En esta hoja tratamos los artículos 359–366 con los que acaba [Gau86]. Los dos primeros, están relacionados con la resolubilidad por radicales y los dos últimos son conclusiones de todo el trabajo. Los cuatro restantes, 361–364, hablan esencialmente de considerar en vez $e^{2\pi i/n}$, algunas funciones trigonométricas del ángulo $2\pi/n$. Eso no tiene la mayor importancia y no entiendo por qué Gauss se detiene en ello. Nosotros nos los saltaremos. Tu tarea es leer el resto, esta vez no habrá problemas como los de otras veces por el carácter especial de los artículos, los primeros muy teóricos y los últimos un compendio de lo hecho.

Recordemos primero lo último que habíamos visto en la hoja anterior: Si $n-1=ef$ y $f=e'f'$, entonces

$$(f,\lambda)=\sum_{l=0}^{e'-1}(f',\lambda g^{el}) \tag{1}$$

y el resultado fundamental es que los $(f',\lambda g^{el})$ son soluciones de una ecuación de grado e' con coeficientes que dependen de los periodos (f,μ).

El artículo 359 comienza diciendo algo genérico que sugiere que era opinión común en 1801 que las ecuaciones generales de grado mayor que cuatro no son resolubles por radicales (aunque Abel todavía no había nacido) y anuncia que estas ecuaciones para los periodos sí lo son. Así dicho sin especificar más y siendo muy puntilloso, esto es trivial porque todos los elementos de $\mathbb{Q}(\zeta)$, $\zeta=e^{2\pi i/n}$ son expresables con radicales ya que $\zeta=\sqrt[n]{1}$. Lo que en realidad va a probar Gauss es algo mucho más profundo: que la ecuación mencionada en el párrafo anterior se puede resolver usando sólo $\sqrt[e']{1}$ y con otras raíces e'-ésimas que dependen de los coeficientes. Esto está en el artículo 360. He de confesar que este artículo me cuesta y no sé si lo estoy entendiendo del todo. Te cuento mi versión, que trata de reflejar el argumento que aparece allí. Como en la hoja anterior, la notación de Gauss es $e=\alpha$, $e'=\beta$, $f'=\gamma$. La situación es que suponemos los (f,λ) conocidos y queremos resolver la ecuación para los (f',ν) que están contenidos en ellos según (1). Consideremos los polinomios (relacionados con lo que hoy llamamos las *resolventes de Lagrange*)

$$L_j(x)=\sum_{l=0}^{e'-1}(f',\lambda g^{e(l+j)})x^l \quad j=0,1,2,\dots e'-1 \qquad \text{y} \qquad P(x)=\frac{1}{e'}\sum_{j=0}^{e'-1}\big(L_j(x)\big)^{e'}.$$

Los L_j, que Gauss considera ya evaluados en $\sqrt[e']{1}$, son el mismo polinomio de grado $e'-1$ permutando cíclicamente los coeficientes, lo que corresponde a cambiar $(f',\lambda g^{el})$ por $(f',\lambda g^{e(l+j)})$. Eso significa que al expandir las potencias en P y escribir los coeficientes en términos de los (f',ν), todos los $(f',\lambda g^{e(l+j)})$ aparecerán multiplicados por lo mismo. En virtud de (1), se tiene que $P(x)=\sum_{k=0}^{e-1}(f,g^k)p_k(x)$, para ciertos polinomios $p_k\in\mathbb{Q}[x]$. Nota que (f,g^k) recorre todos los periodos.

Si ξ es una raíz e'-ésima de la unidad, digamos $\xi = e^{2\pi i/e'}$, entonces $L_0(\xi) = \xi^j L_j(\xi)$. Esto no tiene nada que ver con periodos, es más fácil, se debe a que los coeficientes vienen de permutaciones circulares de orden e'. Introduciendo esto en la definición de P,

$$(L_0(\xi))^{e'} = P(\xi) = \sum_{k=0}^{e-1} (f, g^k) p_k(\xi)$$

que es una cantidad conocida si lo son los (f, λ) y ξ, porque los p_k son polinomios con coeficientes racionales. Si la llamamos T_1 (Gauss escribe T, T', T'' para mis T_j) lo que se tiene es

$$\sqrt[e']{T_1} = \sum_{l=0}^{e'-1} (f', \lambda g^{el}) \xi^l$$

para alguna elección del argumento, y si en vez de tomar ξ hubiera tomado otra raíz e'-ésima ξ^j se tendría en general

$$\sqrt[e']{T_j} = \sum_{l=0}^{e'-1} (f', \lambda g^{el}) \xi^{jl} \qquad \text{para} \quad j = 1, 2, \dots, e' \qquad \text{y} \qquad T_j = (L_0(\xi^j))^{e'}.$$

Escribiendo $x_l = (f', \lambda g^{el})$ esto es una sistema lineal de e' ecuaciones con e' incógnitas con determinante de Vandermonde y, por tanto no singular. Incluso (como hace Gauss) es posible escribir su solución explícita. Para nuestros propósitos basta decir que cada periodo x_l que aparece en (1) se expresa en términos de las raíces e'-ésimas $\sqrt[e']{T_j}$ y ξ. En definitiva, las ecuaciones que dan los (f', ν) en términos de los (f, λ) se resuelven utilizando solo radicales de índice e'.

1) Dado que a mí me cuesta seguir el artículo 360, solo te pido que le des un vistazo después de haber leído mi versión. Lo mismo me estoy obcecando y a ti te resulta más claro.

Los artículos finales 365 y 366 son un especie de resumen y conclusión que además contienen dos observaciones sobre dos cosas que no se han tratado. La primera es que en principio las ecuaciones de grado mayor que dos que aparecen en el algoritmo cuando $n - 1 \neq 2^r$, podrían ser todas reducibles y sus soluciones expresables con raíces cuadradas. Eso suena muy raro, sobre todo después de que ha demostrado que un factor e' de $n - 1$ da lugar a una raíz e'-ésima. Gauss afirma que tiene prueba "con todo rigor" de ello pero que no la incluye. Hoy sería tan fácil como decir que al añadir raíces cuadradas siempre el grado de una extensión es una potencia de dos. La segunda cosa, es que al pasar de primos a compuestos, el caso de potencias de primos es problemático. Aquí lo que deja caer indirectamente es que el grado del polinomio mínimo de $e^{2\pi i/p^\alpha}$ es $(p-1)p^{\alpha-1}$ para p primo pero no da indicios de cómo lo sabe,

¿quizá con una variante del artículo 341? Nosotros ya vimos en la hoja 2 que bastaba estudiar el caso $\alpha = 2$ que sale del criterio de Eisenstein.

2) Lee con cuidado los artículos 365 y 366.

Esta vez en lo que me tienes que entregar tienes bastante libertad.

3) Escribe lo que quieras de los artículos 359 y 360. Puede ser tan breve como prefieras porque la resolubilidad por radicales no es tan importante en la construcción de polígonos regulares. Lo que te pido que hagas, sin poner límites de espacio, es que tomando como base los artículos 365 y 366 y conectándolo con las hojas anteriores, escribas por qué hemos probado que el polígono regular de n lados es construible cuando los factores primos de n son dos (quizá con multiplicidad) y primos de Fermat distintos.

Referencias

[Gau86] C. F. Gauss. *Disquisitiones arithmeticae.* Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.