INFORMACIÓN NACIONAL

El trabajo matemático de Pedro Berrizbeitia[1]

T. G. Berry

Pedro Berrizbeitia obtuvo su licenciatura en matemáticas en la Universidad Simón Bolívar en el año 1981. En 1982 fue al MIT para estudiar para su doctorado, que obtuvo, bajo la dirección de Nesmith Ankeny, en 1986, con la tesis "An explicit reciprocity theorem for finite extensions of $\mathbb{Q}_p$". Después de un par de años posdoctorales en Ohio State University, el Dr. Berrizbeitia regresó a Venezuela para incorporarse al Departamento de Matemáticas de la Universidad Simón Bolívar, donde ha estado hasta el presente. Actualmente ocupa la posición de Coordinador de Matemáticas.

Los trabajos de Berrizbeitia abarcan una amplia gama de tópicos matemáticos, desde álgebras C^* a teoría de grafos, pero sus contribuciones más importantes son a la teoría aditiva de números y a la teoría de pruebas de primalidad, y son estos los que se describirán en el presente artículo.

Teoría aditiva de números.

En [19] se prueba:
Teorema. *Sea F un cuerpo, y sea G un subgrupo de índice finito n del grupo multiplicativo F^*. Entonces existe un entero N que depende solo de n tal que, si car $F = 0$ o si car $F > N$ entonces $G - G = F$. Más aún, si $G - G = F$ y $m > 1$ entonces $mG = \{g_1 + \ldots + g_m |\ g_1, \ldots, g_m \in G\} = F$ si, y sólo si, -1$\in (m-1)G$.*

Para el caso en el que F es un cuerpo finito, el teorema de Berrizbeitia es una consecuencia inmediata de resultados clásicos de la Teoría de Números sobre número de soluciones de ecuaciones del tipo $x^m + y^m = t$. Una solución elemental que Berrizbeitia encontró para este problema para el caso $m = 3$ en su estadía en Ohio State University fue lo que dió origen al desarrollo del tema, y en última instancia, al teorema de Berrizbeitia. Por otra parte, el problema está relacionado con el de decidir si un número (racional o tal vez tomado de otro sistema) puede ser escrito como diferencia de dos potencias n-ésimas, o suma de d potencias n-ésimas, donde d y n son enteros positivos dados.

Para probar su teorema, Berrizbeitia introdujo una idea completamente original, que involucraba el uso de un teorema de Van der Waerden, o más precisamente una generalización de este teorema que se debe a Gallai, que

[1]Premio Lorenzo Mendoza Fleury 2005 de la Fundación Polar. Ver Boletín XII, 1.

pertenece al área conocida como "Teoría de Ramsey" y que a primera vista no tiene nada que ver con el tema. El teorema reza como sigue:
Teorema. (Van der Waerden).*Sean dados enteros positivos k, r. Entonces, existe un entero N, que depende de k y de r tal que, si se colorea los enteros $\{1, 2, \ldots N\}$ con r colores, siempre existe una sucesión aritmética monocromática de longitud k.*

El teorema de Gallai es la generalización a $\mathbb{Z}^n$. Este uso de la teoría de Ramsey, originado por Berrizbeitia , ha resultado ser una herramienta muy poderosa en problemas relacionados con el de [19]. Aunque Berrizbeitia mismo no prosiguió el tópico, [2] su paper ha tenido una influencia considerable, como atestiguan [BS],[RA] y [TU].

En colaboración con Peter Elliott, de la Universidad de Colorado en Boulder, Berrizbeitia hizo dos contribuciones ([9] y [12]) adicionales a la teoría aditiva de números, en las cuales se combina teoría analítica de números con ideas combinatorias de Berrizbeitia para producir resultados notables. Por ejemplo, ellos prueban que cualquier número racional que puede ser representado por un producto de números de la forma $p + 1$ o de sus inversos, p primo, puede ser representado por un producto de exactamente 19 tales números.

Pruebas de primalidad.

El problema de decidir si un entero es primo ha fascinado a los matemáticos durante varios siglos. Aqui la opinión de ese olimpiano de las matemáticas, Carl-Friedrich Gauss, en su "Disquisitiones Aritmeticae", (1801). (Este párrafo aparece como el "Abstract" del paper [GR][3]).

> "The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and difficult that even for numbers that do not exceed the limits of tables constructed by estimable men, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers ... It frequently happens

[2]Esto no es estrictamente cierto. El tiene unos resultados aún sin publicar que se espera en algún momento salgan a la luz del día.

[3]Este paper es un survey para matemáticos no-especializados y su lectura resulta muy accesible

> that the trained calculator will be sufficiently rewarded by reducing large numbers to their factors so that it will compensate for the time spent. Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated ... It is in the nature of the problem that any method will become more complicated as the numbers get larger. Nevertheless, in the following methods the difficulties increase rather slowly ... The techniques that were previously known would require intolerable labor even for the most indefatigable calculator."

En términos modernos, los métodos tales que "the difficulties increase rather slowly" son algorítmos que involucran un número de operaciones sobre bits que es una función polinomial del tamaño del input. Dicho tamaño, para el input n, es el número de bits en el desarollo binario de n, que es $\lceil \log n \rceil$. (log significa $\log_2$ siempre). En la notación O, pues, se buscan algorítmos que son $O(\log^k n)$ para algún k.

Desde el siglo 17, cuando empieza, con Fermat, la época moderna de los estudios de primalidad, hasta tiempos relativamente recientes, se consideraba principalmente el problema de hallar criterios para la primalidad de números de forma especial, como los números de Fermat $2^{2^n}+1$ y los números de Mersenne 2^p-1 (p primo). Con la llegada de las computadoras, y más particularmente con el invento de ciertos criptosistemas, muy usados en el Internet, cuyo funcionamiento requiere hallar unos números primos grandes (alrededor de 150 cifras decimales actualmente), el énfasis cambió hacia el de hallar criterios para decidir si un entero arbitrario es primo.

Berrizbeitia ha contribuido en ambas corrientes. Los trabajos publicados [2-8,11] tratan de pruebas de primalidad para números de forma especial. En estos trabajos, se generalizan unas ideas del siglo 19, que usan la reciprocidad cuadrática para producir criterios de primalidad para números de Fermat y más generalmente números $A2^n \pm 1$. Para entender el uso de reciprocidad, he aquí el bisabuelo de todas las pruebas, la de Pépin para los números de Fermat. Primero, hay que recordar la definición y propiedades del símbolo de Legendre. Sea p un primo y a un entero no divisible entre p. Se define el símbolo de Legendre $\left(\frac{a}{p}\right)$ por

$$\begin{aligned}\left(\frac{a}{p}\right) &= +1 \text{ si } x^2 \equiv a \bmod p \text{ tiene solución} \\ &= -1 \text{ si no}\end{aligned}$$

Se tiene
Propiedad 1.

$$\left(\frac{a}{b}\right) \equiv a^{p-1/2} \bmod p$$

y, la joya en la corona, la Ley de Reciprocidad Cuadrática:
Propiedad 2. Si p y q son primos impares, entonces

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ si } p \text{ y } q \text{ son ambos } \equiv 3 \bmod 4$$
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ en todo otro caso}$$

La ley de reciprocidad cuadrática usualmente se completa con *ansätze* evaluando $\left(\frac{2}{p}\right)$ y $\left(\frac{-1}{p}\right)$, pero no necesitamos estos aquí.

Ahora podemos dar el criterio de Pépin.
Teorema. *Sea $F_n = 2^{2^n}+1$ el n-esimo número de Fermat. Entonces F_n es primo si y sólo si $3^{F_n-1/2} \equiv -1 \bmod F_n$.*
Dem. Suponga primero que F_n sea primo. Entonces, por la ley de reciprocidad cuadrática $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$. Pero, ya que, por la definición, el valor de $\left(\frac{a}{p}\right)$ depende solamente de la clase de $a \bmod p$, y $F_n = 2^{2^n}+1 \equiv (-1)^{2^n}+1 \equiv 2 \bmod 3$, se tiene $\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$ este último puesto que, por inspección, 2 no es un cuadrado mod 3. Asi $\left(\frac{F_n}{3}\right) = -1$, y, usando Propiedad 1

$$3^{F_n-1/2} \equiv -1 \bmod F_n$$

Para la recíproca, suponga que la congruencia arriba está satisfecha, y sea q un divisor primo de F_n. Vamos a mostrar que $q \geq F_n$, seguramente implica que F_n es primo. De hecho, la congruencia mod F_n implica que también $3^{F_n-1/2} \equiv -1 \bmod q$ puesto que q divide a F_n. Esto dice que 3 tiene orden $F_n - 1$ en el grupo $(\mathbb{Z}/(q))^*$, que a su vez implica $F_n - 1$ divide a $q-1$, y se concluye $q \geq F_n$.

En el siglo 19 Proth generalizó el método de Pépin para dar criterios de primalidad para números $A2^n + 1$, donde $A \leq 2^n$. Resulta que la famosa prueba de Lucas-Lehmer para primalidad de los números de Mersenne también se puede establecer usando reciprocidad cuadrática, aunque esta no es la demostración original. Berrizbeitia y colaboradores generalizaron todos estos resultados, dando criterios muy eficientes para números $Ap^s \pm 1$ para una variedad de primos p y un criterio algo menos eficiente para números $Am^s \pm 1$. Aún cuando criterios similares habían sido propuestos por Hugh Williams, (de la Universidad de Calgary) y colaboradores en la década de los 70, la metodología usada por Berrizbeitia y colaboradores resultó más clara y eficiente. Para estas generalizaciones se usa el análogo del símbolo de Legendre, el "símbolo de potencia residual", que trata de potencias s-ésimas mod p, con $s > 2$, y que toma sus valores en las raíces s-ésimas de la unidad, y que satisface una "ley de reciprocidad superior". Las demostraciones de estos criterios generales todas siguen el patrón de Pépin: el criterio de primalidad de N implica, si N es primo, mediante uso de las propiedades básicas del símbolo que cierta ecuación

debe cumplirse. En la otra dirección, las hipótesis implican la existencia de un elemento de orden muy grande en cierto grupo asociado con un supuesto divisor primo, lo que implica que el divisor resulta $> \sqrt{N}$. Sin embargo, el manejo del símbolo de potencia residual no es nada fácil, y presenta muchas dificultades técnicas, la principal deriva del hecho que el anillo $\mathbb{Z}[e^{2\pi i/s}]$ en general no es un dominio de factorización única. En los trabajos [2,5-7,11] se ve como domina Berrizbeitia el andamio conceptual y las técnicas computacionales de la teoría de reciprocidad superior.

El trabajo [3] introduce otro método elemental pero astuto para probar primalidad. Allí se extiende la noción de Pseudocuadrados, introducida por Lehmer hace más de 50 años, a la de Pseudocubos. Según Bernstein, la técnica de primalidad basada en la teoría de pseudocuadrados deriva en el algoritmo más eficiente de primalidad para números de hasta 80 dígitos binarios. Hugh Williams había estado trabajando en la posibilidad de extender esa noción desde hace muchos años. Es la técnica introducida por Berrizbeitia la que finalmente hace que esta extensión se haya logrado en [3]. Desde el punto de vista práctico, el algoritmo presentado en [3], basado en la noción de pseudocubos supera al algoritmo basado en la noción de pseudocuadrados.

El trabajo [8] trata de una técnica diferente, la de pruebas probabilistas de primalidad, que permiten concluir que un entero es "probablemente primo", con probabilidad de error no mayor que cierta cantidad pequeña. Aunque sobreseido como prueba general, la prueba de este trabajo sigue siendo útil para ciertos números de forma especial, como por ejemplo $1 + a + a^2 + \cdots + a^{p-1}$, p primo, a cualquiera.

Finalmente, llegamos al trabajo [1], que es una contribución a la búsqueda de un criterio de primalidad de un entero arbitrario, sin forma especial. Es seguramente la contribución de mayor impacto internacional que ha obtenido hasta ahora Berrizbeitia . El contexto es el siguiente. El objetivo es tener un algoritmo polinomial, es decir $O(\log^k n)$ para algun k, que decide la primalidad de n. Los algoritmos conocidos hasta la decada de los ochenta del siglo pasado eran, por contraste, *exponenciales*, es decir $O(k^{\log n})$ en vez de $O(\log^k n)$.

En los años 80, Adleman, Pomerance, Rumely Cohen y Lenstra desarollaron, mediante el uso de métodos muy sofisticados de la teoría álgebraica de números, un algorítmo entre polinomial y exponencial, y al que en realidad le faltaba poco para ser polinomial. (Este algorítmo, conocido en honor a sus inventores como APRCL, sigue siendo en la práctica el más rápido conocido.) Por casi veinte años no hubo progreso significativo hacia un algorítmo verdaderamente polinomial, hasta que, en agosto 2002, tres hindúes, Agrawal, Kayal y Saxena, dejaron atónito al mundo matemático cuando publicaron como preprint un tal algorítmo (llamado ahora algorítmo AKS), basado en ideas bastante elementales. Se sigue con una reseña muy breve del algorítmo AKS.

Todo empieza con el pequeño teorema de Fermat:
Teorema F1. *Si p es primo y a un entero, entonces $a^p \equiv a \bmod p$.*
La recíproca es incierta, asi que el teorema no da un criterio de primalidad. Pero, al nivel de polinomios, se tiene:
Teorema F2. *El entero n es primo si y solo si $(x+1)^n \equiv x+1 \bmod n$.*
Sin embargo, y en contraste la situación con enteros, la complejidad del cálculo de $(x+1)^n \bmod n$ es exponencial, asi que F2 tampoco brinde un criterio polinomial para la primalidad de n. Fue el genio de los tres Hindúes el ver que F2, conocido y despreciado por todos los han trabajado en el campo, podia modificarse a dar un criterio polinomial. Ellos probaron[4]:
Lema (AKS). *Sea n un entero positivo. Entones existe $r \leq \lceil 16 \log^5 n \rceil$ tal que el orden de n mod r es $> 4 \log^2 n$.*
Teorema (AKS). *Sea n un entero positivo y r como en el lema AKS. Suponga que:*

1. *n no tiene divisores menores que $\sqrt{r} \log n$.*
2. *n no es una potencia (≥ 2) de un primo.*
3. *$(a+x)^n \equiv a + x \bmod (n, x^r - 1)$ para todo a tal que $0 < a < \sqrt{r} \log n$.*

Entonces, n es primo.

Un cálculo demuestra que usar el teorema para determinar la primalidad de n es de complejidad $\tilde{O}(\log^{10.5} n)$.[5] El punto clave es que el cálculo de $(a + x)^n \bmod (n, x^r - 1)$ se vuelve polinomial debido al término $(x^r - 1)$ en el módulo.

La demostración es por contradicción. Suponga que n satisface las hipótesis del teorema AKS pero es compuesto (de manera que n tiene por lo menos dos factores primos). Sea p un factor primo de n, y sea $h(x)$ un factor del polinomio ciclotómico $\phi_r(x)$ irreducible en $\mathbb{Z}_p[x]$. Para m fijo los polinomios $g(x) \in \mathbb{Z}[x]$ tales que $g(x)^m \equiv g(x^m) \bmod (p, x^r - 1)$ generan un subgrupo G del grupo multiplicative del cuerpo $\mathbb{Z}_p[x]/(h)$ y la hipótesis (iii) del teorema AKS provee miembros de G (y m escogido apropriadamente). Mediante un argumento de tipo combinatorio se prueba que estos elementos generan un subgrupo grande de G, lo que provee una cota inferior para el orden de G, y por otro lado se prueba que si n tiene por lo menos dos factores primos el orden de G es menor que la cota inferior calculada, una contradicción.

La aparición del preprint AKS desató un "feeding frenzy" entre los especialistas de la materia. En el original los autores probaron que el algorítmo era de complejidad $\tilde{O}(\log^{12} n)$. Por los esfuerzos de varios matemáticos destacados esto se mejoró a $\tilde{O}(\log^6 n)$, pero las mejoras se obtuvieron esencialmente debido a un análisis más fino del algorítmo, y no por mejoras en el algorítmo mismo.

[4]La versión dada aqui es la de la segunda versión del preprint, que ya incorpora unas mejoras.

[5]$\tilde{O}(f(k))$ significa $O(f(k)g(\log f(k))$ donde g es un polinomial.

En noviembre 2003 Berrizbeitia publicó un preprint, en el cual, usando ideas nuevas, y evidentemente influido por sus trabajos anteriores sobre pruebas de primalidad para números de forma especial, él produjó una modificación de AKS que para una familia grande de números es $\tilde{O}(\log^4 n)$. La versión final del teorema apareció en [1], con r una potencia de 2 y $n \equiv 1 \bmod 4$. La generalización a todo r se debe a Bernstein y Mihalescu-Avanzi, independientemente.
Teorema. *Sea n un entero positivo, y sea r un divisor de $n-1$, y suponga que $c\log^2 n > r > \log^2 n$, donde c es una constante que no depende de n. Suponga además que si d divide a n entonces $\equiv 1 \bmod r$. Sea a un entero tal que $\omega = a^{n-1/r}$ tiene orden r mod n, y también mod cualquier divisor primo de n. Suponga*

1. *n no tiene divisores primos menores que r.*
2. *n no es una potencia (≥ 2) de un primo.*
3. *$(1+x)^n \equiv 1 + x^n \bmod (n, x^r - a)$ Entonces, n es primo.*

Claro, la gran ventaja de este sobre el AKS original yace en (3), que requiere una sóla exponenciación polinomial en vez de $\sqrt{r}\log n - 1$.

Trabajos subsecuentes de D. Bernstein y otros han logrado extender las ideas de Berrizbeitia hasta el punto en que ahora se tiene un algorítmo $\tilde{O}(\log^4 n)$ para todos los enteros. Ver [BN] para las últimas noticias. A Berrizbeitia le queda el crédito de haber suministrado la idea fundamental sin la cual no se habría logrado la mejora de $\tilde{O}(\log^6 n)$ a $\tilde{O}(\log^4 n)$, mejora que deja AKS al borde de ser el mejor algorítmo tanto en la práctica como en la teoría para probar primalidad.

Referencias

[BN] D. J. Bernstein. *Distinguishing prime numbers from composite numbers: the state of the art in 2004.* URL: http://cr.yp.to/papers.html#prime2004

[BS] V. Bergelson and D. Shapiro. *Multiplicative subgroups of finite index in a ring.* Proc. Amer. Math.Soc. 116 (1992) 885-896.

[GR] Andrew Granville. *It is easy to determine whether a given integer is prime.* Bull. Amer. Math. Soc. 42 (2005), 3-38. (Disponible gratis on-line. URL: www.ams.org/journals).

[RA] Rapinchuk, Andrei S.; Segev, Yoav; Seitz, Gary M.*Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable.* J. Amer. Math. Soc. 15 (2002), no. 4, 929–978

[TU] Gerhardt Turnwald. *Multiplicative subgroups of finite index in a division ring.* Proc. Amer. Math.Soc. 120 (1994) 377-381.

Publicaciones de Pedro Berrizbeitia

1. P. Berrizbeitia *Sharpening "Primes is P" for a large family of numbers* Math. of Comp. Vol. 74 , num 252, pp. 2043–2059 (2005).

2. P. Berrizbeitia y T. G. Berry. *Biquadratic reciprocity and a Lucasian primality test.* Math. Comp. Vol 73, pp. 1559–1564 (2004).

3. P. Berrizbeitia, S. Mueller y H. C. Williams. *Pseudocubes and Primality Testing.* Proceedings of ANTS VI. Lecture Notes in Computer Science (LNCS). Vol. 3076. pp. 102–116 (2004).

4. P. Berrizbeitia y R. Giudici. *On Cycles in the sequence of Unitary Cayley Graphs.* Discrete Math. Vol. 282, no.1-3, pp. 239–243 (2004).

5. P. Berrizbeitia, T. G. Berry, y J. Tena-Ayuso. *A Generalization of the Proth Theorem.* Acta Arithmetica. 110.2, 107–115 (2003).

6. P. Berrizbeitia, M. Odreman y J. Tena. *Primality Test for Numbers M with a high power of* 5 *dividing* $M^4 - 1$. Latin American Theoretical Informatics (Punta del Este, 2000). Theor. Comp. Sci. 297, no.1-3, 25–36 (2003).

7. P. Berrizbeitia. *Pruebas Determinísticas de Primalidad.* Gaceta Real Ac. Esp. Vol. 4, no. 2, 447–456 (2001).

8. P. Berrizbeitia y B. Iskra. *Deterministic primality test for numbers of the form* $A^2 3^n + 1, n > 3$ *odd.* Proc. Am. Math. Soc. Vol 130, Num 2, 363–365. (2001).

9. P. Berrizbeitia y T.G. Berry. *Generalized Strong Pseudoprime Tests and Applications.* J. Symb. Comp. 30, No. 2, 151–160. (2000).

10. P. Berrizbeitia y P.D.T.A. Elliott. *Product Basis for the Rationals.* Canad. Math. Bull. 42, No. 4, 441–444. (1999).

11. P. Berrizbeitia y T.G. Berry. *Cubic Reciprocity and Generalised Lucas-Lehmer Tests for Primality of* $A3^n \pm 1$. Proc. Amer. Math. Soc. 127, no.7, 1923–1925. (1999).

12. J.L. Palacios, J.M. Renom, P. Berrizbeitia. *Random walks on edge-transitive graphs.* Stat. and Prob. Lett. 43, No. 1, 25–32. (1999).

13. P. Berrizbeitia y P.D.T.A. Elliott. *On Product of Shifted Primes. Paul ErdL·Ls(1913-1996)* Ramanujam J. 2, no 1–2, pp 219–223. (1998).

14. P. Berrizbeitia y R. Giudici. *Counting K-cycles in Unitary Cayley Graphs.* Disc. Math. vol. 149, 11–18. (1996).

15. P. Berrizbeitia. *A note on Fixed Points of Polynomials*. Acta Científica Venezolana. Vol 46, No.3, 159–160. (1995).

16. P. Berrizbeitia. *Additive Properties of Multiplicative Subgroups of Finite Index in Fields*. Proc. Amer. Math. Soc., volume 112, No. 2, 365–369. (1991).

17. P. Berrizbeitia, L. Mata-Lorenzo y L. Recht. *A uniqueness Theorem for the Unitary Part of a Reflexion*. Jour. of Math. Analysis and App. Vol 152, No.2, 448–454. (1990).

Monografías

1. P. Berrizbeitia. *Algoritmos Deterministas de Primalidad*. XVII Escuela Venezolana de Matemáticas, Asociación Matemática Venezolana, Centro de Estudios Avanzados, Ivic. Caracas, Venezuela. 2004. ISBN: 980-261-077-1.

2. P. Berrizbeitia. Algunos Aspectos Introductorios de la Teoría de Números. IV Escuela Venezolana de Matemáticas, A.M.V., C.E.A., I.V.I.C. Caracas, Venezuela. 1991.