Matemática Universitária Nº 9/10, dezembro de 1989

Raizes Primitivas e a Conjectura de Artin

José Felipe Voloch

IMPA
Estrada Dona Castorina, 110
22460 Rio de Janeiro

Ao Elon, nos seus 60 anos, com um abraço

1. Raízes primitivas.

Dado um número primo p, uma *raiz primitiva módulo* p é um inteiro g tal que todo inteiro não divisível por p é congruente a uma potência de g módulo p.

Em outras palavras, uma raiz primitiva g módulo p é um inteiro cuja classe gera o grupo cíclico multiplicativo $(\mathbf{Z}/p\mathbf{Z})^x = \mathbf{Z}/p\mathbf{Z} - \{0\}$. Provaremos adiante que, de fato, $(\mathbf{Z}/p\mathbf{Z})^x$ é cíclico para todo primo p e, conseqüentemente, existem raízes primitivas módulo p. Esse fato foi primeiramente provado por Gauss.

O nome raiz primitiva provém da analogia com as raízes da unidade, já que todo elemento $x \in (\mathbf{Z}/p\mathbf{Z})^x$ satisfaz $x^{p-1} \equiv 1 \pmod{p}$, isto é, são "raízes $(p-1)$-ésimas da unidade". Esse resultado é conhecido como pequeno Teorema de Fermat.

Raízes primitivas são muito úteis para cálculos módulo p. Em particular, é bastante conveniente quando 10 é uma raiz primitiva módulo p, pois sabemos quem são as potências de 10 sem fazer conta. Já um computador fica feliz quando 2 é raiz primitiva módulo p. Existe ainda uma maneira simples de ver se 10 é raiz primitiva módulo p, isso ocorre se e somente se o período da expansão decimal da fração $1/p$ é $p-1$. (Prove!)

Quão freqüentemente 10 é raiz primitiva módulo p? Gauss já havia notado que isse ocorre para aproximadamente um terço dos primos, até onde ele fez as contas. Um número mais preciso: 37,396% dos primos tem 10 como raiz primitiva . Que sentido faz isso e de onde vem esse número? Responderemos a essa pergunta no §2. Antes porém vamos demonstrar o resultado de Gauss mencionado acima com uma das duas provas que ele mesmo deu ([5] art. 55).

Teorema (Gauss). *Se p é um número primo então $(\mathbf{Z}/p\mathbf{Z})^x$ é um grupo cíclico.*

PROVA: Lembremos que $\mathbf{Z}/p\mathbf{Z}$ é um corpo e que, num corpo, um polinômio não nulo de grau n tem, no máximo, n raízes. Segue-se que para cada $d > 1$, $d|(p-1)$ existe $x \not\equiv 0(p)$ tal que $x^{(p-1)/d} \not\equiv 1(p)$, já que $p > (p-1)/d + 1$.

Seja $p - 1 = q_1^{r_1} \dots q_m^{r_m}$ a fatoração de $p-1$ em primos, onde $q_1, \dots, q_m$ são primos distintos. Aplicando a observação acima obtemos, para $i = 1, \dots, m$, um inteiro b_i, tal que $b_i \not\equiv 0(p)$ e $b_i^{(p-1)/q_i} \not\equiv 1(p)$. Note agora que $c_i = b_i^{(p-1)/q_i^{r_i}}$ tem ordem $q_i^{r_i}$. De fato a ordem de c_i divide $q_i^{r_i}$ e, se dividisse $q_i^{r_i-1}$, teríamos $b_i^{(p-1)/q_i} = c_i^{q_i^{r_i-1}} \equiv 1(p)$, absurdo. Não é difícil então verificar que $g = c_1 \dots c_m$ tem ordem $p-1$, isto é, g é uma raiz primitiva módulo p.

2. A conjectura de Artin.

Lembremos que o conjunto dos números primos é infinito e, mais ainda, se x é um número grande existem aproximadamente $x/\log x$ primos entre 0 e x como nos diz o teorema dos números primos de Hadamard e de la Valleé-Poussin. (O leitor interessado pode consultar [**10**] para uma discussão informal e [1] para uma prova simples desse teorema).

Artin conjecturou (veja [**3**], introdução) que, dado um inteiro $g \neq 0, \pm 1$ e que não é um quadrado perfeito, g é raiz primitiva módulo p para uma infinidade de primos p e, mais ainda, o número desses primos menores que x para x grande deveria ser aproximadamente $C(g)x/\log x$ para uma certa constante $C(g) > 0$. (Por exemplo $C(10) = 0,37396\dots$). Que $g = 0, \pm 1$ têm de ser excluídos, é claro. Se $g = h^2$ e p é um primo ímpar, $p \not| g$, então,

$g^{(p-1)/2} \equiv h^{p-1} \equiv 1(p)$ e g não é raiz primitiva módulo p, por isso os quadrados são excluídos também.

A origem da conjectura é o seguinte raciocínio heuristico:

Se p é um primo e g não é uma raiz primitiva módulo p então o subgrupo gerado por g em $(\mathbf{Z}/p\mathbf{Z})^x$ tem um certo índice $d > 1$ o qual é divisível por um certo primo ℓ. Temos então que $\ell|(p-1) = \#(\mathbf{Z}/p\mathbf{Z})^x$ e $g^{(p-1)/\ell} \equiv 1(p)$.

Vamos contar, para um primo ℓ fixo, os primos p que satisfazem $p \equiv 1(\ell)$ e $g^{(p-1)/\ell} \equiv 1(p)$. Primeiramente existem ℓ classes módulo ℓ mas um primo $p \neq \ell$ nunca satisfaz $p \equiv 0(\ell)$; por outro lado entre as outras classes nenhuma é privilegiada, logo a probabilidade de um primo p safisfazer $p \equiv 1(\ell)$ é $1/(\ell-1)$. (Isso é corroborado pelo teorema dos números primos em progressões aritméticas, ver [1]). Se $p \equiv 1(\ell)$ seja $a = g^{(p-1)/\ell}$, então $a^\ell \equiv 1(p)$. Por outro lado existem ℓ soluções de $x^\ell \equiv 1(p)$ e nenhuma delas é privilegiada logo a probabilidade de que $a \equiv 1(p)$ é $1/\ell$ (a justificativa desse raciocínio é dada pelo difícil teorema de Chebotarev). Vemos então que a proporção dos primos satisfazendo $p \equiv 1(\ell)$ e $g^{(p-1)/\ell} \equiv 1(p)$ é $1/\ell(\ell-1)$. Logo a proporção dos primos que não safisfazem isso é $1 - 1/\ell(\ell-1)$. Se essas condições fossem independentes, a proporção dos primos que não as satisfazem para nenhum ℓ (isto é, aqueles primos para os quais g é raiz primitiva) seria $C = \prod_{\ell \text{primo}} (1 - 1/\ell(\ell-1)) = 0.37396\ldots$!

Infelizmente essas condições não são independentes. Por exemplo se g é livre de quadrados (i.e., é produto de primos distintos) e $g \equiv 1(4)$ então se p satisfaz $p \equiv 1(\ell)$, $g^{(p-1)/\ell} \equiv 1(p)$ para cada primo $\ell|g$ então $g^{(p-1)/2} \equiv 1(p)$. Para ver isso, note que p é quadrado módulo ℓ para cada $\ell|g$ logo, pela lei de reciprocidade quadrática,

$$(\frac{g}{p}) = \prod_{\ell|g}(\frac{\ell}{p}) = \prod_{\ell|g}(\frac{p}{\ell})(-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\sum_{\ell|g}(\ell-1)/2}.$$

Porém $\sum_{\ell|g}(\ell-1)/2 \equiv (g-1)/2 \equiv 0\ (2)$, por hipótese. Logo $g^{(p-1)/2} \equiv 1(p)$.

Em casos como o acima o raciocínio que leva a conjectura de Artin deve ser modificado e dá um valor diferente de C para $C(g)$. Mas se, por exemplo, g é livre de quadrados e $g \not\equiv 1(4)$ (por

exemplo $g = 2$ ou 10) então a conjectura de Artin deve valer com $C(g) = C = \prod_{\ell}(1 - 1/\ell(\ell - 1))$.

Em [7], Hooley demonstrou que, supondo-se a validade da chamada Hipótese de Riemann Generalizada, a conjectura de Artin é verdadeira. Sem nenhuma hipótese adicional o melhor resultado é o de Heath-Brown ([8]) que melhorou idéias de Gupta e Murty.

O resultado completo de Heath-Brown é complicado de enunciar mas algumas conseqüências são que "quase todos" os inteiros g são raízes primitivas para uma infinidade de primos e que no máximo dois primos g são raízes primitivas para apenas um número finito de primos (mas não sabemos quem são essas duas possíveis exceções!).

3. Um problema análogo.

Seja q uma potência de um número primo e $\mathbf{F}_q$ o corpo finito de q elementos. O anel de polinômios $\mathbf{F}_q[x]$ se comporta de maneira muito parecida a $\mathbf{Z}$. Por exemplo vale a fatoração única de polinômios em polinômios irredutíveis (que fazem o papel dos primos) a menos de constantes (ver [6] cap. I). Também vale que se $f(x) \in \mathbf{F}_q[x]$ é irredutível então $\mathbf{F}_q[x]/(f(x))$ é um corpo finito. Segue que $(\mathbf{F}_q[x]/(f(x)))^x$ é um grupo finito cíclico como se mostra com uma prova análoga a feita acima para $\mathbf{Z}$.

Dado $g(x) \in \mathbf{F}_q[x]$ podemos então formular o seguinte análogo da conjectura de Artin: será que há infinitos polinômios irredutíveis $f(x)$ tais que a classe de $g(x)$ módulo $f(x)$ gera o grupo cíclico $(\mathbf{F}_q[x]/(f(x)))^x$? Claramente a resposta sera não se $g(x) \in \mathbf{F}_q$ ou se $g(x)$ é uma potência d-ésima em $\mathbf{F}_q[x]$ para algun $d > 1$, $d|(q-1)$. Nos outros casos vale o seguinte Teorema ([4]) que provaremos a seguir:

Teorema (Bilharz). *Se $g(x) \in \mathbf{F}_q[x]$, $g(x) \notin \mathbf{F}_q$ não é uma potência d-ésima para nenhum $d > 1$ $d|(q-1)$ então existem infinitos polinômios irredutíveis $f(x) \in \mathbf{F}_q[x]$, tais que $g(x)$ gera o grupo multiplicativo $(\mathbf{F}_q[x]/(f(x)))^x$.*

PROVA: Se $f(x)$ é um polinômio irredutível de grau n então $\mathbf{F}_q[x]/(f(x))$ é isomorfo a $\mathbf{F}_{q^n}$ o corpo de q^n elementos. Um isomorfismo é obtido passando ao quociente a aplicação $\mathbf{F}_q[x] \to \mathbf{F}_{q^n}$

que manda x em $\alpha \in \mathbf{F}_{q^n}$, onde $f(\alpha) = 0$. Por esse isomorfismo a classe de $g(x)$ fica sendo $g(\alpha)$. Reciprocamente, se $\alpha \in \mathbf{F}_{q^n}$ é tal que $\mathbf{F}_{q^n} = \mathbf{F}_q[\alpha]$ então α satisfaz uma equação irredutível $f(\alpha) = 0$ de grau n. Note também que se $\alpha \in \mathbf{F}_{q^d}$, $d < n$, $d|n$, então $g(\alpha) \in \mathbf{F}_{q^d}$ logo não pode gerar o grupo multiplicativo $\mathbf{F}_{q^n}^x$. Com isso em mente vamos que para provar o teorema basta provar que para todo n suficientemente grande existe $\alpha \in \mathbf{F}_{q^n}$ tal que $g(\alpha)$ gera $\mathbf{F}_{q^n}^x$. Seja então $M = M_n = \#\{\alpha \in \mathbf{F}_{q^n} \mid g(\alpha) \text{ gera } \mathbf{F}_{q^n}^x\}$. Provaremos que dado $\varepsilon > 0$ existe C_ε tal que

$$|M_n - \varphi(q^n - 1)| \leq C_\varepsilon (\deg g) q^{\frac{1}{2}n+\varepsilon} \tag{1}$$

Onde φ é a função de Euler. O resultado segue então dessa desigualdade.

Para provar a desigualdade (1) vamos usar o seguinte resultado que é caso especial da chamada hipótese de Riemann para curvas, provadada por Weil (uma prova elementar desse resultado pode ser vista em [9]).

Se $g(x)$ não é potência d'-ésima pra nenhum $d' > 1$, $d'|d$ então

$$\left|\#\{(x,y) \in \mathbf{F}_{q^n} \times \mathbf{F}_{q^n} \mid y^d = g(x)\} - q^n\right| \leq d/\deg g \cdot q^{n/2}.$$

Seja $d|(q^n - 1)$ e $N_d = \#\{\alpha \in \mathbf{F}_{q^n} \mid g(\alpha) \text{ é potência } d\text{-ésima}\}$ então pela desigualdade acima, e pelas hipóteses, $|N_d - q^n/d| \leq \deg g \cdot q^{n/2}$. Por outro lado é fácil ver que

$$M = \sum_{d|(q^n-1)} \mu(d) N_d$$

onde μ é a função de Möbius definida por

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^r, & n = \ell_1 \ldots \ell_r, \ell_1, \ldots, \ell_r \text{ primos distintos} \\ 0, & \text{caso contrário.} \end{cases}$$

Finalmente, escrevendo $N_d = q^n/d + R_d$

$$M = q^n \sum_{d|(q^n-1)} \frac{\mu(d)}{d} + \sum_{d|(q^n-1)} \mu(d) R_d.$$

Pela fórmula de Euler, $\varphi(m) = m \prod_{\substack{\ell \mid m \\ \ell \text{ primo}}} (1 - l/\ell) = m \sum_{d \mid m} \mu(d)/d$,

logo:

$$M = \frac{q^n}{(q^n-1)}\varphi(q^n-1) + \sum_{d \mid (q^n-1)} \mu(d) R_d$$

$$= \varphi(q^n-1) - \frac{\varphi(q^n-1)}{q^n-1} + \sum_{d \mid (q^n-1)} \mu(d) R_d.$$

A desigualdade (1) então segue de propriedades conhecidas da função μ em particular que $\sum_{d \mid m} |\mu(d)| = d(m) = 0(m^\varepsilon)$, $\forall \varepsilon > 0$. (Ver [2] 13.10).

Bibliografia

1. Aarão, J.O.G., *O teorema dos números primos Dissertação de Mestrado*, Informes de Matemática Série E nº 032, IMPA (1989).
2. Apostol, T., "Introduction to analytic number theory," Springer.
3. Artin, E., "Collected Papers," S. Lang and S. Tate, eds..
4. Bilharz, H., *Prinsdivisoren mit Vorgegebener Primitivwurzel*, Math. Ann. **114** (1937), 476–492.
5. Gauss, C.F., "Disquisitiones Arithmeticae," Tradução em ingles, Springer.
6. Garcia, A. e Lequain, Y., "Algebra: Um Curso de Introdução," IMPA, Rio de Janeiro, 1989.
7. Hooley, C., *On Artin's conjecture*, Crelle **225** (1967), 209–220.
8. Heath-Brown, D.R., *On Artin's conjecture*, Quarterly J. of Maths. (2) **37** (1986), 39–47.
9. Schimidt, W.M., "Equations Over Finite Fields, an Elementary Approach," LNM 536, Springer, Heidelberg, 1976.
10. Voloch, J.F., *O teorema dos números primos*, Matemática Universitária **6** (1988).