***Números** AROLMAR*

1. Introducción

1.1 Definición de los números Arolmar

Un número Arolmar es el producto de dos o más números primos semiconsecutivos que tiene la propiedad de que la media aritmética de dichos factores es otro número primo. Son libres de cuadrados, ya que sus factores primos son distintos, y es la representación más pequeña, por lo que los primeros factores deben ser los primeros primos consecutivos. Un número será Arolmar y se denotará como $N_{arm} = p_1 \cdot p_2 \cdot \ldots \cdot p^n$ si, y sólo si,

$$Mp = \frac{p_1 + p_2 + \ldots + p_n}{n} = w, \quad w \in \mathrm{P}.$$

1.2 Origen y primeros desarrollos

Con fecha 23 de febrero de 2011, el profesor de matemáticas jubilado don Antonio Roldán Martínez, publicó en su blog http://hojaynumeros.blogspot.com/2011/02/primos-por-todas-partes.html, la secuencia $21,33,57,69,85,93,105,129,133,145,177,195,\ldots$ y una pregunta: *¿sabes qué propiedades comparten estos números?* La respuesta la contesta él mismo: *Tienen todos sus factores primos distintos, son números libres de cuadrados, y el promedio de esos factores es un número primo*.

Con fecha 4 de marzo de 2011, aparece la secuencia OEIS A187073, que queda registrada como http://oeis.org/A187073.

Con fecha 10 de marzo de 2011, y a través de http://www.hojamat.es/, web propiedad del profesor Roldán Martínez, aparece publicada en Facebook, donde se presentan varios ejemplos sobre las características de estos números, que continúan en días sucesivos, ya que su estructura ha despertado gran interés entre los entendidos en la materia.

La versatilidad de estos números se pone de manifiesto al tratar de aplicar sus características al número 2011, que también es primo. Aún limitando el producto y suma a nueve cifras, los números necesarios crecen de una manera desorbitada, lo que hace imposible su búsqueda mediante la secuencia A187073, por lo que les hace idóneos para los cifrados en criptosistemas.

TABLA I Representación del 2011

	factores primos										
media	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**suma**	**producto**
2011	3	4019								4022	12.057
2011	3	19	6011							6033	342.627
2011	3	5	19	8017						8044	2.284.845
2011	3	5	7	31	10009					10055	32.579.295
2011	3	5	7	11	29	12011				12066	402.308.445
2011	3	5	7	11	13	29	14009			14077	6.100.008.915
2011	3	5	7	11	13	17	31	16001		16088	126.614.392.905
2011	3	5	7	11	13	17	19	37	17987	18099	3.227.663.994.555

2. Secuencia A187073 y los números Arolmar

2.1 La secuencia A187073

En la información que nos ha llegado del profesor Roldán Martínez, a través de distintos medios, la secuencia recoge la cantidad *mínima* en que puede ser representado un número como producto y media aritmética de dos o más factores primos. En este sentido, la secuencia **A187073** recoge este principio, pero también aparecen otros que, no siendo *mínimos*, sí se ajustan a las características requeridas. Esta visión queda mucho más patente cuando la secuencia se contempla desde el punto de vista de la media aritmética y no desde el producto.

Si p es un número primo, que es media aritmética de dos o más factores, y k la cantidad de dichos factores, entonces

$$p=\frac{2p}{2}=\frac{3p}{3}=\frac{kp}{k}=\frac{q_1+q_2}{2}=\frac{q_1+q_2+q_3}{3}=\frac{q_1+q_2+q_3+\ldots+q_k}{k}$$

2.2 Los números Arolmar

Por la Conjetura de Goldbach, sabemos que un número puede ser descompuesto en suma de números primos, con distinta combinaciones, dependiendo de la cantidad de que se trate. La mayor dispersión entre los primos nos llevará a un número *mínimo* en su producto, siendo el resto de productos meras representaciones como asociados. Por ejemplo, para el número primo 41, tenemos:

$$41=\frac{82}{2}=\frac{123}{3}=\frac{164}{4}=\frac{205}{5}=\frac{3+79}{2}=\frac{3+7+113}{3}=\frac{3+5+7+149}{4}=\frac{3+5+7+11+179}{5}$$

que serían las representaciones mínimas. Los números Arolmar generados, resultan ser

$3\times79=237$; $3\times7\times113=2373$; $3\times5\times7\times149=15645$; $3\times5\times7\times11\times179=206745$

Estos deben ser los verdaderos números primos *Arolmar*. Pero hay otras representaciones del número 41 a las que llamaremos asociados, así

$82=11+71=23+59=29+53$
Asociados: 781, 1357, 1537

$123=5+11+113=7+13+103=11+23+89=13+31+79=17+23+83=19+31+73$
$=23+29+71=29+41+53$
Asociados: 6215, 9373, 22517, 31837, 32453, 42997, 47357, 63017

$164=5+7+13+139=7+11+19+127=11+13+31+109=13+17+31+103=17+19+31+97$
$=19+23+43+79=23+29+41+71=29+31+37+67=31+37+43+53$
Asociados: 63245, 185801, 483197, 705653, 971261, 1484489, 1941637, 2228621, 2614013

$205=5+7+11+19+163=7+11+13+17+157=11+13+17+37+127=13+17+19+29+127$
$=17+19+23+37+109=19+23+29+37+97=23+29+31+43+79=29+31+37+47+61$
$=31+37+41+43+53$
Asociados: 1192345, 2671669, 11423269, 15464917, 29961157, 45483397, 70239769, 95365021, 107174533

Todos estos números pertenecen a la secuencia A187073, pero no son números primos Arolmar, tal vez ¿asociados? ¿enteros asociados?.

2.3 Representación de los números primos como números Arolmar

Para fijar ideas, vamos a calcular las representaciones de los números primos comprendidos entre $5 \le P \le 103$, con $k = 2$.

TABLA II, Números primos del 5 al 103

Números Arolmar				Números asociados						
P	q_1	q_2	$2P$	Representaciones de kP						
5	3	7	10							
7	3	11	14							
11	3	19	22	5+17						
13	3	23	26	7+19						
17	3	31	34	5+29	11+23					
19	7	31	38							
23	3	43	46	5+41	17+29					
29	5	53	58	11+47	17+41					
31	3	59	62	19+43						
37	3	71	74	7+67	13+61	31+43				
41	3	79	82	11+71	23+59	29+43				
43	3	83	86	7+79	13+73	19+67				
47	5	89	94	11+83	23+71	41+53				
53	3	103	106	5+101	17+89	23+83	47+59			
59	5	113	118	11+107	17+101	29+89	47+71			
61	13	109	122	19+103	43+79					
67	3	131	134	7+127	31+103	37+97	61+73			
71	3	139	142	5+137	11+131	29+113	41+101	53+89	59+83	
73	7	139	146	19+127	37+109	43+103	67+79			
79	7	151	158	19+139	31+127	61+97				
83	3	163	166	17+149	29+137	53+113	59+107			
89	5	173	178	11+167	29+149	41+137	47+131	71+107		
97	3	191	194	13+181	31+163	37+157	43+151	67+127		
101	3	199	202	5+197	11+191	23+179	29+173	53+149	71+131	89+113
103	7	199	206	13+193	43+163	67+139	79+127	97+109		

3. Números idóneos en los criptosistemas

3.1 Estudio preliminar

En el año 1997 los profesores Thomas W. Cusick, de la Universidad de Búfalo en USA; Cunsheng Ding, de la Universidad de Hong Kong en China, y Ari Renvall, de la Universidad de Turku en Finlandia, participaron en un proyecto sobre cuáles serían las características de los números para ser utilizados en criptosistemas. De este proyecto salió un libro denominado Stream Ciphers and Number Theory, publicado en 2004 con ISBN: 0-444-51631-X. Las conclusiones fueron de que ciertos números primos presentan una menor vulnerabilidad a los ataques a mensajes cifrados que otros. Aunque son muchos, algunos de estos primos los recogemos en los apartados siguientes.

3.2 Primos Fuertes

Un número Fuerte es un número primo que es mayor que la media aritmética de sus primos predecesor y antecesor, que podemos representar como $P_f = P_n > \frac{P_{n-1} + P_{n+1}}{2}$. Por ejemplo, 499 es un primo Fuerte ya que $499 > ((491-1)+(503+1))/2 = 499 > 497$. Alguno primos con estas características se pueden encontrar en A051634:

11	17	29	37	41	59	67	71	79	97	101	107	127	137	149
163	179	191	197	223	227	239	251	269	277	281	307	311	347	367
379	397	419	431	439	457	461	479	487	499	521	541	557	569	587

Un número primo p es primo Fuerte si satisface las siguientes condiciones:

$p-1=aq,$ o bien $p\equiv 1(mód.q),$ donde a es un entero y q un primo grande.
$q-1=br,$ o bien $q\equiv 1(mód.r),$ donde b es un entero y r un primo grande.
$p+1=cs,$ o bien $p\equiv -1(mód.s),$ donde c es un entero y s un primo grande.

Por ejemplo, el número 277 es un primo Fuerte, ya que

$$1)\ 277-1=12\cdot 23,\ \ 2)\ 23-1=2\cdot 11,\ \ 3)\ 277+1=2\cdot 139$$

También se cumple de forma modular, ya que

$$1)\ 277\equiv 1(mód.23),\ \ 2)\ 23\equiv 1(mód.11)\ \ 3),\ \ 277\equiv -1(mód.139)$$

Se generan tres números primos (277,139,23) que pueden ser combinación, dos a dos, de una clave RSA.

3.3 Primos Buenos

Un primo Bueno es un número primo cuyo cuadrado es mayor que el producto de dos números primos en el mismo número de posiciones antes y después de que en la secuencia de números primos. Un primo Bueno satisface la desigualdad $P_n^2 > P_{(n-i)}P_{(n+i)}$ con $1\le i\le n-i$ y donde P_n es el enésimo primo. Por ejemplo, el 37 es un primo Bueno, ya que $P_n^2 > P_{n-1}\cdot P_{n+1} = 37^2 > 31\cdot 41 = 1369 > 1271.$ Algunos primos con estas características se pueden encontrar en A28388:

5	11	17	29	37	41	53	59	67	71	97	101	127	149	179
191	223	227	251	257	269	307	311	331	347	419	431	541	557	563
569	587	593	599	641	727	733	739	809	821	853	929	937	967	1009

3.4 Primos Equilibrados

Un número primo Equilibrado es igual a la media aritmética de sus primos predecesor y sucesor. Satisfacen la igualdad $P_e = \frac{P_{n-1}+P_{n+1}}{2}$. Por ejemplo, el número 257 es un primo Equilibrado, ya que $(251+263)/2 = 514/2 = 257.$ Algunos primos con estas características los podemos encontrar en A006562:

5	53	157	173	211	257	263	373	563	593	607	653	733	947	977
1103	1123	1187	1223	1367	1511	1747	1753	1907	2287	2417	2677	2903	2963	3307
3313	3637	3733	4013	4409	4457	4597	4657	4691	4993	5107	5113	5303	5387	5393

3.5 Primos Débiles

Por su alta vulnerabilidad se consideran primos Débiles para la criptografía a los que tienen la forma $P_d = P_n < \frac{P_{n-1}+P_{n+1}}{2}$. Por ejemplo, 109 es un número débil ya que $109 < (107+113)/2 = 109 < 110.$ Algunos primos con estas características se pueden encontrar en A051635:

3	7	13	19	23	31	43	47	61	73	83	89	103	109	113
131	139	151	167	181	193	199	229	233	241	271	283	293	313	317
337	349	353	359	383	389	401	409	421	433	443	449	463	467	491

3.6 Primos de Sophie Germain

Los primos de Sophie Germain son de la forma $P_{sg} = \{p, 2p+1\}$ donde ambos resultan ser primos. Por ejemplo, el 419 es primo de Sophie Germain ya que $\{p, 2p+1\} = 419,839$. He aquí algunos primos con estas características que pueden encontrar en A005384:

2	3	5	11	23	29	41	53	83	89	113	131	173	179	191
233	239	251	281	293	359	419	431	443	491	509	593	641	653	659
683	719	743	761	809	911	953	1013	1019	1031	1049	1103	1223	1229	1289

3.7 Polinomio Ciclotómico

Se llama Polinomio Ciclotómico de índice n a $\Phi_n(z) = (z-p_1)(z-p_2)\cdot\ldots\cdot(z-p_k)$, donde $p_1, p_2, \ldots, p_k$ son las k raíces primitivas enésima de la unidad en el cuerpo de los números complejos, siendo $k = \varphi(n)$ la función de Euler. Los polinomios Φ_n tienen sus coeficientes en $\mathbb{Z}$, son irreductibles sobre $\mathbb{Q}$ y verifican que $z^p - 1 = \prod_{d/p} \Phi_p(z)$.

Si p es primo distinto de 2, cualquier primo q que divida a $2^p - 1$ debe ser uno más que un múltiplo de $2p$. Proposición que también se cumple cuando $2^p - 1$ es primo. Por ejemplo, para $2^5 - 1 = 31 = 1 + 6\cdot 5$ ó $2^{11} - 1 = 2047 = 23\cdot 89 \rightarrow \begin{cases} 23 = 1 + 2\cdot 11 \\ 89 = 1 + 8\cdot 11 \end{cases}$.

Para cualquier primo p, si $\varphi(p^k) = p^{k-1}(p-1)$, y teniendo en cuenta que $n = 2^{q-1}(2^q - 1)$, donde $Mq = 2^q - 1$, se deduce que son primos de Mersenne si y sólo si, q es primo. Por ejemplo, el número 13 es un primo de Mersenne ya que $2^{13} - 1 = 8191$ es primo. He aquí algunos primos con estas características:

2	3	5	7	13	17	19	31	61	89	107	127	521	607	1279
2203	2281	3217	4253	4423	9689	9941	11213	19937	21701	23209	44497	86243	110503	132049

Un número de Wagstaff es un número primo de la forma $P_w = \frac{2^q + 1}{3}$ donde $q \in P$. Por ejemplo, 2731 es un primo de Wagstaff ya que $(2^{13} + 1)/3 = 2731$. Son números que crecen muy rápidamente. Pueden encontrar alguna representación más en A000979:

3	11	43	683	2731	43691	174763	2796203	715827883	2932031007403

Algunos de los exponentes q que generan este tipo de números los pueden encontrar en la secuencia A000978:

3	5	7	11	13	17	19	23	31	43	61	79	101	127	167

Los número Repunits se definen como $R_n = \frac{10^n - 1}{10 - 1}$, $n \geq 1$. El número Repunit costa de n ejemplares del dígito 1, por lo que la secuencia sería $1,11,111,1111,\ldots,1111111$, como pueden comprobar en A002275. En el número primo Repunit es fácil mostrar que si n es divisible

por a, entonces R_n es divisible por R_a, esto es $R_n = \frac{1}{9}\prod_{d/n}\Phi_d(10)$, donde Φ_d es el Polinomio Ciclotómico y d oscila más allá de los divisores de n. También es la función Indicatriz $\varphi(n)$ de Euler. Para p primo, $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$, que posee la forma esperada de un Repunit cuando x se sustituye por un 10. Así, para que R_n sea primo, n debe ser primo. Pero no es suficiente el que n sea primo, por ejemplo, $R_3 = 111 = 3 \cdot 37$, no es primo. Para R_n, en la secuencia A004023 encontramos los siguientes valores de n en donde se asegura que generan números primos:

2	19	23	317	1031

Cuando se cambia la base 10 por una base b, el Repunit se convierte en $R_n^b = \frac{b^n - 1}{b-1}$, $n \geq 1$. Por ejemplo, para la base 3 y $n = 3, 7, 13, \ldots$ obtenemos:

13	1093	797161

todos primos, con un crecimiento desorbitado.

4. Vulnerabilidad de los números Arolmar

4.1 Como números Fuertes, Equilibrados y Débiles

Dependiendo de su grado de vulnerabilidad para la criptografía, los números pueden ser Fuertes, Equilibrados y Débiles, según tengan la forma de

$$P_f = P_n > \frac{P_{n-1} + P_{n+1}}{2}, \quad P_e = \frac{P_{n-1} + P_{n+1}}{2}, \quad P_d = Pn < \frac{P_{n-1} + P_{n+1}}{2}$$

Para números Arolmar y números primos, obtenemos

n	Sobre números Arolmar	Sobre números primos
33	33<(21+57)/2 = 33 < 39	33<(31+37)/2 = 33 < 34
57	57>(33+69)/2 = 57 > 51	57>(53+59)/2 = 57 > 56
69	69<(57+85)/2 = 69<71	69>(67+71)/2 ≠ 69=69
85	85>(69+93)/2=85>81	85<(83+89)/2=85<86
93	93<(85+105)/2 = 93<95	93>(89+97)/2 ≠ 93=93
105	105<(93+129)/2 = 105<111	105<(103+107)/2 ≠ 105=105
129	129>(105+133)/2=129>119	129>(127+131)/2 ≠ 129=129
133	133<(129+145)/2=133<137	133<(131+137)/2=133<134
145	145<(133+177)/2=145<155	145>(139+149)/2=145>144
177	177>(145+195)/2=177>170	177>(173+179)/2=177>176

con un resultado muy variado.

4.2 Como números Buenos

Un primo Bueno satisface la desigualdad $P_n^2 > P_{(n-i)}P_{(n+i)}$ con $1 \le i \le n-i$ y donde P_n es el enésimo primo.
Para números Arolmar y números primos, obtenemos

n	Sobre números Arolmar	Sobre números primos
33	$33^2 < (21 \cdot 57) = 1089 < 1197$	$33^2 < (31 \cdot 37) = 1089 < 1147$
57	$57^2 > (33 \cdot 69) = 3249 > 2277$	$57^2 > (53 \cdot 59) = 3249 > 3127$
69	$69^2 < (57 \cdot 85) = 4761 < 4845$	$69^2 > (67 \cdot 71) = 4761 > 4757$
85	$85^2 > (69 \cdot 93) = 7225 > 6417$	$85^2 < (83 \cdot 89) = 7225 < 7387$
93	$93^2 < (85 \cdot 105) = 8649 < 8925$	$93^2 > (89 \cdot 97) = 8649 > 8633$
105	$105^2 < (93 \cdot 129) = 11025 < 11997$	$105^2 > (103 \cdot 107) = 11025 > 11021$
129	$129^2 > (105 \cdot 133) = 16641 > 13965$	$129^2 > (127 \cdot 131) = 16641 > 16637$
133	$133^2 < (129 \cdot 145) = 17689 < 18705$	$133^2 < (131 \cdot 137) = 17689 < 17945$
145	$145^2 < (133 \cdot 177) = 21025 < 23541$	$145^2 > (139 \cdot 149) = 21025 > 20711$
177	$177^2 > (145 \cdot 195) = 31329 > 28275$	$177^2 > (173 \cdot 179) = 31329 > 30967$

donde predomina la variedad aunque con cierta tendencia positiva en los números primos.

5. Criptografía

5.1 Seguridad en los sistemas criptográficos

Sea G un grupo abeliano finito con $g \in G$. Sea $< g >$ el subgrupo de G generado por g. Si $h \in < g >$, el *problema del logaritmo discreto* (DLP), es encontrar un entero **n** tal que $g^n = h$. Efectivamente, conocidos **g** y **n** es computacionalmente sencillo calcular **h**, sin embargo, dados **g** y **h**, la solución es imposible. El logaritmo discreto consiste en resolver la ecuación $h \equiv g^x (mód.n)$, donde **h** y **g** son constantes y **x** es la incógnita que se busca. Es clara la similitud de esta ecuación con la del logaritmo, sin embargo, el uso de modulares introduce una complejidad grande al problema. La mayoría de los métodos utilizan el logaritmo discreto para calcular las claves públicas y privadas.

5.2 Codificación de mensajes

Códigos para codificar mensajes claros, basados en Tablas de Códigos ASCII formato de caracteres estándares.

TABLA III: Códigos ASCII del alfabeto español

	Letras mayúsculas															
Letra	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**
Código	65	66	67	68	69	70	71	72	73	74	75	76	77	78	209	79
Letra	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**Á**	**É**	**Í**	**Ó**	**Ú**
Código	80	81	82	83	84	85	86	87	88	89	90	193	201	205	211	218
	Letras minúsculas															
Letra	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**ñ**	**o**
Código	97	98	99	100	101	102	103	104	105	106	107	108	109	110	241	111
Letra	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**á**	**é**	**í**	**ó**	**ú**
Código	112	113	114	115	116	117	118	119	120	121	122	225	233	237	243	250
	Números y operaciones															
Números	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**+**	**-**	*****	**/**	**=**	**^**
Códigos	48	49	50	51	52	53	54	55	56	57	43	45	42	47	61	94
	Signos varios															
Signos		**¡**	**!**	**¿**	**?**	**(**	**)**	**{**	**}**	**[**	**]**	**<**	**>**	**%**	**@**	**&**
Códigos	32	161	33	191	63	40	41	123	125	91	93	60	62	37	64	38

5.3 RSA: Generación de claves

A quiere enviar a **B** un mensaje **m** secreto que sólo ellos puedan leer. A tal efecto, establecen una serie de claves de la siguiente forma:

1. **A** selecciona **p** y **q**, dos números primos grandes, y calcula $n = p \cdot q$. A continuación calcula $\varphi(n) = (p-1)(q-1)$, utilizando la función Indicatriz de Euler, o bien $mcm(p-1, q-1) = s$, si utiliza la función de Carmichael.
2. Selecciona un entero **e** tal que $mcd(s,e) = 1$, con $1 < e < s$, y calcula **d** donde $e \cdot d \equiv 1(mód.s)$, o bien $d \equiv e^{-1}(mód.s)$. La clave Pública será $\{e,n\}$ y la clave Privada $\{d,n\}$.

Operación de cifrado:

Texto claro **m**, con $0 < m < p$. Texto cifrado $C \equiv m^e (mód.n)$

Operación de descifrado:

Texto cifrado **C**. Texto descifrado $m \equiv C^d (mód.n)$

Ejemplo: Sea $n = 41 \cdot 79 = 3239$, $s = \varphi(3239) = (41-1)(79-1) = 3120$, $mcd(s,23) = 1 \rightarrow e = 23$ de donde $23d \equiv 1(mód.s) \rightarrow d = 407$. **A** debe enviar a **B** el mensaje $m = 1234$, y procede a su cifrado:

Cifrado de **A**: $C \equiv 1234^{23}(mód.3239) = 269$, y lo envía a **B**.
Descifrado de **B**: $m \equiv 269^{407}(mód.3239) = 1234$.

Los números primos 41 y 79 proceden de $(3+79)/2=41$, donde $3 \cdot 79=237$ y $7 \cdot 151=1057$, son números primos Arolmar, ya que $(3+79)/2=41$ y $(7+151)/2=79$. El valor de $e = 23$ se ha determinado por $(23+59)/2=41$, donde $23 \cdot 59=1357$ es un número asociado de Arolmar.

5.4 Protocolo: Diffie-Hellman

Dos personas, **A** y **B**, desean establecer una clave secreta para intercambiar información. El protocolo que establecen es el siguiente:

1. **A** y **B** conciertan un número primo **p** suficientemente grande, y **g**, un generador multiplicativo que es una raíz primitiva módulo **p**. Ambos pueden ser públicos.
2. **A** elige aleatoriamente un entero **a**, $a \in \{1,2,...,p-1\}$, que mantiene en secreto, y calcula $A \equiv g^a (mód.p)$ cuyo resultado envía a **B**.
3. **B** elige **b**, $b \in \{1,2,...,p-1\}$, que mantiene en secreto, y calcula $B \equiv g^b (mód.p)$ cuyo resultado transmite a **A**.
4. **A** y **B** crean como clave secreta **K**, donde $K \equiv g^{ab} (mód.p)$. Para ello, **A** calcula $K \equiv \mathrm{B}^a (mód.p)$ y **B** calcula $K \equiv \mathrm{A}^b (mód.p)$.

La fortaleza del protocolo se basa en que, conocidos $\{p,g\}$ y $\{A=g^b, B=g^a\}$, se puede calcular g^{ab}. Efectivamente, $K\equiv g^{ab}\equiv A^b\equiv B^a(mód.p)$

Ejemplo: Sea $p=179,\ g=19,\ a=7,\ b=11.$ Calcular el protocolo de intercambio de claves entre **A** y **B**.

A calcula $A\equiv 19^7(mód.179)=155$ y **B** calcula $B\equiv 19^{11}(mód.179)=142.$

La clave secreta viene determinada por $K\equiv 19^{7\cdot 11}(mód.179)=124,$ que cada uno comprueba al calcular $K\equiv 155^{11}(mód.179)=124$ y $K\equiv 142^7(mód.179)=124.$ Esto último queda demostrado por $K\equiv 19^{7\cdot 11}\equiv 155^{11}\equiv 142^7(mód.179)=124.$

El número primo 179 se ha obtenido como $(5+353)/2=179,$ donde $5\cdot 353=1765$ es un número primo Arolmar. Los valores 19, 7 y 11 proceden de $(5+7+11+19+853)/5=179,$ $5\cdot 7\cdot 11\cdot 19\cdot 853=6239695,$ un número asociado Arolmar.

5.5 Criptosistemas con: ElGamal

Basado en el protocolo de Diffie - Hellman, ElGamal constan de tres partes: el generador de claves, y los algoritmos de cifrado y descifrado.

Generación de claves: El usuario **A** elige un número primo **p** y un generador **g,** que es una raíz primitiva módulo **p**. De forma aleatoria, elige **a**, $a\in\{1,2,...,p-1\}$, y calcula $A\equiv g^a(mód.p)$. Clave pública $\{A,p,g\}$ y clave privada $\{a\}$.

Cifrado: Un usuario **B** quiere enviar un mensaje **m**, $1<m<p,$ al usuario con clave pública $\{A,p,g\}$. Elige **b**, $b\in\{1,2,...,p-1\}$, y calcula $B\equiv g^b(mód.p)$ y $C\equiv A^b m(mód.p)$. El mensaje cifrado es el par (B,C).

Descifrado: El usuario con clave pública $\{A,p,g\}$ y privada $\{a\}$, recibe (B,C) y calcula $K\equiv B^a(mód.p)$ y recupera el mensaje como $m\equiv C/K(mód.p),$ ya que $K\equiv g^{ab}\equiv A^b(mód.p).$ Se puede evitar la división módulo **p**, ya que $m\equiv B^{p-1-a}C(mód.p).$ En efecto

$$B^{(p-1-a)}C\equiv g^{b(p-1-a)}g^{ab}m\equiv (g^{p-1})^b m\equiv m(mód.p)$$

Ejemplo: Sean $p=179,\ g=11,\ a=7,\ b=6.$ Calcular el protocolo de intercambio de claves entre **A** y **B** para que **B** remita a **A** el mensaje $m=123.$

Los valores de **A** y **B** son $A\equiv 11^7(mód.179)=157$ y $B\equiv 11^6(mód.179)=177,$ respectivamente. En cuanto a la clave secreta **K**, $K\equiv 11^{7\cdot 6}(mód.179)=51,$ como se puede comprobar a nivel de usuario, $K\equiv 157^6\equiv 177^7(mód.179)=51.$

La codificación del mensaje, es $C\equiv 157^6 123(mód.179)=8.$ Por tanto, **B** remite a **A** el par de números $(B,C)=(177,8)$ como clave pública y guarda como clave privada $\{b\}=\{6\}.$

A puede descifrar el mensaje mediante $m \equiv 177^{(179-1-7)}8(mód.179) = 123.$ Y puede comprobar la firma mediante $m \equiv (11^{179-1})^6 123(mód.179) = 123$ y $C \equiv 11^{6(179-1-7)}11^{7\cdot 6}8(mód.179) = 8.$

5.6 Criptosistemas con: MASSEY - OMURA

Supongamos que un conjunto de usuarios deciden usar en común un número primo, suficientemente grande, al que llamaremos **p**. El conjunto de mensajes, tanto claros como cifrados, será sobre $\mathbb{Z}p.$ Para el establecimiento de claves se opera de la siguiente forma:

Generación de claves: Cada usuario **u**, $u \in U,$ elige al azar un entero **e**, $0 < e_u < p-1,$ con $mcd(e_u, p-1) = 1$ y calcula $d_u \equiv 1(mód.p-1).$ Ambos enteros son privados.

Intercambio de mensajes: Supongamos que el usuario **A** desea enviar al usuario **B** un mensaje **m**. Opera de la siguiente forma:

1. El usuario **A** calcula $r \equiv m^{e_a}(mód.p)$ y lo envía a **B**.
2. El usuario **B** calcula $s \equiv r^{e_b}(mód.p)$ y lo envía a **A**.
3. El usuario **A** calcula $t \equiv s^{d_a}(mód.p)$ y lo envía a **B**.
4. Finalmente, el usuario **B** recupera el mensaje **m** mediante d_b ya que $t^{d_b} \equiv m(mód.p).$

Ejemplo: Para el intercambio de mensajes, **A** y **B** acuerdan, mediante el número primo **p**, $p = 733,$ generar como claves secretas $e_a = 7 \in A$ y $e_b = 13 \in B.$ **A** envía a **B** como primer mensaje la palabra **Arolmar,** que una vez codificada resulta $m = \{65,114,111,108,109,97,114\}.$
A calcula $7d_a \equiv 1(mód.733-1) \rightarrow d_a = 523$ y **B** calcula $13d_a \equiv 1(mód.733-1) \rightarrow d_b = 169,$ ambas como claves públicas.

El intercambio de mensajes sigue el siguiente proceso:

1. **A** envía a **B**: $r \equiv m^{e_a}(mód.p) \rightarrow r \equiv m^7(mód.733) = \{214,96,223,573,491,576,96\}.$
2. **B** envía a **A**: $s \equiv r^{e_b}(mód.p) \rightarrow s \equiv r^{13}(mód.733) = \{238,627,214,88,20,416,627\}.$
3. **A** envía a **B**: $t \equiv s^{d_a}(mód.p) \rightarrow t \equiv s^{523}(mód.733) = \{682,158,65,47,80,239,158\}.$
4. **B** envía a **A**: $t^{d_b} \equiv m(mód.p) \rightarrow t^{169} \equiv m(mód.733) = \{65,114,111,108,109,97,114\}.$

con lo que se alcanza la codificación de **Arolmar**.
Algunas propiedades matemáticas de este sistema:

$$r \equiv m^{e_a} \equiv m^{e_a e_b d_b}(mód.p) \equiv m^7 \equiv m^{7\cdot 13\cdot 169}(mód.733) = \{214,96,223,573,491,576,96\}$$
$$s \equiv r^{e_b} \equiv m^{e_a e_b}(mód.p) \equiv r^{13} = m^{7\cdot 13}(mód.733) = \{238,627,214,88,20,416,627\}$$
$$t^{d_b} \equiv m^{e_b d_b}(mód.p) \equiv t^{169} \equiv m^{13\cdot 169}(mód.733) = \{65,114,111,108,109,97,114\}$$

Para la codificación de este sistema hemos utilizado números Arolmar. Veamos cómo. Hemos buscado un número primo **p** de la forma $p = 2mq + 1$ en donde **m** es un entero compuesto pequeño y **q** es un número primo grande. El primo en cuestión resulta ser $p = 2mq + 1 = 2 \cdot 6 \cdot 61 + 1 = 733.$ Este número lo sometemos al test de vulnerabilidad para la criptografía:

$$733-1=6\cdot 61\rightarrow 733\equiv 1(mód.61)$$
$$61-1=12\cdot 5\rightarrow 61\equiv 1(mód.5)$$
$$733+1=2\cdot 367\rightarrow 733\equiv -1(mód.367)$$

que lo pasa, a pesar de que $733\geq(727+739)/2=733=733$ es la media aritmética de los números primos anterior y posterior de 733 y, por tanto, un número primo Equilibrado.

El valor de $e_a=7$ se ha determina por $(7+1459)/2=733,$ donde $7\cdot 1459=10213$ es un número primo Arolmar. El valor de $e_b=13$ corresponde a $(13+1453)/2=733,$ donde $13\cdot 1453=18889$ es un número asociado Arolmar.

He tomado los números primos **1123** y **1847**. Mediante la función de Carmichael, he calculado **1035606** por lo que $d=691397$ y $e=103943.$ De acuerdo con las Tablas de Códigos ASCCII, he codificado el mensaje **m** = *{68, 101, 115, 101, 111, 32, 117, 110, 97, 32, 102, 101, 108, 105, 122, 32, 97, 110, 100, 97, 100, 117, 114, 97, 32, 97, 32, 108, 111, 115, 32, 110, 250, 109, 101, 114, 111, 115, 32, 65, 114, 111, 108, 109, 97, 114}* y lo he criptografiado de la forma *{1920746, 198422, 1953583, 198422, 175170, 530855, 1342805, 1313237, 1962883, 530855, 1586509, 198422, 75369, 1953269, 1010714, 530855, 1962883, 1313237, 1380087, 1962883, 1380087, 1342805, 796752, 1962883, 530855, 1962883, 530855, 75369, 175170, 1953583, 530855, 1313237, 2039978, 919863, 198422, 796752, 175170, 1953583, 530855, 1124410, 796752, 175170, 75369, 919863, 1962883, 796752}.*

Con un poco de paciencia, alguien descifrará mis deseos hacia estos números.

6. Conclusiones

Se denomina Arolmar al número $N,$ que es producto de $k,\ \mathrm{k}\geq 3$ factores primos semiconsecutivos y distintos, que tiene la propiedad de que la media aritmética $q,\ \mathrm{q}\in \mathrm{P}$ de dichos factores es otro número primo y que, en su acepción más amplia, están recogidos en la secuencia OEIS A187073.

$$21,33,57,69,85,93,105,129,133,145,177,195,205,213,217,231,237,249,253,265,...$$

Si q es un número primo y k es el número de particiones de $qk=p_1+p_2+...+p_k$ donde $p_1,p_2,...,p_k$ son números primos distintos. Como se cumple que $q=(p_1+p_2+...+p_k)/k$ es la media aritmética, llamamos número Arolmar al producto $N=p_1\cdot p_2\cdot ...\cdot p_k.$ Si N es la mínima representación, serán números primos Arolmar. Por ejemplo: para $q=23$ y $k=3,$ si $qk=3\cdot 23=69,$ tenemos que

$$23=(3+5+61)/3\ \rightarrow\ N=3\cdot 5\cdot 61=915$$
$$23=(3+7+59)/3\ \rightarrow\ N=3\cdot 7\cdot 59=1239$$

el primero es un número primo Arolmar y el segundo es un número asociado Arolmar. Y decimos que es asociado porque el primero es menor que el segundo.
Como $m=kq,\ \mathrm{q}\in \mathrm{P},$ podemos establecer una base matemática sobre las secuencias que representen a estos números primos Arolmar, así la secuencia

$$21,33,57,69,93,217,129,265,177,213,...$$

se genera teniendo en cuenta que $k=2$ y, por tanto $N=p_1\cdot p_2$ y $q=(p_1+p_2)/2.$ es la media aritmética. Por ejemplo: Por ejemplo: $265=5\cdot 53,\ (5+53)/2=29.$ Ver tabla IV.

TABLA IV: Números primos Arolmar

k	q	$m=kq$	p_1, p_2	$q=(p_1+p_2)/k$	$N=p_1\cdot p_2$
2	5	10	3,7	5	21
2	7	14	3,11	7	33
2	11	22	3,19	11	57
2	13	26	3,23	13	69
2	17	34	3,31	17	93
2	19	38	7,31	19	217
2	23	46	3,43	23	129
2	29	58	5,53	29	265
2	31	62	3,59	31	177
2	37	74	3,71	37	213

Utilizando el mismo procedimiento, para valores de $k=3,4,5,\ldots$ podemos crear las siguientes secuencias:

$105,195,483,465,645,987,915,1185,1743,1545,\ldots$
$1365,3045,3885,5565,6405,12045,10605,11445,24765,15645,\ldots$
$33495,50505,68145,91455,102795,201705,173355,214305,206745,361095,\ldots$

Todos estos números pueden ser obtenidos mediante la secuencia OEIS A187073, pero no de forma consecutiva.

Si tomamos la serie de números Arolmar $N\le 1000,$

21,**33**,**57**,**69**,85,**93**,**105**,**129**,133,145,**177**,**195**,205,**213**,**217**,231,**237**,**249**,253,**265**,**309**,**393**,**417**,
445,**465**,469,**483**,**489**,493,505,517,553,**565**,**573**,**597**,609,627,633,**645**,663,669,685,697,**753**,
781,793,**813**,817,861,**865**,889,897,913,**915**,**933**,935,949,969,**973**,985,**987**,**993**.

son números primos Arolmar los sombreados en **negrilla,** siendo el resto números asociados. Por tanto, podríamos solicitar a OEIS, como números primos Arolmar, la frecuencia

21,**33**,**57**,**69**,**93**,**105**,**129**,**177**,**195**,**213**,**217**,**237**,**249**,**265**,**309**,**393**,**417**,
445,**465**,**483**,**489**,**565**,**573**,**597**,**645**,**753**, **813**, **865**, **915**,**933**, **973**, **987**,**993**.

La versatilidad de estos números y la manera desorbitada de crecimiento, cualquiera que sea la forma de conseguirlos, les hace idóneos para los cifrados en criptosistemas, circunstancia ésta que debe ser valorada por los expertos.

ANEXO I: Números Arolmar

Primos	1	2	3	4	5	6	7	8	9	suma	NÚMEROS
5	3	7								10	21
7	3	11								14	33
11	3	19								22	57
13	3	23								26	69
17	3	31								34	93
5	3	5	7							15	105
23	3	43								26	129
31	3	59								62	177
7	3	5	13							21	195
19	7	31								38	217
29	3	53								58	265
13	3	5	31							39	465
11	3	7	23							33	483
17	3	5	43							51	645
23	3	5	61							69	915
19	3	7	47							57	987
29	3	5	79							87	1185
7	3	5	7	13						28	1365
31	3	7	83							93	1743
11	3	5	7	29						44	3045
13	3	5	7	37						52	3885
17	3	5	7	53						68	5565
19	3	5	7	61						76	6405
29	3	5	7	101						116	10605
31	3	5	7	109						124	11445
23	3	5	11	73						92	12045
11	3	5	7	11	29					55	33495
13	3	5	7	13	37					65	50505
17	3	5	7	11	59					85	68145
19	3	5	7	13	67					95	91455
23	3	5	7	11	89					115	102795
31	3	5	7	13	127					155	173355
29	3	5	7	17	113					145	201705
11	3	5	7	11	17	23				66	451605
13	3	5	7	11	23	29				78	770385
17	3	5	7	11	17	59				102	1158465
19	3	5	7	11	17	71				114	1394085
23	3	5	7	11	23	89				138	2364285
29	3	5	7	11	17	131				174	2572185
31	3	5	7	11	23	137				186	3639405
13	3	5	7	11	13	23	29			91	10015005
17	3	5	7	11	13	19	61			119	17402385
19	3	5	7	11	13	23	71			133	24519495
23	3	5	7	11	13	19	103			161	29384355
31	3	5	7	11	13	29	149			217	64879815
29	3	5	7	11	13	37	127			203	70155485
13	3	5	7	11	13	17	19	29		117	140645505
17	3	5	7	11	13	17	19	61		136	295840545
19	3	5	7	11	13	17	23	73		152	428573145
23	3	5	7	11	13	17	19	109		184	528633105
29	3	5	7	11	13	17	19	157		232	761425665
31	3	5	7	11	13	17	19	173		248	839023185
17	3	5	7	11	13	17	19	31	47	153	7066224165
19	3	5	7	11	13	17	19	23	73	171	8142889755
23	3	5	7	11	13	17	19	23	109	207	12158561415
29	3	5	7	11	13	17	19	23	163	261	18182068905
31	3	5	7	11	13	17	19	23	181	279	20189904735

ANEXO II: Primos Arolmar

Primos	1	2	3	4	5	6	7	8	9	suma	NÚMEROS
5	3	7								10	21
5	3	5	7							15	105
7	3	11								14	33
7	3	5	13							21	195
7	3	5	7	13						28	1365
11	3	19								22	57
11	3	7	23							33	483
11	3	5	7	29						44	3045
11	3	5	7	11	29					55	33495
11	3	5	7	11	17	23				66	451605
13	3	23								26	69
13	3	5	31							39	465
13	3	5	7	37						52	3885
13	3	5	7	13	37					65	50505
13	3	5	7	11	23	29				78	770385
13	3	5	7	11	13	23	29			91	10015005
13	3	5	7	11	13	17	19	29		117	140645505
17	3	31								34	93
17	3	5	43							51	645
17	3	5	7	53						68	5565
17	3	5	7	11	59					85	68145
17	3	5	7	11	17	59				102	1158465
17	3	5	7	11	13	19	61			119	17402385
17	3	5	7	11	13	17	19	61		136	295840545
17	3	5	7	11	13	17	19	31	47	153	7066224165
19	7	31								38	217
19	3	7	47							57	987
19	3	5	7	61						76	6405
19	3	5	7	13	67					95	91455
19	3	5	7	11	17	71				114	1394085
19	3	5	7	11	13	23	71			133	24519495
19	3	5	7	11	13	17	23	73		152	428573145
19	3	5	7	11	13	17	19	23	73	171	8142889755
23	3	43								26	129
23	3	5	61							69	915
23	3	5	11	73						92	12045
23	3	5	7	11	89					115	102795
23	3	5	7	11	23	89				138	2364285
23	3	5	7	11	13	19	103			161	29384355
23	3	5	7	11	13	17	19	109		184	528633105
23	3	5	7	11	13	17	19	23	109	207	12158561415
29	3	53								58	265
29	3	5	79							87	1185
29	3	5	7	101						116	10605
29	3	5	7	17	113					145	201705
29	3	5	7	11	17	131				174	2572185
29	3	5	7	11	13	37	127			203	70155485
29	3	5	7	11	13	17	19	157		232	761425665
29	3	5	7	11	13	17	19	23	163	261	18182068905
31	3	59								62	177
31	3	7	83							93	1743
31	3	5	7	109						124	11445
31	3	5	7	13	127					155	173355
31	3	5	7	11	23	137				186	3639405
31	3	5	7	11	13	29	149			217	64879815
31	3	5	7	11	13	17	19	173		248	839023185
31	3	5	7	11	13	17	19	23	181	279	20189904735

ANEXO III: Números Arolmar desde el 21 hasta el 99949

21, 33, 57, 69, 85, 93, 105, 129, 133, 145, 177, 195, 205, 213, 217,
231, 237, 249, 253, 265, 309, 393, 417, 445, 465, 469, 483, 489, 493,
505, 517, 553, 565, 573, 597, 609, 627, 633, 645, 663, 669, 685, 697,
753, 781, 793, 813, 817, 861, 865, 889, 897, 913, 915, 933, 935, 949,
969, 973, 985, 987, 993, 1057, 1077, 1137, 1149, 1177, 1185, 1221,
1239, 1257, 1265, 1273, 1285, 1329, 1333, 1345, 1357, 1365, 1389,
1393, 1417, 1419, 1437, 1441, 1465, 1477, 1497, 1513, 1537, 1545,
1569, 1581, 1599, 1633, 1653, 1689, 1717, 1729, 1743, 1765, 1837,
1857, 1887, 1893, 1897, 1909, 1945, 1957, 1977, 2067, 2073, 2101,
2121, 2139, 2149, 2173, 2229, 2245, 2255, 2265, 2305, 2353, 2373,
2409, 2413, 2465, 2509, 2517, 2533, 2545, 2577, 2581, 2589, 2605,
2607, 2641, 2649, 2653, 2679, 2733, 2751, 2757, 2761, 2769, 2773,
2785, 2821, 2893, 2895, 2913, 2915, 2967, 3045, 3073, 3085, 3117,
3129, 3133, 3165, 3193, 3201, 3219, 3273, 3277, 3335, 3337, 3349,
3367, 3369, 3397, 3417, 3435, 3453, 3505, 3507, 3513, 3589, 3597,
3615, 3633, 3669, 3693, 3723, 3777, 3781, 3805, 3817, 3829, 3837,
3849, 3865, 3873, 3885, 3905, 3909, 3937, 3957, 3973, 3985, 3995,
4011, 4033, 4047, 4069, 4117, 4123, 4141, 4173, 4191, 4197, 4209,
4213, 4245, 4249, 4285, 4301, 4321, 4333, 4353, 4369, 4393, 4405,
4407, 4429, 4449, 4453, 4485, 4497, 4533, 4537, 4623, 4629, 4645,
4695, 4713, 4715, 4717, 4765, 4767, 4777, 4837, 4845, 4849, 4857,
4873, 4885, 4897, 4929, 4965, 5017, 5019, 5053, 5065, 5073, 5089,
5137, 5169, 5173, 5217, 5253, 5257, 5277, 5289, 5293, 5307, 5313,
5317, 5377, 5379, 5389, 5397, 5401, 5423, 5433, 5487, 5497, 5509,
5533, 5545, 5559, 5565, 5595, 5613, 5617, 5629, 5637, 5677, 5713,
5719, 5757, 5773, 5793, 5809, 5833, 5853, 5883, 5885, 5901, 5905,
5917, 5937, 5965, 5989, 6013, 6035, 6045, 6063, 6097, 6099, 6117,
6135, 6145, 6153, 6157, 6189, 6215, 6297, 6313, 6349, 6385, 6405,
6433, 6445, 6493, 6505, 6513, 6531, 6537, 6567, 6585, 6609, 6643,
6657, 6693, 6697, 6729, 6757, 6769, 6785, 6805, 6873, 6913, 6937,
6945, 6973, 7009, 7017, 7033, 7089, 7093, 7107, 7113, 7149, 7153,
7161, 7165, 7197, 7201, 7269, 7273, 7293, 7359, 7377, 7405, 7513,
7565, 7597, 7609, 7633, 7653, 7667, 7683, 7685, 7737, 7773, 7801,
7809, 7813, 7837, 7849, 7881, 7897, 7917, 7969, 8007, 8043, 8065,
8113, 8157, 8185, 8193, 8241, 8257, 8277, 8313, 8341, 8401, 8413,
8421, 8439, 8509, 8529, 8545, 8553, 8555, 8565, 8585, 8593, 8601,
8605, 8617, 8645, 8653, 8709, 8773, 8797, 8817, 8857, 8889, 8911,
8913, 8917, 8953, 9057, 9073, 9087, 9095, 9097, 9139, 9141, 9165,
9169, 9177, 9185, 9193, 9213, 9231, 9249, 9301, 9303, 9313, 9373,
9385, 9445, 9483, 9489, 9505, 9529, 9545, 9553, 9573, 9577, 9635,
9673, 9681, 9717, 9745, 9753, 9757, 9789, 9813, 9843, 9853, 9879,
9913, 9915, 9919, 9937, 9951, 9969, 9993

10021, 10033, 10057, 10059, 10095, 10117, 10129, 10131, 10149, 10173,
10189, 10203, 10213, 10237, 10249, 10261, 10293, 10297, 10311, 10329,
10365, 10389, 10393, 10417, 10419, 10473, 10489, 10537, 10573, 10605,
10635, 10653, 10669, 10681, 10689, 10707, 10713, 10717, 10777, 10797,
10833, 10835, 10857, 10873, 10887, 10929, 10965, 10969, 10977, 10981,
11017, 11033, 11049, 11065, 11073, 11089, 11137, 11139, 11157, 11165,
11211, 11217, 11229, 11293, 11339, 11341, 11377, 11413, 11427, 11445,
11469, 11485, 11509, 11533, 11569, 11589, 11607, 11615, 11645, 11653,
11679, 11685, 11773, 11785, 11797, 11823, 11829, 11859, 11893, 11905,
11917, 11931, 11949, 12009, 12013, 12045, 12057, 12111, 12129, 12133,
12153, 12169, 12193, 12205, 12217, 12229, 12313, 12327, 12345, 12477,
12507, 12597, 12649, 12657, 12745, 12765, 12777, 12793, 12813, 12815,
12817, 12849, 12901, 12905, 12913, 12937, 12939, 12949, 12995, 12997,
13021, 13045, 13057, 13069, 13101, 13137, 13165, 13213, 13269, 13317,
13409, 13429, 13449, 13453, 13485, 13561, 13645, 13685, 13699, 13705,
13749, 13773, 13777, 13805, 13813, 13821, 13839, 13845, 13857, 13865,
13897, 13909, 13957, 13983, 13989, 14037, 14041, 14073, 14077, 14101,
14113, 14137, 14217, 14253, 14271, 14277, 14287, 14289, 14305, 14349,
14377, 14433, 14469, 14473, 14485, 14487, 14493, 14559, 14577, 14613,
14617, 14637, 14677, 14701, 14761, 14785, 14793, 14829, 14833, 14845,
14853, 14857, 14893, 14917, 14927, 14977, 14993, 15009, 15065, 15067,
15081, 15117, 15133, 15177, 15205, 15207, 15215, 15229, 15253, 15297,
15333, 15369, 15387, 15397, 15495, 15515, 15521, 15529, 15531, 15537,
15553, 15577, 15585, 15603, 15613, 15637, 15639, 15645, 15657, 15673,
15685, 15693, 15697, 15709, 15721, 15747, 15757, 15765, 15769, 15841,
15853, 15969, 15981, 15997, 16005, 16017, 16035, 16045, 16053, 16071,
16105, 16115, 16117, 16153, 16213, 16235, 16237, 16257, 16297, 16309,
16321, 16377, 16395, 16401, 16437, 16445, 16471, 16485, 16509, 16593,
16621, 16629, 16645, 16647, 16685, 16717, 16737, 16745, 16773, 16809,
16837, 16899, 16907, 16935, 16945, 17015, 17049, 17065, 17085, 17089,
17097, 17105, 17133, 17135, 17169, 17197, 17205, 17233, 17241, 17259,
17269, 17305, 17329, 17353, 17373, 17413, 17473, 17553, 17557, 17563,
17589, 17593, 17617, 17619, 17673, 17677, 17709, 17765, 17769, 17817,
17857, 17869, 17889, 17907, 18069, 18085, 18109, 18129, 18165, 18177,
18237, 18337, 18361, 18377, 18393, 18489, 18529, 18649, 18673, 18735,
18753, 18813, 18815, 18853, 18877, 18887, 18889, 18901, 18969, 18985,
19023, 19041, 19077, 19105, 19113, 19131, 19137, 19177, 19203, 19295,
19297, 19311, 19357, 19365, 19509, 19513, 19527, 19537, 19561, 19565,
19617, 19633, 19693, 19761, 19797, 19815, 19849, 19869, 19895, 19897,
19921, 19933, 19945, 19957, 19977.

20005, 20073, 20077, 20083, 20085, 20157, 20193, 20197, 20209, 20213,
20245, 20247, 20257, 20317, 20319, 20337, 20365, 20405, 20427, 20437,
20461, 20463, 20469, 20497, 20557, 20581, 20589, 20643, 20665, 20679,
20683, 20685, 20689, 20715, 20723, 20733, 20757, 20769, 20785, 20797,
20833, 20839, 20881, 20915, 20917, 20953, 21037, 21045, 21057, 21085,
21131, 21237, 21241, 21253, 21265, 21291, 21337, 21349, 21361, 21435,
21457, 21477, 21507, 21543, 21553, 21597, 21605, 21633, 21651, 21669,
21709, 21723, 21729, 21733, 21793, 21795, 21829, 21849, 21867, 21877,
21913, 21939, 21949, 21957, 21965, 21973, 21995, 22009, 22029, 22045,
22053, 22055, 22081, 22083, 22105, 22117, 22119, 22173, 22177, 22209,
22213, 22297, 22309, 22317, 22335, 22351, 22353, 22357, 22405, 22417,
22489, 22513, 22517, 22533, 22537, 22609, 22633, 22649, 22657, 22713,
22749, 22773, 22789, 22809, 22849, 22865, 22873, 22911, 22917, 22929,
22957, 22969, 22983, 23073, 23077, 23097, 23109, 23149, 23165, 23169,
23171, 23217, 23221, 23233, 23277, 23289, 23317, 23365, 23397, 23413,
23433, 23437, 23461, 23529, 23533, 23577, 23649, 23705, 23737, 23739,
23779, 23793, 23797, 23885, 23901, 23937, 23941, 23959, 23965, 24033,
24045, 24063, 24085, 24099, 24117, 24153, 24193, 24215, 24217, 24253,
24277, 24289, 24313, 24333, 24385, 24387, 24397, 24433, 24445, 24457,
24493, 24497, 24537, 24553, 24567, 24577, 24603, 24605, 24613, 24639,
24645, 24657, 24661, 24721, 24757, 24765, 24789, 24801, 24829, 24853,
24913, 24933, 24945, 24963, 24981, 24997, 25017, 25053, 25071, 25093,
25123, 25141, 25145, 25197, 25213, 25257, 25273, 25293, 25323, 25327,
25365, 25369, 25393, 25405, 25449, 25467, 25477, 25485, 25557, 25573,
25593, 25617, 25629, 25669, 25681, 25689, 25753, 25765, 25813, 25845,
25861, 25917, 25955, 25957, 26013, 26077, 26085, 26089, 26137, 26173,
26185, 26233, 26295, 26305, 26329, 26331, 26337, 26377, 26445, 26473,
26477, 26517, 26545, 26581, 26609, 26617, 26619, 26637, 26653, 26673,
26689, 26709, 26727, 26749, 26765, 26769, 26773, 26835, 26855, 26857,
26889, 26905, 26917, 26923, 26941, 26943, 26945, 26961, 26965, 26977,
26989, 27001, 27033, 27051, 27069, 27071, 27085, 27129, 27133, 27157,
27193, 27217, 27229, 27249, 27267, 27273, 27303, 27339, 27347, 27357,
27373, 27385, 27401, 27429, 27447, 27465, 27469, 27485, 27493, 27505,
27553, 27573, 27589, 27609, 27637, 27645, 27665, 27699, 27717, 27721,
27757, 27761, 27769, 27789, 27829, 27849, 27861, 27863, 27865, 27933,
27937, 27965, 27969, 27973, 28009, 28029, 28059, 28063, 28085, 28093,
28101, 28177, 28189, 28209, 28245, 28261, 28317, 28333, 28345, 28357,
28381, 28389, 28391, 28497, 28501, 28509, 28581, 28585, 28655, 28693,
28779, 28833, 28849, 28869, 28873, 28893, 28957, 28993, 28995, 29005,
29049, 29053, 29065, 29085, 29103, 29113, 29121, 29149, 29157, 29193,
29217, 29245, 29265, 29337, 29341, 29353, 29377, 29391, 29409, 29427,
29445, 29465, 29509, 29533, 29577, 29593, 29607, 29613, 29649, 29659,
29677, 29697, 29713, 29737, 29793, 29809, 29821, 29857, 29859, 29893,
29931, 29941, 29949, 29967, 29977.

30003, 30117, 30147, 30157, 30163, 30165, 30193, 30245, 30297, 30327,
30363, 30381, 30397, 30409, 30453, 30471, 30477, 30485, 30515, 30601,
30633, 30635, 30669, 30673, 30687, 30785, 30865, 30909, 30913, 30921,
30965, 30973, 30993, 30997, 31047, 31057, 31083, 31171, 31173, 31191,
31201, 31227, 31263, 31273, 31345, 31369, 31377, 31389, 31453, 31479,
31623, 31645, 31659, 31677, 31749, 31753, 31773, 31789, 31813, 31837,
31845, 31861, 31897, 31909, 31947, 31969, 31989, 32021, 32053, 32073,
32113, 32161, 32219, 32253, 32271, 32277, 32281, 32293, 32313, 32315,
32351, 32433, 32437, 32449, 32453, 32469, 32493, 32565, 32577, 32581,
32593, 32613, 32629, 32649, 32677, 32739, 32809, 32817, 32881, 32883,
32901, 32953, 32973, 33005, 33009, 33027, 33063, 33065, 33121, 33133,
33153, 33157, 33177, 33189, 33193, 33217, 33265, 33285, 33313, 33315,
33335, 33387, 33433, 33445, 33477, 33495, 33549, 33567, 33605, 33657,
33661, 33685, 33695, 33709, 33711, 33729, 33785, 33793, 33837, 33853,
33873, 33897, 33909, 33927, 33933, 33935, 33943, 33973, 33981, 34071,
34089, 34117, 34149, 34197, 34221, 34235, 34365, 34397, 34413, 34417,
34449, 34453, 34477, 34585, 34609, 34621, 34629, 34665, 34669, 34717,
34719, 34737, 34777, 34799, 34809, 34813, 34861, 34881, 34885, 34917,
34989, 34993, 35015, 35029, 35061, 35079, 35097, 35101, 35113, 35137,
35157, 35193, 35209, 35233, 35371, 35377, 35389, 35445, 35465, 35545,
35619, 35637, 35653, 35709, 35717, 35737, 35745, 35749, 35765, 35773,
35853, 35855, 35871, 35877, 35913, 35915, 35929, 35953, 35979, 36001,
36033, 36121, 36127, 36133, 36141, 36145, 36213, 36249, 36253, 36301,
36349, 36429, 36553, 36577, 36589, 36627, 36635, 36649, 36661, 36685,
36707, 36717, 36733, 36745, 36769, 36789, 36829, 36841, 36879, 36935,
36941, 36969, 36993, 37029, 37033, 37037, 37059, 37095, 37129, 37165,
37173, 37237, 37245, 37265, 37297, 37333, 37381, 37383, 37393, 37429,
37453, 37473, 37477, 37527, 37533, 37563, 37565, 37585, 37599, 37617,
37639, 37645, 37697, 37743, 37797, 37837, 37849, 37857, 37887, 37909,
37933, 37945, 37969, 37981, 37985, 37999, 38013, 38017, 38031, 38041,
38049, 38103, 38109, 38161, 38165, 38173, 38181, 38193, 38211, 38227,
38229, 38265, 38285, 38301, 38373, 38389, 38413, 38473, 38555, 38577,
38581, 38589, 38689, 38697, 38785, 38787, 38877, 38881, 38885, 38937,
38967, 39005, 39037, 39045, 39057, 39085, 39091, 39117, 39145, 39155,
39165, 39183, 39205, 39219, 39245, 39253, 39265, 39277, 39297, 39309,
39337, 39353, 39399, 39403, 39405, 39433, 39453, 39477, 39491, 39493,
39577, 39579, 39597, 39613, 39637, 39695, 39757, 39759, 39817, 39867,
39889, 39957, 39961, 39973.

40021, 40029, 40045, 40057, 40069, 40089, 40137, 40139, 40173, 40197,
40205, 40209, 40369, 40389, 40415, 40465, 40479, 40501, 40533, 40551,
40565, 40569, 40573, 40587, 40595, 40641, 40657, 40663, 40669, 40677,
40695, 40715, 40767, 40789, 40807, 40845, 40861, 40919, 40921, 40929,
41037, 41053, 41055, 41089, 41109, 41133, 41169, 41205, 41217, 41235,
41289, 41329, 41353, 41361, 41365, 41379, 41433, 41437, 41451, 41493,
41497, 41541, 41565, 41613, 41629, 41685, 41689, 41749, 41793, 41829,
41833, 41883, 41889, 41919, 41973, 41977, 41997, 42037, 42045, 42145,
42153, 42207, 42249, 42251, 42277, 42279, 42361, 42369, 42421, 42469,
42485, 42495, 42505, 42515, 42541, 42565, 42637, 42657, 42673, 42685,
42753, 42765, 42817, 42819, 42845, 42865, 42877, 42911, 42913, 42927,
42997, 42999, 43005, 43017, 43033, 43057, 43069, 43089, 43183, 43213,
43233, 43257, 43269, 43297, 43323, 43333, 43345, 43359, 43417, 43429,
43431, 43453, 43465, 43477, 43485, 43509, 43621, 43689, 43703, 43705,
43737, 43773, 43809, 43835, 43837, 43845, 43849, 43873, 43917, 43955,
43957, 44045, 44097, 44113, 44121, 44185, 44197, 44205, 44285, 44321,
44329, 44349, 44367, 44377, 44413, 44437, 44493, 44557, 44569, 44619,
44629, 44677, 44693, 44707, 44713, 44735, 44763, 44799, 44833, 44853,
44857, 44889, 44977, 44989, 44997, 45069, 45093, 45097, 45141, 45145,
45157, 45193, 45205, 45217, 45273, 45277, 45285, 45287, 45305, 45313,
45353, 45397, 45409, 45451, 45457, 45485, 45601, 45609, 45637, 45735,
45787, 45805, 45879, 45937, 45973, 46033, 46069, 46077, 46079, 46113,
46117, 46129, 46177, 46213, 46249, 46293, 46295, 46297, 46321, 46329,
46333, 46347, 46353, 46357, 46393, 46405, 46437, 46465, 46531, 46533,
46543, 46561, 46635, 46671, 46693, 46705, 46749, 46753, 46777, 46779,
46797, 46805, 46833, 46869, 46885, 46895, 46897, 46929, 46959, 46981,
47031, 47037, 47067, 47085, 47101, 47103, 47139, 47141, 47185, 47193,
47197, 47233, 47305, 47337, 47345, 47357, 47435, 47465, 47485, 47541,
47589, 47593, 47615, 47617, 47679, 47689, 47715, 47733, 47751, 47769,
47833, 47841, 47957, 48039, 48081, 48129, 48145, 48147, 48185, 48217,
48229, 48237, 48241, 48253, 48257, 48277, 48307, 48309, 48349, 48365,
48489, 48529, 48549, 48597, 48613, 48635, 48637, 48693, 48709, 48745,
48777, 48793, 48795, 48811, 48849, 48901, 48909, 48913, 48937, 48939,
48957, 49017, 49029, 49063, 49065, 49093, 49129, 49165, 49181, 49189,
49213, 49237, 49285, 49321, 49335, 49371, 49389, 49445, 49487, 49501,
49515, 49567, 49645, 49693, 49705, 49713, 49753, 49785, 49803, 49813,
49837, 49839, 49857, 49893, 49981, 49987.

50001, 50037, 50061, 50089, 50109, 50113, 50137, 50141, 50145, 50163,
50173, 50185, 50233, 50257, 50269, 50307, 50315, 50317, 50353, 50397,
50413, 50415, 50437, 50449, 50451, 50473, 50505, 50509, 50529, 50533,
50541, 50557, 50615, 50629, 50649, 50685, 50689, 50737, 50739, 50757,
50793, 50845, 50883, 50917, 50945, 50965, 51027, 51035, 51097, 51117,
51121, 51171, 51189, 51253, 51277, 51285, 51319, 51357, 51369, 51445,
51477, 51505, 51513, 51573, 51601, 51639, 51645, 51657, 51685, 51729,
51733, 51747, 51801, 51873, 51877, 51927, 51937, 51961, 52017, 52033,
52041, 52053, 52055, 52071, 52077, 52149, 52197, 52213, 52217, 52261,
52273, 52285, 52287, 52357, 52359, 52413, 52429, 52473, 52507, 52513,
52547, 52557, 52597, 52621, 52633, 52657, 52685, 52845, 52873, 52945,
52953, 52977, 52989, 52993, 53005, 53015, 53065, 53097, 53131, 53133,
53157, 53159, 53169, 53209, 53293, 53295, 53313, 53349, 53413, 53445,
53473, 53529, 53547, 53565, 53567, 53581, 53583, 53589, 53641, 53669,
53691, 53735, 53769, 53797, 53799, 53805, 53809, 53817, 53869, 53893,
53905, 53915, 53989, 54033, 54035, 54069, 54073, 54097, 54159, 54165,
54253, 54303, 54337, 54365, 54373, 54393, 54433, 54465, 54553, 54645,
54681, 54685, 54739, 54745, 54753, 54757, 54791, 54853, 54913, 54933,
54937, 54969, 54995, 54997, 55029, 55041, 55113, 55153, 55165, 55187,
55245, 55273, 55285, 55293, 55317, 55347, 55353, 55357, 55369, 55393,
55453, 55477, 55489, 55527, 55535, 55549, 55561, 55581, 55605, 55637,
55685, 55707, 55709, 55729, 55749, 55753, 55783, 55789, 55801, 55833,
55869, 55873, 55885, 55957, 55969, 55977, 55993, 56013, 56015, 56017,
56029, 56037, 56067, 56085, 56137, 56165, 56211, 56233, 56317, 56337,
56365, 56409, 56461, 56465, 56517, 56535, 56577, 56617, 56643, 56689,
56705, 56757, 56787, 56805, 56881, 56931, 56937, 56967, 56977, 57065,
57101, 57147, 57157, 57165, 57181, 57253, 57293, 57337, 57345, 57365,
57517, 57541, 57545, 57553, 57577, 57579, 57597, 57605, 57651, 57757,
57759, 57761, 57777, 57851, 57913, 57949, 57957, 57961, 57985, 57997,
58011, 58083, 58101, 58105, 58157, 58173, 58177, 58213, 58227, 58233,
58273, 58297, 58317, 58333, 58355, 58381, 58389, 58405, 58449, 58489,
58501, 58533, 58535, 58585, 58587, 58593, 58633, 58677, 58713, 58717,
58773, 58807, 58809, 58813, 58821, 58839, 58857, 58873, 58929, 58945,
58949, 58985, 59005, 59017, 59037, 59081, 59097, 59137, 59173, 59217,
59257, 59289, 59293, 59317, 59361, 59363, 59401, 59529, 59533, 59563,
59585, 59593, 59677, 59721, 59773, 59845, 59893, 59899, 59953, 59961,
59977.

60001, 60009, 60033, 60065, 60117, 60151, 60171, 60181, 60213, 60253,
60297, 60395, 60469, 60481, 60505, 60529, 60549, 60567, 60605, 60645,
60657, 60665, 60721, 60729, 60753, 60755, 60769, 60873, 60909, 60949,
60963, 60969, 60985, 61033, 61061, 61069, 61077, 61087, 61143, 61189,
61273, 61329, 61377, 61395, 61405, 61411, 61415, 61429, 61449, 61477,
61501, 61513, 61579, 61597, 61617, 61629, 61665, 61701, 61719, 61745,
61753, 61773, 61777, 61797, 61827, 61835, 61845, 61849, 61873, 61899,
61917, 61953, 61989, 61993, 62005, 62007, 62061, 62077, 62113, 62133,
62173, 62185, 62209, 62223, 62269, 62281, 62317, 62329, 62341, 62353,
62437, 62445, 62449, 62457, 62509, 62511, 62529, 62565, 62583, 62593,
62601, 62673, 62677, 62709, 62737, 62809, 62821, 62833, 62843, 62845,
62853, 62857, 62977, 63013, 63017, 63049, 63061, 63069, 63087, 63123,
63177, 63193, 63205, 63215, 63245, 63253, 63265, 63271, 63273, 63285,
63305, 63339, 63365, 63373, 63501, 63519, 63565, 63573, 63597, 63613,
63633, 63637, 63673, 63779, 63877, 63879, 63889, 63915, 63937, 63969,
63971, 63973, 64093, 64095, 64113, 64117, 64129, 64137, 64201, 64213,
64257, 64261, 64273, 64293, 64309, 64321, 64365, 64393, 64419, 64465,
64477, 64509, 64537, 64543, 64549, 64583, 64599, 64677, 64681, 64705,
64743, 64745, 64821, 64869, 64909, 64933, 64993, 65021, 65137, 65185,
65191, 65197, 65229, 65233, 65285, 65389, 65391, 65409, 65427, 65435,
65473, 65605, 65613, 65641, 65685, 65733, 65749, 65797, 65823, 65829,
65833, 65857, 65859, 65877, 65879, 65893, 65913, 65917, 65949, 65977,
66009, 66011, 66013, 66057, 66073, 66121, 66129, 66133, 66147, 66153,
66155, 66183, 66217, 66229, 66273, 66277, 66313, 66333, 66381, 66433,
66481, 66513, 66515, 66561, 66565, 66577, 66613, 66615, 66637, 66673,
66703, 66723, 66777, 66793, 66867, 66937, 66965, 66985, 66993, 67009,
67029, 67045, 67117, 67137, 67173, 67199, 67237, 67281, 67297, 67317,
67333, 67345, 67357, 67393, 67449, 67485, 67497, 67513, 67533, 67541,
67569, 67597, 67621, 67629, 67633, 67643, 67657, 67677, 67693, 67713,
67715, 67731, 67765, 67773, 67805, 67813, 67857, 67885, 67893, 67897,
67917, 68057, 68077, 68097, 68145, 68149, 68199, 68245, 68269, 68271,
68293, 68341, 68349, 68353, 68377, 68415, 68419, 68545, 68557, 68565,
68605, 68613, 68653, 68667, 68677, 68685, 68765, 68797, 68809, 68847,
68889, 68893, 68937, 68941, 68953, 68977, 69009, 69013, 69133, 69145,
69217, 69279, 69285, 69297, 69315, 69349, 69423, 69443, 69469, 69517,
69529, 69549, 69553, 69565, 69585, 69637, 69639, 69657, 69693, 69695,
69729, 69747, 69765, 69769, 69785, 69841, 69861, 69913, 69933, 69967,
69973, 69979, 69985, 69989.

70089, 70093, 70151, 70165, 70179, 70197, 70231, 70235, 70273, 70293,
70295, 70333, 70369, 70377, 70397, 70405, 70431, 70449, 70453, 70485,
70505, 70513, 70539, 70557, 70561, 70565, 70597, 70669, 70689, 70719,
70765, 70777, 70797, 70801, 70813, 70837, 70869, 70909, 70933, 70935,
70989, 70993, 71029, 71041, 71053, 71085, 71097, 71135, 71151, 71173,
71187, 71245, 71277, 71285, 71369, 71401, 71445, 71509, 71529, 71555,
71565, 71617, 71621, 71637, 71641, 71645, 71677, 71737, 71743, 71745,
71749, 71773, 71781, 71817, 71841, 71845, 71889, 71913, 71989, 71997,
72001, 72057, 72097, 72157, 72195, 72213, 72217, 72239, 72249, 72285,
72393, 72397, 72409, 72413, 72429, 72445, 72465, 72517, 72519, 72541,
72553, 72601, 72631, 72633, 72669, 72697, 72699, 72743, 72751, 72771,
72789, 72805, 72829, 72845, 72885, 72913, 72935, 73033, 73093, 73149,
73173, 73203, 73213, 73245, 73257, 73261, 73285, 73295, 73297, 73337,
73365, 73393, 73437, 73489, 73497, 73501, 73509, 73545, 73605, 73617,
73653, 73657, 73669, 73707, 73715, 73743, 73753, 73789, 73801, 73805,
73813, 73837, 73887, 73921, 73957, 74011, 74015, 74037, 74049, 74073,
74089, 74103, 74113, 74121, 74129, 74165, 74193, 74229, 74281, 74285,
74373, 74391, 74397, 74445, 74465, 74473, 74485, 74499, 74533, 74593,
74607, 74643, 74685, 74749, 74773, 74785, 74803, 74809, 74829, 74833,
74845, 74877, 74893, 74895, 74913, 74937, 74953, 74965, 74985, 75057,
75073, 75093, 75095, 75147, 75185, 75237, 75265, 75317, 75373, 75385,
75417, 75433, 75439, 75453, 75469, 75489, 75515, 75529, 75597, 75651,
75657, 75661, 75669, 75673, 75723, 75745, 75769, 75785, 75805, 75813,
75815, 75817, 75829, 75849, 75865, 75909, 75939, 75943, 75949, 76017,
76021, 76057, 76069, 76117, 76173, 76237, 76269, 76281, 76309, 76317,
76393, 76443, 76447, 76477, 76569, 76633, 76681, 76693, 76737, 76751,
76785, 76789, 76839, 76845, 76861, 76885, 76897, 76917, 76929, 76983,
76985, 77005, 77027, 77037, 77089, 77109, 77113, 77127, 77173, 77217,
77281, 77287, 77293, 77329, 77433, 77435, 77451, 77457, 77473, 77487,
77533, 77577, 77585, 77605, 77677, 77703, 77709, 77721, 77779, 77793,
77829, 77833, 77905, 77917, 77919, 77941, 77953, 77989, 77997, 78009,
78037, 78061, 78097, 78117, 78133, 78145, 78169, 78205, 78249, 78285,
78313, 78349, 78353, 78369, 78373, 78403, 78433, 78441, 78457, 78477,
78495, 78549, 78589, 78609, 78613, 78657, 78661, 78673, 78693, 78733,
78745, 78753, 78805, 78817, 78881, 78909, 78965, 78973, 78985, 78999,
79009, 79017, 79021, 79033, 79045, 79069, 79081, 79089, 79093, 79107,
79113, 79129, 79177, 79205, 79249, 79293, 79297, 79373, 79437, 79449,
79485, 79573, 79753, 79773, 79845, 79871, 79897, 79953, 79989.

80069, 80137, 80189, 80193, 80227, 80241, 80269, 80277, 80301, 80365,
80377, 80413, 80437, 80445, 80497, 80517, 80581, 80585, 80601, 80617,
80637, 80641, 80727, 80731, 80765, 80817, 80853, 80857, 80881, 80889,
80941, 80977, 81085, 81123, 81129, 81145, 81165, 81253, 81257, 81309,
81337, 81345, 81393, 81411, 81455, 81493, 81501, 81537, 81571, 81573,
81609, 81635, 81679, 81771, 81789, 81877, 81885, 81889, 82023, 82115,
82117, 82131, 82137, 82149, 82165, 82177, 82205, 82243, 82249, 82273,
82321, 82329, 82331, 82405, 82417, 82419, 82441, 82491, 82513, 82533,
82535, 82573, 82597, 82599, 82671, 82681, 82689, 82693, 82707, 82715,
82753, 82779, 82833, 82841, 82869, 82873, 82887, 82909, 82921, 82933,
82993, 83017, 83105, 83157, 83229, 83249, 83253, 83289, 83329, 83377,
83397, 83409, 83413, 83469, 83473, 83499, 83503, 83517, 83533, 83569,
83629, 83721, 83731, 83733, 83821, 83893, 83897, 83929, 83931, 83953,
83977, 84037, 84045, 84049, 84057, 84169, 84185, 84193, 84219, 84237,
84245, 84297, 84309, 84333, 84345, 84365, 84373, 84381, 84405, 84419,
84433, 84445, 84487, 84489, 84561, 84597, 84601, 84613, 84633, 84661,
84757, 84759, 84769, 84777, 84781, 84817, 84849, 84853, 84877, 84885,
84937, 84939, 84973, 85019, 85053, 85069, 85105, 85117, 85119, 85177,
85233, 85263, 85273, 85281, 85289, 85317, 85321, 85353, 85415, 85445,
85485, 85497, 85519, 85533, 85537, 85573, 85629, 85677, 85693, 85753,
85777, 85803, 85809, 85811, 85845, 85861, 85911, 85929, 85945, 85957,
86019, 86037, 86041, 86053, 86101, 86203, 86207, 86307, 86313, 86343,
86361, 86377, 86437, 86457, 86529, 86557, 86565, 86577, 86605, 86613,
86615, 86631, 86645, 86665, 86713, 86737, 86749, 86765, 86773, 86793,
86809, 86833, 86853, 86855, 86865, 86867, 86917, 86965, 86991, 87045,
87153, 87157, 87189, 87207, 87217, 87243, 87279, 87283, 87333, 87349,
87351, 87369, 87377, 87385, 87409, 87445, 87457, 87469, 87515, 87529,
87537, 87585, 87657, 87665, 87733, 87753, 87757, 87763, 87781, 87783,
87791, 87817, 87829, 87909, 87913, 87933, 87963, 88045, 88077, 88089,
88269, 88273, 88285, 88329, 88345, 88365, 88385, 88393, 88413, 88473,
88489, 88549, 88557, 88593, 88597, 88633, 88645, 88717, 88753, 88757,
88791, 88847, 88939, 88957, 88971, 88981, 89049, 89079, 89105, 89133,
89173, 89281, 89295, 89311, 89331, 89349, 89421, 89439, 89445, 89497,
89509, 89569, 89581, 89605, 89617, 89629, 89639, 89691, 89709, 89713,
89727, 89737, 89799, 89869, 89881, 89893, 89907.

90049, 90069, 90133, 90139, 90169, 90177, 90181, 90229, 90249, 90253,
90287, 90309, 90357, 90385, 90391, 90421, 90501, 90517, 90553, 90577,
90589, 90627, 90633, 90637, 90645, 90673, 90683, 90741, 90777, 90813,
90815, 90827, 90843, 90861, 90885, 90913, 90933, 90957, 90965, 90973,
91093, 91095, 91117, 91149, 91177, 91185, 91213, 91257, 91293, 91329,
91345, 91383, 91417, 91455, 91477, 91537, 91549, 91561, 91567, 91605,
91617, 91633, 91637, 91657, 91693, 91705, 91743, 91749, 91805, 91817,
91851, 91885, 91887, 91897, 91903, 91933, 91981, 92005, 92029, 92053,
92065, 92085, 92137, 92149, 92157, 92193, 92247, 92265, 92283, 92289,
92301, 92497, 92543, 92553, 92653, 92677, 92685, 92773, 92793, 92869,
92911, 92917, 92929, 92949, 92985, 93003, 93005, 93013, 93021, 93057,
93061, 93073, 93081, 93085, 93093, 93129, 93147, 93153, 93237, 93245,
93277, 93335, 93349, 93361, 93365, 93373, 93381, 93397, 93433, 93471,
93477, 93515, 93545, 93597, 93613, 93673, 93733, 93745, 93769, 93793,
93815, 93853, 93867, 93877, 93903, 93957, 93961, 94029, 94163, 94209,
94235, 94245, 94263, 94341, 94345, 94357, 94415, 94417, 94549, 94569,
94585, 94587, 94593, 94605, 94609, 94629, 94685, 94729, 94753, 94839,
94893, 94929, 94957, 94965, 94983, 95019, 95041, 95053, 95073, 95077,
95095, 95135, 95183, 95185, 95197, 95205, 95221, 95253, 95271, 95293,
95313, 95329, 95361, 95365, 95377, 95381, 95397, 95433, 95437, 95521,
95523, 95533, 95631, 95653, 95685, 95719, 95765, 95797, 95847, 96005,
96007, 96037, 96073, 96099, 96121, 96133, 96169, 96189, 96209, 96243,
96261, 96313, 96315, 96357, 96373, 96393, 96407, 96429, 96573, 96607,
96609, 96613, 96645, 96649, 96673, 96691, 96695, 96701, 96709, 96753,
96765, 96801, 96829, 96865, 96877, 96899, 96949, 97017, 97051, 97057,
97089, 97093, 97113, 97141, 97149, 97165, 97179, 97293, 97297, 97329,
97377, 97413, 97417, 97467, 97477, 97485, 97509, 97565, 97593, 97597,
97629, 97633, 97691, 97693, 97745, 97773, 97791, 97881, 97885, 97897,
97935, 97957, 98053, 98085, 98113, 98141, 98157, 98169, 98173, 98281,
98285, 98305, 98345, 98353, 98449, 98461, 98465, 98485, 98493, 98497,
98509, 98511, 98517, 98545, 98547, 98557, 98617, 98619, 98701, 98747,
98749, 98763, 98797, 98805, 98879, 98913, 98949, 98977, 99035, 99051,
99093, 99097, 99157, 99177, 99185, 99193, 99205, 99265, 99273, 99301,
99303, 99357, 99383, 99485, 99561, 99609, 99631, 99633, 99637, 99663,
99757, 99843, 99853, 99897, 99933, 99949.

BIBLIOGRAFÍA

CUSICK, DING, RENVALL, Stream Ciphers and Number Theory, ISBN: 0-444-51631-X
HUSEMöLLER, Dale, Elliptic Curves, ISBN: 0-387-95490-2
KOBLITZ, Neal, A Course in Number Theory and Cryptography, ISBN: 0-387-94293-9
SHOUP, Victor, A Computational Introduction to Number Theory and Algebra, ISBN: 0-521-85154-8

AYUDA INTERNET

http://en.wikipedia.org/wiki/Good_prime
http://es.wikipedia.org/wiki/Cuerpo_ciclot%C3%B3mico
http://es.wikipedia.org/wiki/N%C3%BAmero_primo_de_Sophie_Germain
http://es.wikipedia.org/wiki/N%C3%BAmero_primo_fuerte
http://es.wikipedia.org/wiki/Polinomio_ciclot%C3%B3mico
http://es.wikipedia.org/wiki/RSA
http://hojaynumeros.blogspot.com/2011/02/primos-por-todas-partes.html
http://web.usal.es/~hernando/segi2010/11HerrMat.pdf
http://www.hojamat.es/
http://hojaynumeros.blogspot.com/2011/05/numeros-arolmar.html