El mínimo no-residuo cuadrático y otros problemas relacionados

Enrique Treviño

Swarthmore College

Universidad de Colima
7 de mayo, 2012

Cuadrados

Considera la secuencia

$$2, 5, 8, 11, \ldots$$

¿Puede contener cuadrados?

- Todo entero positivo n cae en una de tres categorías: $n \equiv 0, 1$ ó $2 \pmod 3$.
- Si $n \equiv 0 \pmod 3$, entonces $n^2 \equiv 0^2 = 0 \pmod 3$.
- Si $n \equiv 1 \pmod 3$, entonces $n^2 \equiv 1^2 = 1 \pmod 3$.
- Si $n \equiv 2 \pmod 3$, entonces $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Cuadrados

Considera la secuencia

$$2, 5, 8, 11, \ldots$$

¿Puede contener cuadrados?

- Todo entero positivo n cae en una de tres categorías: $n \equiv 0$, 1 ó 2 $\pmod 3$.
- Si $n \equiv 0 \pmod 3$, entonces $n^2 \equiv 0^2 = 0 \pmod 3$.
- Si $n \equiv 1 \pmod 3$, entonces $n^2 \equiv 1^2 = 1 \pmod 3$.
- Si $n \equiv 2 \pmod 3$, entonces $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Cuadrados

Considera la secuencia

$$2, 5, 8, 11, \ldots$$

¿Puede contener cuadrados?

- Todo entero positivo n cae en una de tres categorías: $n \equiv 0$, 1 ó 2 $\pmod 3$.
- Si $n \equiv 0 \pmod 3$, entonces $n^2 \equiv 0^2 = 0 \pmod 3$.
- Si $n \equiv 1 \pmod 3$, entonces $n^2 \equiv 1^2 = 1 \pmod 3$.
- Si $n \equiv 2 \pmod 3$, entonces $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Cuadrados

Considera la secuencia

$$2, 5, 8, 11, \ldots$$

¿Puede contener cuadrados?

- Todo entero positivo n cae en una de tres categorías: $n \equiv 0$, 1 ó 2 $\pmod 3$.
- Si $n \equiv 0 \pmod 3$, entonces $n^2 \equiv 0^2 = 0 \pmod 3$.
- Si $n \equiv 1 \pmod 3$, entonces $n^2 \equiv 1^2 = 1 \pmod 3$.
- Si $n \equiv 2 \pmod 3$, entonces $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Cuadrados

Considera la secuencia

$$2, 5, 8, 11, \ldots$$

¿Puede contener cuadrados?

- Todo entero positivo n cae en una de tres categorías: $n \equiv 0$, 1 ó 2 $\pmod 3$.
- Si $n \equiv 0 \pmod 3$, entonces $n^2 \equiv 0^2 = 0 \pmod 3$.
- Si $n \equiv 1 \pmod 3$, entonces $n^2 \equiv 1^2 = 1 \pmod 3$.
- Si $n \equiv 2 \pmod 3$, entonces $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Residuos y no-residuos cuadráticos

Sea n un entero positivo. Para $q \in \{0, 1, 2, \ldots, n-1\}$, llamamos a q residuo cuadrático mod n si existe un entero x tal que $x^2 \equiv q \pmod{n}$. Si no existe tal x, decimos que q es un no-residuo cuadrático módulo n.

- Para $n = 3$, los residuos cuadráticos son $\{0, 1\}$ y el no-residuo es 2.
- Para $n = 5$, los residuos cuadráticos son $\{0, 1, 4\}$ y los no-residuos son $\{2, 3\}$.
- Para $n = 7$, los residuos cuadráticos son $\{0, 1, 2, 4\}$ y los no-residuos son $\{3, 5, 6\}$.
- Para $n = p$, un primo impar, hay $\frac{p+1}{2}$ residuos cuadráticos y $\frac{p-1}{2}$ no-residuos cuadráticos.

El mínimo no-residuo cuadrático

¿Qué tan grande puede ser el mínimo no-residuo cuadrático?

- Para que el mínimo sea > 2 necesitamos que 2 sea residuo cuadrático, por lo tanto $p \equiv \pm 1 \pmod 8$, por lo que $p = 7$ es el primer ejemplo.
- Para que el mínimo sea > 3 necesitamos que 2 y 3 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$ y $p \equiv \pm 1 \pmod{12}$, que implica $p \equiv \pm 1 \pmod{24}$, dándonos a $p = 23$ como el primer ejemplo.
- Para que el mínimo sea > 5 necesitamos que $2, 3$ y 5 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ y $p \equiv \pm 1 \pmod 5$, lo cual implica $p \equiv \pm 1, \pm 49 \pmod{120}$, dándonos a $p = 71$ como el primer ejemplo.

El mínimo no-residuo cuadrático

¿Qué tan grande puede ser el mínimo no-residuo cuadrático?

- Para que el mínimo sea > 2 necesitamos que 2 sea residuo cuadrático, por lo tanto $p \equiv \pm 1 \pmod 8$, por lo que $p = 7$ es el primer ejemplo.
- Para que el mínimo sea > 3 necesitamos que 2 y 3 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$ y $p \equiv \pm 1 \pmod{12}$, que implica $p \equiv \pm 1 \pmod{24}$, dándonos a $p = 23$ como el primer ejemplo.
- Para que el mínimo sea > 5 necesitamos que $2, 3$ y 5 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ y $p \equiv \pm 1 \pmod 5$, lo cual implica $p \equiv \pm 1, \pm 49 \pmod{120}$, dándonos a $p = 71$ como el primer ejemplo.

El mínimo no-residuo cuadrático

¿Qué tan grande puede ser el mínimo no-residuo cuadrático?

- Para que el mínimo sea > 2 necesitamos que 2 sea residuo cuadrático, por lo tanto $p \equiv \pm 1 \pmod 8$, por lo que $p = 7$ es el primer ejemplo.
- Para que el mínimo sea > 3 necesitamos que 2 y 3 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$ y $p \equiv \pm 1 \pmod{12}$, que implica $p \equiv \pm 1 \pmod{24}$, dándonos a $p = 23$ como el primer ejemplo.
- Para que el mínimo sea > 5 necesitamos que $2, 3$ y 5 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ y $p \equiv \pm 1 \pmod 5$, lo cual implica $p \equiv \pm 1, \pm 49 \pmod{120}$, dándonos a $p = 71$ como el primer ejemplo.

El mínimo no-residuo cuadrático

¿Qué tan grande puede ser el mínimo no-residuo cuadrático?

- Para que el mínimo sea > 2 necesitamos que 2 sea residuo cuadrático, por lo tanto $p \equiv \pm 1 \pmod 8$, por lo que $p = 7$ es el primer ejemplo.
- Para que el mínimo sea > 3 necesitamos que 2 y 3 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$ y $p \equiv \pm 1 \pmod{12}$, que implica $p \equiv \pm 1 \pmod{24}$, dándonos a $p = 23$ como el primer ejemplo.
- Para que el mínimo sea > 5 necesitamos que $2, 3$ y 5 sean residuos cuadráticos, por lo tanto $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ y $p \equiv \pm 1 \pmod 5$, lo cual implica $p \equiv \pm 1, \pm 49 \pmod{120}$, dándonos a $p = 71$ como el primer ejemplo.

Heurśtica

Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. Sea p_i el primo i, es decir, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- Si $k = \log \pi(x)/\log 2$ esperaríamos sólo un primo satisfaciendo $g(p) = p_k$, así que si k es un poco más grande, no se esperaría tener un primo con tan grande mínimo no-residuo cuadrático.
- Entonces queremos $k \approx C \log x$, y como $p_k \sim k \log k$ entonces tenemos $g(x) \approx C \log x \log \log x$.

Heurśtica

Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. Sea p_i el primo i, es decir, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- Si $k = \log \pi(x)/\log 2$ esperaríamos sólo un primo satisfaciendo $g(p) = p_k$, así que si k es un poco más grande, no se esperaría tener un primo con tan grande mínimo no-residuo cuadrático.
- Entonces queremos $k \approx C \log x$, y como $p_k \sim k \log k$ entonces tenemos $g(x) \approx C \log x \log\log x$.

Heurśtica

Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. Sea p_i el primo i, es decir, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- Si $k = \log \pi(x)/\log 2$ esperaríamos sólo un primo satisfaciendo $g(p) = p_k$, así que si k es un poco más grande, no se esperaría tener un primo con tan grande mínimo no-residuo cuadrático.
- Entonces queremos $k \approx C \log x$, y como $p_k \sim k \log k$ entonces tenemos $g(x) \approx C \log x \log\log x$.

Heurśtica

Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. Sea p_i el primo i, es decir, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- Si $k = \log \pi(x) / \log 2$ esperaríamos sólo un primo satisfaciendo $g(p) = p_k$, así que si k es un poco más grande, no se esperaría tener un primo con tan grande mínimo no-residuo cuadrático.
- Entonces queremos $k \approx C \log x$, y como $p_k \sim k \log k$ entonces tenemos $g(x) \approx C \log x \log \log x$.

Heurśtica

Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. Sea p_i el primo i, es decir, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- Si $k = \log \pi(x)/\log 2$ esperaríamos sólo un primo satisfaciendo $g(p) = p_k$, así que si k es un poco más grande, no se esperaría tener un primo con tan grande mínimo no-residuo cuadrático.
- Entonces queremos $k \approx C \log x$, y como $p_k \sim k \log k$ entonces tenemos $g(x) \approx C \log x \log\log x$.

Heurśtica

Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. Sea p_i el primo i, es decir, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- Si $k = \log \pi(x)/\log 2$ esperaríamos sólo un primo satisfaciendo $g(p) = p_k$, así que si k es un poco más grande, no se esperaría tener un primo con tan grande mínimo no-residuo cuadrático.
- Entonces queremos $k \approx C \log x$, y como $p_k \sim k \log k$ entonces tenemos $g(x) \approx C \log x \log\log x$.

Teoremas sobre el mínimo no-residuo cuadrático mod p

Sea $g(p)$ el mínimo no-residuo cuadrático mod p. La heurística propone la conjetura

$$g(p) = O(\log p \log\log p).$$

- Usando GRH, Bach demostró $g(p) \leq 2\log^2 p$.
- Incondicionalmente, Burgess demostró $g(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- En la dirección de una cota inferior, Graham and Ringrose demostraron que hay infinitos p satisfaciendo $g(p) \gg \log p \log\log\log p$, es decir

$$g(p) = \Omega(\log p \log\log\log p).$$

Teoremas sobre el mínimo no-residuo cuadrático mod p

Sea $g(p)$ el mínimo no-residuo cuadrático mod p. La heurística propone la conjetura

$$g(p) = O(\log p \log\log p).$$

- Usando GRH, Bach demostró $g(p) \leq 2\log^2 p$.
- Incondicionalmente, Burgess demostró $g(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- En la dirección de una cota inferior, Graham and Ringrose demostraron que hay infinitos p satisfaciendo $g(p) \gg \log p \log\log\log p$, es decir

$$g(p) = \Omega(\log p \log\log\log p).$$

Teoremas sobre el mínimo no-residuo cuadrático mod p

Sea $g(p)$ el mínimo no-residuo cuadrático mod p. La heurística propone la conjetura

$$g(p) = O(\log p \log\log p).$$

- Usando GRH, Bach demostró $g(p) \leq 2\log^2 p$.
- Incondicionalmente, Burgess demostró $g(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- En la dirección de una cota inferior, Graham and Ringrose demostraron que hay infinitos p satisfaciendo $g(p) \gg \log p \log\log\log p$, es decir

$$g(p) = \Omega(\log p \log\log\log p).$$

Teoremas sobre el mínimo no-residuo cuadrático mod p

Sea $g(p)$ el mínimo no-residuo cuadrático mod p. La heurística propone la conjetura

$$g(p) = O(\log p \log\log p).$$

- Usando GRH, Bach demostró $g(p) \leq 2\log^2 p$.
- Incondicionalmente, Burgess demostró $g(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- En la dirección de una cota inferior, Graham and Ringrose demostraron que hay infinitos p satisfaciendo $g(p) \gg \log p \log\log\log p$, es decir

$$g(p) = \Omega(\log p \log\log\log p).$$

Cotas explicitas para el mínimo no-residuo cuadrático

Norton demostró

$$g(p) \leq \begin{cases} 3.9p^{1/4}\log p & \text{si } p \equiv 1 \pmod 4, \\ 4.7p^{1/4}\log p & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Theorem (ET)

Sea $p > 3$ un primo. Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. *Entonces*

$$g(p) \leq \begin{cases} 0.9p^{1/4}\log p & \text{si } p \equiv 1 \pmod 4, \\ 1.1p^{1/4}\log p & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Cotas explicitas para el mínimo no-residuo cuadrático

Norton demostró

$$g(p) \leq \begin{cases} 3.9p^{1/4}\log p & \text{si } p \equiv 1 \pmod 4, \\ 4.7p^{1/4}\log p & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Theorem (ET)

Sea $p > 3$ un primo. Sea $g(p)$ el mínimo no-residuo cuadrático mod$p$. *Entonces*

$$g(p) \leq \begin{cases} 0.9p^{1/4}\log p & \textit{si } p \equiv 1 \pmod 4, \\ 1.1p^{1/4}\log p & \textit{si } p \equiv 3 \pmod 4. \end{cases}$$

Campos cuadráticos y primos inertes

- Sea d un entero libre de cuadrados.
- $\mathbb{Q}(\sqrt{d})$ es un campo cuadrático.
- Un primo $p \in \mathbb{Z}$ es inerte si permanece primo en el campo cuadrático.
- Por ejemplo, consideremos $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. En este campo, los primos inertes son los primos $p \equiv 3 \pmod 4$.
- Nótese que 5 no es primo en $\mathbb{Q}(i)$ por que $(1 + 2i)(1 - 2i) = 5$. Similarmente cualquier primo $p \equiv 1 \pmod 4$ no es primo en $\mathbb{Q}(i)$ ya que p puede ser escrito como $a^2 + b^2$ para algunos $a, b \in \mathbb{Z}$ y por lo tanto $p = (a + bi)(a - bi)$.

Caracterización de los primos inertes en campos cuadráticos

- La discriminante D del campo cuadrático $\mathbb{Q}(\sqrt{d})$ es d si $d \equiv 1 \pmod 4$ y $4d$ de lo contrario.
- El primo p es inerte en $\mathbb{Q}(\sqrt{d})$ sí y sólo sí el símbolo de Kronecker $(D/p) = -1$.
- El símbolo de Kronecker es una generalización del símbolo de Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático } \bmod p, \\ -1 & \text{si } a \text{ es un no-residuo cuadrático } \bmod p, \\ 0 & \text{si } p \mid a. \end{cases}$$

Caracterización de los primos inertes en campos cuadráticos

- La discriminante D del campo cuadrático $\mathbb{Q}(\sqrt{d})$ es d si $d \equiv 1 \pmod 4$ y $4d$ de lo contrario.
- El primo p es inerte en $\mathbb{Q}(\sqrt{d})$ sí y sólo sí el símbolo de Kronecker $(D/p) = -1$.
- El símbolo de Kronecker es una generalización del símbolo de Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático } \bmod p, \\ -1 & \text{si } a \text{ es un no-residuo cuadrático } \bmod p, \\ 0 & \text{si } p \mid a. \end{cases}$$

Caracterización de los primos inertes en campos cuadráticos

- La discriminante D del campo cuadrático $\mathbb{Q}(\sqrt{d})$ es d si $d \equiv 1 \pmod 4$ y $4d$ de lo contrario.
- El primo p es inerte en $\mathbb{Q}(\sqrt{d})$ sí y sólo sí el símbolo de Kronecker $(D/p) = -1$.
- El símbolo de Kronecker es una generalización del símbolo de Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático } \bmod p, \\ -1 & \text{si } a \text{ es un no-residuo cuadrático } \bmod p, \\ 0 & \text{si } p \mid a. \end{cases}$$

El mínimo primo inerte en un campo real cuadrático

Theorem (Granville, Mollin and Williams, 2000)

Para cualquier discriminante fundamental $D > 3705$, existe al menos un primo $p \leq \sqrt{D}/2$ tal que el símbolo de Kronecker $(D/p) = -1$.

Theorem (ET, 2012)

Para cualquier discriminante fundamental $D > 1596$, existe al menos un primo $p \leq D^{0.45}$ tal que el símbolo de Kronecker $(D/p) = -1$.

El mínimo primo inerte en un campo real cuadrático

Theorem (Granville, Mollin and Williams, 2000)

Para cualquier discriminante fundamental $D > 3705$, existe al menos un primo $p \leq \sqrt{D}/2$ tal que el símbolo de Kronecker $(D/p) = -1$.

Theorem (ET, 2012)

Para cualquier discriminante fundamental $D > 1596$, existe al menos un primo $p \leq D^{0.45}$ tal que el símbolo de Kronecker $(D/p) = -1$.

Ideas de la demostración

- Usar una computadora para checar los casos “pequeños”. Granville, Mollin y Williams usaron el Manitoba Scalable Sieving Unit.
- Usar técnicas analíticas para demostrar el “caso infinito”, es decir, cuando D es muy grande. La herramienta usada por Granville et al. es la desigualdad de Pólya–Vinogradov. En mi caso use una versión “lisa” de la desigualdad.
- Usar Pólya–Vinogradov junto con computación para llenar el hueco.

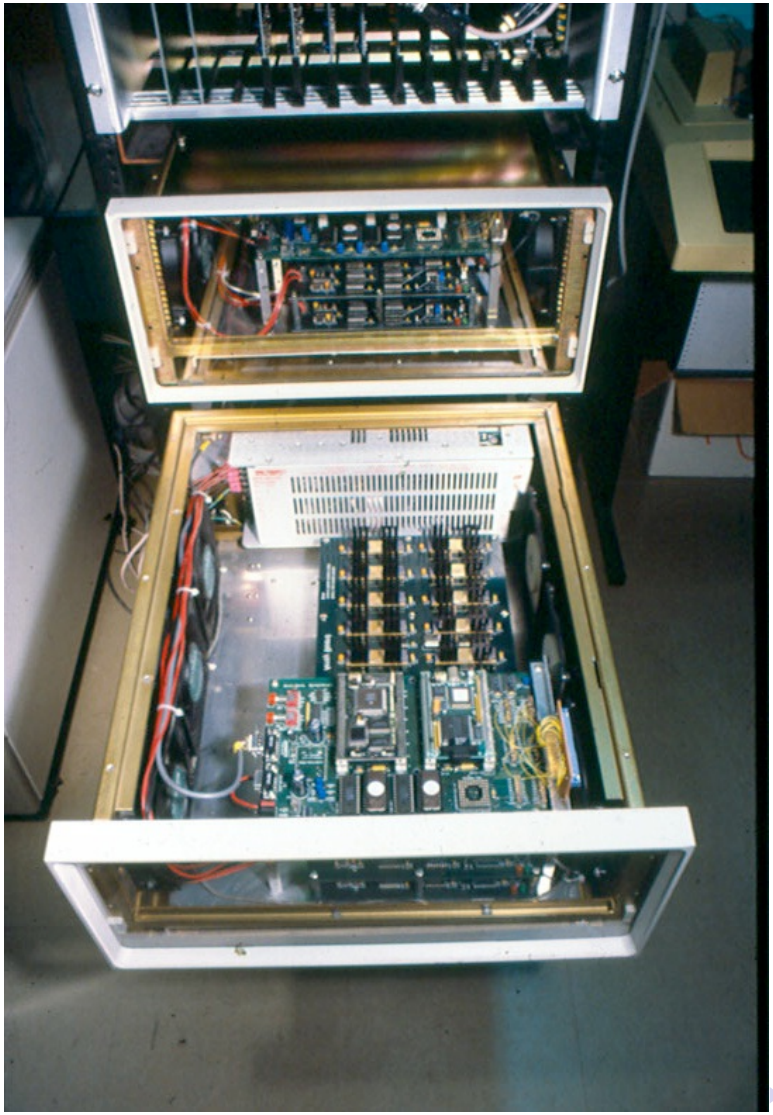
Ideas de la demostración

- Usar una computadora para checar los casos “pequeños”. Granville, Mollin y Williams usaron el Manitoba Scalable Sieving Unit.
- Usar técnicas analíticas para demostrar el “caso infinito”, es decir, cuando D es muy grande. La herramienta usada por Granville et al. es la desigualdad de Pólya–Vinogradov. En mi caso use una versión “lisa” de la desigualdad.
- Usar Pólya–Vinogradov junto con computación para llenar el hueco.

Ideas de la demostración

- Usar una computadora para checar los casos “pequeños”. Granville, Mollin y Williams usaron el Manitoba Scalable Sieving Unit.
- Usar técnicas analíticas para demostrar el “caso infinito”, es decir, cuando D es muy grande. La herramienta usada por Granville et al. es la desigualdad de Pólya–Vinogradov. En mi caso use una versión “lisa” de la desigualdad.
- Usar Pólya–Vinogradov junto con computación para llenar el hueco.

Manitoba Scalable Sieving Unit



Carácter de Dirichlet

Sea n un entero positivo.
$\chi : \mathbb{Z} \to \mathbb{C}$ es un carácter de Dirichlet mod n si las siguientes tres condiciones son satisfechas:

- $\chi(a+n) = \chi(a)$ para toda $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ para toda $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ sí y sólo sí $\gcd(a, n) > 1$.

Ejemplos de carácteres de Dirichlet son el símbolo de Legendre y el símbolo de Kronecker.

Carácter de Dirichlet

Sea n un entero positivo.
$\chi : \mathbb{Z} \to \mathbb{C}$ es un carácter de Dirichlet mod n si las siguientes tres condiciones son satisfechas:

- $\chi(a+n) = \chi(a)$ para toda $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ para toda $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ sí y sólo sí $\gcd(a, n) > 1$.

Ejemplos de carácteres de Dirichlet son el símbolo de Legendre y el símbolo de Kronecker.

Carácter de Dirichlet

Sea n un entero positivo.
$\chi : \mathbb{Z} \to \mathbb{C}$ es un carácter de Dirichlet mod n si las siguientes tres condiciones son satisfechas:

- $\chi(a+n) = \chi(a)$ para toda $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ para toda $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ sí y sólo sí $\gcd(a, n) > 1$.

Ejemplos de carácteres de Dirichlet son el símbolo de Legendre y el símbolo de Kronecker.

Carácter de Dirichlet

Sea n un entero positivo.
$\chi : \mathbb{Z} \to \mathbb{C}$ es un carácter de Dirichlet mod n si las siguientes tres condiciones son satisfechas:

- $\chi(a+n) = \chi(a)$ para toda $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ para toda $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ sí y sólo sí $\gcd(a, n) > 1$.

Ejemplos de carácteres de Dirichlet son el símbolo de Legendre y el símbolo de Kronecker.

Carácter de Dirichlet

Sea n un entero positivo.
$\chi : \mathbb{Z} \to \mathbb{C}$ es un carácter de Dirichlet mod n si las siguientes tres condiciones son satisfechas:

- $\chi(a+n) = \chi(a)$ para toda $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ para toda $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ sí y sólo sí $\gcd(a, n) > 1$.

Ejemplos de carácteres de Dirichlet son el símbolo de Legendre y el símbolo de Kronecker.

Pólya–Vinogradov

Sea χ un carácter de Dirichlet módulo $q > 1$. Definamos

$$S(\chi) = \max_{M,N} \left| \sum_{n=M+1}^{M+N} \chi(n) \right|$$

La desigualdad Pólya–Vinogradov (1918) dice que existe una constante universal c tal que para cualquier carácter de Dirichlet $S(\chi) \leq c\sqrt{q}\log q$.

Asumiendo GRH, Montgomery y Vaughan demostraron que $S(\chi) \ll \sqrt{q}\log\log q$.

Paley demostró en 1932 que hay infinitos caracteres cuadráticos tales que $S(\chi) \gg \sqrt{q}\log\log q$.

Pólya–Vinogradov explícito

Theorem (Hildebrand, 1988)

Para χ un carácter primitivo módulo $q > 1$, tenemos

$$|S(\chi)| \leq \begin{cases} \left(\frac{2}{3\pi^2} + o(1)\right)\sqrt{q}\log q & , \quad \chi \text{ par}, \\ \left(\frac{1}{3\pi} + o(1)\right)\sqrt{q}\log q & , \quad \chi \text{ impar}. \end{cases}$$

Theorem (Pomerance, 2009)

Para χ un carácter primitivo módulo $q > 1$, tenemos

$$|S(\chi)| \leq \begin{cases} \frac{2}{\pi^2}\sqrt{q}\log q + \frac{4}{\pi^2}\sqrt{q}\log\log q + \frac{3}{2}\sqrt{q} & , \quad \chi \text{ par}, \\ \frac{1}{2\pi}\sqrt{q}\log q + \frac{1}{\pi}\sqrt{q}\log\log q + \sqrt{q} & , \quad \chi \text{ impar}. \end{cases}$$

Burgess

Theorem (Burgess, 1962)

Sea χ un carácter primitivo $\bmod q$, donde $q > 1$, r es un entero positivo y $\varepsilon > 0$ es un número real. Entonces

$$|S_\chi(M,N)| = \left| \sum_{M<n\leq M+N} \chi(n) \right| \ll N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\varepsilon}$$

para $r = 1, 2, 3$ y para cualquier $r \geq 1$ si q es libre de cubos. La constante implícita depende sólo en ε y r.

Burgess Explícito

Theorem (Iwaniec-Kowalski-Friedlander)

Sea χ un carácter de Dirichlet no principal mod p (un primo). Sean M y N enteros no-negativos tales que $N \geq 1$ y sea $r \geq 2$, entonces

$$|S_\chi(M,N)| \leq 30 \cdot N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Theorem (ET)

Sea p un primo. Sea χ un carácter de Dirichlet no principal mod *p. Sean M y N enteros no-negativos tales que $N \geq 1$ y sea r un entero positivo. Entonces, para $p \geq 10^7$, tenemos*

$$|S_\chi(M,N)| \leq 2.71 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Burgess Explícito

Theorem (Iwaniec-Kowalski-Friedlander)

Sea χ un carácter de Dirichlet no principal mod p (un primo). Sean M y N enteros no-negativos tales que $N \geq 1$ y sea $r \geq 2$, entonces

$$|S_\chi(M,N)| \leq 30 \cdot N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Theorem (ET)

Sea p un primo. Sea χ un carácter de Dirichlet no principal mod p. *Sean M y N enteros no-negativos tales que $N \geq 1$ y sea r un entero positivo. Entonces, para $p \geq 10^7$, tenemos*

$$|S_\chi(M,N)| \leq 2.71 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Algunas aplicaciones de las cotas explícitas

- La cota explícita para el mínimo no-residuo cuadrático mostrada anteriormente.
- Booker calculó el número de clase de un campo con una discriminante de 32 dígitos usando Burgess explícito.
- McGown demostró que no hay campos cúbicos cíclicos que son norm-Euclidean si la discriminante del campo es $> 10^{140}$.
- Levin y Pomerance demostraron una conjetura de Brizolis que dice que para todo primo $p > 3$ existe una raíz primitiva g y un entero $x \in [1, p-1]$ tal que $\log_g x = x$, es decir, $g^x \equiv x \pmod{p}$.

Algunas aplicaciones de las cotas explícitas

- La cota explícita para el mínimo no-residuo cuadrático mostrada anteriormente.
- Booker calculó el número de clase de un campo con una discriminante de 32 dígitos usando Burgess explícito.
- McGown demostró que no hay campos cúbicos cíclicos que son norm-Euclidean si la discriminante del campo es $> 10^{140}$.
- Levin y Pomerance demostraron una conjetura de Brizolis que dice que para todo primo $p > 3$ existe una raíz primitiva g y un entero $x \in [1, p-1]$ tal que $\log_g x = x$, es decir, $g^x \equiv x \pmod{p}$.

Algunas aplicaciones de las cotas explícitas

- La cota explícita para el mínimo no-residuo cuadrático mostrada anteriormente.
- Booker calculó el número de clase de un campo con una discriminante de 32 dígitos usando Burgess explícito.
- McGown demostró que no hay campos cúbicos cíclicos que son norm-Euclidean si la discriminante del campo es $> 10^{140}$.
- Levin y Pomerance demostraron una conjetura de Brizolis que dice que para todo primo $p > 3$ existe una raíz primitiva g y un entero $x \in [1, p-1]$ tal que $\log_g x = x$, es decir, $g^x \equiv x \pmod{p}$.

Algunas aplicaciones de las cotas explícitas

- La cota explícita para el mínimo no-residuo cuadrático mostrada anteriormente.
- Booker calculó el número de clase de un campo con una discriminante de 32 dígitos usando Burgess explícito.
- McGown demostró que no hay campos cúbicos cíclicos que son norm-Euclidean si la discriminante del campo es $> 10^{140}$.
- Levin y Pomerance demostraron una conjetura de Brizolis que dice que para todo primo $p > 3$ existe una raíz primitiva g y un entero $x \in [1, p-1]$ tal que $\log_g x = x$, es decir, $g^x \equiv x \pmod{p}$.

Una aplicación reciente

Theorem (ET)

Sea $g(p)$ el mínimo no-residuo cuadrático módulo p. Sea p un primo mayor a 10^{4685}, entonces $g(p) < p^{1/6}$.

La desigualdad clave en la desigualdad de Burgess

Theorem (Burgess, Booker, ET)

Sean h y w enteros positivos. Sea χ un carácter de Dirichlet primitivo mod *p, entonces*

$$\sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} < (2w-1)!!p\,h^{w} + (2w-1)\sqrt{p}\,h^{2w}.$$

Bosquejo de la demostración

- $$\sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} = \sum_{l_1,l_2,\ldots,l_{2w}}\ \sum_{x \bmod p}\chi(q(x)),$$

  donde

  $$q(x) = \frac{(x+l_1)(x+l_2)\ldots(x+l_w)}{(x+l_{w+1})(x+l_{w+2})\ldots(x+l_{2w})}.$$

- Si $q(x)$ no es una k-ésima potencia (donde k es el orden de χ), entonces

  $$\left|\sum_{x \bmod p}\chi(q(x))\right| \leq (r-1)\sqrt{p},$$

  donde r es el número de raíces distintas de $q(x)$.

Bosquejo de la demostración

- $$\sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} = \sum_{l_1,l_2,\ldots,l_{2w}}\ \sum_{x \bmod p}\chi(q(x)),$$

  donde

  $$q(x) = \frac{(x+l_1)(x+l_2)\ldots(x+l_w)}{(x+l_{w+1})(x+l_{w+2})\ldots(x+l_{2w})}.$$

- Si $q(x)$ no es una k-ésima potencia (donde k es el orden de χ), entonces

  $$\left|\sum_{x \bmod p}\chi(q(x))\right| \leq (r-1)\sqrt{p},$$

  donde r es el número de raíces distintas de $q(x)$.

Applicaciones

Theorem (ET)

Sea $p > 3$ un primo y k un entero positivo que divide a $p-1$. Sea $g(p,k)$ el mínimo no-residuo de las k potencias mod$p$. *Entonces*

$$g(p,k) \leq \begin{cases} 1.1p^{1/4}\log p & \text{si } p \equiv 3 \bmod 4 \text{ y } k = 2, \\ 0.9p^{1/4}\log p & \text{de lo contrario.} \end{cases}$$

Theorem (ET, 2012)

Si χ es un carácter de Dirichlet no principal módulo p, para p primo, tal que χ es constante en $(N, N+H]$, entonces

$$H \leq \begin{cases} 3.64p^{1/4}\log p, & \text{para todo primo impar } p, \\ 1.55p^{1/4}\log p, & \text{para } p \geq 2.5 \cdot 10^9. \end{cases}$$

Applicaciones

Theorem (ET)

Sea $p > 3$ un primo y k un entero positivo que divide a $p-1$. Sea $g(p,k)$ el mínimo no-residuo de las k potencias mod$p$. *Entonces*

$$g(p,k) \leq \begin{cases} 1.1p^{1/4}\log p & \text{si } p \equiv 3 \bmod 4 \text{ y } k = 2, \\ 0.9p^{1/4}\log p & \text{de lo contrario.} \end{cases}$$

Theorem (ET, 2012)

Si χ es un carácter de Dirichlet no principal módulo p, para p primo, tal que χ es constante en $(N, N+H]$, entonces

$$H \leq \begin{cases} 3.64p^{1/4}\log p, & \text{para todo primo impar } p, \\ 1.55p^{1/4}\log p, & \text{para } p \geq 2.5 \cdot 10^9. \end{cases}$$

Pólya–Vinogradov Lisa

Sean$M$, N números reales tales que $0 < N \leq q$, entonces definamos $S^*(\chi)$ de la siguiente manera:

$$S^*(\chi) = \max_{M,N} \left| \sum_{M \leq n \leq M+2N} \chi(n) \left(1 - \left| \frac{n-M}{N} - 1 \right| \right) \right|.$$

Theorem (Levin, Pomerance, Soundararajan, 2009)

Sea χ un carácter primitivo módulo $q > 1$, y sean M, N reales tales que $0 < N \leq q$, entonces

$$S^*(\chi) \leq \sqrt{q} - \frac{N}{\sqrt{q}}.$$

Cota inferior para la Pólya–Vinogradov lisa

Theorem (ET)

Sea χ un carácter primitivo módulo $q > 1$, y sean M, N reales tales que $0 < N \leq q$, entonces

$$S^*(\chi) \geq \frac{2}{\pi^2}\sqrt{q}.$$

Por lo tanto, el tamaño de $S^*(\chi)$ es del orden de $\sqrt{q}$.

PV lisa con información aritmética

Theorem (ET, 2012)

Sea χ un carácter de Dirichlet primitivo módulo $q > 1$, y sean M, N números reales tales que $0 < N \leq q$. Entonces

$$\left| \sum_{M \leq n \leq M+2N} \chi(n) \left(1 - \left| \frac{n-M}{N} - 1 \right| \right) \right| \leq \frac{\phi(q)}{q} \sqrt{q} + 2^{\omega(q)-1} \frac{N}{\sqrt{q}}.$$

Usando la PV lisa en el problema del mínimo primo inerte

Sea $\chi(p) = \left(\frac{D}{p}\right)$ (el símbolo de Kronecker). Ya que D es una discriminante fundamental, χ es un carácter primitivo módulo D. Consideremos

$$S_\chi(N) = \sum_{n \leq 2N} \chi(n) \left(1 - \left|\frac{n}{N} - 1\right|\right).$$

Entonces por el smoothed PV, tenemos

$$|S_\chi(N)| \leq \frac{\phi(D)}{D}\sqrt{D} + 2^{\omega(D)-1}\frac{N}{\sqrt{D}}.$$

Ahora,

$$S_\chi(N) = \sum_{\substack{n\leq 2N\\(n,D)=1}} \left(1-\left|\frac{n}{N}-1\right|\right) - 2\sum_{\substack{B<p\leq 2N\\ \chi(p)=-1}} \sum_{\substack{n\leq \frac{2N}{p}\\(n,D)=1}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Por lo tanto,

$$\frac{\phi(D)}{D}\sqrt{D}+2^{\omega(D)-1}\frac{N}{\sqrt{D}} \geq \frac{\phi(D)}{D}N-2^{\omega(D)-2}-2\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Ahora, tomando $N = c\sqrt{D}$ para alguna constante c tenemos

$$0 \geq c-1-2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}}-\frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right)$$

Ahora,

$$S_\chi(N) = \sum_{\substack{n\leq 2N\\(n,D)=1}} \left(1-\left|\frac{n}{N}-1\right|\right) - 2\sum_{\substack{B<p\leq 2N\\ \chi(p)=-1}} \sum_{\substack{n\leq \frac{2N}{p}\\(n,D)=1}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Por lo tanto,

$$\frac{\phi(D)}{D}\sqrt{D}+2^{\omega(D)-1}\frac{N}{\sqrt{D}} \geq \frac{\phi(D)}{D}N-2^{\omega(D)-2}-2\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Ahora, tomando $N = c\sqrt{D}$ para alguna constante c tenemos

$$0 \geq c-1-2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}}-\frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right)$$

Ahora,

$$S_\chi(N) = \sum_{\substack{n\leq 2N\\(n,D)=1}} \left(1-\left|\frac{n}{N}-1\right|\right) - 2\sum_{\substack{B<p\leq 2N\\ \chi(p)=-1}} \sum_{\substack{n\leq \frac{2N}{p}\\(n,D)=1}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Por lo tanto,

$$\frac{\phi(D)}{D}\sqrt{D}+2^{\omega(D)-1}\frac{N}{\sqrt{D}} \geq \frac{\phi(D)}{D}N-2^{\omega(D)-2}-2\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Ahora, tomando $N = c\sqrt{D}$ para alguna constante c tenemos

$$0 \geq c-1-2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}}-\frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right)$$

Eventualmente tenemos,

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2c}{\log B} e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) \prod_{\substack{p > \frac{2N}{B} \\ p \mid D}} \frac{p}{p-1}.$$

Para $D \geq 10^{24}$ esto es una contradicción.

Caso Híbrido

Como en el caso anterior, tenemos

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}} \frac{D}{\phi(D)} \sum_{\substack{n \leq \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right)$$

En este caso, como ya no nos tenemos que preocupar por el caso “infinito”, podemos usar una versión más fea de la desigualdad para

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

La idea es considerar 2^{13} casos, uno para cada posibilidad de $\gcd(D, M)$ cuando $M = \prod_{p \leq 41} p$.

- Consideramos los valores pares y nones por separado. Para los nones, después de checar todos los casos, el teorema queda demostrado para todo D mayor o igual a $21853026051351495 = 2.2\ldots \times 10^{16}$.
- Para los pares, queda demostrado para todo D mayor o igual a $1707159924755154870 = 1.71\ldots \times 10^{18}$.
- Como no lo obtuvimos para 1.04×10^{18}, entonces tenemos que trabajar un poco más duro. Encontramos los 12 casos especiales y lidiamos con ellos uno por uno.
- QED.

- Consideramos los valores pares y nones por separado. Para los nones, después de checar todos los casos, el teorema queda demostrado para todo D mayor o igual a $21853026051351495 = 2.2\ldots \times 10^{16}$.
- Para los pares, queda demostrado para todo D mayor o igual a $1707159924755154870 = 1.71\ldots \times 10^{18}$.
- Como no lo obtuvimos para 1.04×10^{18}, entonces tenemos que trabajar un poco más duro. Encontramos los 12 casos especiales y lidiamos con ellos uno por uno.
- QED.

- Consideramos los valores pares y nones por separado. Para los nones, después de checar todos los casos, el teorema queda demostrado para todo D mayor o igual a $21853026051351495 = 2.2\ldots \times 10^{16}$.
- Para los pares, queda demostrado para todo D mayor o igual a $1707159924755154870 = 1.71\ldots \times 10^{18}$.
- Como no lo obtuvimos para 1.04×10^{18}, entonces tenemos que trabajar un poco más duro. Encontramos los 12 casos especiales y lidiamos con ellos uno por uno.
- QED.

- Consideramos los valores pares y nones por separado. Para los nones, después de checar todos los casos, el teorema queda demostrado para todo D mayor o igual a $21853026051351495 = 2.2\ldots \times 10^{16}$.
- Para los pares, queda demostrado para todo D mayor o igual a $17071599247551548 70 = 1.71\ldots \times 10^{18}$.
- Como no lo obtuvimos para 1.04×10^{18}, entonces tenemos que trabajar un poco más duro. Encontramos los 12 casos especiales y lidiamos con ellos uno por uno.
- QED.

Trabajo Próximo

- Generalizar a otros caracteres, no sólo el símbolo de Kronecker.
- Acotar el segundo no-residuo cuadrático.
- Mejorar el resultado de McGown sobre campos cúbicos cíclicos que son norm-Euclidean.
- Atacar el problema de que pasa en promedio.

¡Muchas Gracias!