JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

Distribución del número de puntos en familia de curvas sobre cuerpos finitos

E. Lorenzo[1], G. Meleleo[2], P. Milione[3]

[1] *Universiteit Leiden, The Netherlands, e.lorenzo.garcia@math.leidenuniv.nl*
[2] *Università degli Studi "Roma Tre", Italia, meleleo@mat.uniroma3.it*
[3] *Universitat de Barcelona, España, pmilione@ub.edu*

Uno de los resultados más influyentes en teoría de números es el teorema de densidad de Čebotarev: este generaliza el teorema de Dirichlet sobre la equidistribución de primos racionales en progresión aritmética y proporciona un conocimiento completo de la distribución de los primos en una extensión galoisiana de cuerpos de números fijada. Pasando de cuerpos de números a cuerpos de funciones (en un paralelo que siempre ha enriquecido la teoría de números) nos encontramos con que un problema análogo es considerado por la conjetura de Sato-Tate para curvas: esta estudia la distribución de los endomorfismos de Frobenius de las diferentes reducciones módulo p de un modelo entero de una curva fijada. Este estudio puede continuarse en varias direcciones, una de ellas pudiéndose formular en el problema siguiente: dada una familia de curvas definidas sobre $\mathbf{F}_p$ y de género g, comprender cómo se distribuyen las trazas de los endomorfismos de Frobenius de las curvas dentro de la familia. Los resultados en este sentido pueden encontrarse a veces bajo el nombre de *conjectura de Sato-Tate vertical* pues el primo p es ahora fijado y es la curva que varía dentro de la familia. Ahora bien, dos enfoques diferentes son posibles según si se estudia esta distribución en los límites para g tendiendo a infinito o para p tendiendo a infinito.

Los primeros ejemplos de tales investigaciones consideran familias de curvas hiperelípticas de género g definidas sobre $\mathbf{F}_q$, siendo q una potencia de p: en [5] se estudia la distribución sobre esta familia al q-límite (aplicando un resultado de equidistribución de Deligne) y en el artículo fundador [4] se obtiene la distribución mencionada al g-límite, expresada ahora como suma de $q+1$ variables aleatorias independientes.

A partir de ese momento, históricamente se comienza a tratar este problema de forma sistemática, considerando familias de curvas siempre más generales. Concretamente, en [1] se estudia el caso de familias de curvas que son recubrimientos trigonales cíclico de la recta proyectiva, en [7] se estudia la familia de curvas trigonales y en [2, 3] se consideran ya familias de curvas que son recubrimientos cíclicos de la recta proyectiva, de grado un primo arbitrario ℓ .Dentro de este panorama parece entonces consecuente estudiar estas distribuciones para familias de curvas que constituyen un recubrimiento no cíclico de la recta proyectiva: es por esta razón que en [6] se estudia la familia de curvas cuyo cuerpo de funciones es un recubrimiento bicuadrático de $\mathbf{F}_q(t)$ y se logra calcular para ella la distribución tanto al g-límite como al q-límite.

Con esta exposición se pretende introducir la audiencia a las ideas básicas concernientes las distribución de puntos en familias de curvas sobre cuerpos finitos, con particular atención a los resultados obtenidos en el caso de recubrimientos bicuadráticos. Concretamente, el resultado obtenido es el que se enuncia a continuación.

Sea $\mathscr{B}_g(\mathbf{F}_q)$ la familia de curvas de género g y definidas sobre $\mathbf{F}_q$ que son un recubrimiento bicuadrático de la recta proyectiva $\mathbf{P}_{\mathbf{F}_q}$ sobre $\mathbf{F}_q$ y considérese la descomposición siguiente como unión desjunta de ciertas subfamilias de curvas hiperelípticas:

$$\mathscr{B}_g(\mathbf{F}_q) = \bigcup_{g_1+g_2+g_3=g} \mathscr{B}_{(g_1,g_2,g_3)}(\mathbf{F}_q), \tag{1}$$

en donde $\mathscr{B}_{(g_1,g_2,g_3)}(\mathbf{F}_q)$ denota la subfamilia de curvas $C \in \mathscr{B}_g(\mathbf{F}_q)$ tales que sus tres cocientes hiperelípticos tienen géneros g_1, g_2 y g_3.

Entonces en el límite para g_1, g_2, g_3 tendiendo a infinito, se tiene la distribución siguiente:

$$\frac{|\{C \in \mathscr{B}_{(g_1,g_2,g_3)}(\mathbf{F}_q) : \mathrm{Tr}(\mathrm{Frob}_C) = -M\}|'}{|\mathscr{B}_{(g_1,g_2,g_3)}(\mathbf{F}_q)|'} = \mathrm{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right) \tag{2}$$

en donde X_j son variables aleatorias, independientes e idénticamente distribuidas, tales que

$$X_j = \begin{cases} -1 & \text{with probability} \quad \frac{3(q+2)}{4(q+3)} \\ 1 & \text{with probability} \quad \frac{6}{4(q+3)} \\ 3 & \text{with probability} \quad \frac{q}{4(q+3)} \end{cases} . \tag{3}$$

References

[1] A. Bucur, C. David, B. Feigon, and M. Lalín, *Statistics for traces of cyclic trigonal curves over finite fields*, Int. Math. Res. Not. (2009).

[2] A. Bucur, C. David, B. Feigon, and M. Lalín, *Biased statistics for traces of cyclic p-fold covers over finite fields*, WIN - Women in Number, Fields Institute Communications, American Mathematical Society, (2011).

[3] A. Bucur, C. David, B. Feigon, N. Kaplan, M. Lalín, E. Ozman, and M. Wood, *The distribution of points on cyclic covers of genus g*, (preprint) (2015).

[4] P. Kurlberg and Z. Rudnick, *The fluctuation in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory **129**, 3, pp. 580-587 (2009).

[5] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[6] E.Lorenzo, G. Meleleo and P. Milione, *Statistics for biquadratic covers of the projective line over finite fields*, (preprint), (2015).

[7] M. Wood, *The distribution of the number of points on trigonal curves over* $\mathbf{F}_q$, Int. Math. Res. Not. **2012**, 23, pp. 5444-5456 (2012).