

## CONTENIDOS POR ARTICULO.

---

*En la siguiente tabla los traductores indicamos los contenidos de cada artículo de las Disquisitiones Arithmeticae. Para ayudar al lector, nos permitimos utilizar lenguaje moderno, es decir, se usan términos introducidos después del tiempo de Gauss.*

### SECCION PRIMERA. DE LA CONGRUENCIA DE LOS NUMEROS EN GENERAL.

Artículo 1. Definición de *congruente*, *módulo* y *residuo*.

2. Clases módulo  $m$ ; notación para congruencias.
3. Las clases módulo  $m$  forman una partición de los enteros.
4. Residuos mínimos.
5. Congruencias según módulos compuestos; transitividad de congruencias.
6. Sumas de números congruentes.
7. Múltiplos de números congruentes.
8. Productos de números congruentes.
9. Polinomios de números congruentes.
10. Período de un polinomio módulo  $m$ .
11. Criterio necesario para resolver polinomios racionales.
12. Aplicaciones de la teoría a las reglas de aritmética elemental.

## SECCION SEGUNDA. SOBRE LAS CONGRUENCIAS DEL PRIMER GRADO

13. Lema para §14.
14. Si  $p|ab$  entonces  $p|a$  o  $p|b$ .
15. Extensión de §14 a productos de varios factores.
16. Teorema fundamental de aritmética.
17. Fórmula para  $\tau(A)$ , el número de factores de un entero compuesto  $A$ .
18. Cálculo del máximo común divisor y mínimo común múltiplo.
19. Propositiones elementales acerca de enteros relativamente primos.
20. Factorización primaria de una  $n$ -ésima potencia.
21. Factores de una  $n$ -ésima potencia.
22. División de una congruencia por un factor relativamente primo al módulo.
23. Si  $a$  y  $m$  son relativamente primos,  $a$  genera los enteros módulo  $m$  aditivamente.
24. Solubilidad de una congruencia lineal módulo  $m$ .
25. Congruencias trascendentales y algebraicas.
26. La solución de una congruencia consiste de varias clases de congruencia.
27. Algoritmo para resolver una congruencia lineal módulo un primo.
28. Método de Euler y Lagrange usando fracciones continuas.
29. Reducción del caso de un módulo compuesto.
30. Otro método para el caso de un módulo compuesto.
31. Cocientes módulo  $c$ .
32. Teorema chino del residuo.
33. Caso de §32 cuando los módulos son primos entre sí.
34. Posibilidad de que una congruencia sea superflua o inconsistente.
35. Ejemplo numérico del Teorema chino del residuo.
36. Otro algoritmo si los módulos son relativamente primos.
37. Sistemas de congruencias lineales.
38. Cálculo de la función  $\varphi(A)$  de Euler.
39. Inversión de Möbius de la función de Euler.
40. El máximo común divisor como combinación lineal.
41. Divisibilidad de un coeficiente multinomial por un primo.
42. El lema de Gauss para un producto de polinomios con coeficientes racionales.
43. Una congruencia de grado  $m$  tiene a lo sumo  $m$  raíces.
44. Comentarios sobre el teorema de §43.

## SECCION TERCERA. SOBRE RESIDUOS DE LAS POTENCIAS.

45. En el grupo multiplicativo  $U(p)$  de enteros relativamente primos al módulo  $p$ , todo elemento es de orden finito menor que  $p$ .
46. Subgrupo generado por un elemento  $a \in U(p)$ .
47. Cálculo de potencias módulo  $p$ .
48. Si  $|a| = t$  y  $a^k \equiv 1 \pmod{p}$ , entonces  $t|k$ .
49. Si  $p$  es primo,  $a \in U(p)$  y  $|a| = t$ , entonces  $t|p-1$ .
50. El pequeño teorema de Fermat:  $a^{p-1} \equiv 1 \pmod{p}$ , un primo que no divide a  $a$ .
51. La  $p$ -ésima potencia de una suma es la suma de las  $p$ -ésimas potencias mod.  $p$ .
52. Si  $d|p$ , ¿cuál es el número  $\psi(d)$  de elementos de  $U(p)$  de orden  $d$ ?
53. La prueba de que  $\psi(d) = \varphi(d)$  o  $\psi(d) = 0$ .
54. En efecto  $\psi(d) = \varphi(d)$ .
55. Existencia de raíces primitivas módulo  $p$ ; una segunda prueba de esto.
56. Historia de pruebas anteriores de la existencia de raíces primitivas.
57. El *índice* de un elemento  $b$  respecto a una raíz primitiva  $a$  módulo  $p$ .
58. Índice de un producto y de una potencia.
59. Índice de un cociente.
60. Cálculo de raíces módulo  $p$ .
61. Cálculo directo de raíces de la unidad módulo  $p$ : primera reducción.
62. Raíces cuadradas de la unidad.
63. Cálculo directo de raíces de la unidad: segunda reducción.
64. ¿Cuándo es  $-1$  un residuo cuadrático?
65. Cálculo de  $n$ -ésimas raíces cuando  $n|p-1$ .
66. ¿Cuándo existen  $n$ -ésimas raíces de  $A$  módulo  $p$ ?
67. Cálculo del orden  $t$  de  $A$  módulo  $p$ .
68. Cálculo de las demás raíces a partir de una.
69. Cambio de raíz primitiva como base.
70. Invariancia del m. c. d. del índice y  $p-1$ .
71. Elección de la base para que un entero tenga un índice determinado.
72. Escogencia conveniente de la raíz primitiva como base.
73. Algoritmo para encontrar raíces primitivas.
74. Ejemplo de encontrar una raíz primitiva módulo 73.
75. Producto de los elementos de un subgrupo cíclico de  $U(p)$ .
76. El Teorema de Wilson:  $(p-1)! \equiv -1 \pmod{p}$ .
77. Segunda prueba del Teorema de Wilson.
78. Generalización del Teorema de Wilson a bases compuestas.

- 79. Suma de los elementos de un subgrupo cíclico de  $U(p)$ .
- 80. Producto de todas las raíces primitivas.
- 81. Suma de todas las raíces primitivas.
- 82. Caso de módulos compuestos.
- 83. Orden de  $a \in U(m)$  divide a  $\varphi(M)$ .
- 84. No hay más que  $t$  raíces  $t$ -ésimas de 1 módulo  $p^n$ .
- 85. Número exacto de raíces  $t$ -ésimas de 1 módulo  $p^n$ .
- 86. Prueba de §85: primera parte.
- 87. Prueba de §85: segunda parte.
- 88. Prueba de §85: tercera parte.
- 89. Cálculos con raíces primitivas módulo  $p^n$ .
- 90. Máximo orden en  $U(2^n)$ .
- 91. Cálculos con índices módulo  $2^n$ .
- 92. Cálculos módulo un entero compuesto.
- 93. Trabajos de Euler sobre estos temas.

#### SECCION CUARTA. SOBRE LAS CONGRUENCIAS DE SEGUNDO GRADO.

- 94. Número máximo posible de residuos cuadráticos módulo  $m$ .
- 95. Definición de *residuo* y *no residuo*.
- 96. Número de residuos cuadráticos módulo  $p$  primo.
- 97. Segunda prueba de §96; ejemplos con  $p \leq 17$ .
- 98.  $AB$  es un residuo sii  $A$  y  $B$  son ambos residuos o ambos no residuos.
- 99. ¿Cuando un producto de varios factores es un residuo?; uso de tablas.
- 100. Número de residuos cuadráticos módulo  $p^n$ .
- 101. Si  $a$  no es divisible por  $p$ , es un residuo de  $p$  sii es un residuo de  $p^n$ .
- 102. ¿Cuando un entero divisible por  $p$  es un residuo módulo  $p^n$ ?
- 103. Residuos cuadráticos módulo  $2^n$ .
- 104. Número de raíces  $\sqrt{A}$  si  $A$  es un residuo módulo  $p^n$ .
- 105. Número de raíces  $\sqrt{A}$  si  $A$  es un residuo módulo  $m$  cualquiera.
- 106. Criterio de Euler para residuos cuadráticos.
- 107. Problema fundamental: dado  $a$ , encontrar todo  $p$  del cual  $a$  es un residuo.
- 108.  $-1$  es un residuo de  $p$  primo sii  $p = 4n + 1$ .
- 109. Otra prueba de §108.
- 110. Referencia al trabajo de Euler; relación al Teorema de Wilson.
- 111. Caracterización de los enteros para los cuales  $-1$  es un residuo.

112. Estudio de §107 cuando  $a = \pm 2$  y  $p \equiv 3$  o  $5 \pmod{8}$ .
113. Estudio de §107 cuando  $a = \pm 2$  y  $p \equiv 7 \pmod{8}$ .
114. Estudio de §107 cuando  $a = \pm 2$  y  $p \equiv 1 \pmod{8}$ .
115. Otra prueba de §114.
116. Caracterización de los enteros para los cuales  $\pm 2$  es un residuo; historia.
117. Estudio de §107 cuando  $a = \pm 3$  y  $p \equiv 5$  u  $11 \pmod{12}$ .
118. Estudio de §107 cuando  $a = \pm 3$  y  $p \equiv 7 \pmod{12}$ .
119. Estudio de §107 cuando  $a = \pm 3$  y  $p \equiv 1 \pmod{12}$ .
120. Caracterización de los enteros para los cuales  $\pm 3$  es un residuo; historia.
121. Estudio de §107 cuando  $a = \pm 5$  y  $p \equiv 2$  o  $3 \pmod{5}$ .
122. Estudio de §107 cuando  $a = \pm 5$  y  $p \not\equiv 1$  ni  $9 \pmod{20}$ .
123. Ley de Reciprocidad Cuadrática para  $a = \pm 5$ .
124. Discusión de §107 cuando  $a = \pm 7$ .
125. Todo  $p \equiv 1 \pmod{4}$  es un no residuo de algún primo  $q < p$ ; prueba si  $p \equiv 5 \pmod{8}$ .
126. Primer lema para probar el caso  $p \equiv 1 \pmod{8}$  de §125.
127. Segundo lema para probar el caso  $p \equiv 1 \pmod{8}$  de §125.
128. Tercer lema para probar el caso  $p \equiv 1 \pmod{8}$  de §125.
129. Prueba de §125.
130. Evidencia numérica para la Ley de Reciprocidad Cuadrática.
131. Enunciado de la Ley de Reciprocidad Cuadrática; notación.
132. Consecuencias de §131 con números compuestos.
133. Reciprocidad cuadrática generalizada a enteros compuestos.
134. Prueba de §133, suponiendo §131.
135. Ley de Reciprocidad Cuadrática (L. R. C.): hipótesis inductiva.
136. Prueba de L. R. C.: comienzo de la inducción; división en casos.
137. Prueba de L. R. C.: caso 1,  $a \equiv p \equiv 1 \pmod{4}$ ,  $\pm pRa$ .
138. Prueba de L. R. C.: caso 2,  $a \equiv 1$ ,  $p \equiv 3$ ,  $\pm pRa$ .
139. Prueba de L. R. C.: caso 3,  $a \equiv p \equiv 1$ ,  $\pm pNa$ .
140. Prueba de L. R. C.: caso 4,  $a \equiv 1$ ,  $p \equiv 3$ ,  $\pm pNa$ .
141. Prueba de L. R. C.: caso 5,  $a \equiv p \equiv 3$ ,  $pRb$ .
142. Prueba de L. R. C.: caso 6,  $a \equiv 3$ ,  $p \equiv 1$ ,  $pRb$ .
143. Prueba de L. R. C.: caso 7,  $a \equiv p \equiv 3$ ,  $pNb$ .
144. Prueba de L. R. C.: caso 8,  $a \equiv 3$ ,  $p \equiv 1$ ,  $pNb$ .
145. Otra prueba de §114.
146. Resumen del método para determinar si  $Q$  es un residuo de  $P$ ; ejemplo.

- 147. Formas de los divisores de  $x^2 - A$ : enunciado.
- 148. Prueba de §147 cuando  $A \equiv 1 \pmod{4}$ .
- 149. Prueba de §147 cuando  $A \equiv 2$  o  $3 \pmod{4}$ .
- 150. Corolario de §147 con  $B$  compuesto.
- 151. Historia de la Ley de Reciprocidad Cuadrática.
- 152. Resolución de congruencias  $ax^2 + bx + c \equiv 0$ .

## SECCION QUINTA. SOBRE LAS FORMAS Y LAS ECUACIONES INDETERMINADAS DE SEGUNDO GRADO.

- 153. Definición de *formas cuadráticas*; notación.
- 154. Representación de un número  $M$ ; el determinante.
- 155. La raíz cuadrada  $\sqrt{D}$  del determinante es una clase módulo  $M$ .
- 156. Representaciones que corresponden a valores iguales u opuestos de  $\sqrt{D}$ .
- 157. Transformaciones lineales de formas; formas equivalentes; transformaciones propias e impropias.
- 158. Equivalencia propia e impropia; ejemplo; problemas a ver.
- 159. Transitividad de implicación de formas; formas opuestas.
- 160. Formas contiguas.
- 161. Divisores comunes de los coeficientes de formas.
- 162. Encontrar todas las transformaciones de una forma a otra que la contiene.
- 163. Formas ambiguas.
- 164. Condición necesaria y suficiente para que una forma implique a otra propia e impropriamente.
- 165. Ejemplo de §164; existencia de una forma ambigua en una clase.
- 166. Representación de números por formas transformadas.
- 167. Determinantes de formas equivalentes.
- 168. Toda representación de un entero  $M$  conduce a una forma propiamente equivalente con primer coeficiente  $M$ .
- 169. Aplicación de la teoría de transformaciones a la de representaciones.
- 170. Caso de §168 con una forma ambigua.
- 171. Formas con determinante negativo: reducción a forma reducida.
- 172. Condiciones para que dos formas reducidas de determinante  $-D$  sean propiamente equivalentes.
- 173. Condiciones para que dos formas reducidas de determinante  $-D$  sean equivalentes.
- 174. El número de formas reducidas de determinante  $-D$ .
- 175. Clases de formas de determinante  $-D$ .

- 176. Tabla de clases de formas de determinante  $-D$ ,  $D \leq 12$ .
- 177. Transformaciones propias entre formas contiguas.
- 178. Cálculo de una transformación propia entre formas propiamente equivalentes.
- 179. Cálculo de todas las transformaciones entre formas equivalentes.
- 180. Algoritmo para encontrar todas las representaciones de  $M$  por una forma de determinante  $-D$ .
- 181. Caso de §180 con coeficientes no relativamente primos.
- 182. Aplicación a la representación de  $M$  como  $x^2 + ny^2$ ,  $n = 1, 2, 3$ .
- 183. Formas con determinante positivo no cuadrado: reducción a forma reducida.
- 184. Propiedades de formas reducidas con determinante positivo no cuadrado.
- 185. Algoritmos para encontrar todas las formas reducidas de determinante  $D$ .
- 186. Período de una forma  $F$ .
- 187. Propiedades de períodos; formas asociadas.
- 188. Sustitución  $\alpha, \beta, \gamma, \delta$ ; ejemplo de período de una forma reducida.
- 189. Signos y otras propiedades de las formas en un período.
- 190. Lema para §191.
- 191. Aproximación racional a  $\sqrt{D}$ .
- 192. Convergentes de la fracción continuada de  $\sqrt{D}$ .
- 193. Formas reducidas propiamente equivalentes están en el mismo período.
- 194. Otra prueba del Teorema de §165.
- 195. Algoritmo que determina si formas del mismo determinante son equivalentes.
- 196. Algoritmo para encontrar una transformación propia entre formas propiamente equivalentes.
- 197. Relevancia de la ecuación de Pell al estudio de formas.
- 198. Solución fundamental de la ecuación de Pell.
- 199. Aplicación de fracciones continuadas a §198.
- 200. Solución general de la ecuación de Pell.
- 201. Comentarios sobre la solución de la ecuación de Pell.
- 202. Historia de la ecuación de Pell.
- 203. Algoritmo para encontrar todas las transformaciones entre formas equivalentes.
- 204. Observaciones sobre §203.
- 205. Algoritmo para encontrar todas las representaciones de un entero por una forma dada.
- 206. Formas reducidas con determinante  $h^2$ .
- 207. Toda clase contiene una sola forma reducida.
- 208. Encontrar una transformación entre formas equivalentes con determinante  $h^2$ .

- 209. Encontrar las demás transformaciones de §208.
- 210. Criterio para equivalencia impropia de formas reducidas  $(a, h, 0)$ .
- 211. Número de clases de formas de determinante  $h^2$ .
- 212. Algoritmo de §205 para el caso de formas de determinante  $h^2$ .
- 213. Criterio para que una forma de determinante  $D$  implique una de determinante  $De^2$ .
- 214. Encontrar todas las transformaciones correspondientes a §213.
- 215. Formas de determinante igual a cero.
- 216. Resolución de la ecuación cuadrática general de dos incógnitas.
- 217. Continuación de §216.
- 218. Caso de §216 con determinante cuadrado y  $M = 0$ .
- 219. Caso general de §216 con determinante cero.
- 220. Caso especial de §216 con determinante cero.
- 221. Ejemplo del método de §217.
- 222. Notas históricas acerca de formas cuadráticas.
- 223. División de las formas de determinante  $D$  en clases.
- 224. Usos de las clases; clases opuestas; clases ambiguas.
- 225. Clases positivas y negativas.
- 226. Formas primitivas; división de clases en órdenes; ejemplos.
- 227. Uso de clases propiamente primitivas.
- 228. Una forma primitiva representa un número infinito de enteros no divisibles por  $p$ .
- 229. Una forma primitiva representa sólo residuos o sólo no residuos módulo  $p$ .
- 230. Caracteres de una forma primitiva.
- 231. División de órdenes en géneros; forma principal.
- 232. Ejemplos con clases positivas y negativas.
- 233. Raíz cuadrada de una forma; números característicos de una forma.
- 234. Lema para §239 y §240.
- 235. Forma compuesta; seis propiedades.
- 236. Construcción de una forma compuesta.
- 237. Forma compuesta de formas transformadas.
- 238. Forma compuesta de formas equivalentes.
- 239. Equivalencia de las compuestas de formas equivalentes.
- 240. Asociatividad de composición.
- 241. Asociatividad generalizada de composición.
- 242. Propiedades de la composición de formas.



- 243. Clases de formas tienen la estructura de un grupo.
- 244. Representación de un producto por una forma compuesta.
- 245. Composición de órdenes.
- 246. Composición de géneros.
- 247. Producto de géneros está bien definido para formas primitivas.
- 248. Producto de géneros está bien definido en general.
- 249. Composición de clases.
- 250. Forma más simple de un orden.
- 251. Una forma primitiva que transforma formas del mismo orden.
- 252. Existe el mismo número de clases en cada género del mismo orden.
- 253. Discusión del número de clases en órdenes distintos.
- 254. Composición de la forma más simple de un orden con una primitiva.
- 255. Clases propiamente primitivas que representan un entero cuadrado.
- 256. Comparación del número de clases primitivas de órdenes distintos.
- 257. Número de formas ambiguas primitivas  $(A, 0, C)$  y  $(A, A/2, C)$ .
- 258. Conteo del número de clases ambiguas propiamente primitivas.
- 259. Conteo del número de clases ambiguas impropiedades primitivas.
- 260. Número de clases propiamente primitivas  $k$  con  $k^2 = K$ .
- 261. La mitad de los caracteres no pertenece a un género propiamente primitivo.
- 262. Otra prueba de la L. R. C. para ciertos residuos.
- 263. Los caracteres que corresponden a géneros.
- 264. Caracteres para géneros negativos y géneros impropiedades primitivos.
- 265. Método para descomponer un primo como suma de dos cuadrados.  
*Una digresión conteniendo un estudio de formas ternarias.*
- 266. Introducción al estudio de formas ternarias.
- 267. Formas ternarias: notación, adjunta y determinante.
- 268. Transformación de formas ternarias.
- 269. Formas ternarias equivalentes.
- 270. Transitividad de equivalencia.
- 271. Clases de formas ternarias; formas positivas, negativas e indefinidas.
- 272. Reducción de formas ternarias.
- 273. Ejemplos numéricos de la reducción de formas ternarias.
- 274. Segunda reducción de formas ternarias.
- 275. Ejemplos de la composición de transformaciones de formas ternarias.
- 276. El número de clases de formas ternarias de determinante  $D$  es finito.
- 277. Ejemplos de formas ternarias reducidas de determinante pequeño.

- 278. Problemas para considerarse acerca de formas ternarias.
- 279. Lema para §280.
- 280. Algoritmo para encontrar las representaciones propias de un entero por una forma ternaria.
- 281. Representaciones impropias por una forma ternaria.
- 282. Observaciones acerca de la representación de una forma binaria por una forma ternaria.
- 283. Algoritmo para encontrar todas las representaciones de una forma binaria por una forma ternaria.
- 284. Representaciones impropias de una forma binaria por una forma ternaria.
- 285. Equivalencia de formas ternarias.

*Algunas aplicaciones a la teoría de las formas binarias.*

- 286. Toda forma del género principal es el cuadrado de alguna forma.
- 287. Exactamente la mitad de los caracteres corresponden a géneros propiamente primitivos.
- 288. Existencia de formas primitivas negativas de determinante  $-M$  y número característico  $-1$ .
- 289. Representaciones de formas binarias por  $x^2 + y^2 + z^2$ .
- 290. Estudio de §289 para formas binarias de determinante  $-1$  o  $-2$ .
- 291. Las representaciones de un entero positivo por  $x^2 + y^2 + z^2$ .
- 292. Número de representaciones por  $x^2 + y^2 + z^2$ .
- 293. Todo entero positivo es la suma de tres números triangulares.
- 294. Condición necesaria y suficiente para resolver  $ax^2 + by^2 + cz^2 = 0$ .
- 295. Método alternativo para §294.
- 296. Trabajo de Legendre acerca de §294.
- 297. Incompletitud del argumento de Legendre en §296.
- 298. Caso general de §294.
- 299. Representación de cero por formas ternarias.
- 300. Solución racional de una ecuación cuadrática con dos incógnitas.
- 301. Comportamiento asintótico del número de géneros.
- 302. Comportamiento asintótico del número de clases: determinante negativo.
- 303. Tablas acerca de §302; conjetura sobre el número de clase.
- 304. Número de clases: determinante negativo.
- 305. Toda clase es de orden que divide al número de clases.
- 306. Las clases forman un grupo.
- 307. Algoritmo para calcular géneros y clases; ejemplos.

## SECCION SEXTA. APLICACIONES VARIAS DE LAS INVESTIGACIONES PRECEDENTES.

- 308. Introducción y resumen de la sección.
- 309. Descomposición de una fracción con denominador  $ab$ .
- 310. Descomposición de una fracción con denominador  $abc \dots$ .
- 311. Unicidad de la descomposición de §310.
- 312. Mantisa decimal de una fracción.
- 313. Cálculo del numerador a partir de la mantisa y del denominador.
- 314. Período de una fracción  $a/p^\mu$ .
- 315. Cálculo del período de  $b/p^\mu$  a partir del período de  $a/p^\mu$ .
- 316. Comentarios sobre las tablas de los períodos de fracciones.
- 317. Método de cálculo de expansiones decimales en general.
- 318. Mantisa de una fracción en el caso general.
- 319. Métodos para resolver una congruencia  $x^2 \equiv A \pmod{m}$ .
- 320. Método de exclusión para la congruencia  $x^2 \equiv A \pmod{m}$ .
- 321. Números excluyentes que conviene escoger en el método de exclusión.
- 322. Atajos que se pueden usar en el método de exclusión.
- 323. Otro método para resolver  $mx^2 + ny^2 = A$ .
- 324. Uso de números excluyentes en §323.
- 325. Un ejemplo del método de §323 y §324.
- 326. Observaciones para acortar el cálculo en §323.
- 327. Otro método para resolver  $x^2 \equiv A \pmod{M}$  cuando  $A < 0$ .
- 328. Ejemplos numéricos del método de §327.
- 329. Métodos de factorización de enteros: observaciones elementales.
- 330. Primer método de factorización: residuos cuadráticos de  $M$ .
- 331. Técnicas para la aplicación de §330.
- 332. Tres métodos para encontrar los residuos cuadráticos de  $M$ .
- 333. Segundo método de factorización: valor de  $\sqrt{-D} \pmod{M}$ .
- 334. Aplicaciones de §333.

## SECCION SETIMA. ECUACIONES QUE DEFINEN SECCIONES DE UN CIRCULO.

- 335. Introducción a la ciclotomía; generalizaciones futuras posibles.
- 336. Reducción al caso de la división del círculo en  $p$  (primo) partes.
- 337. Las raíces de  $x^n - 1$  son  $\exp(2\pi k/n) = \cos(2\pi k/n) + i \sin(2\pi k/n)$ .
- 338. La fórmula de Newton para la suma de las  $\lambda$ -ésimas potencias de las raíces.

- 339. La estructura cíclica de las raíces  $\Omega$  de un polinomio ciclotómico  $X$ .
  - 340. Sustitución de raíces de un polinomio ciclotómico en un polinomio.
  - 341. Irreducibilidad de polinomios ciclotómicos sobre los racionales.
  - 342. Factorización del polinomio ciclotómico depende de  $p - 1$ .
  - 343. Subgrupos y clases laterales de las raíces de un polinomio ciclotómico.
  - 344. Clases laterales de  $\Omega$  forman una partición.
  - 345. Productos de períodos en  $\Omega$ .
  - 346. Grado de subextensiones del campo ciclotómico.
  - 347. Sustitución de un período en un polinomio simétrico.
  - 348. Coeficientes de un polinomio son funciones simétricas de las raíces.
  - 349. Aplicación del Teorema de Newton al cálculo de los coeficientes.
  - 350. Generalización de §347 con subperíodos.
  - 351. Cálculo de polinomio mínimo de un período; ejemplo  $n = 19$ .
  - 352. Algoritmo para encontrar las raíces de un polinomio ciclotómico.
  - 353. Cálculo completo de §352 cuando  $n = 19$ .
  - 354. Cálculo completo de §352 cuando  $n = 17$ .
  - 355. Uso de números complejos en §352.
  - 356. Cálculo de sumas gaussianas.
  - 357. El polinomio ciclotómico se descompone como  $\frac{1}{4}(y^2 \mp pz^2)$ .
  - 358. Distribución de las raíces  $\Omega$  en tres períodos.
  - 359. Conjetura de la imposibilidad de resolver polinomios de grado  $\geq 5$  por radicales.
  - 360. Uso de resolventes de Lagrange para resolver el polinomio ciclotómico.
  - 361. Cálculo de  $\sin \omega$  y  $\cos \omega$  donde  $\omega = 2\pi k/n$ .
  - 362. Cálculo de las otras funciones trigonométricas de  $\omega$ .
  - 363. Factorización del polinomio con raíces  $\sin k\omega$ , etc.
  - 364. Observaciones sobre §363; automorfismos de una extensión; ejemplos.
  - 365. Se construye un  $p$ -gono sii  $p$  es un primo de Fermat.
  - 366. Caracterización de los  $n$  para los cuales el  $n$ -gono es construible.
-