonces k3 = = 0 (mód. 9).  
Si3 ,(Á entonces (k 9) = 1 y, de acuerdo con el teorema de Euler se tiene:  
  
kº(º) = 1 (mód. 9).  
.Pero A(9) = 6: por consiguiente.  
| k = (mod 9).  
10.10. De a.cuerdo con el teorema de Fermat,  
14 —2“\*—34 —44 1(mód 5).  
  
“Sean= 4k + T, donde k, r son enteros y 0 <r < 3. Entonces si a es 1º'ual a 1,2,36  
  
4, se tiene  
— a" = afa" = a" (mód. 5),  
  
por consiguiente  
17 +2"+3"+4"=1"4+2"+3"+4"(mód. 5).  
De aquí se desprende que:  
  
4(mód. 5) si r =0,  
  
n ion¿anáin— ) O(mód. 5)sir=1,  
s O (mód. 5) sir =?,  
  
- O (mód. 5) si7 =3.  
  
116  
  
Scanned by CamScanner  
  
  
--- Página 119 ---  
  
Por consiguiente, 1" + 2" + 3" + 4" es divisible por 5 si y sólo si n ño es divisible  
por 4.  
  
10.11. Obsérvese que, si n = 1, entonces la ecuación no tiene solución entera, y si n =2  
entonces m = 1.  
  
Sea n = 4k + r, donde k y r son enteros con 0 <r < 3. De acuerdo con el teorema de  
  
Fermat se tiene  
  
\* = 1(mód. 5),  
luego  
34k+ — 34 37 =3" (mód. 5).  
Por tanto:  
  
1 (mód. 5) si n = 0 (mód. 4),  
  
3= .3 (mód. 5) sin =1 (mód. 4),  
  
\_ 4 (mód. 5) si n =2 (mód. 4),  
  
2 (mód. 5) sin = 3 (mód. 4).  
  
De la ecuación 3"-5" =4 se t1ene \_  
4 (mod 5),  
  
- por consiguiente n = 2 (mod 4) Entonces podemos tomar n = 4k +2 = 2t, donde  
  
= 2k +1. Luego, !  
3 -—4= 5"1  
(3"—2).(3+2) =57,  
y por tanto, si n > 2 entonces ambos factores de la 1zqu1erda son diferentes de 1 y deben  
verificarse, simultáneamente, las congruencias: .  
  
3 =2(mód. 5) y3º = —2(mód. 5)  
  
lo cual nO es pos¡ble -—Por consiguiente, la única solución en enteros positivos esn= 2  
=1. , u  
  
10.12. Si p =2, entonces p divide a 2" —n para todo entero par n. Supongamos p impar.  
  
Consideremos un entero positivo cualquiera m y tomemos  
n = (mp— 1p — 1).  
Entonces se tiene:  
n= mp2.— mMp-p+1=1(mód. p).  
Por otra parte, aplicando el teorema de Fermat,  
  
27 = (20-1)9"7=1 =1=1 = 1 (mód. p).  
  
117  
  
Scanned by CamScanner  
  
  
--- Página 120 ---  
  
Por consiguiente, 2" —n = 0 (mód. p) para infinitos valores de n.  
  
- . . ... nn+1  
10.13. La suma de los primeros n enteros positivos es Sn = —(——2+—-2, y su Pproducto es  
  
n!. Hay que demostrar que Sn|n! si y sólo si n +1 no es primo.  
Supongamos n + 1 primo. De acuerdo con el teorema de Wilson se tiene:  
  
n! = —1(mód. n+1),  
  
de donde (n+1) fn!. Como n > 1 y n+1 es primo, entonces n+1 > 2yen consecuencia es  
impar, luego 5n = —2-)(n + 1) donde % es entero y, por tanto, S, [n!, lo cual contradice  
  
la hipótesis. Por consiguiente, n + 1 no es primo.  
\_ Recíprocamente, supongamos que n + 1 no es primo. Entonces n+1 = ab, donde a y  
b son enteros tales que 1I< a <b<n+1. Consideremos dos casos.  
  
a) Si a < b entonces los factores a, b aparecen entre los números 1,2,...,7—]. Como  
n! =n(n — 1)!, se puede escribir '  
- n! = nabk.  
. ! . Nn+1  
Luego n(n + 1)|n! y, en consecuencia, —(—-9——2 n.  
b) Si a = b entonces n.+1= a? y por tanto, entre los números 1,2,...,7 + 1 aparece  
  
l - u - - U , 7 . .. . 2 c  
a= (n+1)?. Debemos ver que a aparece como fáctor de otro término. El siguiente término  
que contiene un factor de a es:  
  
1  
2a = n+1)7.  
  
Es preciso verificar que 2(n + 1)% <n-—1. Esto es,  
  
4(n+1) <n?-2n+1,  
n? — 6n-—3>0.  
  
lad  
  
La desigualdad se cumple si n > 7. ÁAhora bien, los únicos enteros n menores que 7  
para los cuales n + 1 no es primo son 3 y 5. En el caso n =3 se tiene 53 =3! = 6, luego  
S1|3!. En el caso n = 5,n+1 = 6 no es cuadrado perfecto y estamos en el caso (a). Por  
consiguiente, para todo n > 1, si n + 1 no es primo entonces Su|n!.  
  
Sección 11.  
  
11.1. Si 15|(57 + 1)(37 + 2) entonces 3|(57 + 1(3r + 2) y 5(57 + 1)(37 + 2). Ahora bien,  
37+2=2 (mód. 3) luego 3 /(3x +2) y necesariamente se tiene: -  
  
57 + 1 = 0(mód. 3),  
  
118  
  
Scanned by CamScanner  
  
  
--- Página 121 ---  
  
\_ PÓNES AA de NAA de  
  
$e  
  
REbPÁN A —  
  
FOO  
  
- a- — -  
  
ENE Y\_.\_',.  
  
\_,  
-  
  
A ..  
  
— aaa ad a  
  
— — NA d a n CEA NR  
  
de donde  
57 = —1(mód. 3),  
—z = —1(mód. 3),  
  
z = 1(mód. 3). (1)  
  
Similarmente se observa que \_  
37 +2=0(mód. 5),  
  
de donde  
37 = —-2(mód. 5),  
  
—27 = —2(mód. 5),  
z =1(mód. 5). (2)  
De (1) y (2) se deduce inmediatamente que (57 + 1)(3z +2) es divisible por 15 para todos  
  
los z tales que >  
z = 1(mód. 15).  
  
11.2. Se requiere hallar todos los enteros z tales que, simultáneamente,  
  
“(z=1 (mód.3) :fr=1 (mód.14) =1 (mód. 5)  
ó ' () ó  
z=2 (mód. 3), r=2 (mód. 4), ==2 (mód. 5). -  
Empleando la misma notación usada.en el texto, se tiene:  
m = 3, m = 4, m3 = 5, m= 60, V . Í\_'\_\_\_\_\_  
A 9097 =15 =1  
m mao m;  
  
20b; = 1(mód. 3) = 1= —1,  
125 = 1(mód. 5) =>b5= 2— \* .  
= —20a; — 15a; — 24az(mód. 6).  
  
Asignándoles a a1,a2,a; los valores 1 ó 2, se forma la tabla:  
  
az zm(mód.60)  
  
aj a  
  
1 1 1 1  
1 1 2 -23  
1 2 1 -14  
1 2 2 22  
2 1 1 -19  
2 1 2 17  
2 2 1 26  
2 2 2 2  
  
119  
  
Scanned by CamScanner  
  
  
--- Página 122 ---  
  
E T OAPEEREE NEO ERE  
el  
  
O INE  
  
11.3. La congruencia 7? -1 = O(mód. 56) es equivalente al par de congruenciag.  
  
T-—1= O(mód. 8),  
T-1= O(mód. 7).  
  
Por inspección, en sistemas completos de restos módulo 8 y módulo 7 respeºtivmnente, s  
observa que la primera congruencia tiene por soluciones 7 = 1,3,5 6 7 (mód. 8) mientra  
que las soluciones de la segunda congruencia son 7 =1 66 (mód. 7). Por consiguiente  
la congruencia z? — 1 = 0 (mód. 56) tiene 8 soluciones, a saber, las soluciones de los  
siguientes sistemas de congruencias:  
  
7=1 (mód. 8) ( + =3 (mód. 8), / 7=5 (mód. 8), f +T=7 (mód. 8),  
=1 (mód. 7) | \*=1 (mód. 7). |7 =1 (mód. 7). | 7 =1 (mód. 7).  
  
=1 (mód. 8) [ +=3 (mód. 8), [ 7=5 (mód. 8), f +=7 (mód. 8),  
7 =6 (mód. 7). | 7 =6 (mód. 7). | 7 =6 (mód. 7). | \* =6 (mód. 7).  
Estos sistemas pueden resolverse aplicando el teorema chino del resto, y se obtienen las  
  
soluciones: \*  
7 =1,—13, —27,15, —15,27, 136 — l(mód.\_\_ 56).  
  
11.4. Como 210 = 2.3.5.7, la congruencia llz+1=0 (mód. 210) es equivalente al sistema  
  
de congruencias:  
ll7 +1=0(mód. 2),  
  
l17 +1=0(mód. 3),  
llz +1=0(mód. 5), -  
117 +1=0(mód. 7), ' |  
  
de donde: ¡ ' .  
7 = 1 (mód. 2),  
7 =l(mód. 3),  
7 = -1 (móád, 5), - N “.  
  
7=—2(mód. 7).  
  
Aplicando el teorema chino del resto a estas cuatro congruencias se obtiene la solución  
  
7 = 19 (mód. 210).  
  
11.5. Como 35 — 5.7, la congruencia 512 +7 -3=0 (mód. 35) es equivalente al par de  
congruencias: o ,  
S +Tr-3= O(mód. 5),  
  
b +77-3= O(mód. 7),  
En virtud de las identidades 57? = 0 (mód, 5) y TT = (1 (mód. 7), las congruencías  
anteriores se reducen a:  
72 = 3(mód. 5), (1)  
  
120  
  
Scanned by CamScanner  
  
  
--- Página 123 ---  
  
O ÓN Eny uEl  
  
p de  
  
5? = 3(mád. 7). (2)  
De (1) se deduce que 7 = 4 (mód. 5) y de (2) se tiene que 7 = 3 (mód. 7) ó7 = 4  
(mód. 7), luego la congruencia 5772 + 77 - 3=0 (mód. 35) tiene dos soluciones, que son  
las de los sistemas de congruencias:  
(1: = 4 (mód. 5), z =4 (mód 5),  
7 =3 (mód. 7). z =4 (mód. 7).  
Aplicando el teorema chino del resto se obtienen las soluciones 7 = —11 (mód. 35) y  
7 =4 (mód. 35).  
  
11.6. Consideremos k enteros positivos que sean primos dos a dos, por ejemplo, k números  
primos diferentes: p¡,p2,...,p. Entonces, para todo i, j = 1,...,k, se tiene (p3,p3) =1  
y, de acuerdo con el teorema chino del resto, las congruencias: '  
  
—1(mód. p?),  
—2(mód. p3),  
  
z  
  
— Z 2  
r = —k(mód. p?),  
tienen soluciones simultáneas. Si Tq es una de tales soluciones, se tiene:  
  
Pil(zo +1),  
P2llzo +2),  
  
conforme se quería demostrar.  
  
Sección 12.  
  
12.1. Los enteros positivos menores o iguales que 3600 que tienen un factor común con  
3600 son aquellos que no son primos con 3600, luego su nNúmero es:  
  
3600 — $(3600) = 3600 — 960 = 2640.  
  
12.2. Sea n = p?rp?...p?. Si p|n entonces P coincide con alguno de los p;(i =  
  
= 1,...,k). Podemos suponer, sin pérdida de generalidad, que p = p,. Entonces se tiene:  
np=Ptpy...pO  
121  
  
Scanned by CamScanner  
  
  
--- Página 124 ---  
  
2 E P  
  
pl ia aal e lag d  
  
(2.3600 + 1,2.3600 + 2, 2.3600'+ 3,...,3.3600),  
  
(6.3600 + 1,6.3600 + 2,6.3600 + 3,...,7.3600), .  
  
son sistemas completos de restos módulo 3600, luego cada uno de ellos contiene el mismo  
número de enteros primos con 3600, esto es, $(3600) = 960. En total hay:  
  
7.960 = 6720  
de tales números.  
12.8. Este resultado es una generalización del pr6b1ema. anterior. L<.)slconjuntos:  
[1,2,3,...,m),  
(m+ 1,m+2,m+3,...,2m],  
(2m+1,2m+2,2m+3,... ,3m), -  
  
[(k—l)rn+l,(k—i)m+2,(k—1)\*n+-3,...,km],  
  
son k sistemas completos de restos módulo m, en cada uno de los cuales hay 6é(m) números  
primos con m. En total, el número de enteros -positivos menores o iguales que mk que son  
  
primos con m es kó(m).  
  
12.9. Sean m y n dos enteros positivos tales que (m,n) — 1. Los divisores de mn son de  
la forma díd2, donde di|m, de|n y (d1,d2)=1. Entonces, \* -  
  
fmn)= Y) a(dd)= Y) oaa(d:)=  
  
.¿¡?¡[mn dí d:|mN  
= Y> 9(d1) Y. a(d) = AMÁ(?).  
diim di|m "  
  
12.10. Consideremos la función identidad g definida en el conjunto de los enteros positivos;  
esto es, 9(d) = d para todo entero positivo d. Obviamente, y es multiplicativa y, de acuerdo  
con el problema 12.9., también lo es la función f definida por:  
  
f(7) =Y 9) = ).  
din din  
Para todo primo p. la suma de los divisores de p” es  
a+1 \_ 1  
l+p+7 +...+p9 = —  
p-1  
123  
  
Scanned by CamScanner  
  
  
--- Página 125 ---  
  
é(nP) = np(l - E) (1 - ;;>(1 - pk>!,  
élnp) = póln). :  
Si p /n, entonces (p, n) = 1 y se tiene:  
  
é(np) = Aln)s(P) = (P — 1)s(n).  
  
12.3. Se sabe que:  
  
p|imn  
  
Si n|m entonces todo primo p que divide a n, divide también a m. luego:  
  
de donde ¿m = 'm'n T <1 \_ %) = nélm). - !  
  
p|m  
  
12.4. Sin = pf1p9? ... p entonces, de la ígualdad  
  
ó(n) = p1'py\* ...P. , m »  
  
se deduce: .b(n) = py 971 ...py\*'(p1 — 1(p2 — 1)...(px — 1), donde se observa que  
  
si alguno de los p;(1 =1,...., k) es impar, entonces p; — 1 es par y, por consiguiente, ¿(n)  
e< par. Accnás, sin =2" y a > 1, :.ionces 2%-1 es par y á(n), en consecuencia, también  
lo es. Lu-. , los únicos enteros n y. 1 los cu:: i A7 + impar son 1y2.  
  
12.5. De acuerdo con el problema 12.2, $(21) = 26(n) si 2|n y o(2a) = á(n) in 2 ín  
luego $(2n) = á(n) si n es impar y S(2n) > é(n) si n es par.  
  
?  
  
12.6. Si n = 5“, entonces  
  
p(n) = 'º'.<1 — —>= 4.5€-1,  
que no es divisible por 3 para ningún entero a.  
12.7. Obsérvese que 25200 = 7.3600. Los conjuntos:  
(1,2,3,...,3600),  
(3600 + 1, 3600 + 2,3600 + 3,...,2.3600),  
122  
  
Scanned by CamScanner  
  
  
--- Página 126 ---  
  
. AE ' RE —  
¿e T Ea e A e ad a DR ae  
.  
  
| PRO EE NRE MN  
  
(2.3600 + 1,2.3600 +2, 2.3600+ 3,...,3.3600),  
  
(6.3600 + 1,6.3600 +2, 6.3600 + 3,..-, 7.3600), .  
ada uno de ellos contiene el mismo  
  
son sistemas completos de restos módulo 3600, luego c  
960. En total hay:  
  
número de enteros primos con 3600, esto es, $(3600) =  
  
7.960 = 6720  
  
de tales números.  
  
12.8. Este resultado es una generalización del problema anterior. Los conjuntos:  
  
(1,2,3,...,m),  
(m+1,m+2,m+3,...,2m],  
(2m+1,2m+2,2m+3,...,3m) -  
  
((k-1)m+1,(k- Dm+ 2,'(k — m £3,...,km),  
  
son k sistemas completos de restos módulo m, en cada uno de los cuales hay 6(m) números  
  
primos con m. En total, el número de enterospositivos menores o iguales que mk que son  
  
primos con m es kó(m).  
  
12.9. Sean m y n dos enteros positivos tales que (m,n) — 1. Los divisores de mn son de  
la forma díd2, donde di|m, di|n y (d1,d2) =1. Entonces, \* -  
  
fímn)= Y) a(did)= Y) a(do(4)=  
  
,d¡£i;[mn di d |MN  
= Y) a(d1) Y> a(da) = f(m)f(n).  
  
12.10. Consideremos la función identidad y definida en el conjunto de los enteros positivos;  
esto es, g( d) = d para todo entero positivo d. Obviamente, g es multiplicativa y, de acuerdo  
con el problema 12.9., también lo es la función f definida por:  
  
f(n) = Y 9(d) = Y d.  
d|n d|n  
Para todo primo p. la suma de los divisores de p“ es  
pa+1 —1  
  
p—-1  
  
b  
  
123  
  
Scanned by CamScanner