9. RESTOS CUADRATICOS Y LEY DE RECIPROCIDAD CUADRÁTICA

9.1 Restos cuadráticos

1.1 Concepto de restos.

Si la congruencia $x \equiv a(mód.m)$ es una relación de equivalencia que permitirá clasificar a los números enteros, y por tanto los naturales, en clases de equivalencia, conjuntos formados por cada número entero y todos sus congruentes. En este caso se llaman clases de restos o residuales, porque cada clase se puede representar por el resto que resulta al dividir cualquier elemento entre el $módulo\, m$.
Las clases $módulo\, m$ se representan por $\mathbb{Z}/m\mathbb{Z}$ ó por $\mathbb{Z}m$.

1. Para $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$, que son los dos restos producidos al dividir entre 2. El elemento 0 representa a los números pares y el 1 a los números impares.
2. Para $\mathbb{Z}/5\mathbb{Z} = \{0,1,2,3,4\}$, en el que, por ejemplo el elemento 3 representa a los números $3,8,13,18,23,\ldots$, que dan resto 3 al dividir por 5.

La clase $\mathbb{Z}/m\mathbb{Z}$ contiene exactamente *m* elementos: $\{0,1,3,4,5,6,\ldots,m-1\}$. A veces se usan restos mínimos, admitiendo números positivos y negativos, mediante la elección entre *a* y $a-m$ del número con menor valor absoluto.
En los sistemas algebraicos las clases de restos tienen estructura de *anillo* para la suma y el producto. El grupo aditivo de ese anillo es cíclico, pues para cada elemento **a** del mismo existe un **h** tal que $a \cdot h = 0$. Ese número h ha de ser divisor del $módulo\, m$.
No todos los elementos tienen inverso. En caso afirmativo, se llaman inversibles, y su conjunto coincide con las clases representadas por números primos con *m*, incluyendo el 1. Por tanto, su número coincide con $\varphi(m) = m(1-1/p_1),\ldots,(1-1/p_n)$, denominado indicador de Euler o función *fi*. El inverso vendrá determinado por $a^{\varphi(m)} \equiv 1(mód.m)$.
Los elementos inversibles forman un grupo multiplicativo, al que representaremos por $\mathbb{Z}*m$, que son las clases residuales reducidas. Este carácter de grupo da lugar a que, si a es inversible en $\mathbb{Z}*m$, existe un número natural *r* tal, que $a^r = 1$. El número r mínimo que cumple la anterior igualdad se llama, para todos los grupos $orden,\ índice\ o\ gaussiano\ de\ a$. Es fácil ver que si $a^n \equiv 1(mód.m)$, el exponente *n* deberá ser múltiplo del orden *r*. Otra consecuencia es que, si a es primo con m y se cumple que $a^x = a^y$ entonces, han de ser $x = y$.
Si *m* es primo, serán inversibles todos los elementos y constituirán un cuerpo.
Se llama ***sistema completo de restos*** al conjunto de *m* enteros tomados, cada uno de ellos, de una de las clases de restos $módulo\, m$, donde $\{0,1,3,4,5,6,\ldots,m-1\}$.
Se llama ***sistema reducido de restos*** al conjunto de *m* enteros tomados, cada uno de ellos, de una de las clases de restos $módulo\, m$, que no comparten con *m* factores comunes. Se denotan mediante la función $\varphi(m) = m(1-1/p_1),\ldots,(1-1/p_n)$ que da el número de enteros que son primos con m.
Se llaman ***restos potenciales*** del número natural ***n***, respecto a un módulo dado ***m***, a los restos producidos por las distintas potencias naturales de **n**.
El conjunto de ***restos potenciales*** sigue unas pautas muy sencillas de seguir:

1. Si ***m*** sólo contiene factores primos con ***n***, se llegará a cierta potencia de ***n*** que será múltiplo de ***m*** y por tanto, a partir de ella todos los restos potenciales serán *nulos*.
2. Si ***m*** es primo con ***n***, los restos son periódicos en periodo *gaussiano* con ***n*** respecto a ***m***. El resto 1 se producirá en los múltiplos de ese *gaussiano*.
3. Si el $mcd(m,n)=d$, con $d>1$, los restos potenciales tendrán una parte periódica y otra no periódica.

El sistema reducido de restos, respecto al módulo *p,* consta de $(p-1)/2$ restos cuadráticos, los cuales son congruentes con los números 1^2, 2^2, 3^2,...,$((p-1)/2)^2$ y de $(p-1)/2$ no-restos cuadráticos. Si *a* es un resto cuadrático respecto al $módulo\ p$, se tiene $a^{(p-1)/2}\equiv 1(mód.p)$; si *a* es no resto cuadrático respecto al módulo *p*, entonces $a^{(p-1)/2}\equiv -1(mód.p)$. Esto se conoce como *criterio de Euler*. Según el teorema de Fermat, $a^{p-1}\equiv 1(mód.p)$, luego $\left(a^{(p-1)/2}-1\right)\left(a^{(p-1)/2}+1\right)\equiv 0(mód.p)$. Esto nos lleva a que, el número de restos cuadráticos de la forma $(p-1)/2$ es igual al número de restos no cuadráticos.
El producto de dos restos o de dos no restos siempre es un resto cuadrático, y el producto de Un restos cuadrático con otro no cuadrático produce un no resto.
El conjunto de restos cuadráticos forma un grupo multiplicativo en $\mathbb{Z}/\mathbb{Z}p$, de índice 2.

1.2 Calcular los sistemas completo y reducido de restos del número 10.

El sistema completo de restos es el conjunto de *m* enteros, tomados cada uno de ellos, de una de las clases de restos respecto al $módulo\ m$, esto es, $\{0,1,2,3,\ldots,m-1\}$. En nuestro caso, para el número 10 tendremos $\{0,1,2,3,4,5,6,7,8,9\}$. Observar que si se produce un resto **0,** la división es exacta y, por tanto, el número es de la forma $10m$ y genera un cociente que es divisor de $10m$.
El sistema reducido de restos es el conjunto de *m* enteros tomados, cada uno de ellos, de una de las clases de restos $módulo\, m$, que no comparten con *m* factores comunes. La función $\varphi(m)=m(p_1-1/p_1),\ldots,(p_n-1/p_n)$ da el número de enteros que son primos con *m*. En nuestro caso, para el número 10, $\varphi(10)=10(1-1/2)(1-1/5)=10(1/2\cdot 4/5)=4$. Cuatro números que son coprimos con *10*, $\{1,3,5,7\}$. Es la solución del problema.

1.3 Calcular los restos potenciales de 5 respecto al módulo 13.

Si el sistema completo de restos, respecto al número 13 es $\{1,2,3,4,5,6,7,8,9,10,11,12\}$, los restos potenciales de 5, respecto a 13 serán $\{5,\ 12,\ 8,\ 1,\ 5,\ 12,\ 8,\ 1,\ 5,\ 12,\ 8,\ 1\}$, que hemos calculado de la siguiente forma:

$$\begin{array}{lll} 5^1\equiv 5 & 5^5\equiv 5 & 5^9\equiv 5 \\ 5^2\equiv 12 & 5^6\equiv 12 & 5^{10}\equiv 12 \\ 5^3\equiv 8 & 5^7\equiv 8 & 5^{11}\equiv 8 \\ 5^4\equiv 1 & 5^8\equiv 1 & 5^{12}\equiv 1 \end{array}$$

Si observamos los cálculos anteriores, podemos establecer un método sencillo para obtener estos restos.
Supongamos que $r_1,r_2,r_3,\ldots,r_h$ son los restos de n respecto al módulo m, esto es,

$$\begin{aligned} n &\equiv r_1(mód.m) \\ n^2 &\equiv r_2(mód.m) \\ n^3 &\equiv r_3(mód.m) \\ &\ldots\ldots \\ n^h &\equiv r_h(mód.m) \end{aligned}$$

Entonces, para encontrar el resto r_{h+1} de la potencia n_{h+1}, bastará multiplicar las congruencias primera y última anteriores, es decir, $n \cdot n_h = n^{h+1} \equiv r_1 \cdot r_h(mód.m)$, por lo que bastará con calcular $r_1 \cdot r_h(mód.m)$, siendo $r_1 \cdot r_h$ un número más pequeño que n^{h+1}.
En nuestro caso particular

$$\begin{aligned} 5^1 &\equiv 5(mód.13) \\ 5^2 = 25 &\equiv 12(mód.13) \\ 5^3 = 5^2 \cdot 5 &\equiv 8(mód.13) \\ 5^4 = 5^2 \cdot 5^2 &\equiv 1(mód.13) \\ &\ldots\ldots \end{aligned}$$

1.4 Calcular los restos cuadráticos respecto al módulo 17.

El sistema completo de restos, respecto al módulo 17 es $\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$.
El sistema cuadrático de restos, respecto a 17 es $\{1,4,9,16,8,2,15,13,13,15,2,8,16,9,4,1\}$, que hemos calculado de la siguiente forma:

$$\begin{array}{llll} 1^2 \equiv 1 & 5^2 \equiv 8 & 9^2 \equiv 13 & 13^2 \equiv 16 \\ 2^2 \equiv 4 & 6^2 \equiv 2 & 10^2 \equiv 15 & 14^2 \equiv 9 \\ 3^2 \equiv 9 & 7^2 \equiv 15 & 11^2 \equiv 2 & 15^2 \equiv 4 \\ 4^2 \equiv 16 & 8^2 \equiv 13 & 12^2 \equiv 8 & 16^2 \equiv 1 \end{array}$$

Observar que los restos cuadráticos, respecto a un módulo, forman parejas donde la suma de las bases es igual al módulo. Esto forma un conjunto simétrico que nos permite obtener la totalidad de restos cuadráticos utilizando sólo la mitad de los números base. Veamos cómo:

$$\begin{array}{ll} 1^2 \ y\ 16^2 \equiv 1(mód.17) & 5^2 \ y\ 12^2 \equiv 8(mód.17) \\ 2^2 \ y\ 15^2 \equiv 4(mód.17) & 6^2 \ y\ 11^2 \equiv 2(mód.17) \\ 3^2 \ y\ 14^2 \equiv 9(mód.17) & 7^2 \ y\ 10^2 \equiv 15(mód.17) \\ 4^2 \ y\ 13^2 \equiv 16(mód.17) & 8^2 \ y\ 9^2 \equiv 13(mód.17) \end{array}$$

1.5 Resolver la ecuación $x^2 + 8 \equiv 0(mód.11)$.

La ecuación $x^2 + 8 \equiv 0(mód.11)$ se puede escribir como $x^2 \equiv 3(mód.11)$. Esta ecuación tendrá solución sí, y sólo si, 3 es un resto cuadrático respecto al módulo 11.
Los restos cuadráticos respecto al módulo 11 son $\{1,4,9,5,3,3,5,9,4,1\}$ donde aparece el número 3 luego, la ecuación tiene solución. Dado que el número 3 se encuentra en el epicentro del

conjunto de restos, y dado que las bases de este epicentro serán $\frac{11-1}{2}=5$ y $\frac{11+1}{2}=6,$ estas serán las soluciones de la ecuación. Efectivamente, $5^2-3=22=2\cdot 11$ y $6^2-3=33=3\cdot 11.$ Podemos decir que, del sistema completo de restos $\{1,2,3,4,5,6,7,8,9,10\},$ el 5 y el 6 satisfacen a la ecuación.

Para la determinación de si un número es o no resto cuadrático respecto a un módulo m, podemos utilizar el *criterio de Euler*, $a^{(p-1)/2}\equiv \pm 1(mód.m),$ con m primo y donde a representa el número a investigar. Para nuestro caso, $3^{(11-1)/2}=3^5\equiv 1(mód.11),$ donde el resto de la unidad positiva denota que 3 es resto cuadrático respecto al módulo 11.

1.6 Si a es restos cuadrático respecto al módulo p, siendo $mcd(a,p)=1,$ demostrar que $x^2\equiv a(mód.p)$ admite dos soluciones.

Si a es resto cuadrático, la congruencia $x^2\equiv a(mód.p)$ admite la solución $x\equiv x_1(mód.p)$ entonces, como $(-x_1)^2=x^2,$ la misma congruencia admitirá una segunda solución, esto es, $x\equiv -x_1(mód.p),$ que es distinta a la anterior. Luego, $x^2\equiv a(mód.p)$ admitirá como soluciones $x\equiv x_1,x_2(mód.p)$ si, y sólo si, a es resto cuadrático respecto al módulo p.

1.7 Resolver la ecuación $x^2\equiv 3(mód.13).$.

Si aplicamos el *criterio de Euler*, $3^{(13-1)/2}=3^6\equiv 1(mód.13)$ que denota que el 3 es resto cuadrático respecto al módulo 13.

El sistema completo de restos del número 13 es $\{1,2,3,4,5,6,7,8,9,10,11,12\},$ de los que el 4 y el 9 satisfacen a la ecuación $x^2\equiv 3(mód.13)$ por tanto, $x_1=4+13t$ y $x_2=9+13t$ son sus soluciones.

El sistema cuadrático de restos respecto al módulo 13 es:

$$1^2\ y\ 12^2\ \equiv\ 1(mód.13)\qquad 4^2\ y\ 9^2\equiv\ 3(mód.13)$$
$$2^2\ y\ 11^2\equiv\ 4(mód.13)\qquad 5^2\ y\ 8^2\equiv 12(mód.13)$$
$$3^2\ y\ 10^2\equiv\ 9(mód.13)\qquad 6^2\ y\ 7^2\equiv 10(mód.13)$$

1.8 Resolver la ecuación $x^2\equiv 19(mód.29).$.

Mediante el criterio de Euler, $19^{(29-1)/2}=19^{14}\equiv -1(mód.29),$ que indica que 19 no es resto cuadrático respecto al módulo 29. Efectivamente, el sistema de restos cuadráticos respecto a 29, es

$$\{1,4,9,16,25,7,20,6,23,13,5,28,24,22,22,24,28,5,13,23,6,20,7,25,16,9,4,1\}$$

en donde no aparece el número 19, por tanto, la ecuación no tiene solución.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	28	27	26	25	24	23	22	21	20	19	18	17	16	15
Raíces	**1**	**4**	**9**	**16**	**25**	**7**	**20**	**6**	**23**	**13**	**5**	**28**	**24**	**22**

Observar la simetría de las bases del exponente formando parejas cuya suma es 29.

9.2 Símbolos de Legendre y Jacobi

2.1 Símbolo de Legendre y sus propiedades.

Sea p un primo impar. Diremos que un número natural a primo con p es un *resto cuadrático* módulo p si $x^2 \equiv a(mód.p)$, para cierto entero x. En caso contrario, siempre suponiendo que p es primo, diremos que a es un *resto no cuadrático*. Se conoce como *símbolo de Legendre* a la expresión

$$\left(\frac{a}{p}\right)=(a/p)=\begin{cases} 1 \text{ si } a \text{ es resto cuadratico } \textit{módulo } p \\ -1 \text{ si } a \text{ es resto no cuadrático } \textit{módulo } p \\ 0 \text{ si } p \mid a \end{cases}$$

Si a es un resto cuadrático respecto al módulo p, se tiene $a^{\frac{p-1}{2}} \equiv 1(mód.p)$. Si a es un no cuadrático respecto al módulo p, se tiene $a^{\frac{p-1}{2}} \equiv -1(mód.p)$. En efecto, según el teorema de Fermat, $a^{p-1} \equiv 1(mód.p)$ donde $\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right) \equiv 0(mód.p)$. De aquí podemos deducir que $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)(mód.p)$ que nos permite la solución a la ecuación $x^2 \equiv a(mód.p)$ aplicando propiedades del símbolo de Legendre.
El símbolo de Legendre satisface algunas propiedades interesantes como:

i. Si $a \equiv b(mód.p)$, entonces $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$. Esta propiedad se debe a que los números de una misma clase son simultáneamente restos o no restos cuadráticos.

ii. Si $a \equiv 1(mód.p)$, tenemos $\left(\frac{1}{p}\right)=1$. En efecto, $1=1^2$ y, por tanto, 1 es un resto cuadrático.

iii. Si $a \equiv -1(mód.p)$, entonces $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. Esta propiedad se deduce de la anterior para $a=-1$ y denota un resto no cuadrático.

iv. Si $a \equiv 2(mód.p)$, entonces $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

v. Si $a \equiv -3(mód.p)$, entonces $\left(\frac{-3}{p}\right)=\begin{cases} 1 \text{ si } p \equiv 1(mód.6) \\ -1 \text{ si } p \equiv 5(mód.6) \end{cases}$.

vi. Si $a \equiv 5(mód.p)$, entonces $\left(\frac{5}{p}\right)=\begin{cases} 1 \text{ si } p \equiv 1,9(mód.10) \\ -1 \text{ si } p \equiv 3,7(mód.10) \end{cases}$.

vii. Sea $\left(\frac{abb}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{b}{p}\right)$. Se deduce, en particular, que $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{a}{p}\right)$, ya que $\left(\frac{b}{p}\right)^2=1$. Esto significa que en el numerador del *símbolo de Legendre* se puede eliminar cualquier factor cuadrático.

viii. Si p y q son números primos impares, $\left(\frac{q}{p}\right)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\left(\frac{p}{q}\right)$. Esta propiedad es conocida como *Ley de Reciprocidad Cuadrática*.

Nota: La *Ley de Reciprocidad Cuadrática* tiene un papel muy importante en la teoría de los números, ya que en base a ésta, se han obtenido otros resultados interesantes en diversos campos de las matemáticas. Descubierta por $Euler$ ($1707-1783$) en 1742, gracias a los trabajos realizados por $Fermat$ ($1601-1665$, revisada en 1772, fue publicada en su *Opuscula Analitica* de 1873, después de su muerte. $Legendre$ ($1752-1833$) fue otro de los pioneros en el estudio de esta ley, de hecho fue el primero en dar una demostración. Basándose en los trabajos de Euler, en 1798 publica en su obra *Essai sur la Théorie des Nombres* un lema que hoy se conoce como *símbolo de Legendre*. El primero que ofrece una demostración completa de la *Ley de Reciprocidad Cuadrátic*a fue $Gauss$ ($1777-1855$), a la que llama *Theorema Aureum* (Teorema áureo), recogida en su obra Disquisitiones Arithmeticae y publicada en 1796.

2.2 Símbolo de Jacobi y sus propiedades.

Consideremos el símbolo $\left(\frac{n}{m}\right)$ ó (n/m) para números impares m con $m>1,$ no necesariamente primos, donde $m=p_1\cdot p_2\cdot\ldots\cdot p_n,$ con $mcd(n,m)\neq 1.$
El *Símbolo de Jacobi* se define como

$$\left(\frac{n}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_2}\right)\ldots\left(\frac{l}{p_n}\right)$$

Sus propiedades son similares a las propiedades al S*ímbolo de Legendre*.
El uso del S*ímbolo de Jacobi* proporciona la generalización del S*ímbolo de Legendre* y la del teorema de los recíprocos cuadráticos $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{(m-1)(n-1)/4}$, para m,n relativamente primos enteros, con $n\geq 3.$ Esta igual es equivalente a

$$\left(\frac{m}{n}\right)=(-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$$

que también podemos escribir como:

$$\left(\frac{n}{m}\right)=\begin{cases}+\left(\frac{m}{n}\right)\text{ para } m\ ó\ n\equiv 1(mód.4)\\ -\left(\frac{m}{n}\right)\text{ para }\quad m,n\equiv 3(mód.4)\end{cases}.$$

Estos es lo que hemos definido anteriormente como *Ley de Reciprocidad Cuadrática*.

2.3 Demostrar que si p es primo y a y b son dos enteros con $a\equiv b(mód.p),$ entonces $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$

El valor de $\left(\frac{a}{p}\right)$ depende sólo de si a es restos cuadrático, esto es, si $x^2\equiv a(mód.p)$ tiene solución. Como esto sólo depende de la clase de equivalencia de a respecto a $p,$ se verifica que $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ si, y sólo si $a\equiv b(mód.p).$

Si p es primo y $mcd(a,p)=1,$ obtenemos $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2}(mód.p),$ que es el *criterio de Euler*. Por el *pequeño teorema de Fermat* sabemos que $a^{p-1}\equiv 1(mód.p),$ esto nos permite deducir que $\left(a^{p-1}\right)^2\equiv a^{p-1}\equiv \pm 1(mód.p),$ y para que $a^{p-1}\equiv 1(mód.p)$ será necesario que $\left(\frac{a}{p}\right)=1.$

Por ejemplo, si $a=7$ y p es de la forma $p\equiv 1(mód.4),$ tenemos

$$\left(\frac{7}{p}\right)=\left(\frac{p}{7}\right)=\begin{cases} 1\ si\ p\equiv 1,2,4(mód.7) \\ -1\ si\ p\equiv 3,5,6(mód.7)\end{cases}$$

Si p es de la forma $p\equiv 3(mód.4),$ tenemos

$$\left(\frac{7}{p}\right)=-\left(\frac{p}{7}\right)=\begin{cases} 1\ si\ p\equiv 3,5,6(mód.7) \\ -1\ si\ p\equiv 1,2,4(mód.7)\end{cases}$$

o, también

$$\left(\frac{7}{p}\right)=\begin{cases} 1\ si\ p\equiv 1,3,9,19,25,27(mód.28) \\ -1\ si\ p\equiv 5,11,13,15,17,23(mód.28)\end{cases}$$

2.4 Demostrar que si p es primo y a y b son dos enteros no divisibles con $q,$ entonces $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$

Sabemos que $a^{(p-1)/2}\equiv\left(\frac{a}{p}\right)(mód.p),$ entonces $(ab)^{(p-1)/2}\equiv\left(\frac{ab}{p}\right)(mód.p)$ donde $mcd(ab,p)=1,$

como $a^{(p-1)/2}\equiv\left(\frac{a}{p}\right)(mód.p)$ y $b^{(p-1)/2}\equiv\left(\frac{b}{p}\right)(mód.p),$ se cumple que $\left(\frac{ab}{p}\right)\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(mód.p),$ y

como p no es par, $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$ luego $\left(\frac{ab}{p}\right)=a^{(p-1)/2}b^{(p-1)/2}=(ab)^{(p-1)/2}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(mód.p).$

2.5 Demostrar que si p es impar, entonces $\left(\frac{2}{p}\right)=(-1)(p^2-1)/2.$

Sea $\left(\frac{a}{p}\right)=(-1)^k$ donde k es el número de restos que son mayores que $p/2,$ como $(-1)^8\equiv k(mód.2),$ entonces

$$\left(\frac{2}{p}\right)=(-1)^k=(-1)^{(p^2-1)/8}$$

El profesor Vinogradov llega a esta conclusión utilizando el S*ímbolo de Jacobi*. Este matemático dice que si *P* es impar mayor que la unidad, esto es, $m = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ que es la descomposición factorial de P, y si el $mcd(a,P)=1,$ entonces el Símbolo de Jacobi $\left(\frac{a}{m}\right)$ se define por la igualdad:

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_r}\right)=\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

A partir de lo expuestos podemos obtener otras igualdades como

$$\left(\frac{a}{p}\right)=\left(\frac{ab^2}{p}\right),\ \left(\frac{1}{p}\right)=1 \text{ ó } \left(\frac{1}{p}\right)=(-1)^{(p-1)/2}\left(\frac{1}{p}\right)=(-1)^{(p-1)/2}$$

y también

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\frac{a+p}{2}}{p}\right)=\left(\frac{\frac{a+p}{2}}{p}\right)$$

que nos lleva a que

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}},$$

de la que nos permite deducir dos propiedades muy importantes del *Símbolo de Legendre*. La primera es que para $a=1$:

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

la segunda es que si *p* es de la forma $p=8m+s,$ donde *s* es uno de los números *1, 3, 5, 7*, y además

$$\left(\frac{p^2-1}{8}\right)=8m^2+2ms+\frac{s^2-1}{8}$$

entonces este número será par si $s=1$ ó $s=7,$ e impar si $s=3$ ó $s=5.$ Por tanto, el número *2* será resto cuadrático respecto al módulo *p* si *p* es de la forma $p=8m+1$ ó $p=8m+7$ y será no resto cuadrático respecto al módulo *p* si *p* es de la forma $p=8m+3$ ó $p=8m+5.$

2.6 Demostrar que si P y Q son números impares positivos, primos entre sí, entonces $\left(\frac{Q}{P}\right)=(-1)^{(P-1)(Q-1)/4}\left(\frac{P}{Q}\right)$.

Como $\left(\frac{P-1}{2}\right)\cdot\left(\frac{Q-1}{2}\right)$ es impar solamente cuando ambos números, P y Q, son de la forma $4m+3$, y es par si al menos uno de estos números es de la forma $4m+1$, la propiedad señalada se puede formular así:

Si ambos números, P y Q, son de la forma $4m+3$, entonces $\left(\frac{Q}{P}\right)=-\left(\frac{P}{Q}\right)$.

Si al menos uno de los números, P y Q, es de la forma $4m+1$, entonces $\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)$.

Supongamos que $Q=q_1\cdot q_2\cdot\ldots\cdot q_n$ es la descomposición de Q en factores primos, se tiene

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\cdot\left(\frac{Q}{p_2}\right)\cdot\ldots\cdot\left(\frac{Q}{p_n}\right)=\coprod_{\alpha=1}^{s}\cdot\coprod_{\beta=1}^{t}\left(\frac{Q_\beta}{P_\alpha}\right)$$

y como

$$\coprod_{\alpha=1}^{s}\cdot\coprod_{\beta=1}^{t}\left(\frac{Q_\beta}{P_\alpha}\right)=(-1)^{\left(\sum_{\alpha=1}^{r}\frac{P_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{Q_\beta-1}{2}\right)}\coprod_{\alpha=1}^{s}\cdot\coprod_{\beta=1}^{t}\left(\frac{P_\alpha}{Q_\beta}\right)$$

resulta:

$$\left(\frac{Q}{P}\right)=(-1)^{\left(\sum_{\alpha=1}^{r}\frac{P_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{Q_\beta-1}{2}\right)}\frac{P}{Q}.$$

Si ahora hacemos que

$$\frac{P-1}{2}=\sum_{\alpha=1}^{r}\frac{P_\alpha-1}{2}+2N \text{ y } \frac{Q-1}{2}=\sum_{\beta=1}^{s}\frac{Q_\beta-1}{2}+2N_1,$$

entonces:

$$\left(\frac{Q}{P}\right)=(-1)^{(P-1)(Q-1)/4}\left(\frac{P}{Q}\right).$$

2.7 Resolver la ecuación $x^2\equiv 28(mód.37)$.

Sea $\left(\frac{28}{37}\right)=\left(\frac{2^2\cdot 7}{37}\right)=\left(\frac{2\cdot 2\cdot 7}{37}\right)$. Para $\left(\frac{2}{37}\right)=\left(\frac{37}{2}\right)(-1)^{(37^2-1)/8}=\left(\frac{1}{2}\right)=1$, ya que $37\equiv 1(mód.2)$.

Por tanto, como $\left(\frac{28}{37}\right)=1$, 28 es resto cuadrático respecto al módulo 37, y la ecuación planteada tiene solución. Efectivamente, del sistema completo de restos respecto al módulo 37, la

pareja central compuesta por el 18 y 19, satisfacen a la ecuación $x^2 \equiv 28(mód.37),$ por tanto son sus soluciones.

Dado que $28 = 2^2 \cdot 7$ y sabiendo por vii que en el numerador del S*ímbolo de Legendre* se pueden eliminar cualquier factor cuadrático, resulta para:

$$\left(\frac{28}{37}\right) = \left(\frac{2^2 \cdot 7}{37}\right) = \left(\frac{7}{37}\right)$$

Utilizando la *Ley de Reciprocidad Cuadrática*

$$\left(\frac{7}{37}\right) = \left(\frac{37}{7}\right)(-1)^{((37-1)(7-1))/2} = \left(\frac{37}{7}\right) = \left(\frac{2}{7}\right)$$

ya que $37 \equiv 2(mód.7).$

Como $\left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = 1,$ resulta para $\left(\frac{28}{37}\right) = 1,$ por tanto 28 es restos cuadrático respecto a 37.

2.8 Resolver la ecuación $x^2 \equiv 174(mód.239).$

Como $174 = 2 \cdot 3 \cdot 29,$ $\left(\frac{174}{239}\right) = \left(\frac{2}{239}\right)\left(\frac{3}{239}\right)\left(\frac{29}{239}\right).$

Por la *Ley de Reciprocidad Cuadrática*, se tiene que

Para $\left(\frac{2}{239}\right) = \left(\frac{239}{2}\right)(-1)^{(239^2-1)/8} = 1,$ ya que $239 \equiv 1(mód.2).$

Para $\left(\frac{3}{239}\right) = \left(\frac{239}{3}\right)(-1)^{(239-1)/2} = -\left(\frac{239}{3}\right) = -\left(\frac{2}{3}\right) = \left(\frac{1}{3}\right) = 1,$ ya que $3 \equiv 1(mód.2).$

Para $\left(\frac{29}{239}\right) = \left(\frac{239}{29}\right)(-1)^{(239/2)(28/2)} = -\left(\frac{239}{29}\right) = \left(\frac{7}{29}\right) = 7,$ ya que $239 \equiv 7(mód.29).$

Para $\left(\frac{7}{29}\right) = \left(\frac{29}{7}\right)(-1)^{(28/2)(8/2)} = \left(\frac{29}{7}\right) = \left(\frac{7}{29}\right) = 1,$ ya que $29 \equiv 1(mód.7).$

Como

$$\left(\frac{174}{239}\right) = \left(\frac{2}{239}\right)\left(\frac{3}{239}\right)\left(\frac{29}{239}\right). = (+1)(+1)(+1) = 1$$ 174

es restos cuadrático respecto a 239 por tanto, la ecuación $x^2 \equiv 174(mód.239)$ tiene como solución $x \equiv 37, 202(mód.239).$

2.9 Resolver la ecuación $x^2 \equiv 864(mód.857)$.

Como $864 = 2^5 \cdot 3^3$, $\left(\frac{864}{857}\right) = \left(\frac{2^5}{857}\right)\left(\frac{3^3}{857}\right) = \left(\frac{2}{857}\right)\left(\frac{3}{857}\right)$.

Por la L*ey de Reciprocidad Cuadrática*, se tiene que

Para $\left(\frac{2}{857}\right) = \left(\frac{857}{2}\right)(-1)^{(857^2-1)/8} = 1,$ ya que $557 \equiv 1(mód.2)$.

Para $\left(\frac{3}{857}\right) = \left(\frac{857}{3}\right)(-1)^{(857-1)/2} = \left(\frac{2}{3}\right) = -1,$ ya que $2+1 \equiv 0(mód.3)$

Como

$$\left(\frac{864}{857}\right) = \left(\frac{2^5}{857}\right)\left(\frac{3^3}{857}\right) = \left(\frac{2}{857}\right)\left(\frac{3}{857}\right) = (+1)(-1) = -1, \ 864$$

no es resto cuadrático respecto al módulo 857, por tanto $x^2 \not\equiv 864(mód.857)$ no tiene solución.

9.3 Símbolo de Kronecker y Lema de Gauss

3.1 Símbolo de Kronecker y sus propiedades.

El S*ímbolo de* Kronecker, que podemos denotar como $\left(\frac{n}{m}\right)$ ó (n/m), es una extensión del *Símbolo de Jacobi,* descubierto por el matemático alemán Leopold Kronecker (1823-1891) y que comparte las mismas reglas que éste.
Algunas de sus propiedades son:

Para $m = -1$, $\left(\frac{n}{-1}\right) = \begin{cases} -1 \text{ si } n < 0 \\ 1 \text{ si } n > 0 \end{cases}$

Para $m = 2$, $\left(\frac{n}{2}\right) \equiv \begin{cases} 0 \text{ para } n \text{ par} \\ 1 \text{ para } n \text{ impar, } n \equiv \pm 1(mód.8) \\ -1 \text{ para } n \text{ impar, } n \equiv \pm 3(mód.8) \end{cases}$

o también, $\left(\frac{n}{2}\right) \equiv \begin{cases} 0 \text{ para } 4 \mid n \\ 1 \text{ para } n \equiv 1(mód.8) \\ -1 \text{ para } n \equiv 5(mód.8) \end{cases}$

3.2 Utilizando el símbolo de Kronecker, resolver $\left(\frac{85}{2}\right)$..

Como $\left(\frac{85}{2}\right) = -1,$ entonces $85 \equiv 5(mód.8)$.

3.3 Utilizando el símbolo de Kronecker, resolver $\left(\frac{131}{248}\right)$..

Como $248=8\cdot 31$, $\left(\frac{131}{8}\right)=-1$ ya que $131\equiv 3(mód.8)$.

3.4 Lema de Gauss: definición.

Sea p un primo impar, sea a un entero no divisible por p y sea $u=\left(\frac{p-1}{2}\right)$. Si al dividir los números $\{a,2a,3a,\ldots,a[(p-1)/2]\}$ por p hay exactamente s elementos cuyo resto es mayor que u, entonces $\left(\frac{a}{p}\right)=(-1)^s$. Esto se conoce como *Lema de Gauss* en honor a Carl Friedrich Gauss (1777-1855) que la descubrió.

Por el *criterio de Euler*, $\left(\frac{a}{p}\right)\equiv a^u(mód.p)$, como $u!$ no es divisible por p, obtenemos:

$$a^u\equiv(-1)^s(mód.p)$$

luego

$$\left(\frac{a}{p}\right)\equiv(-1)^s(mód.p)$$

3.5 Utilizando el lema de Gauss, resolver $\left(\frac{5}{17}\right)$.

Tenemos $p=17$, $a=5$ y $s=\frac{17-1}{2}=8$. Si multiplicamos por 5 los números entre 1 y 8, obtenemos $\{5,10,15,20,25,30,35\ y\ 40\}$. Estos números, respecto al módulo 17, generan el sistema de restos $\{5,10,15,3,8,13,1,6\}$ de los que $\{10,15\ y\ 13\}$ son mayores que $u=8$, por tanto

$$\left(\frac{5}{17}\right)=(-1)^3=-1$$

que es lo mismo que $5^8\equiv(-1)^3(mód.17)\ \Rightarrow\ 5^8+1\equiv(mód.17)$.

3.6 Utilizando el lema de Gauss, resolver $\left(\frac{5}{31}\right)$.

Tenemos que $s=\frac{31-1}{2}=15$ y $\frac{p}{2}=15,5$. Sea $E=\{5,2\cdot 5,3\cdot 5,\ldots,15\cdot 5\}$, los residuos módulo 31 de los elementos de E son

$$\overline{E}=\{5,10,15,20,25,30,,9,14,19,24,29,3,8,13\}$$

luego el conjunto de los elementos de $\overline{E}$ mayores que $15,5$ vienen determinados por

$$A=\{19,20,24,25,29,30\}$$

entonces tenemos que $A=6,$ de donde

$$\frac{5}{31}=(-1)^6=1$$

Esto queda demostrado por la *función generatriz o criterio de Euler,* ya que, si tenemos en cuenta que $5^{(31-1)/2}\equiv 1(mód.31),$ la ecuación $x^2\equiv 5(mód.31)$ tiene como solución las raíces primitivas $x_1=6+31t\ y\ x_2=25+31t.$

3.7 Utilizando el lema de Gauss, resolver $\left(\frac{3}{13}\right).$

Del conjunto $\{3,6,9,12,15,18\}$ son restos respecto a 13 $\{3,6,9,12,2,5\}.$ De estos hay dos elementos que son mayores a $13/2,$ luego

$$\left(\frac{3}{13}\right)=(-1)^2=1$$

3.8 Lema de Eisenstein: definición.

Sea p un número primo impar y sea a un entero no divisible por p. Sea $s=\sum_{j=1}^{u}[ja/p].$

Si a es impar, entonces $\left(\frac{a}{p}\right)=(-1)^s.$

Si $a=2$, entonces $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}.$

Si hacemos que

$$\sum_{j=1}^{u}ja=\sum_{j=1}^{u}(ja/p)p+\sum_{j=1}^{u}r_j=sp+\sum_{r_j\le u}r_j+\sum_{r_j>u}r_j \text{ y si } \sum_{j=1}^{u}j=\sum_{r_j\le u}r_j+\sum_{r_j>u}(p-r_j)$$

restando ambas ecuaciones obtenemos

$$(a-1)\sum_{j=1}^{u}j=sp-pl+2\sum_{r_j>u}r_j$$

Si a es impar, entonces $(a-1)\equiv 0(mód.2),\ p\equiv 1(mód.2)$ y $l\equiv s(mód.2).$ El resultado se sigue por el Lema de Gauss.

Supongamos que $a=2.$ Si $1\le j\le u,$ tenemos $(2j/p)=0$ puesto que $p>2j.$ Así, $s=0.$
Como

$$\sum_{j=1}^{u} j = \frac{u(u+1)}{2} = \frac{p^2-1}{8}$$

podemos establecer que $\frac{p^2-1}{8} \equiv l(mód.2)$, resultado que se sigue por el Lema de Gauss.

El Lema de Eisenstein fue descubierto por el matemático *alemán Ferdinand Gotthold Eisenstein(1823-1852).*

3.9 Determinar todos los números primos impares p tales que 3 es restos cuadrático . $(mód.p)$.

Por la Ley de Reciprocidad Cuadrática, tenemos que

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{(p-1)/2}$$

de donde

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{1}{3}\right) \; si \; p \equiv 1(mód.3) \\ \left(\frac{1}{3}\right) \; si \; p \equiv 2(mód.3) \end{cases}$$

y

$$(-1)^{(p-1)/2} = \begin{cases} 1 \; si \; p \equiv 1(mód.4) \\ \text{-}1 \; si \; p \equiv 3(mód.4) \end{cases}$$

por tanto

$$\left(\frac{3}{p}\right) = 1$$

si, y solamente si

$$p \equiv 1(mód.3),\ p \equiv 1(mód.4) \text{ ó } p \equiv 2(mód.3),\ p \equiv 3(mód.4)$$

es decir:

$$p \equiv 1(mód.12) \; ó \; p \equiv 11(mód.12)$$

9.4 Algunas Aplicaciones: Pascua de Resurrección

4.1 Calendario Juliano

Calendario solar hecho en tiempos de Julio César por el astrónomo griego de Alejandría, Losígenes, el año 45 a.C. con la intención de aplicarlo a todo el Imperio de Roma. Constaba de doce meses y consideraba como bisiestos todos los años cuyo número de días fuera divisible por 4, aunque terminasen el siglo. Cada mes estaba dedicado devocionalmente a un dios: Enero estaba dedicado a Jano y a la diosa Juno; Febrero, a Neptuno; Marzo, a Minerva; Abril, a Venus; Mayo, a Apolo; Junio, a Mercurio, Julio, a Júpiter; Agosto, a Ceres; Septiembre, a Vulcano; Octubre, a Marte; Noviembre, a Diana, y Diciembre, a Vesta.

Al establecerse el cómputo anual a partir del año del Trópico de Cáncer, cuya duración es de 365 días y 6 horas, exactamente, se producía un error de 11 minutos y 12 segundos de exceso por cada año, lo que provocaba la aparición de un día de más en el equinoccio cada 129 años. El calendario juliano estuvo vigente en Inglaterra hasta 1752, aunque en el resto del mundo occidental desde el año 1582 ya se había adoptado el calendario gregoriano, modificado por mandato del papa Gregorio XIII. En la actualidad todavía lo conservan los cismáticos griegos, y en las naciones musulmanas lo utilizan para los cálculos astronómicos y los usos en la agricultura.

4.2 Calendario Gregoriano

Calendario establecido por el papa Gregorio XIII en el año 1582 a partir de una serie de modificaciones hechas sobre el calendario juliano: corrió diez días en el mes de octubre y no contabilizó como bisiestos los años que terminan siglo, excepto cuando caen en decena de siglo. En la actualidad es el adoptado por el mundo occidental, salvo los griegos ortodoxos.

Pese a todas las correcciones, ajustes y mejoras, el calendario juliano, que establecía un año equivalente a 365'25 días, no llegaba a ajustarse de manera precisa a la duración de 365'242199 días del año trópico. La diferencia de 11 minutos y 14 segundos por año fue acumulándose, lo que motivó, por ejemplo, serias preocupaciones entre los participantes en el Concilio de Nicea (325), donde se comprobó que el equinoccio de primavera había coincidido con la fecha del 21 de marzo en vez de con el 25 de marzo previsto. El desajuste de 10 días que se alcanzó en 1545 era ya lo suficientemente importante como para que el Concilio de Trento autorizase e instase a su corrección al Papa Pablo III. Tras algunos años en que se sucedieron diversos estudios y propuestas de reforma, el Papa Gregorio XIII confió en 1572 la cuestión al astrónomo jesuita Cristóbal Clavius (1537-1612) y en 1582 se llegó al acuerdo de abolir el calendario juliano (que siguen utilizando sólo los ortodoxos griegos y algunas naciones musulmanas con fines astronómicos y agrícolas), corregir el desajuste de diez días, comenzar un nuevo cómputo del calendario y establecer una nueva duración del año equivalente a 365'2422 días, con lo que la diferencia con respecto al año trópico quedaría reducida a un exceso de 3 días cada 10.000 años, mucho más de acuerdo con el ciclo natural de lo que nunca estuvo el calendario juliano. Además, si anteriormente el calendario juliano contaba como bisiestos todos los años cuyo número fuera divisible por 4, aunque terminasen siglo, el calendario gregoriano estipuló no computar como bisiestos los años que terminasen siglo excepto cuando cayesen en decena de siglo; es decir, que estableció que el último año de cada siglo dejara de ser bisiesto en el nuevo sistema, salvo cuando se tratara de un múltiplo de 400 (1600, 2000, 2400, etc.). En aplicación de las nuevas normas sobre el calendario, el jueves 4 de octubre de 1582 fue seguido por el viernes 15 de octubre de 1582.

La adopción del nuevo calendario gregoriano planteaba problemas de adaptación que encontró serias resistencias en numerosos países. Aunque algunos lo aceptaron en los primeros años de su vigencia, algunas naciones no católicas no lo hicieron hasta el siglo XVIII e inclu-

so siglos posteriores: Gran Bretaña y sus colonias lo adoptaron en 1752, la URSS en 1918, y Grecia en 1923, si bien la celebración de sus fiestas religiosas sigue rigiéndose por el calendario juliano. En la actualidad, el calendario gregoriano ha logrado una implantación prácticamente universal, aunque algunos pueblos siguen usando, aunque limitados mayormente a las celebraciones festivas y religiosas, calendarios propios. Tal sucede con los países de religión musulmana, judía e hindú. A pesar de que su cómputo empieza en la fecha que tradicionalmente se consideró como la del nacimiento de Cristo, la documentación histórica indica que en realidad el Cristo histórico debió nacer 4 años antes del inicio del calendario cristiano.

4.3 Los Cómputos

Procedentes del latín *computare* (calcular), han llegado hasta nuestros días las palabras *cómputo* (cálculo), *computación* (método de cálculo), *contar* y demás voces derivadas de la misma etimología. El idioma inglés la ha tomado para designar el *computer*, que ha pasado a nuestro idioma como *computador* (o computadora), palabra de uso corriente junto con *ordenador*, de origen francés. Los elementos del cómputo anual son: la letra dominical, el número áureo, la epacta, el ciclo solar y la indicción romana.

I. La **letra dominical**, de la A a la G, indica qué día de la semana es el primer domingo del año: A (1 de enero), B (2 de enero), C (3 de enero), D (4 de enero), E (5 de enero), F (6 de enero) y G (y de enero). Si el año es bisiesto, se indican dos letras: a la letra correspondiente se le añade la precedente. Así por ejemplo, para el año 1972, BA, para 1956, AG.
II. El **número áureo** indica el lugar que ocupa un año en un periodo de 19 años, intervalo tras el cual las lunaciones recaen casi en los mismos días. Los periodos se inician en el año 1 de la era cristiana al que se asignó el número 2. La finalidad del número áureo es establecer la correspondencia del año lunar. Por ejemplo los últimos periodos han sido/serán 1957-1975; 1976-1994; 1995-2014.
III. La **epacta** indica la edad de la lunación justo antes del 1 de enero, para un periodo de 29 años. Una lunación exacta (tiempo entre dos lunas nuevas) dura 29 días, 12 horas, 44 minutos y 2,8 segundos. Llamamos luna nueva al momento en que la Luna no es visible desde la Tierra. La epacta es 0 si la luna nueva cae en 31 de diciembre, 5 si la luna nueva tiene 5 días (cayó el 26 de diciembre).
IV. El **ciclo solar** es un periodo de 28 años julianos que lleva los mismos días de la semana en las mismas fechas del mes. Los últimos periodos han sido 1952-1979; 1980-2007.
V. La **indicción romana** indica el lugar que ocupa un año en un periodo de 15 años que se renuevan perpetuamente. Se obtiene sumando 3 al número del año y dividiendo el resultado por 15. El residuo expresa la indicción de dicho año. Si no hay residuo, la indicción es 15. Las bulas papales se fecha según la indicción. Los últimos periodos de indicción han sido 1978-1992; 1993-2007.

4.4 La fecha de Pascua de Resurrección

La epacta se utiliza para calcular la fecha de Pascua. En el concilio de Nicea del año 325, se estableció que la fiesta de Pascua de Resurrección debe celebrarse el domingo siguiente al plenilunio posterior al 21 de marzo, día del equinoccio de primavera. La Pascua debe situarse entre el 22 de marzo y el 25 de abril. La fecha de Pascua condiciona las demás celebraciones cristianas:

Miércoles de Ceniza	: 46 días antes de Pascuas
Primer domingo de Cuaresma	: 42 días
Jueves Santo	: 3 días
Viernes Santo	: 2 días
Ascensión	: 9 días después de Pascua
Pentecostés	: 49 días
Trinidad	: 56 días
Corpus Christi	: 63 días
Sagrado Corazón	: 68 días

4.5 Cálculo de la fecha de Pascua de Resurrección.

Antes de proseguir es preciso dejar claro que en términos astronómicos, el equinoccio puede tener lugar el 20 o el 19 de marzo, si bien en el calendario gregoriano se establecen unas fechas astronómicas que, aún difiriendo ligeramente de las fechas astronómicas reales, son las que se emplean para el cálculo. Así las cosas, queda claro que la Pascua de Resurrección no puede ser antes del 22 de marzo (en caso de que el plenilunio fuese sábado), y tampoco puede ser más tarde del 25 de abril, (suponiendo que el 21 de marzo fuese el día siguiente al plenilunio, habría que esperar una lunación completa (29 días) para llegar al siguiente plenilunio, que sería el 18 de abril, el cual, si cayese en domingo, desplazaría la Pascua una semana para evitar la coincidencia con la pascua judía, quedando: 18+7 el 25 de abril).

Si bien durante el Renacimiento se extrajeron tablas de cálculo para la Pascua en función del número áureo y otras más complejas, hoy en día la fórmula más sencilla de calcular esta fecha es mediante la fórmula desarrollada por Gauss. Esta fórmula requiere la definición de cinco variables, a,b,c,d y e. Además de dos constantes M y N, que para los años comprendidos entre 1900 y 2300 tomarán los siguientes valores:

Años	M	N
1900-2099	*24*	*5*
2100-2199	*24*	*6*
2200-2299	*25*	*0*

Llamando A al año del que queremos calcular la Pascua, los valores de las variables establecidas son:

$$A \equiv a(mód.19),\ \ A \equiv b(mód.4),\ \ A \equiv c(mód.7)$$
$$19a + M \equiv d(mód.30),\ 2b + 4c + 6d + N \equiv e(mód.7)$$

Interpretación:

Si $d + e < 10,$ entonces la Pascua caerá el día $(d + e + 22)$ de marzo.

Si $d + e > 9,$ entonces la Pascua caerá el día $(d + e - 9)$ de abril.

Si la fecha obtenida es el 26 de abril, la Pascua caerá el 19 de abril.

Si la fecha obtenida es el 25 de abril, con $d = 28,\ \ e = 6$ y $a > 10,$ entonces la Pascua caerá en el 18 de abril.

Vamos a calcular la fecha de Pascua correspondiente al año 2011. Aplicando las fórmulas anteriores, obtenemos para $a = 16,\ b = 3,\ c = 2.$ Ahora:

$$19 \cdot 16 + 24 \equiv 28(mód.30) \text{ y } 2 \cdot 3 + 4 \cdot 2 + 6 \cdot 28 + 5 \equiv 5(mód.7)$$

Como 28+5=33>9, entonces 33-9 corresponde al 24 de abril de 2011 que se celebrará la Pascua de Resurrección.

Por este mismo procedimiento podemos conocer que la Pascua de Resurrección caerá el 8 de abril en 2012 y en 31 de marzo en 2013.

BIBLIOGRAFIA:

APOSTOL, Tom M., Cálculus Tomo I, ISBN: 84-291-5002-1
BOLKER, Ethan D., Elementary Number Theory, ISBN: 0-486-45807-5
CRANTZ, Paul, Aritmética y Álgebra, Edición 1926
JOUETTE, André, El Secreto de los Números, ISBN: 84-95601-00-1 (Todo el tema relacionado con la fecha de Pascua)
KOSHY, Thomas, Elementary Number Theory with Applications, ISBN: 978-0-12-372487-8
LANG, Serge, Algebraic Number Theory, ISBN: 0-387-94225-4
NATHANSON, Melvyn B. Elementary Methods in Number Theory, ISBN: 0-387-98912-9
PHILLIPS, BUTTS y SHAUGHNESSY, Álgebra con Aplicaciones, ISBN: 968-6034-93-5
SWOKOWSKI y COLE, Álgebra y Trigonometría con Geometría Analítica, ISBN: 968-7529-26-1
TATTERSALL, James T., Elementary Number Theory in Nine Chapters, ISBN: 0-521-61524-0

APOYO INTERNET

http://es.wikipedia.org/wiki/Ley_de_reciprocidad_cuadr%C3%A1tica
http://es.wikipedia.org/wiki/Residuo_cuadr%C3%A1tico
http://hojamat.es/sindecimales/congruencias/diccio/diccong.htm
http://www.akiti.ca/Mathfxns.html (Solución de ecuaciones)
http://www.famaf.unc.edu.ar/publicaciones/documents/serie_c/CMat31-3.pdf
http://www.vadenumeros.es/actividades/division-por-ruffini.htm (Programa matemático)
http://www.vadenumeros.es/actividades/division-por-ruffini.htm (Soluciones Ruffini)
http://www.wolframalpha.com/examples/ (Programa matemático)
http://www.wolframalpha.com/examples/ (Soluciones algebraicas)

FECHA DE PASCUA: APOYO INTERNET

http://www.divvol.org/recursos/fecha_pascua.htm (Calcula la fecha de Pascua)
http://www.huevosdepascuas.com.ar/Historia/historia_de_la_pascua_catolica.htm
http://es.wikipedia.org/wiki/Pascua
http://www.statveritas.com.ar/Liturgia/La%20Pascua%20de%20Resurreccion.htm