En la carpeta que te he dado está el plan sobre el trabajo. Por favor léetelo. También he incluido fotocopias de la sección VII de [Gau86]. Así no dependes de que haya ejemplares en la biblioteca. Está en inglés. Hay alguna edición en español pero no sé si está disponible en la UAM. Te adjunto el índice de contenidos para que te sea más fácil encontrar las cosas y un apéndice de notas de Gauss aunque creo que sólo hay dos que se apliquen a nuestra parte.

Como ya te he dicho, lo que te va a costar más es leer un texto de hace más de 200 años. Posiblemente te dé la sensación de que escribe demasiadas palabras y que la notación es rara y farragosa. Por eso, creo que es conveniente que tengas de antemano una idea somera de las líneas generales. En esta primera hoja, que es muy diferente al resto, voy a explicarte algunos aspectos básicos y tratarte de convencer de que es sencillo y muy bonito. Las pruebas y los enunciados más concretos los iremos viendo según vayamos leyendo a Gauss.

Considera la ecuación $x^p - 1$ con $p \neq 2$ primo, ya veremos que el caso general $x^n - 1 = 0$ de alguna forma se reduce a éste. Sus soluciones son claramente $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ con $\zeta = e^{2\pi i/p}$ (Gauss escribe a partir de cierto momento n en lugar de p y $[m]$ en lugar de ζ^m). Esencialmente lo que probó Gauss es que si la factorización en primos de $p-1$ es $p-1 = q_1 q_2 \cdots q_s$ con $q_1 \leq q_2 \leq \cdots \leq q_s$ entonces se puede expresar ζ como solución de una "cadena" de ecuaciones de grados $q_1, q_2, \ldots, q_s$. Aquí "cadena" significa que la primera ecuación tiene coeficientes racionales y en cada uno de los pasos siguientes uno puede tener coeficientes más complicados dados por combinaciones de raíces de las ecuaciones anteriores. Imagina que $p-1 = 2^n$, entonces según este resultado, $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ se puede obtener como una cadena de ecuaciones de segundo grado. ¿Por qué esto es interesante? Porque cuando usamos regla y compás hacemos intersecciones de rectas (regla) y circunferencias (compás) tomando longitudes ya construidas y entonces podemos construir longitudes que vengan de cadenas de ecuaciones cuadráticas (ya lo veremos con más cuidado si no lo has estudiado todavía). En particular, se pueden construir longitudes que midan $\cos\frac{2\pi}{p}$ y $\sin\frac{2\pi}{p}$ y así se dibuja el ángulo de $2\pi/p$ radianes y con ello un polígono regular de p lados. Gauss concluyó que hay una construcción con regla y compás del polígono de $17 = 2^4 + 1$ lados, lo cual desconocían los antiguos griegos.

1) Por ahora se conocen sólo 5 primos con $p - 1 = 2^n$, ¿sabes cuáles son? Si no, intenta hacer un sencillo programita en SAGE o lo que prefieras para hallarlos.

Lo bonito es que este resultado de Gauss que conecta temas en principio muy alejados de álgebra y geometría plana de los griegos está basado en ideas simples de simetría que son la base de la teoría de Galois.

Comencemos recordando un resultado básico de teoría de números que probablemente te han contado. Es más profundo de lo que parece. La prueba es breve pero no un ejercicio (si tienes curiosidad mira [Cla84] o [DH96]). Para cualquier primo p existe un $1 \leq g < p$ tal que $g^0, g^1, \ldots, g^{p-2}$ da el conjunto restos $1, 2, \ldots, p-1$ (quizá en otro orden) módulo p. Por

ejemplo, para $p = 5$ valen $g = 2$ y $g = 3$ porque

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3 \qquad \text{y} \qquad 3^0 \equiv 1,\ 3^1 \equiv 3,\ 3^2 \equiv 4,\ 3^3 \equiv 2.$$

Gauss incluso en una sección que no leeremos de [Gau86] halló una fórmula para saber cuántos g válidos hay para un p dado (de nuevo, si tienes curiosidad [HW08]).

2) Halla todos los g válidos para 7 y algún g válido para 11.

Vamos ahora con las simetrías. Fijemos p y g, diremos que una expresión $P(\zeta)$ con $P \in \mathbb{Q}[x]$ tiene la simetría S_d (notación que me acabo de inventar) con $d \mid p-1$ si $P(\zeta) = P\big(\zeta^{g^d}\big)$. Cosa que no habría que explicar: $\zeta^{g^d} = \zeta^{(g^d)} \neq \big(\zeta^g\big)^d$.

Pensemos en el caso $p = 5$ con $g = 3$ y vamos a ir reduciendo las simetrías de $P(\zeta) = \zeta + \zeta^2 + \zeta^3 + \zeta^4$. Para eso ordenamos los exponentes según aparecen en g^k, $k = 1, \ldots, 4$ módulo p y vamos tomando uno de cada dos elementos. De esta forma se consigue el árbol binario

$$\begin{array}{lcccc}
S_1: & & \zeta^1+\zeta^3+\zeta^4+\zeta^2 & & \\
& & \diagup \quad\quad \diagdown & & \\
S_2: & & \zeta+\zeta^4 & & \zeta^3+\zeta^2 \\
& & \diagup \quad \diagdown & & \diagup \quad \diagdown \\
S_4: & & \zeta \quad \zeta^4 & & \zeta^3 \quad \zeta^2
\end{array}$$

En realidad S_4 es no decir nada porque $g^4 \equiv 1 \pmod 5$. En general, siempre que $p - 1 = 2^n$, procediendo de esta forma se pasa de $\sum \zeta^k$ hasta las raíces sueltas en n pasos con simetrías S_{2^k}, $k = 1, \ldots, 2^n$.

En el caso $p = 17$ con $g = 3$ la primera descomposición sería

$$\begin{array}{lcc}
S_1: & \zeta^1+\zeta^3+\zeta^9+\zeta^{10}+\zeta^{13}+\zeta^5+\zeta^{15}+\zeta^{11}+\ldots & \\
& \diagup \qquad\qquad\qquad\qquad\qquad\qquad \diagdown & \\
S_2: & \zeta+\zeta^9+\zeta^{13}+\zeta^{15}+\ldots \qquad & \zeta^3+\zeta^{10}+\zeta^5+\zeta^{11}+\ldots
\end{array}$$

3) Completa los puntos suspensivos.

En el caso $p - 1 \neq 2^n$ hay algo similar salvo que en vez de cogerlos de dos en dos hay que cogerlos de q_i en q_i donde q_i son los factores primos de $p - 1$ y el árbol no es binario, pero de eso no nos ocuparemos ahora. Gauss llamó a las expresiones intermedias *periodos*.

El resultado fundamental es que cualquier expresión que tenga la simetría S_d se puede escribir como combinación lineal (con coeficientes racionales) de las expresiones que aparecen en el piso S_d del árbol. Antes de seguir, recuerda o aprende que el número en la cima del árbol es muy sencillo:

4) Prueba que $\sum_{k=1}^{p-1} \zeta^k = -1$.

Con el resultado fundamental anterior para $p-1=2^n$ (el único caso del que nos ocuparemos en el resto de la hoja), Gauss hizo algo muy ingenioso: tomó la suma y el producto de dos expresiones que tenía el mismo padre en el árbol. Esa suma y ese producto adquieren las simetrías del piso de arriba. Por ejemplo en el caso $p=5$,

$$S=(\zeta+\zeta^4)+(\zeta^3+\zeta^2) \qquad \text{y} \qquad P=(\zeta+\zeta^4)(\zeta^3+\zeta^2)$$

tienen simetría S_1 y por tanto son una combinación lineal racional de un sólo número (un múltiplo racional) de $\zeta^1+\zeta^3+\zeta^4+\zeta^2=-1$. Es decir, son números racionales que podemos calcular.

5) Calcula S y P.

Pero resulta que (fíjate que ingenioso) $\zeta+\zeta^4$ y $\zeta^3+\zeta^2$ son las raíces de la ecuación cuadrática $x^2-Sx+P=0$ y resolviéndola tendremos una fórmula explícita con raíces cuadradas para $r_1=\zeta+\zeta^4$ y $r_2=\zeta^3+\zeta^2$.

6) Calcula r_1 y r_2.

De la misma forma la suma y el producto de ζ y ζ^4 tienen las simetrías de su padre, S_2, y son combinación lineal de r_1 y r_2, lo cual es casi inmediato:

$$\zeta+\zeta^4=r_1 \qquad \text{y} \qquad \zeta\cdot\zeta^4=1=-r_1-r_2.$$

Entonces ζ y ζ^4 son raíces de la ecuación $x^2-r_1x-r_1-r_2=x^2-r_1x+1=0$ y obtendremos una fórmula con raíces cuadradas para ζ.

7) ¿Qué formula es? Da fórmulas lo más simples posibles para $\cos(2\pi/5)$ y $\sin(2\pi/5)$. Indicación: En realidad para esto último te basta r_1.

El caso $p=17$ es un demasiado largo como para proponerte que lo hagas completo. A ver si consigues dar el primer paso:

8) Halla una fórmula explícita para $\zeta+\zeta^9+\zeta^{13}+\zeta^{15}+\dots$ que apareció en el caso $p=17$. Indicación: Si haces el cálculo directo, ayúdate de un ordenador para no aburrirte. Una alternativa para hacerlo a mano es que ya sabes que este número por su hermano es un múltiplo de $\zeta+\zeta^2+\cdots+\zeta^{16}$. Basta con que halles el coeficiente de ζ.

Hay una cosa que debes tener clara:

9) ¿Por qué la suma y el producto de los dos hijo siempre adquieren la simetría de su padre? Intenta convencerte a ti mismo.

Todos los ejercicios que te he puesto hasta ahora son para que te entrenes. Si tienes dudas me puedes preguntar pero no hace falta que me los mandes escritos en limpio. El único ejercicio que tienes que entregarme es el siguiente:

10) Redacta lo que has aprendido de forma breve y con tus propias palabras para conseguir una primera versión del apartado 1 en la propuesta de temario. Intenta que sea algo ligero, sin demostraciones, que resulte atractivo para un lector que no sabe nada previo.

Referencias

[Cla84] A. Clark. *Elements of Abstract Algebra*. Dover Books on Mathematics Series. Dover Publications, 1984.

[DH96] J. R. Dorronsoro and E. Hernández. *Números grupos y anillos*. Addison-Wesley Iberoamericana-UAM, 1996.

[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.

[HW08] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.