El tema principal de esta hoja es una aplicación de las sumas de Gauss a la teoría de números para demostrar lo que se llama la *ley de reciprocidad cuadrática* que es un sorprendente resultado sobre congruencias que conjeturó Euler y demostró Gauss de varias formas distintas.

Esta ley establece una relación entre la solubilidad de $x^2 \equiv p\ (q)$ y la de $x^2 \equiv q\ (p)$ cuando $p, q > 2$ son primos distintos, lo cual es muy chocante porque, en principio, las congruencias módulos coprimos no tienen absolutamente nada que ver. Aquí y en lo sucesivo empleo la notación reducida de congruencias escribiendo (p) en lugar de (mód p).

Para suscitar tu curiosidad te propongo que hagas primero un análisis experimental, con ordenador, como el que pudo hacer Euler a mano (aunque, en realidad, procedió calculando otras cantidades). Para cada par de primos distintos $p, q > 2$ diremos que las ecuaciones $x^2 \equiv p\ (q)$ y $x^2 \equiv q\ (p)$ son incoherentes si una tiene solución y la otra no. Por ejemplo, para $p = 3$, $p = 7$ lo son pues $x \equiv 3\ (7)$ no tiene solución, mientras que $x \equiv 7\ (3)$ sí tiene solución, concretamente $x \equiv 1\ (3)$. En caso contrario, diremos que son coherentes. Esto es lo que ocurre para $p = 5$, $q = 7$ pues ni $x \equiv 5\ (7)$ ni $x \equiv 7\ (5)$ tienen solución. En principio, uno esperaría que la coherencia o incoherencia tuviera un comportamiento "aleatorio". La sorpresa es que puede determinarse fácilmente simplemente examinando cierta paridad. Más sorprendente aún es que no exista una prueba realmente sencilla de ello.

1) Escribe un programa que considere los primos $2 < p < q < 100$ y elabore una tabla asignando a cada par de primos C o I dependiendo de si $x^2 \equiv p\ (q)$ y $x^2 \equiv q\ (p)$ son coherentes o incoherentes. Cruza esa tabla con otra que indique si $(p-1)(q-1)/4$ es par o impar y extrae un patrón que te lleve a una conjetura.

Si vas a incluir líneas de código en tu trabajo y no sabes cómo hacerlo, revisa cómo uso el paquete `listings` en la fuente LaTeX de este documento para escribir el siguiente ejemplo en `sagemath` que muestra en pantalla todos los pares de primos admisibles en el ejercicio anterior.

```
for p in prime_range(3,100):
    for q in prime_range(p+1,100):
        print(p,q)
```

Para $n \in \mathbb{Z}$ y p primo $p \nmid n$ se define el *símbolo de Legendre* como

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv n\ (p) \text{ tiene solución,} \\ -1 & \text{si } x^2 \equiv n\ (p) \text{ no tiene solución.} \end{cases}$$

Se completa la definición con 0 si $p \mid n$, pero es indiferente para esta hoja.

Los tres ejercicios siguientes extienden lo que sabíamos sobre la evaluación de las sumas de Gauss cuando el denominador es primo. El primero de ellos es sencillo.

2) Si $\left(\frac{q}{p}\right) = 1$ con p primo y $q \in \mathbb{Z}$, $p \nmid q$, explica por qué $G(q,p) = G(1,p)$.

3) Si $\left(\frac{q}{p}\right) = -1$ con $p > 2$ primo y $q \in \mathbb{Z}$, $p \nmid q$, prueba que

$$q(\pm 1)^2,\ q(\pm 2)^2,\ \ldots,\ q\Big(\pm\frac{p-1}{2}\Big)^2,\ 0,\ (\pm 1)^2,\ (\pm 2)^2,\ \ldots,\ \Big(\pm\frac{p-1}{2}\Big)^2$$

dan todas las clases módulo p sin repeticiones cuando se fija uno de los dos signos. Deduce de ello $2\sum_{k=0}^{p-1} e(k/p) = G(q,p) + G(1,p)$. Indicación: Una vez probado que las clases son distintas, necesariamente son todas porque $\frac{p-1}{2} + 1 + \frac{p-1}{2} = p$.

4) Deduce la fórmula

$$G(q,p) = \Big(\frac{q}{p}\Big) G(1,p) \qquad \text{para } p > 2 \text{ primo y } q \in \mathbb{Z},\ p \nmid q. \tag{1}$$

En realidad, se puede incluir el caso $p = 2$ para el que el resultado es trivial.

Con todo esto, lo que sabemos sobre evaluar sumas de Gauss es suficiente para obtener el resultado deseado.

5) Con la propiedad multiplicativa del penúltimo ejercicio de la hoja anterior, la evaluación de $G(1,pq)$ y (1), concluye la ley de reciprocidad cuadrática en la forma

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{(p-1)(q-1)/4}. \qquad \text{para } p, q > 2 \text{ primos distintos.} \tag{2}$$

Se suele preferir este enunciado simétrico, aunque quizá sea más informativa la siguiente traducción: $\left(\frac{p}{q}\right)$ es $-\left(\frac{q}{p}\right)$ si $4 \mid p+1$ y $4 \mid q+1$ y es $\left(\frac{q}{p}\right)$ en el resto de los casos.

Normalmente se añaden a la ley de reciprocidad cuadrática un par de evaluaciones de evaluaciones del símbolo de Legendre llamadas "leyes suplementarias", aunque no tienen ni mucho menos la misma profundidad. Son las siguientes:

$$\Big(\frac{-1}{p}\Big) = (-1)^{(p-1)/2} \qquad \text{y} \qquad \Big(\frac{2}{p}\Big) = (-1)^{(p^2-1)/8} \qquad \text{para } p > 2 \text{ primo.}$$

6) Utilizando que $G(-1,p)$ es el conjugado de $G(1,p)$, prueba la primera ley suplementaria.

Aunque (1) es también válido para $p = 2$, el hecho de que $G(1,2) = 0$ invalida su uso.

7) Aplica (1) con $q = 8$ y adapta la demostración que has dado de (2) para concluir la segunda ley suplementaria. Indicación: ¿Por qué $G(8,p) = G(2,p)$?

La definición del símbolo de Legendre se extiende a módulos compuestos. Concretamente, para $m > 2$ impar cuya factorización en primos es $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ se define el *símbolo de Jacobi* como

$$\Big(\frac{n}{m}\Big) = \prod_{j=1}^{k} \Big(\frac{n}{p_j}\Big)^{\alpha_j}.$$

Si m no es primo, la solubilidad de $x^2 - n \equiv 0\ (m)$ no está asegurada porque valga uno. Esto está relacionado con el "quadratic residuosity problem" [4] que es la base del criptosistema del último ejercicio.

Esta definición permite extender (1) al caso compuesto. Veámoslo para potencias de primos.

8) Justifica las siguientes igualdades para p y q como en (1) y $k \geq 2$ entero:

$$G(q,p^k) = \sum_{m=0}^{p-1} \sum_{\ell=0}^{p^{k-1}-1} e\Big(\frac{q(p^{k-1}m+\ell)^2}{p^k}\Big) = p \sum_{\ell=0,\, p|\ell}^{p^{k-1}-1} e\Big(\frac{q\ell^2}{p^k}\Big) = p\, G(q,p^{k-2}).$$

Demuestra con ello que (1) es cierto reemplazando p por p^k.

Una pequeña sorpresa a este nivel es que el símbolo de Legendre es multiplicativo es su primer argumento, por tanto, el de Jacobi también. Aunque sea un poco retorcido, vamos a proceder usando las sumas de Gauss.

9) Con variaciones de los dos ejercicios que llevaron a (1), separando los casos $\left(\frac{q_2}{p}\right) = \pm 1$, muestra que para $q_1, q_2 \in \mathbb{Z}$ y $p > 2$ primo $p \nmid q_1 q_2$ se tiene $G(q_1 q_2, p) = \left(\frac{q_2}{p}\right) G(q_1, p)$. Deduce que el símbolo de Jacobi es completamente multiplicativo, esto es,

$$\Big(\frac{q_1 q_2}{m}\Big) = \Big(\frac{q_1}{m}\Big)\Big(\frac{q_2}{m}\Big) \qquad \text{para } q_1, q_2 \in \mathbb{Z} \text{ y } m \in \mathbb{Z}^+ \text{ impar.}$$

Indicación: ¿Por qué basta considerar el caso en que m es primo?

Una vez que sabemos que los símbolos de Jacobi son multiplicativos en ambos argumentos, se sigue una ley de reciprocidad cuadrática para los símbolos de Jacobi, esto es, una generalización de (2). Vamos a descomponer la prueba en dos ejercicios. Si necesitas ayuda para el segundo, da un vistazo a la demostración (muy esquemática) que doy en [1, Prop. 1.3.8] (también [2, §3.6] te puede resultar útil). Además, se cumplen las leyes suplementarias. No nos meteremos en ello para no alargar más la hoja.

10) Prueba que (2) también se verifica si se sustituyen p y q por p^k y q^ℓ con $k, \ell \in \mathbb{Z}^+$. Indicación: Si k y ℓ no son ambos impares, $(p^k - 1)(q^\ell - 1)/4$ es par y el resultado es bastante obvio.

11) Demuestra

$$\Big(\frac{n}{m}\Big)\Big(\frac{m}{n}\Big) = (-1)^{(n-1)(m-1)/4} \qquad \text{para } n, m \in \mathbb{Z}^+ \text{ impares y coprimos.}$$

Empleando todo lo que has aprendido estamos en condiciones de obtener la evaluación completa de las sumas de Gauss generalizadas $G(a,b,q)$ cuando q es impar. A ver si consigues resolver el siguiente ejercicio sin indicaciones.

12) Demuestra que para $q \in \mathbb{Z}^+$ (no necesariamente primo) se cumple

$$G(a,b,q) = i^{(q-1)^2/4}\sqrt{q}\Big(\frac{a}{q}\Big)e\Big(-\frac{\overline{4a}b^2}{q}\Big)$$

donde $\overline{4a}$ indica el inverso módulo q, esto es, $4a\overline{4a} \equiv 1\ (q)$.

La reciprocidad cuadrática de los símbolos de Jacobi permite elaborar un algoritmo eficiente para decidir si $x^2 \equiv n\ (m)$ tiene solución o no para n y m de tamaño razonable [2, §3.6] (tal algoritmo se amplia a cualquier ecuación de segundo grado [1]). Si n y m son astronómicamente grandes, tal algoritmo, que requiere la factorización, colapsa con nuestros conocimientos y ordenadores actuales. Esta es la base del *criptosistema de Goldwasser-Micali*. Hay que aclarar que en la práctica no es muy interesante porque otros criptosistemas lo superan.

13) Lee en [3] acerca del criptosistema de Goldwasser-Micali y escribe unas líneas sobre él. Si ves que no lo entiendes bien o estás corto de espacio, basta con que pongas una referencia.

Tarea a entregar. Escribe un documento que combine las soluciones de los ejercicios anteriores. La extensión recomendada es de 6 páginas con el formato de esta hoja o de la plantilla. Si te ves apurado, reduce al mínimo el último ejercicio y da solo una idea de la prueba de la reciprocidad cuadrática de los símbolos de Jacobi. El resultado conformará un segundo capítulo de tu TFG llamado *La ley de reciprocidad cuadrática* o algo parecido.

Referencias

[1] F. Chamizo. La ley de reciprocidad cuadrática. Curso de teoría de números `https://matematicas.uam.es/~fernando.chamizo/asignaturas/2223tenum/notes/sec1.3.pdf`, 2022.

[2] L.-K. Hua. Introduction to number theory. Transl. from the Chinese by P. Shiu. Berlin-Heidelberg-New York: Springer-Verlag, 1982.

[3] Wikipedia contributors. Goldwasser-Micali cryptosystem — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Goldwasser%E2%80%93Micali_cryptosystem&oldid=1172066465`, 2023. [Online; accessed 7-October-2024].

[4] Wikipedia contributors. Quadratic residuosity problem — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Quadratic_residuosity_problem&oldid=1190957329`, 2023. [Online; accessed 10-October-2024].