Esta hoja continúa la anterior y contiene los argumentos más importantes en el razonamiento de Gauss [Gau86]. En pocas palabras, lo que se prueba es que cada periodo compuesto por f raíces de la unidad es raíz de un polinomio de grado d cuyos coeficientes son periodos compuestos por df raíces. Para que lo conectes con lo primero que vimos, si piensas en el caso $n = 17$, hay 16 raíces de la unidad distinta de la trivial. Cada una de ellas forma un periodo $(1, \lambda)$, entonces son soluciones de ecuaciones cuadráticas con coeficientes que se escriben en términos de $(2, \lambda)$ y así sucesivamente, hasta llegar a $(16, \lambda)$ que es la suma de todas las raíces no triviales que sabemos que es -1. Esto permite escribir $\zeta = e^{2\pi i/17}$ como una iteración de raíces cuadradas y así probar que el polinomio de 17 lados es contruible con regla y compás.

Recuerda para lo que sigue la definición de periodo:

$$(f, \lambda) = \sum_{k=0}^{f-1} \zeta^{\lambda g^{ek}} \qquad \text{con } f \mid n-1,\ e = (n-1)/f,\ \zeta = e^{2\pi i/n} \text{ y } g \text{ un generador de } \mathcal{U}(\mathbb{Z}_p).$$

Comencemos con el artículo 347. Lo que dice el teorema que se enuncia allí, con notación modernizada, es que si $F \in \mathbb{Q}[x_1, \ldots, x_f]$ es un polinomio simétrico entonces

$$F\big(\zeta^{\lambda}, \zeta^{\lambda g^e}, \zeta^{\lambda g^{2e}}, \ldots, \zeta^{\lambda g^{e(f-1)}}\big) = A + \sum_{j=0}^{e-1} a_j (f, g^j) \qquad \text{con } A, a_j \in \mathbb{Q}.$$

1) Lee con cuidado el enunciado del teorema del artículo 347 hasta entender que corresponde con lo que acabo de mencionar.

La demostración, esencialmente es que al cambiar λ por λg^{me}, los argumentos de F se reordenan y como F es simétrico el resultado final no cambia. Entonces si al operar y simplificar sale en algún sitio un $a\zeta^{\lambda b}$, también sale un $a\zeta^{\lambda b g^{me}}$ y así se obtienen todos los del periodo $(f, \lambda b)$.

2) Lee la demostración que da Gauss del teorema del artículo 347.

3) Para ver si lo has entendido, considera $n = 7$, $e = 2$, $f = 3$ (recuerda, $n - 1 = ef$) y $F = x(y + 2) + z(x + 2) + y(z + 2)$. Escribe $F(\zeta, \zeta^2, \zeta^4)$ en términos de los periodos (f, λ).

Al operar $P = (x - x_1)(x - x_2) \cdots (x - x_f)$, los coeficientes de P son funciones simétricas en $x_1, x_2, \ldots, x_f$. Por ejemplo, el coeficiente de x^{f-1} es $-(x_1 + x_2 + \cdots + x_n)$ y el término independiente es $(-1)^f x_1 x_2 \cdots x_f$. Entonces tomando como x_i las raíces de la unidad que aparecen en (f, λ) se tiene a partir del teorema que los coeficientes se pueden escribir en términos de los (f, μ). éste es el contenido del artículo 348 donde también se muestra un ejemplo, mientras que en el 349 Gauss explica como abreviar los cálculos si f es grande usando las identidades de Newton.

4) Da un vistazo por encima al primer artículo y te puedes saltar el segundo porque hoy en día no tiene mucho interés hacer cálculos a mano con f grande.

5) En el caso $n = 7$, se tiene $(3, 1) = \zeta + \zeta^2 + \zeta^4$. Calcula los coeficientes de $P = (x - \zeta)(x - \zeta^2)(x - \zeta^4)$ en términos de los periodos.

El teorema del artículo 350 es una extensión del teorema del artículo 347. En lugar de sustituir raíces separadas, se sustituyen periodos. Digamos que $n-1 = ef$ y $f = e'f'$, entonces cada periodo (f, λ) está compuesto por periodos (f', μ). Concretamente

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

6) Demuestra esta igualdad.

Lo que dice el artículo 350 es que para cualquier polinomio simétrico F, siempre se tiene

$$F\big((f', \lambda), (f', \lambda g^e), (f', \lambda g^{2e}), \ldots, (f', \lambda g^{e(e'-1)})\big) = A + \sum_{j=0}^{e-1} a_j (f, g^j).$$

La notación de Gauss es $e = \alpha$, $e' = \beta$, $f' = \gamma$ y los argumentos de F en principio no están ordenados así (da igual por la simetría). Nota que $f' \mid f$.

7) Lee el artículo 350 completo.

Ahora se puede proceder como antes considerando un polinomio $P = (x-x_1)(x-x_2)\cdots(x-x_{e'})$ y deducir que tomando como x_j los periodos $(f', \lambda g^{(j-1)e})$, los coeficientes de P se escriben en términos de los periodos (f, μ) para cualquier f divisor de $n-1$ y múltiplo de f'. Los artículos 351–354 son explicaciones de esta idea junto con ejemplos, especialmente para $n = 17$ y $n = 19$.

8) Lee el artículo 352, donde está explicado con más letra el modo en el que se va a proceder en la demostración del resultado final.

La idea que tienes que haber sacado, y que ya mencionamos al principio, es que si $n - 1$ factoriza como $p_1 p_2 \cdot p_k$ entonces ζ se puede expresar como la solución una cadena de ecuaciones de grados $p_1, \ldots, p_k$. El orden de los factores da en general diferentes ecuaciones. Más adelante (art. 355) Gauss dice que él pondrá el factor dos (siempre aparece porque n es primo impar) al final para que los cálculos intermedios den lugar a números reales. Nosotros no nos vamos a preocupar de ello.

A la hora de hacer los cálculos, una cosa que quizá te ha pasado inadvertida es algo sencillo que menciona en el caso $n = 19$ en el artículo 353: Si escribimos (por ese orden) los residuos

de módulo n de $g^0, g^1, \ldots, g^{n-2}$, entonces los periodos (f, λ) se están formados por raíces de la unidad cuyos exponentes corresponden a dar saltos de $e = (n-1)/f$ en e en esta lista, es decir, considerar los residuos de g^m, g^{m+e}, g^{m+2e}, etc. pensando que la lista es cíclica.

9) Explica por qué esto funciona (es muy fácil).

Nosotros vamos a analizar con detalles el caso $n = 13$ que es más corto que los que estudia Gauss, seleccionando la factorización $12 = 2 \cdot 2 \cdot 3$. De esta forma, los f correspondientes son $12 = 12/1$, $6 = 12/2$, $3 = 12/(2 \cdot 2)$ y $1 = 12/(2 \cdot 2 \cdot 3)$. El árbol que indica la relación entre estos periodos (los que forman parte de otros), es del tipo:

$$-1 = \zeta + \zeta^2 + \zeta^3 + \ldots \zeta^{12} = (12,1) = \left\{ \begin{array}{l} (6,1) \left\{ \begin{array}{l} (3,1) \left\{ \begin{array}{l} (1,1) = \zeta \\ (1,3) = \zeta^3 \\ (1,9) = \zeta^9 \end{array} \right. \\ ????? \left\{ \begin{array}{l} ???? = ?? \\ ???? = ?? \\ ???? = ?? \end{array} \right. \end{array} \right. \\ (6,2) \left\{ \begin{array}{l} (3,2) \left\{ \begin{array}{l} (1,2) = \zeta^2 \\ (1,5) = \zeta^5 \\ (1,6) = \zeta^6 \end{array} \right. \\ ????? \left\{ \begin{array}{l} ???? = ?? \\ ???? = ?? \\ ???? = ?? \end{array} \right. \end{array} \right. \end{array} \right.$$

10) Halla todo lo que está indicado con interrogaciones.

11) Al operar $\big(x - (6,1)\big)\big(x - (6,2)\big)$ se obtiene $x^2 - (12,1)x + 3(12,1) = x^2 + x - 3$ (no hace falta que lo compruebes). De ahí, $(6,1)$ y $(6,2)$ son $(-1 \pm \sqrt{13})/2$. Para saber cuál es cuál, se usa una calculadora comprobando cuál es positivo y se obtiene $(6,1) = (-1 + \sqrt{13})/2$, $(6,2) = (-1 - \sqrt{13})/2$. Halla una ecuación cuadrática con coeficientes en $\mathbb{Q}(\sqrt{13})$ que tenga a $(3,1)$ como solución y úsala para encontrar una expresión para $(3,1)$ que sólo involucre raíces cuadradas. Indicación: Tiene la pinta $(\sqrt{13} - 1 - i????)/4$.

12) Según la teoría, ζ es raíz del polinomio $P = (x - \zeta)(x - \zeta^3)(x - \zeta^9)$ cuyos coeficientes se expresan en términos de periodos $(3, \lambda)$. Está claro que $P = x^3 + Ax^2 + Bx - 1$. Halla A y B en términos de dichos periodos.

Si has conseguido hacer estos tres ejercicios es que has entendido todo lo necesario con respecto a los periodos. Después de los resultados que hemos estudiado en estas dos hojas,

Gauss todavía dedica unos artículos finales 355–358. El primero, ya lo he mencionado y se refiere al interés de poner un dos al final en la factorización para tener cantidades reales. Eso da igual en el caso de los polígonos contruibles porque todos los factores son doses. Los otros artículos tratan temas más profundos (sobre todo el último), que tienen relación con teoría de números pero no especial importancia para el problema de la construcción de polígonos regulares. No hace falta que los mires.

Te cuento lo que tienes que entregarme. De nuevo, te puedes saltar alguna de las directrices si me convences de alguna alternativa que se te ocurra.

13) El esquema que propongo es el siguiente:

1. Explica con notación moderna el enunciado del teorema del artículo 347 e indica el esquema de la prueba con un poco más de detalle que lo hago yo. Esto corresponde a los ejercicios 1) y 2). Después incluye el ejemplo del ejercicio 3). Explica también la aplicación para polinomios del artículo 348. Es suficiente con que expliques algo como lo que pongo y que después lo ilustres escribiendo el ejemplo del ejercicio 5). Todo esto debería caber a lo más en dos caras.

2. Enuncia el teorema del artículo 350 con notación moderna y menciona la aplicación a polinomios, como ya vimos antes. Éste es el resultado más importante acerca de los periodos. Da la prueba con todo el detalle que seas capaz siguiendo los pasos de Gauss. Esto se ajusta sobradamente a una cara.

3. Explica un poco lo del artículo 352 con tus propias palabras. Unas pocas líneas son suficientes.

4. Ahora es importante que des un ejemplo que ilustre lo que has explicado. Copia el árbol que incluyo con la división de periodos para $n = 13$ (si quieres cambiar el formato, por ejemplo poniéndolo en horizontal, hazlo) con las interrogaciones completadas. Escribe después las expresiones de los periodos intermedios $(6, \lambda)$ y $(3, \lambda)$ en términos de las raíces. Incluye la solución detallada de los ejercicios 10), 11) y 12). Todo ello precedido de una breve introducción indicando la factorización $13 - 1 = 2 \cdot 2 \cdot 3$ y la consecuente elección de las f, seguramente no te ocupe mucho más de dos páginas, pero tienes libertad si necesitas pasarte un poco.

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.