O retorno de Eisenstein: reciprocidade cúbica (participações especiais: Gauss e Jacobi)

Um dos teoremas favoritos de Gauss é a *lei da reciprocidade quadrática*, enunciada a seguir: definimos o símbolo de Legendre por

$$\left(\frac{c}{p}\right) = \begin{cases} 0 & \text{se } p \mid c \\ 1 & \text{se } c \text{ é resíduo quadrático mód } p \\ -1 & \text{se } c \text{ não é resíduo quadrático mód } p \end{cases}$$

Teorema da reciprocidade quadrática. *Sejam p e q primos ímpares positivos. Então*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Além disso, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Você deve provar sem dificuldades as seguintes propriedades:

Propriedades do símbolo de Legendre. *Sejam a, b inteiros e p primo ímpar. Então*

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
- *Se* $a \equiv b \pmod{p}$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ∎

Vamos começar o nosso estudo com uma demonstração desse teorema diferente da mostrada em [2], com o auxílio de números complexos.

1. Alguns fatos preliminares

1.1. Critério de Euler

Uma das ferramentas mais úteis para o nosso estudo é o *critério de Euler*:

Critério de Euler. *Seja p primo, m inteiro positivo e a um inteiro não múltiplo de p. Então a congruência $x^m \equiv a \pmod{p}$ tem solução se, e somente se,*

$$a^{(p-1)/d} \equiv 1 \pmod{p},$$

sendo $d = \text{mdc}(m, p-1)$.

Demonstração

Seja g uma raiz primitiva de p. Então existem k e y tais que $a \equiv g^k \pmod{p}$ e $x \equiv g^y \pmod{p}$. Assim, $x^m \equiv a \pmod{p} \iff g^{my} \equiv g^k \pmod{p} \iff my \equiv k \pmod{p-1}$. Essa equação em y admite solução se, e somente se, $\text{mdc}(m, p-1) \mid k \iff d \mid k$.

Por outro lado, $a^{(p-1)/d} \equiv 1 \pmod{p} \iff g^{(p-1)k/d} \equiv 1 \pmod{p} \iff p-1 \mid (p-1)k/d \iff k \mid d$, de modo que a demonstração está completa.

Vale a pena notar que a equação é equivalente a $y \equiv \frac{k}{d}\left(\frac{m}{d}\right)^{-1} \pmod{\frac{p-1}{d}}$, e considerando que y deve ser considerado módulo $p-1$, admite exatamente d soluções, a saber, $\frac{k}{d}\left(\frac{m}{d}\right)^{-1}$ mód $\frac{p-1}{d} + t\frac{p-1}{d}$, $t = 0, 1, 2, \ldots, d-1$. ∎

1.2. Inteiros algébricos

Um *inteiro algébrico* é uma raiz de uma equação do tipo $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, sendo $a_{n-1}, \ldots, a_1, a_0$ inteiros. Eles formam um *anel*, ou seja, se α e β são inteiros algébricos, então $\alpha \pm \beta$ e $\alpha\beta$ são inteiros algébricos. Para provar isso, sejam $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ e $q(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ os polinômios minimais de α e β, respectivamente (o lema de Gauss garante que tais polinômios minimais são mônicos). Considere o vetor

$$v^t = (1 \ \alpha \ \alpha^2 \ \ldots \ \alpha^{m-1} \ \beta \ \alpha\beta \ \ldots \ \alpha^{m-1} \ \ldots \ \alpha^{m-1}\beta^{n-1})$$

cujas entradas são os números da forma $\alpha^i\beta^j$, $0 \leq i < m$, $0 \leq j < n$.

Vamos primeiro demonstrar que existem matrizes A e B quadradas de ordem mn e com entradas inteiras tais que $A \cdot v = \alpha \cdot v$ e $B \cdot v = \beta \cdot v$ (em outras palavras, v é autovetor de A e B, com autovalores correspondentes α e β). Para isso, é só verificar que $\alpha \cdot v$ tem entradas do tipo $\alpha^i\beta^j$ com $1 \leq i \leq m$ e $0 \leq j < n$. Se $i < m$, obtemos uma entrada de v; se $i = m$, substituímos $\alpha^m\beta^j = -a_{m-1}\alpha^{m-1}\beta^j - \cdots - a_0\beta^j$ e obtemos novamente uma combinação linear (com coeficientes inteiros!) das entradas de v. Colocando os coeficientes dessas combinações lineares em uma matriz, obtemos A. Podemos obter a matriz B de modo análogo.

O que isso tem a ver com os inteiros algébricos? Na verdade, essas matrizes simplicam as contas: note que $(A \pm B) \cdot v = (\alpha \pm \beta)v$ e $AB \cdot v = \alpha\beta \cdot v$, ou seja, $\alpha \pm \beta$ é autovalor de $A \pm B$ e $\alpha\beta$ é autovalor de AB. Como os polinômios característicos de matrizes de entradas inteiras como $A \pm B$ e AB são mônicos e com coeficientes inteiros, $\alpha \pm \beta$ e $\alpha\beta$, raízes desses polinômios característicos, são inteiros algébricos. ∎

Em compensação, nem sempre α/β é inteiro algébrico. Fica para o leitor verificar que $1/2$, por exemplo, não é inteiro algébrico (caso você prefira algo mais "algébrico", trabalhe com $1/\sqrt{2}$ – sim, $\sqrt{2}$ é inteiro algébrico). Alguma semelhança com inteiros? Na verdade, eles se comportam de modo bastante parecido com inteiros, de modo que podemos definir, de forma totalmente análoga aos inteiros, divisibilidade e congruência módulo inteiro algébrico. Consegue-se, então, um teorema análogo ao teorema de Fermat.

Sonho de todo estudante para inteiros algébricos. *Sejam α, β inteiros algébricos e p inteiro (de Z) primo. Então*

$$(\alpha + \beta)^p \equiv \alpha^p + \beta^p \pmod{p}$$

Demonstração

Utilize o binômio de Newton e o fato de que $\binom{p}{k} \equiv 0 \pmod{p}$ para $0 < k < p$:

$$(\alpha + \beta)^p \equiv \alpha^p + \beta^p + \sum_{0<k<p} \binom{p}{k} \alpha^{n-k}\beta^k \equiv \alpha^p + \beta^p \pmod{p}$$

∎

2. Somas quadráticas de Gauss e reciprocidade quadrática

Vamos desenvolver um novo método para demonstrar a reciprocidade quadrática, que pode ser generalizado para reciprocidade em alguns graus maiores.

2.1. Uma introdução e $\left(\frac{2}{p}\right)$

Calculemos primeiro $\left(\frac{2}{p}\right)$. Seja $\zeta = e^{\pi/4}$ a raiz oitava fundamental da unidade. Então, como $\zeta^2 = i$, $\zeta^2 + \zeta^{-2} = 0 \iff (\zeta + \zeta^{-1})^2 = 2$. Por simplicidade, seja $\tau = \zeta + \zeta^{-1}$. Então $\tau^2 = 2$, de modo que $\tau^{p-1} = 2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod{p} \iff \tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p}$.

Mas, pelo sonho de todo estudante, $\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p}$. Lembrando que estamos trabalhando com raízes oitavas, $\zeta^p + \zeta^{-p} = \begin{cases} \zeta + \zeta^{-1} & \text{se } p \equiv \pm 1 \pmod 8 \\ \zeta^3 + \zeta^{-3} & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}$. Todavia, lembrando que

$\zeta^4 = -1$, temos $\zeta^3 + \zeta^{-3} = -\zeta - \zeta^{-1}$, de modo que $\zeta^p + \zeta^{-p} = (-1)^{(p^2-1)/8}\tau$. Logo $(-1)^{(p^2-1)/8}\tau \equiv \left(\frac{2}{p}\right)\tau$ (mód. p). Cuidado! Não podemos "cortar" τ porque infelizmente não temos a lei do cancelamento para inteiros algébricos. Mas podemos multiplicar por τ dos dois lados, e como $\tau^2 = 2$, obtemos $(-1)^{(p^2-1)/8}2 \equiv \left(\frac{2}{p}\right)2 \pmod{p} \iff \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

2.2. Como aproveitar essa idéia para casos maiores?

O número τ é uma versão embrionária das *somas de Gauss*. Para provar a reciprocidade quadrática, usamos outra soma, um pouco mais elaborada: seja $\zeta = e^{2\pi/p}$ uma raiz p-ésima fundamental da unidade.

Você já deve saber que $\sum_{0\le t<p} \zeta^{at} = \begin{cases} p & \text{se } p \mid a \\ 0 & \text{caso contrário} \end{cases}$. Fica como exercício provar, a partir desse fato, que $\sum_{0\le t<p} \zeta^{t(x-y)} = \begin{cases} p & \text{se } x \equiv y \pmod{p} \\ 0 & \text{caso contrário} \end{cases}$.

Além disso, como há $p-1$ resíduos quadráticos módulo p e $p-1$ não resíduos quadráticos módulo p, $\sum_{0\le t<p} \left(\frac{t}{p}\right) = 0$.

Agora, sim, podemos definir a soma quadrática de Gauss.

Definição 2.1. *Uma soma quadrática de Gauss é* $g_a = \sum_{0\le t<p} \left(\frac{t}{p}\right)\zeta^{at}$.

Essas somas tem diversas propriedades:

Lema. *As somas quadráticas de Gauss possuem as seguintes propriedades:*

(i) $g_a = \left(\frac{a}{p}\right)g_1$.

(ii) Sendo $g_1 = g$, $g^2 = (-1)^{(p-1)/2}p$.

Demonstração

(i) Lembrando que, para todo a não divisível por p, $\left(\frac{a}{p}\right)^2 = 1$ e $\{t \bmod p, 0 \le t < p\} = \{at \bmod p, 0 \le t < p\}$,

$$g_a = \sum_{0\le t<p} \left(\frac{t}{p}\right)\zeta^{at} = \sum_{0\le t<p} \left(\frac{a}{p}\right)\left(\frac{at}{p}\right)\zeta^{at} = \left(\frac{a}{p}\right)\sum_{0\le t<p} \left(\frac{at}{p}\right)\zeta^{at} = \left(\frac{a}{p}\right)\sum_{0\le at<p} \left(\frac{at}{p}\right)\zeta^{at} = \left(\frac{a}{p}\right)g_1$$

(ii) Primeiro, note que, pelo item anterior, $g_a^2 = g^2$, pois $\left(\frac{a}{p}\right)^2 = 1$. Calculamos a soma $S = \sum_{0\le a<p} g_a g_{-a}$ de duas maneiras. Por um lado, pelo item anterior,

$$S = \sum_{0\le a<p} \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)g^2 = \sum_{0\le a<p} \left(\frac{-a^2}{p}\right)g^2 = \sum_{0\le a<p} \left(\frac{-1}{p}\right)g^2 = (p-1)\left(\frac{-1}{p}\right)g^2$$

Por outro lado, desenvolvendo as somas e multiplicando obtemos

$$g_a g_{-a} = \sum_{0\le x,y<p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)}$$

Somando sobre a e colocando as expressões somente com x e y em evidência,

$$S = \sum_{0\le x,y<p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\sum_{0\le a<p} \zeta^{a(x-y)}$$

As únicas somas $\sum_{0\le a<p} \zeta^{a(x-y)}$ que não são nulas são quando $x \equiv y \pmod{p} \iff x = y$. Assim,

$$S = \sum_{0\le x<p} \left(\frac{x}{p}\right)\left(\frac{x}{p}\right)p = p(p-1)$$

Logo

$$(p-1)\left(\frac{-1}{p}\right)g^2 = p(p-1) \iff g^2 = (-1)^{(p-1)/2}p$$

∎

Seja $p^* = (-1)^{(p-1)/2}p$ uma espécie de "correção de sinal" de primos. Então $g^2 = p^*$ é a equação análoga a $\tau^2 = 2$ utilizada para calcular $\left(\frac{2}{p}\right)$ e estamos prontos para provar a reciprocidade quadrática.

Seja q um outro primo ímpar. Então $g^{q-1} = p^{*(q-1)/2} \iff g^q = \left(\frac{p^*}{q}\right)g$ e, pelo sonho de todo estudante,

$$g^q \equiv \sum_{0\le t<p}\left(\frac{t}{p}\right)^q \zeta^{tq} = \sum_{0\le t<p}\left(\frac{t}{p}\right)\zeta^{tq} \equiv g_q \equiv \left(\frac{q}{p}\right)g \pmod{q}$$

Logo

$$\left(\frac{p^*}{q}\right)g \equiv \left(\frac{q}{p}\right)g \pmod{q} \implies \left(\frac{p^*}{q}\right)g^2 \equiv \left(\frac{q}{p}\right)g^2 \pmod{q}$$
$$\iff \left(\frac{p^*}{q}\right)p^* \equiv \left(\frac{q}{p}\right)p^* \pmod{q} \iff \left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

que é equivalente à reciprocidade quadrática:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right) \iff \left(\frac{(-1)^{(p-1)/2}p}{q}\right)\left(\frac{q}{p}\right) = 1 \iff \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \iff \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}$$

3. Elevando o χ (ki)

Para desenvolver a teoria de reciprocidade cúbica e biquadrática, precisamos da ajuda dos caracteres:

Definição 3.1. *Um caracter multiplicativo em Z/pZ é uma função $\chi\colon Z/pZ^* \to C^*$ tal que $\chi(ab) = \chi(a)\chi(b)$ para todo $a, b \in Z/pZ^*$.*

Um exemplo é o próprio símbolo de Legendre; outro exemplo é o *caracter trivial* ϵ definido por $\epsilon(a) = 1$ para todo $a \in Z/pZ^*$.

Muitas vezes estenderemos os caracteres para Z/pZ; nesse caso $\chi(0) = 0$ para $\chi \neq \epsilon$ e $\epsilon(0) = 1$.

Vamos a algumas das propriedades dos caracteres multiplicativos.

Propriedades dos caracteres. *Seja χ um caracter multiplicativo em Z/pZ e $a \in Z/pZ^*$. Então*

(i) $\chi(1) = 1$.

(ii) $\chi(a)$ *é uma raiz $(p-1)$-ésima da unidade.*

(iii) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Demonstração

(i) Observando que $\chi(1) \neq 0$, $\chi(1) = \chi(1)\chi(1) \iff \chi(1) = 1$.

(ii) Do teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$, assim $\chi(a)^{p-1} = \chi(1) = 1$.

(iii) $\chi(a)\chi(a^{-1}) = \chi(a \cdot a^{-1}) = \chi(1) = 1 \iff \chi(a^{-1}) = \chi(a)^{-1}$. Além disso, $|\chi(a)| = 1 \iff \chi(a)\overline{\chi(a)} = 1 \iff \overline{\chi(a)} = \chi(a)^{-1}$. ∎

Vimos que a soma dos símbolos de Legendre é zero. Isso se aplica a caracteres também? De fato, pode-se provar que

$$\sum_{0\le t<p}\chi(t) = \begin{cases} p & \text{se } \chi = \epsilon \\ 0 & \text{se } \chi \neq \epsilon \end{cases}$$

Se $\chi = \epsilon$ o resultado é imediato. Suponha então $\chi \neq \epsilon$. Nesse caso, existe a tal que $\chi(a) \neq 1$. Assim, sendo $T = \sum_{0 \leq t < p} \chi(t)$, e lembrando mais uma vez que $aZ/pZ = Z/pZ$ para todo $a \in Z/pZ^*$,

$$\chi(a)T = \sum_{0 \leq t < p} \chi(a)\chi(t) = \sum_{0 \leq t < p} \chi(at) = T \implies (\chi(a) - 1)T = 0 \iff T = 0$$

Os caracteres multiplicativos formam um grupo, considerando como operação $\chi\lambda(a) = \chi(a)\lambda(a)$. Nesse caso, $\chi^{-1}(a) = \chi(a)^{-1}$. A identidade desse grupo é ϵ. Tal grupo é, na verdade, cíclico de ordem $p-1$. Considerando uma raiz primitiva g de p, $a = g^k$ para algum k e, deste modo, $\chi(a) = \chi(g)^k$ está definido em função de $\chi(g)$. Isso quer dizer que *todo* $\chi(a)$ pode ser definido a partir de $\chi(g)$. Como $\chi(g)$ é uma raiz $(p-1)$-ésima da unidade, há no máximo $p-1$ caracteres.

Por outro lado, sendo λ definido por $\lambda(g) = e^{2\pi i/(p-1)}$ (lembre que $\lambda(g)$ define todos os demais valores de $\lambda(a)$). Então não é difícil verificar que $\epsilon, \lambda, \lambda^2, \ldots, \lambda^{p-2}$ são caracteres distintos e, portanto, os elementos do grupo de caracteres de p. Note que se $a \not\equiv 1 \pmod p$, $\lambda(a) = \lambda(g)^k = e^{2k\pi i/(p-1)} \neq 1$.

Agora, vamos fixar $a \not\equiv 1 \pmod p$ e somar sobre todos os caracteres: seja $S = \sum_\chi \chi(a)$. Então $\lambda(a)\sum_\chi \lambda(a)\chi(a) = \sum_\chi \lambda\chi(a)$ e, como $\lambda\chi$ também representa todos os caracteres (uma outra versão do gira-gira, considerando que tanto Z/pZ^* como o grupo dos caracteres são cíclicos), $\lambda S = S \iff S = 0$.

3.1. O que caracteres têm a ver com resíduos?

Os caracteres têm uma relação bastante próxima com congruências do tipo $x^n \equiv a \pmod p$.

Lema. *Se $a \in Z/pZ^*$ e $n \mid p-1$ e $x^n \equiv a \pmod p$ não tem soluções então existe um caracter χ tal que $\chi^n = \epsilon$ e $\chi(a) \neq 1$.*

Demonstração

Basta tomar λ como acima e $\chi = \lambda^{(p-1)/n}$. Então $\chi^n = \lambda^{p-1} = \epsilon$ e, sendo $a = g^k$, g raiz primitiva de p, $\chi(a) = \chi(g)^k = \lambda(g)^{k(p-1)/n} = e^{2\pi ki/n} \neq 1$, pois n não pode dividir k. ∎

Como toda raiz da unidade, os caracteres servem como "marcadores". Assim temos um teorema análogo à fórmula da multisecção:

Teorema. *Denote por $N(x^n = a)$ o número se soluções módulo p de $x^n \equiv a \pmod p$. Então, se $n \mid p-1$ tem-se*

$$N(x^n = a) = \sum_{\chi^n = \epsilon} \chi(a)$$

em que a soma é sobre os caracteres cuja ordem divide n.

Demonstração

Primeiro afirmamos que há exatamente n caracteres dessa forma. Mais uma vez usamos uma raiz primitiva g: temos que $\chi(g)^n = 1$, e $\chi(g)$ determina todos os valores de $\chi(a)$, assim há no máximo n caracteres. Por outro lado, tomando $\chi(g) = e^{2\pi i/n}$, verifica-se que $\epsilon, \chi, \chi^2, \ldots, \chi^{n-1}$ são n caracteres distintos com ordem n.

Agora vamos provar a fórmula: para $a \equiv 0 \pmod p$, note que $N(x^n = 0) = 1$ e $\sum_{\chi^n = \epsilon} \chi(0) = 1$, pois $\epsilon(0) = 1$ e $\chi(0) = 0$ para $\chi \neq \epsilon$.

Suponha agora que $a \not\equiv 0 \pmod p$ e que $x^n \equiv a \pmod p$ tem soluções (que são n; para observar por que, pense novamente em raízes primitivas!). Então $a \equiv b^n \pmod p$ e $\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \epsilon(b) = 1$ e, como há n caracteres, $\sum_{\chi^n = \epsilon} \chi(a) = n$.

Se $x^n \equiv a \pmod p$ não tem solução, utilizamos mais uma vez o gira-gira: seja τ tal que $\tau^n = \epsilon$ e $\tau(a) \neq 1$ e denote por T a soma. Então $\tau(a)T = \sum_{\chi^n = \epsilon} \tau\chi(a) = \sum_{\chi^n = \epsilon} \chi(a) = T \implies T(\tau(a) - 1) = 0 \iff T = 0$. ∎

Exercícios

01. Prove que se $x^n \equiv a \not\equiv 0 \pmod{p}$ tem solução e $n \mid p-1$ então na verdade há exatamente n soluções.

02. (OBM 1995, Problema 2) Encontre o número de funções $f: Z \to Z$ tais que

(a) $f(x+1019) = f(x)$ para todo $x \in Z$;

(b) $f(xy) = f(x)f(y)$ para todos $x, y \in Z$.

03. Resolva o problema anterior para $f: Z \to C$.

04. Verifique que $N(x^2 = a) = \sum_{\chi^2=\epsilon} \chi(a) = 1 + \left(\frac{a}{p}\right)$.

3.2. Somas de Gauss

Podemos generalizar as somas quadráticas de Gauss para caracteres:

Definição 3.2. *Seja χ um caracter de Z/pZ e $a \in Z/pZ$. Defina $g_a(\chi) = \sum_{0 \le t < p} \chi(t)\zeta^{at}$, sendo $\zeta = e^{2\pi i/p}$ a raiz p-ésima fundamental da unidade, como a soma de Gauss de χ sobre Z/pZ.*

Novamente, as somas de Gauss servem como marcadores e propriedades semelhantes às das somas quadráticas aparecem, como era de se esperar.

Propriedades das somas de Gauss. *Para $\chi \neq \epsilon$ e $a \not\equiv 0 \pmod{p}$,*

(i) $g_a(\chi) = \chi(a^{-1})g_1(\chi)$;

(ii) $g_a(\epsilon) = 0$;

(iii) $g_0(\chi) = 0$;

(iv) $g_0(\epsilon) = p$.

Demonstração

(i) $\chi(a)g_a(\chi) = \sum_{0 \le t < p} \chi(a)\chi(t)\zeta^{at} = \sum_{0 \le t < p} \chi(at)\zeta^{at} = \sum_{0 \le t < p} \chi(t)\zeta^t = g_1(\chi)$.

(ii) $g_a(\epsilon) = \sum_{0 \le t < p} \epsilon(t)\zeta^{at} = \sum_{0 \le t < p} \zeta^t = 0$.

(iii) $g_0(\chi) = \sum_{0 \le t < p} \chi(t)\zeta^0 = 0$.

(iv) $g_0(\epsilon) = \sum_{0 \le t < p} \epsilon(t)\zeta^0 = p$. ∎

Denotaremos $g_1(\chi)$ simplesmente por $g(\chi)$. A próxima propriedade é a mais importante.

Lema. *Se $\chi \neq \epsilon$, então $|g(\chi)| = \sqrt{p}$.*

Demonstração

Assim como nas somas quadráticas, vamos calcular $S = \sum_a g_a(\chi)\overline{g_a(\chi)}$ de duas maneiras.

Por um lado, para $a \not\equiv 0 \pmod{p}$, $g_a(\chi) = \chi(a^{-1})g(\chi)$ e $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$ (aqui, utilizamos uma das propriedades dos caracteres). Observando que $g_0(\chi) = 0$, $S = (p-1)\chi(a)\chi(a^{-1})g(\chi)\overline{g(\chi)} = (p-1)|g(\chi)|^2$.

Por outro lado, desenvolvendo o produto $g_a(\chi)\overline{g_a(\chi)}$ obtemos

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{0 \le x,y < p} \chi(x)\overline{\chi(y)}\zeta(x-y)a$$

Somando sobre a obtemos

$$S = \sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_{0 \le x,y < p} \chi(x)\overline{\chi(y)} \sum_{0 \le a < p} \zeta(x-y)a$$

Lembrando que $\sum_{0\le a<p}\zeta(x-y)a = \begin{cases} p & \text{se } x\equiv y \pmod p \\ 0 & \text{caso contrário} \end{cases}$,

$$S = \sum_{0\le x<p} \chi(x)\overline{\chi(x)}p = (p-1)p$$

Assim, $(p-1)|g(\chi)|^2 = (p-1)p \iff |g(\chi)| = \sqrt{p}$. ∎

3.3. Somas de Jacobi

As somas de Jacobi foram desenvolvidas para contar a quantidade de soluções de congruências do tipo

$$x^n + y^n \equiv 1 \pmod p$$

e é aí que os caracteres entram!

Primeiro, note que a quantidade de soluções é igual a

$$N(x^n+y^n=1) = \sum_{\substack{a+b\equiv 1\\ p}} N(x^n=a)N(x^n=b)$$

Lembrando que sabemos contar soluções em função dos caracteres,

$$N(x^n+y^n=1) = \sum_{\substack{a+b\equiv 1\\ p}} \sum_{\substack{\chi^n=\epsilon\\ \lambda^n=\epsilon}} \chi(a)\lambda(b) = \sum_{\substack{\chi^n=\epsilon\\ \lambda^n=\epsilon}} \sum_{\substack{a+b\equiv 1\\ p}} \chi(a)\lambda(b)$$

E assim nasceram as somas de Jacobi.

Definição 3.3. *Sejam χ e λ caracteres de Z/pZ. Então definimos $J(\chi,\lambda) = \sum_{\substack{a+b\equiv 1\\ p}} \chi(a)\lambda(b)$, a que chamamos soma de Jacobi.*

Surpreendentemente, somas de Jacobi e de Gauss estão fortemente relacionadas.

Teorema. *Sejam χ e λ caracteres não triviais. Então*

(i) $J(\epsilon,\epsilon) = p$

(ii) $J(\epsilon,\chi) = 0$.

(iii) $J(\chi,\chi^{-1}) = -\chi(-1)$.

(iv) Se $\chi\lambda \neq \epsilon$ então

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

Demonstração

A parte (i) é imediata e (ii) é bem simples: de fato, $J(\epsilon,\chi) = \sum_a \chi(a) = 0$.

As partes (iii) e (iv) são mais interessantes:

$$J(\chi,\chi^{-1}) = \sum_a \chi(a)\chi(1-a)^{-1} = \sum_a \chi\left(\frac{a}{1-a}\right)$$

Como a imagem de $f\colon Z/pZ\setminus\{\overline{1}\} \to Z/pZ$ tem imagem $Z/pZ\setminus\{\overline{-1}\}$,

$$J(\chi,\chi^{-1}) = \sum_{\substack{c\not\equiv -1\\ p}} \chi(c) = \sum_c \chi(c) - \chi(-1) = -\chi(-1)$$

Enfim,

$$g(\chi)g(\lambda) = \left(\sum_x \chi(x)\zeta^x\right)\cdot\left(\sum_y \lambda(y)\zeta^y\right) = \sum_{x,y}\chi(x)\lambda(y)\zeta^{x+y} = \sum_t\left(\sum_{\substack{x+y\equiv t\\ p}}\chi(x)\lambda(y)\right)\zeta^t$$

Se $t=0$, então $\sum_{\substack{x+y\equiv 0\\ p}}\chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0$ pois $\chi\lambda \neq \epsilon$.

Se $t \not\equiv 0 \pmod p$, então $\sum_{\substack{x+y\equiv t\\ p}}\chi(x)\lambda(y) = \sum_{\substack{x'+y'\equiv 1\\ p}}\chi(x't)\lambda(y't) = \chi\lambda(t)\sum_{\substack{x'+y'\equiv 1\\ p}}\chi(x')\lambda(y') = \chi\lambda(t)J(\chi,\lambda)$. Logo

$$g(\chi)g(\lambda) = J(\chi,\lambda)\sum_t \chi\lambda(t)\zeta^t = J(\chi,\lambda)g(\chi\lambda) \iff J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

∎

Módulo de somas de Jacobi. *Sendo χ e λ caracteres em Z/pZ tais que χ, λ e $\chi\lambda$ são diferentes de ϵ, então $|J(\chi,\lambda)| = \sqrt{p}$.*

Demonstração

Basta usar o fato de que somas de Gauss têm módulo $\sqrt{p}$ e o teorema anterior. ∎

"Telescopando", chegamos ao seguinte resultado:

Lema. *Se $n \mid p-1$ e χ tem ordem $n > 2$, então*

$$g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\ldots J(\chi,\chi^{n-2})$$

Demonstração

Multiplicando as relações

$$J(\chi,\chi) = \frac{g(\chi)g(\chi)}{g(\chi^2)}, \quad J(\chi,\chi^2) = \frac{g(\chi)g(\chi^2)}{g(\chi^3)}, \quad \ldots, \quad J(\chi,\chi^{n-2}) = \frac{g(\chi)g(\chi^{n-2})}{g(\chi^{n-1})}$$

obtemos, lembrando que $\chi^n = \epsilon$,

$$J(\chi,\chi)J(\chi,\chi^2)\ldots J(\chi,\chi^{n-2}) = \frac{g(\chi)^{n-1}}{g(\chi^{n-1})} = \frac{g(\chi)^n}{g(\chi^{-1})g(\chi)}$$

Mas

$$g(\chi^{-1}) = g(\overline{\chi}) = \sum_t \overline{\chi}(t)\zeta^t = \sum_t \overline{\chi(t)}\zeta^t = \overline{\sum_t \chi(t)\zeta^{-t}} = \overline{\sum_t \chi(-1)\chi(-t)\zeta^{-t}} = \overline{\chi(-1)g(\chi)} = \chi(-1)\overline{g(\chi)}$$

pois $\chi(-1)^2 = \chi(1) = 1 \iff \chi(-1) = \pm 1 \in R$. Logo $g(\chi^{-1})g(\chi) = \chi(-1)\overline{g(\chi)}g(\chi) = \chi(-1)|g(\chi)|^2 = \chi(-1)p$ e, substituindo, o resultado segue. ∎

3.4. Duas aplicações de somas de Jacobi

Vamos contar o número de soluções de $x^2 + y^2 \equiv 1 \pmod p$.

Teorema. *A quantidade de soluções de* $x^2 + y^2 \equiv 1 \pmod{p}$ *é*

$$N(x^2+y^2=1) = \begin{cases} p-1 & \text{se } p \equiv 1 \pmod 4 \\ p+1 & \text{se } p \equiv -1 \pmod 4 \end{cases}$$

Demonstração

Utilizando a fórmula que encontramos e observando que os caracteres de ordem 2 são ϵ e $\chi_2(a) = \left(\frac{a}{p}\right)$,

$$\begin{aligned} N(x^2+y^2=1) &= \sum_{\substack{\chi^2=\epsilon \\ \lambda^2=\epsilon}} J(\chi,\lambda) = J(\epsilon,\epsilon) + J(\epsilon,\chi_2) + J(\chi_2,\epsilon) + J(\chi_2,\chi_2) \\ &= p + 0 + 0 - \chi_2(-1) = p - \left(\frac{-1}{p}\right) = p - (-1)^{(p-1)/2}, \end{aligned}$$

e é só verificar para cada classe de congruência módulo 4. ∎

Para cúbicas, aplicamos de novo o resultado: sendo χ um caracter cúbico (ou seja, de ordem 3), os outros são ϵ e χ^2. Então

$$\begin{aligned} N(x^3+y^3=1) &= \sum_{\substack{\chi^3=\epsilon \\ \lambda^3=\epsilon}} J(\chi,\lambda) \\ &= J(\epsilon,\epsilon) + J(\epsilon,\chi) + J(\epsilon,\chi^2) \\ &+ J(\chi,\epsilon) + J(\chi,\chi) + J(\chi,\chi^2) \\ &+ J(\chi^2,\epsilon) + J(\chi^2,\chi) + J(\chi^2,\chi^2) \\ &= p + J(\chi,\chi) + J(\overline{\chi},\overline{\chi}) - \chi(-1) - \chi^2(-1) \end{aligned}$$

Como $\chi(-1) = \chi(-1)^3 = \chi^3(-1) = 1$, $\chi^2(-1) = 1$ e

$$N(x^3+y^3=1) = p - 2 + J(\chi,\chi) + \overline{J(\chi,\chi)} = p - 2 + 2\,\mathrm{Re}\,J(\chi,\chi)$$

Observando que $|J(\chi,\chi)| = \sqrt{p}$ e $|\,\mathrm{Re}\,z| \le |z|$ para todo z complexo, obtemos

Teorema. $|N(x^3+y^3=1) - (p-2)| \le 2\sqrt{p}$. ∎

Para melhorar um pouco o resultado precisamos de mais alguns resultados preliminares.

Lema. *Seja* χ *um caracter cúbico. Então* $g(\chi)^3 = pJ(\chi,\chi)$.

Demonstração

Basta aplicar o lema anterior e observar que $\chi(-1) = 1$: $g(\chi)^3 = \chi(-1)pJ(\chi,\chi) = pJ(\chi,\chi)$. ∎

Como caracteres cúbicos são raízes cúbicas da unidade (pois $\chi(a)^3 = 1$), a soma $J(\chi,\chi)$ é da forma $a + b\omega$, sendo $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Note que $|J(\chi,\chi)| = \sqrt{p} \iff |a+b\omega| = \sqrt{p} \iff a^2 - ab + b^2 = p$. Só existem caracteres de ordem 3 se $3 \mid p-1$, ou seja, $p \equiv 1 \pmod 3$.

Na verdade, dá para obter ainda mais informação:

Lema. *Se* $p \equiv 1 \pmod 3$ *e* χ *é um caracter cúbico,* $J(\chi,\chi) = a + b\omega$, *com* $a \equiv -1 \pmod 3$ *e* $b \equiv 0 \pmod 3$.

Demonstração

Vamos usar o sonho de todo estudante (em inteiros algébricos):

$$g(\chi)^3 \equiv \sum_t \chi(t)^3 \zeta^{3t} \pmod 3$$

Observando que $\chi(0) = 0$ e $\chi(t)^3 = 1$ para $t \not\equiv 0 \pmod p$,

$$g(\chi)^3 \equiv \sum_{t \neq 0} \zeta^{3t} \equiv -1 \pmod 3$$

Como $p \equiv 1 \pmod 3$ e $g(\chi)^3 = pJ(\chi,\chi)$,

$$g(\chi)^3 \equiv pJ(\chi,\chi) \equiv a + b\omega \equiv -1 \pmod 3$$

Conjugando e usando o fato de que $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)} = \overline{g(\chi)}$,

$$\overline{g(\chi)} \equiv pJ(\overline{\chi},\overline{\chi}) \equiv a + b\omega^2 \equiv -1 \pmod 3$$

Subtraindo, obtemos $b(\omega - \omega^2) \equiv 0 \pmod 3 \iff b\sqrt{-3} \equiv 0 \pmod 3 \iff -3b^2 \equiv 0 \pmod 9 \iff 3 \mid b$, isto é, $b \equiv 0 \pmod 3$. Substituindo em $a + b\omega \equiv -1 \pmod 3$ obtemos $a \equiv -1 \pmod 3$. ∎

Agora podemos melhorar um pouco o resultado das soluções cúbicas.

Teorema. *O número de soluções de* $x^3 + y^3 \equiv 1 \pmod p$, $p \equiv 1 \pmod 3$ *primo, é*

$$N(x^3 + y^3 = 1) = p - 2 + A,$$

em que A *é obtido tomando-se* $4p = A^2 + 27B^2$, $A \equiv 1 \pmod 3$.

Demonstração

Primeiro, note que, sendo $J(\chi,\chi) = a + b\omega$, $2\operatorname{Re} J(\chi,\chi) = 2a - b \equiv 1 \pmod 3$. Além disso, $|J(\chi,\chi)| = \sqrt{p} \iff a^2 - ab + b^2 = p \iff (2a-b)^2 + 3b^2 = p$. Tomando $A = 2a - b$ e $B = b/3$, e lembrando que $N(x^3 + y^3 = 1) = p - 2 + 2\operatorname{Re} J(\chi,\chi)$ obtemos o resultado. ∎

É claro que a técnica para somas de Jacobi pode ser utilizada para outras equações (e também pode ser generalizada!).

Exercícios

05. Prove que $N(x^2 + y^3 = 1) = p + \operatorname{Re} J(\chi,\rho)$, sendo χ um caracter cúbico e ρ o símbolo de Legendre.

06. Prove que $N(x^2 + y^4 = 1) = p - 1 + 2\operatorname{Re} J(\chi,\rho)$, sendo χ um caracter de ordem 4 (ou seja, biquadrático) e ρ o símbolo de Legendre.

07. Definimos somas de Jacobi com mais caracteres como

$$J(\chi_1, \chi_2, \ldots, \chi_\ell) = \sum_{\substack{t_1 + \cdots + t_\ell \equiv 1 \\ p}} \chi_1(t_1)\chi(t_2)\ldots\chi_\ell(t_\ell)$$

Defina também

$$J_0(\chi_1, \chi_2, \ldots, \chi_\ell) = \sum_{\substack{t_1+\cdots+t_\ell \equiv 0 \\ p}} \chi_1(t_1)\chi(t_2)\ldots\chi_\ell(t_\ell)$$

Prove que

(a) $J_0(\epsilon, \epsilon, \ldots, \epsilon) = J(\epsilon, \epsilon, \ldots, \epsilon) = p^{\ell-1}$.

(b) Se alguns mas não todos os caracteres χ_i são iguais a ϵ, então $J_0(\chi_1, \chi_2, \ldots, \chi_\ell) = J(\chi_1, \chi_2, \ldots, \chi_\ell) = 0$.

(c) Se $\chi_i \neq \epsilon$, então

$$J_0(\chi_1, \chi_2, \ldots, \chi_\ell) = \begin{cases} 0 & \text{se } \chi_1\chi_2\ldots\chi_\ell \neq \epsilon \\ \chi_\ell(-1)(p-1)J(\chi_1, \chi_2, \ldots, \chi_{\ell-1} & \text{caso contrário} \end{cases}$$

(d) Se $\chi_i \neq \epsilon$ e $\chi_1\chi_2\ldots\chi_\ell \neq \epsilon$ então

$$g(\chi_1)g(\chi_2)\ldots g(\chi_\ell) = J(\chi_1, \chi_2, \ldots, \chi_\ell)g(\chi_1\chi_2\ldots\chi_\ell)$$

(e) Se $\chi_1\chi_2\ldots\chi_\ell \neq \epsilon$ então $|J(\chi_1, \chi_2, \ldots, \chi_\ell)| = p^{(\ell-1)/2}$.

(f) Se $\chi_1\chi_2\ldots\chi_\ell = \epsilon$ então $|J(\chi_1, \chi_2, \ldots, \chi_\ell)| = p^{(\ell-2)/2}$.

4. Inteiros de Eisenstein

Seja $\omega = e^{2\pi/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ a raiz cúbica fundamental da unidade. Definimos $Z[\omega]$ como o conjunto dos números da forma $a + b\omega$, a, b inteiros. Note que, sendo $\omega^2 = -1 - \omega$, $Z[\omega]$ é um anel. Além disso, os elementos de $Z[\omega]$ são inteiros algébricos, portanto faz sentido definir divisibilidade e congruência em $Z[\omega]$.

Mais do que isso, podemos definir divisão euclidiana e, portanto, existem *números primos* em $Z[\omega]$ e também vale fatoração única. Associado a isso está o conceito de *norma*, que substitui o módulo de inteiros. Desse modo, existem as *unidades* em $Z[\omega]$, os números de norma 1.

4.1. Norma de um inteiro de Eisenstein

Definimos a norma de um número $\alpha \in Z[\omega]$ como $N\alpha = \alpha \cdot \overline{\alpha}$. Se $\alpha = a + b\omega$, pode-se provar, sem muito esforço, que $N\alpha = a^2 - ab + b^2$. Uma propriedade muito importante é que a norma é multiplicativa.

4.2. Unidades em $Z[\omega]$

Sendo $\epsilon = a + b\omega$ uma unidade, $N\epsilon = 1 \iff a^2 - ab + b^2 = 1 \iff (2a - b)^2 + 3b^2 = 4$ e temos seis casos:

$$\left|\begin{matrix} 2a-b=1 \\ b=1 \end{matrix}\right. \iff a = b = 1; \quad \left|\begin{matrix} 2a-b=-1 \\ b=1 \end{matrix}\right. \iff a = 0 \text{ e } b = 1; \quad \left|\begin{matrix} 2a-b=1 \\ b=-1 \end{matrix}\right. \iff a = 0 \text{ e } b = -1;$$

$$\left|\begin{matrix} 2a-b=-1 \\ b=-1 \end{matrix}\right. \iff a = b = -1; \quad \left|\begin{matrix} 2a-b=2 \\ b=0 \end{matrix}\right. \iff a = 1 \text{ e } b = 0; \quad \left|\begin{matrix} 2a-b=-2 \\ b=0 \end{matrix}\right. \iff a = -1 \text{ e } b = 0$$

Ou seja, há seis unidades: ± 1, $\pm\omega$, $\pm(-1-\omega) = \pm\omega^2$. Para cada $\alpha \in Z[\omega]$, chamamos de seus *associados* os produtos de α por cada uma das unidades.

4.3. Divisão euclidiana em $Z[\omega]$

Voltando ao primórdios da teoria dos números, usamos o diagrama

$$\begin{matrix} \alpha & \big\lfloor\, \beta \\ r & \overline{\quad q \quad} \end{matrix} \to \alpha = \beta \cdot q + r$$

Mas nesse caso, devemos ter $Nr < N\beta$ ou $r = 0$. Vamos provar que existem q e r nessas condições.

Note que $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N\beta} = c + d\omega$, sendo c e d racionais. Sendo m e n os inteiros mais próximos de c e d, no sentido que $|m - c| \leq \frac{1}{2}$ e $|n - d| \leq \frac{1}{2}$, provaremos que $q = m + n\omega$. De fato, $\alpha - \beta \cdot (m + n\omega) = \beta\left(\frac{\alpha}{\beta} - m + n\omega\right) = \beta((c - m) + (d - n)\omega)$, cuja norma é $N\beta \cdot ((c - m)^2 - (c - m)(d - n) + (d - n)^2) \leq N\beta\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) < N\beta$.

4.4. Fatoração única

Mas o que significa ser primo em anéis diferentes de Z? Duas definições:

Definição 4.1. *Dizemos que π é irredutível em um anel quando não pode ser escrito como produto de dois números, nenhum deles igual a alguma unidade.*

Definição 4.2. *Dizemos que π é primo em um anel quando $\pi \mid \alpha\beta \iff \pi \mid \alpha$ ou $\pi \mid \beta$ para todos α, β no anel.*

Superteorema de anéis euclidianos. *Se um anel é euclidiano, então vale fatoração única nesse anel.*

Demonstração

O caminho é um pouco longo, mas é sempre o mesmo:

(1) Divisão euclidiana $\implies$ Algoritmo de Euclides;

(2) Algoritmo de Euclides $\implies$ Teorema de Bezóut;

(3) Teorema de Bezóut $\implies$ Irredutível = Primo;

(4) Primos $\implies$ Fatoração única.

Vamos dar um esboço de prova:

(1) Havendo norma, pode-se definir $\text{mdc}(\alpha, \beta)$ como um número de maior norma que divide α e β. O algoritmo de Euclides reside no fato de que $\text{mdc}(\alpha, \beta) = \text{mdc}(\beta, \alpha \bmod \beta)$, que decorre diretamente das propriedades de divisibilidade, e substitui (α, β) por $(\beta, \alpha \bmod \beta)$ até que um dos valores seja zero. Como a norma sempre diminui, em algum momento o algoritmo de Euclides acaba.

(2) O teorema de Bezóut, que diz que se $\text{mdc}(\alpha, \beta) = \delta$ então existem x, y tais que $\alpha x + \beta y = \delta$, decorre diretamente do algoritmo de Euclides, substituindo as expressões "ao contrário".

(3) Seja π um irredutível e suponha que $\pi \mid \alpha\beta$. Se $\pi \mid \alpha$, não há o que provar. Então, se π não divide α, então $\text{mdc}(\pi, \alpha) = 1$, pois se não fosse uma unidade π poderia ser escrito como produto de dois números de norma não unitária (um deles seria $\text{mdc}(\pi, \alpha)$). Assim, pelo teorema de Bezóut, existem x e y tais que $\alpha x + \pi y = 1 \iff \alpha\beta x + \pi\beta = \beta$. Como $\pi \mid \alpha\beta$, $\pi \mid \alpha\beta + \pi\beta \iff \pi \mid \beta$.

(4) Indução, e é exatamente igual à demonstração para inteiros. ∎

Note que esse superteorema pode ser utilizado para provar que existe fatoração única também em polinômios sobre corpos, por exemplo (a norma seria o grau do polinômio).

4.5. Primos em $Z[\omega]$

Mudamos de anel, mudamos de primos. De fato, você pode verificar que $7 = (2 - \omega)(3 + \omega)$ não é primo em $Z[\omega]$! Vamos então encontrar os primos em $Z[\omega]$.

Primos em $Z[\omega]$. *Os primos em $Z[\omega]$ são associados a um dos seguintes números:*

- *os primos positivos racionais $p \equiv -1 \pmod 3$;*
- *os números π tais que $N\pi = p$, p primo racional positivo, $p \equiv 1 \pmod 3$;*
- $1 - \omega$.

Demonstração

Primeiro provemos que se π tem norma p primo então π é primo. Caso contrário, $\pi = \alpha\beta$, com $N\alpha, N\beta > 1$. Mas então $p = N\pi = N\alpha \cdot N\beta$ seria o produto de dois inteiros maiores do que 1, absurdo.

Agora, encontremos as possíveis normas dos primos de $Z[\omega]$. Seja π primo e $n = N\pi$. Então $n = \pi\overline{\pi}$, de modo que π divide algum fator primo racional p de n. Assim, $p = \pi\gamma \implies Np = N\pi \cdot N\gamma \iff N\pi \cdot N\gamma = p^2$, de modo que $N\pi = p$ ou $N\pi = p^2$. No segundo caso, γ é unidade e, portanto, π é um associado de p.

Só precisamos classificar os primos. Se $N\pi = p$ e $\pi = a + bi$ então $p = a^2 - ab + b^2 \iff 4p = (2a - b)^2 + 3b^2$. Como b e p são primos entre si, $x^2 \equiv -3 \pmod{p}$, com $x = (2a - b)b^{-1} \bmod p$. Então $\left(\frac{-3}{p}\right) = 1$. Aplicando reciprocidade quadrática, temos $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = \left(\frac{p}{3}\right)$. Logo $\left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod{3}$. Reciprocamente, se $p \equiv 1 \pmod{3}$ então $p \mid x^2 + 3$ para algum $x \in Z$. Mas $x^2 + 3 = (x + 1 + 2\omega)(x - 1 - 2\omega)$ e se p fosse primo então $p \mid 2$, o que não é possível. Então $p = \pi\gamma$ com $N\pi, N\gamma > 1$. Verifica-se que $N\pi = N\gamma = p$ e então os divisores π e $\overline{\pi}$ de p são os primos do segundo caso.

Note que se $p \equiv -1 \pmod{3}$ não é possível que $N\pi = p$. Então p não pode ser fatorado e é, portanto, primo em $Z[\omega]$ também (note que 2 está incluído nessa lista!). Esses são os primos do primeiro caso.

Finalmente, para $p = 3$, observando que $x^2 + x + 1 = (x - \omega)(x - \omega^2)$, para $x = 1$ temos $3 = (1 - \omega)(1 - \omega^2) = -\omega^2(1 - \omega)^2$ e $1 - \omega$ tem norma 3, sendo primo. ∎

4.6. Congruência módulo π (primos são legais)

Assim como em Z, podemos trabalhar com classes de congruência módulo $\alpha \in Z[\omega]$. Em particular, para primos temos um resultado análogo aos inteiros e muito interessante:

Teorema. *Seja π primo. Então as classes de congruência módulo π formam um corpo com $N\pi$ elementos.*

Demonstração

A demonstração é igualzinha à que usamos em Z! É óbvio que os inteiros de Eisenstein módulo π formam um anel. Só falta provar que todo $\alpha \not\equiv 0 \pmod{\pi}$ tem inverso. Mas isso quer dizer que $\mathrm{mdc}(\alpha, \pi) = 1$ e, por Bezóut, existem x, y tais que $\alpha x + \pi y = 1 \implies \alpha x \equiv 1 \pmod{\pi}$ e x é o nosso inverso.

Agora precisamos contar as classes de equivalência para obter a quantidade de elementos.

Se $\pi = q$ é racional, afirmamos que as classes de congruência podem ser representadas por $a + b\omega$, $0 \leq a, b < q$. De fato, para $x + y\omega \in Z[\omega]$, $x + y\omega \equiv r + s\omega \pmod{q}$ com $0 \leq r, s < q$ e $r_1 + s_1\omega \equiv r_2 + s_2\omega \pmod{q} \iff \frac{r_1 - r_2}{q} + \frac{s_1 - s_2}{q}\omega \in Z[\omega] \iff r_1 \equiv r_2 \pmod{q}$ e $s_1 \equiv s_2 \pmod{q} \iff r_1 = r_2$ e $s_1 = s_2$.

Se $N\pi = p \equiv 1 \pmod{3}$, afirmamos que as classes de congruência podem ser representadas por $0, 1, 2, \ldots, p - 1$. Seja $\pi = a + b\omega$ e $x + y\omega \in Z[\omega]$. Então note que p não divide b e existe $t \in Z$ tal que $bt \equiv y \pmod{p} \implies bt \equiv y \pmod{\pi}$, de modo que $x + y\omega \equiv x + bt\omega \equiv x - at \pmod{\pi}$. Podemos reduzir $x - at$ módulo p, obtendo $x + y\omega \equiv j \pmod{\pi}$, com $0 \leq j < p$. Ou seja, todo inteiro de Eisenstein é congruente a um racional entre 0 e $p - 1$. Além disso, essas classes não sõa repetidas: se $i \equiv j \pmod{\pi}$ então $i - j = \pi\gamma \implies N(i - j) = N\pi \cdot N\gamma \iff (i - j)^2 = p \cdot N\gamma \implies p \mid (i - j)^2 \iff p \mid i - j \iff i \equiv j \pmod{p}$.

Enfim, para $\pi = 1 - \omega$, prova-se de modo análogo ao caso anterior que as classes de congruência são $-1, 0, 1$. ∎

4.7. Euler-Fermat para inteiros de Eisenstein

Novamente, usando o bom e velho lema gira-gira prova-se:

Teorema. *Se π é primo e $\alpha \not\equiv 0 \pmod{\pi}$, então*

$$\alpha^{N\pi - 1} \equiv 1 \pmod{\pi}$$

Demonstração

É só verificar que $\alpha\beta \equiv \alpha\gamma \pmod{\pi} \iff \beta \equiv \gamma \pmod{\pi}$ e multiplicar todas as classes de equivalência não nulas, obtendo $\prod \alpha\beta \equiv \prod \beta \pmod{\pi} \iff \alpha^{N\pi-1} \equiv 1 \pmod{\pi}$.

Ou, se você quiser, você pode usar o fato de que as classes de equivalência não nulas formam um grupo multiplicativo. ∎

A partir do teorema de Euler-Fermat nasceu o critério de Euler. Então...

4.8. Um critério para congruências cúbicas

Primeiro, vale a pena notar que para primos π com norma diferente de 3, as classes de congruência 1, ω e ω^2 são diferentes. De fato, se $1 \equiv \omega \pmod{\pi} \iff \omega \equiv \omega^2 \pmod{\pi}$ então $\pi \mid 1-\omega$, o que não é possível pois $1-\omega$ é primo. Enfim, $1 \equiv \omega^2 \pmod{\pi} \iff \pi \mid 1-\omega^2 \iff \pi \mid (1-\omega)(1+\omega) \iff \pi \mid 1-\omega$ (veja que $1+\omega = -\omega^2$ é uma unidade), e chegamos ao mesmo absurdo.

Observamos também que $N\pi \equiv 1 \pmod{3}$ para todo prmo com norma diferente de 3, pois $N\pi =\equiv 1 \pmod{3}$ ou $N\pi = q^2 \equiv (-1)^2 \equiv 1 \pmod{3}$. Temos então o seguinte

Lema. *Seja π um primo de norma diferente de 3. Então $\alpha^{\frac{N\pi-1}{3}} \equiv \omega^i \pmod{\pi}$, em que i é igual a 0, 1 ou 2.*

Demonstração

Basta notar que, sendo $x = \alpha^{\frac{N\pi-1}{3}}$, $x^3 \equiv 1 \pmod{\pi} \iff \pi \mid x^3-1 \iff \pi \mid (x-1)(x-\omega)(x-\omega^2)$. Sendo π primo, $x \equiv 1 \pmod{\pi}$ ou $x \equiv \omega \pmod{\pi}$ ou $x \equiv \omega^2 \pmod{\pi}$. ∎

Vamos relacionar isso com resíduos cúbicos.

Definição 4.3. *Sejam $\alpha \in Z[\omega]$ e π um primo. O caracter cúbico de α módulo π é definido por*

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \text{se } \pi \mid \alpha \\ \alpha^{\frac{N\pi-1}{3}} \text{ mód } \pi & \text{caso contrário} \end{cases}$$

Isto é, se α não é múltiplo de π, então $\left(\frac{\alpha}{\pi}\right)_3 = 1$, ω ou ω^2.

Propriedades análogas às do simbolo de Legendre são verdadeiras:

Propriedades de caracteres cúbicos. *Sejam $\alpha, \beta \in Z[\omega]$ e π primo. Então*

- $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *se, e somente se, $x^3 \equiv \alpha \pmod{\pi}$ tem solução (ou seja, α é resíduo cúbico de π);*
- $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$ *para $\alpha \equiv \beta \pmod{\pi}$;*
- $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

A única afirmação que precisa de mais atenção é a primeira: nesse caso, tomamos um gerador do corpo $Z[\omega]/\pi Z[\omega]$ (a raiz primitiva de π) e fazemos a demonstração análoga à do critério de Euler. ∎

Com isso, podemos trabalhar com os primos racionais: seja $q \equiv -1 \pmod{3}$. Então se n é racional, $\left(\frac{n}{q}\right)_3$ é inteiro e igual a 1. Isso quer dizer que todo inteiro é resíduo cúbico módulo um primo congruente a -1 módulo 3. Mas isso na verdade não é difícil de provar sem inteiros algébricos: se $q \equiv -1 \pmod{3}$, então $((a^{-1})^{(q-2)/3})^3 \equiv a \pmod{q}$.

4.9. Alguém falou em caracteres?

Os caracteres cúbicos são, como veremos posteriormente em alguns casos, caracteres, então vamos adotar por um instante a notação $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$.

Algo que complexos têm que reais não têm são conjugados (OK, reais *têm* conjugados; eles só não têm muita graça...). Mas podemos conjugar tudo em congruências também!

No caso dos nossos caracteres cúbicos, não é difícil ver que $\overline{\chi(\alpha)} = \chi(\alpha)^2 = \chi(\alpha^2)$. Além disso, como

$$\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi} \iff (\overline{\alpha})^{\frac{N\pi-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$$

também temos $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

4.10. A lei da reciprocidade cúbica

Primeiro, vamos "normalizar" os primos.

Definição 4.4. *Um primo π é primário quando $\pi \equiv 2 \pmod{3}$. Isto quer dizer que se $\pi = a + b\omega$ então $a \equiv 2 \pmod{3}$ e $b \equiv 0 \pmod{3}$.*

Isso não nos tira generalidade. De fato, dado um primo, exatamente um de seus associados é primário. Isso é imediato para primos racionais. Para primos não racionais, sendo $\pi = a + b\omega$, seus associados são $a + b\omega$, $-b + (a - b)\omega$, $(b - a) - a\omega$, $-a - b\omega$, $b + (b - a)\omega$, $(a - b) + a\omega$. Note que $a^2 - ab + b^2 = p \equiv 1 \pmod{3}$, de modo que não é possível que a e b sejam ambos múltiplos de 3. Observando $a+b\omega$ e $-b+(a-b)\omega$ podemos supor que a não é múltiplo de 3 (se a é múltiplo de 3, $-b$ não é e intercambiamos os seis associados multiplicando por alguma unidade); se $a \equiv 1 \pmod{3}$, tomamos $-a - b\omega$ no lugar de $a + b\omega$, de modo que podemos supor sem perda $a \equiv 2 \pmod{3}$. Como $a^2 - ab + b^2 \equiv 1 \pmod{3}$ podemos concluir que $b \equiv 0 \pmod{3}$.

Por exemplo: $3 + \omega$, um primo de norma 7, tem como primário associado $(3 + \omega)\omega^2 = 2 + 3\omega$.

Podemos então enunciar a lei da reciprocidade cúbica:

Lei da reciprocidade cúbica. *Sejam π_1 e π_2 primários de normas diferentes, ambas diferentes de 3. Então*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$$

ou, em termos de caracteres,

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$$

Demonstração

Vamos dividir a prova em três casos:

(i) π_1, π_2 ambos racionais. Nesse caso, denotaremos $\pi_1 = q_1$ e $\pi_2 = q_2$.

(ii) π_1 racional e π_2 irracional. Denotaremos $\pi_1 = q$ e $\pi_2 = \pi$.

(iii) π_1, π_2 ambos irracionais. Denotaremos $N\pi_1 = p_1$ e $N\pi_2 = p_2$.

O caso (i) é praticamente imediato, pois $\chi_{q_1}(q_2) = \chi_{q_2}(q_1) = 1$.

Os outros dois casos são mais elaborados. Sendo π um primo complexo com $N\pi = p \equiv 1 \pmod{3}$, o conjunto $Z[\omega]/\pi Z[\omega]$ é um corpo finito com p elementos, com representantes de classes $0, 1, 2, \ldots, p - 1$. Ou seja, podemos associar $Z[\omega]/\pi Z[\omega]$ com Z/pZ e χ_π assume o papel de um caracter cúbico. Desse modo, podemos utilizar somas de Gauss e Jacobi! Relembremos alguns fatos:

- $g(\chi)^3 = pJ(\chi, \chi)$
- $J(\chi, \chi) = a + b\omega$ com $a \equiv 2 \pmod{3}$ e $b \equiv 0 \pmod{3}$.
- $|J(\chi, \chi)| = \sqrt{p}$, ou seja, $J(\chi, \chi)$ tem norma p.

Deste modo, $J(\chi, \chi)$ é primário! Sendo π primário, como será $J(\chi_\pi, \chi_\pi)$?

Lema. $J(\chi_\pi, \chi_\pi) = \pi$.

Demonstração

Seja $J(\chi_\pi, \chi_\pi) = \pi'$. Queremos provar que $\pi' = \pi$. Note que $\pi\overline{\pi} = p = \pi'\overline{\pi'}$, de modo que, sendo todos primários, $\pi' = \pi$ ou $\pi' = \overline{\pi}$. Queremos eliminar esse último caso.

Da definição de $J(\chi, \chi)$ e do critério de Euler,

$$J(\chi_\pi, \chi_\pi) = \sum_{0 \leq x < p} \chi_\pi(x)\chi(1 - \chi_\pi) \equiv \sum_{0 \leq x < p} x^{(p-1)/3}(1-x)^{(p-1)/3} \pmod{\pi}$$

O polinômio $p(x) = x^{(p-1)/3}(1-x)^{(p-1)/3}$ tem grau $2(p-1)/3 < p-1$. Então, lembrando que $\sum_{0 \leq x < p} x^k \equiv 0 \pmod{p}$ (e, portanto, mód π também!) para todo $0 \leq k < p-1$, desenvolvendo $p(x)$ e vendo módulo p obtemos 0. Logo $J(\chi_\pi, \chi_\pi) \equiv 0 \pmod{\pi}$ e portanto $J(\chi_\pi, \chi_\pi) = \pi$. ∎

Note que isso mostra que $g(\chi_\pi)^3 = p\pi$.

Agora podemos provar a reciprocidade (nesse caso). Lembrando que $\chi_q(\alpha) = \alpha^{\frac{Nq-1}{3}} \text{ mód } q = \alpha^{\frac{q^2-1}{3}} \text{ mód } q$, elevando a última igualdade a $\frac{q^2-1}{3}$, e observando que $\chi_q(p) = 1$,

$$g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi) \pmod{q} \iff g(\chi_\pi)^{q^2} \equiv \chi_q(p)\chi_q(\pi)g(\chi_\pi) \equiv \chi_q(\pi)g(\chi_\pi) \pmod{q}$$

O primeiro membro pode ser desenvolvido com o sonho de todo estudante:

$$g(\chi_\pi)^{q^2} \equiv \sum_{0 \leq t < p} \chi_\pi(t)^{q^2}\zeta^{tq^2} \pmod{q}$$

Note que estamos trabalhando com *todos* os inteiros algébricos, não somente com $Z[\omega]$.

Como χ_π é um caracter cúbico e $q^2 \equiv 1 \pmod{3}$,

$$g(\chi_\pi)^{q^2} \equiv \sum_{0 \leq t < p} \chi_\pi(t)\zeta^{tq^2} \equiv g_{q^2}(\chi_\pi) \pmod{q}$$

Mas $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$. Assim, substituindo tudo o que temos,

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)g(\chi_\pi) \equiv \chi_\pi(q)g(\chi_\pi) \pmod{q}$$

Multiplicando por $\overline{g_\chi(\pi)}$ obtemos

$$\chi_q(\pi)|g_\chi(\pi)|^2 \equiv \chi_\pi(q)|g_\chi(\pi)|^2 \pmod{q} \iff \chi_q(\pi)p \equiv \chi_\pi(q)p \pmod{q} \iff \chi_q(\pi) \equiv \chi_\pi(q) \pmod{q}$$

e provamos a reciprocidade nesse caso.

O nosso último caso é um pouco mais complicado, mas seguem as mesmas ideias anteriores. De fato, começando de $g(\chi_{\overline{\pi_1}})^3 = p_1\overline{\pi_1}$, elevando a $(N\pi_2 - 1)/3$ e vendo módulo π_2 obtemos, de modo análogo ao caso anterior,

$$\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\pi_2}(p_1\overline{\pi_1})$$

Começando de $g(\chi_{\pi_2})^3 = p_2\pi_2$, elevando a $(N\pi_1 - 1)/3$ e vendo módulo π_1 obtemos, de modo análogo ao caso anterior,

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2)$$

Enfim, notando que $\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\overline{\pi_1}}(\overline{p_2^2}) = \chi_{\pi_1}(p_2)$, temos, de toda a informação acima,

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi_1}) = \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(\pi_2 p_2) = \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\overline{\pi_1}) = \chi_{\pi_2}(\pi_1)\chi(p_1\overline{\pi_1})$$

Cortando $\chi(p_1\overline{\pi_1})$ obtemos, finalmente $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$ ∎

4.11. E unidades? E se $N\pi = 3$?

Assim como calculamos $\left(\frac{2}{p}\right)$ separadamente, $\left(\frac{\pm\omega}{\pi}\right)_3$ e $\left(\frac{1-\omega}{\pi}\right)_3$ são calculados separadamente.

Quanto às unidades, não há muita dificuldade: primeiro, $\left(\frac{-\omega}{\pi}\right)_3 = \left(\frac{-1}{\pi}\right)_3\left(\frac{\omega}{\pi}\right)_3 = \left(\frac{\omega}{\pi}\right)_3$ e usamos diretamente o critério de Euler.

Em compensação, a demonstração de que $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$, em que $\pi = 3m - 1 + b\omega$, é mais elaborada e não será feita aqui. Para π racional é mais fácil: de $(1-\omega)^2 = -3\omega$ temos $\left(\frac{1-\omega}{q}\right)_3^2 = \left(\frac{-3}{q}\right)_3\left(\frac{\omega}{q}\right)_3 = 1 \cdot \omega^{\frac{q^2-1}{3}}$. Elevando ao quadrado, obtemos $\left(\frac{1-\omega}{q}\right)_3 = \omega^{\frac{2(q^2-1)}{3}}$ e é só substituir $q = 3m - 1$.

Exercícios

08. Seja π primo complexo. Prove que $x^3 \equiv 2 \pmod{\pi}$ se, e somente, se $\pi \equiv 1 \pmod{2}$.

09. Seja $p \equiv 1 \pmod{3}$ um primo (em Z). Mostre que $x^3 \equiv 2 \pmod{p}$ tem solução se, e somente se, existirem inteiros C e D tais que $p = C^2 + 27D^2$.

10. Esse é um exercício beeem grande (escreva um artigo com esse exercício!) Trabalhando agora no anel euclidiano $Z[i]$, com norma $N(a+bi) = a^2 + b^2$, definindo primário como primos $\pi \equiv 1 \pmod{(1+i)^3}$ e sendo χ_π o caracter de ordem 4 que revela se os números são resíduos quárticos módulo π, prove a *lei da reciprocidade biquadrática*: sendo π e γ primários,

$$\chi_\pi(\gamma) = \chi_\gamma(\pi)(-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\gamma)-1}{4}}$$

11. Generalize o símbolo de Legendre para números compostos da seguinte maneira: se $b = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$,

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_k}\right)^{\alpha_k}$$

Nesse caso, vale a reciprocidade quadrática também, embora $\left(\frac{a}{b}\right) = 1$ *não* indique se a é resíduo quadrático módulo b.

Seja $p \equiv 1 \pmod{4}$ um primo (em Z). Prove que:

(a) existem inteiros a e b tais que $p = a^2 + b^2$.

(b) sendo a acima ímpar, $\left(\frac{a}{p}\right) = 1$.

(c) $\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$.

(d) $(a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod{p}$.

(e) sendo f tal que $f^2 \equiv -1 \pmod{p}$ (por que ele existe?), $2^{(p-1)/4} \equiv f^{ab/2} \pmod{p}$.

(f) $x^4 \equiv 2 \pmod{p}$ tem solução se, e somente se, existem inteiros A e B tais que $p = A^2 + 64B^2$.

5. Referências Bibliográficas

[1] A referência principal aqui é o livro *A Classical Introduction to Modern Number Theory*, de Kenneth Ireland e Michael Rosen. Nesse livro, há tópicos mais gerais sobre reciprocidade, função zeta, equações diofantinas de vários tipos, curvas elípticas e um pouco de Geometria Aritmética.

[2] Carlos Shine, *Por que você deveria ter resolvido o problema 2 da OBM 2007*, aula da Semana Olímpica 2008. Nesse artigo tem uma demonstração diferente da reciprocidade quadrática, além de fatos sobre raízes primitivas e polinômios módulo p.

[3] Robin Chapman, *Algebraic Number Theory – summary of notes*. Um resumo de um curso de Teoria Algébrica dos Números que o autor ministrou. A demonstração de que os inteiros algébricos formam um anel foi retirada de lá. Disponível na Internet em

`http://www.secamlocal.ex.ac.uk/people/staff/rjchapma/notes/ant2.pdf`

[4] Guilherme Fujiwara, *Inteiros de Gauss e Inteiros de Eisenstein*, na Eureka! 14. A melhor introdução para $Z[i]$ e $Z[\omega]$.

[5] Carlos Shine, *Um teorema de Gauss sobre uma curva de Fermat*, aula da Semana Olímpica 2005. Um pouco mais sobre cúbicas, mas sob outro ponto de vista. Lá estão somas cúbicas de Gauss e o resultado de $N(x^3 + y^3 = 1)$.