Um teorema de Gauss sobre uma curva de Fermat

1. Senta, que lá vem história!

Era uma vez, um menino muito esperto chamado Gauss. Ele era tão inteligente que, aos 10 anos, podia calcular $1 + 2 + 3 + \cdots + 100$ em pouco segundos!

Esse jovenzinho cresceu e acabou tornando-se um grande matemático, publicando em 1801 o famoso *Disquisiotines Arithmeticae*, no qual mostra diversos resultados na teoria dos números.

Fermat era um advogado que gostava de Matemática. Gostava muito. Não era matemático profissional mas, de tanto provar teoremas essenciais para o desenvolvimento da Matemática, é considerado um dos maiores matemáticos de todos os tempos. Segundo ele mesmo, demonstrou que a equação $x^n + y^n = z^n$ $(*)$ não tem soluções inteiras não triviais para n inteiro maior que 2. A sua demonstração não "caberia na margem". De qualquer forma, a demonstração veio em 1995, três séculos depois.

A partir de $(*)$ vieram as chamadas *curvas de Fermat*, que nada mais são do que as curvas da forma $x^n + y^n = 1$ em R^2.

Gauss provou um teorema bastante interessante sobre a curva de Fermat

$$x^3 + y^3 = 1,$$

só que vista mód p, p primo.

Ah, e Gauss e Fermat não foram contemporâneos. Fermat viveu um século antes de Gauss.

2. E o teorema é...

Antes de mais nada, em vez de pensar na curva

$$x^3 + y^3 = 1$$

vamos pensar na sua versão homogenizada

$$x^3 + y^3 + z^3 = 0$$

e considerar suas soluções no sentido projetivo: vamos ignorar a solução trivial $(0; 0; 0)$ e considerar as soluções $(x; y; z)$ e $(ax; ay; az)$ iguais.

Agora, podemos enunciar o teorema.

Teorema. *(Gauss) Sejam p um número primo positivo e M_p o número de soluções projetivas da congruência*

$$x^3 + y^3 + z^3 \equiv 0 \quad (mód.\ p) \qquad (\star)$$

(a) Se $p \not\equiv 1 \quad (mód.\ 3)$, então $M_p = p + 1$.

(b) Se $p \equiv 1 \quad (mód.\ 3)$, então existem inteiros A e B tais que

$$4p = A^2 + 27B^2$$

A e B são únicos a não ser que troquemos os seus sinais, e se tomarmos o sinal de A tal que $A \equiv 1$ $(mód.\ 3)$, então

$$M_p = p + 1 + A$$

3. E a palavra para o item a é... bijeção!

Vamos fazer a demonstração do item a. Apesar do resultado ser de teoria dos números, a solução é combinatória.

Primeiro, vamos mostrar que o conjunto dos cubos de 0 a $p-1$ reduzidos mód p é igual ao próprio conjunto Z/pZ.

Veja a seguir alguns exemplos:

$p=3$	$p=5$	$p=11$	
$0^3 \equiv 0$	$0^3 \equiv 0$	$0^3 \equiv 0$	
$1^3 \equiv 1$	$1^3 \equiv 1$	$1^3 \equiv 1$	$6^3 \equiv 7$
$2^3 \equiv 2$	$2^3 \equiv 3$	$2^3 \equiv 8$	$7^3 \equiv 2$
	$3^3 \equiv 2$	$3^3 \equiv 5$	$8^3 \equiv 6$
	$4^3 \equiv 4$	$4^3 \equiv 9$	$9^3 \equiv 3$
		$5^3 \equiv 4$	$10^3 \equiv 10$

Como $p \not\equiv 1 \pmod 3$, $p = 3$ ou $p = 3k+2$, k inteiro.

Se $p = 3$, o resultado é imediato, do pequeno teorema de Fermat (olha o Fermat aí de novo, gente!): $x^3 \equiv x \pmod 3$.

Supondo a e b não divisíveis por p,

$$\begin{aligned} a^3 \equiv b^3 \pmod p &\implies a^{3k} \equiv b^{3k} \pmod p \\ &\iff a^{p-2} \equiv b^{p-2} \pmod p \\ &\iff a^{-1} \equiv b^{-1} \pmod p \\ &\iff a \equiv b \pmod p \end{aligned}$$

Se $a \equiv 0 \pmod p$ e $a^3 \equiv b^3 \pmod p$, então $b \equiv 0 \pmod p$.

Assim, todas as p imagens de x^3 mód p, $x = 0, 1, \ldots, p-1$, são distintas, ou seja, só podem ser todos os restos de 0 a $p-1$.

Em outras palavras, o conjunto dos resíduos cúbicos mód p não tem muita graça: é o próprio conjunto de todos os restos mód p! Mas isso tem uma conseqüência interessante: a função x^3 em Z/pZ é uma bijeção e, o mais importante, é inversível (ou se você preferir, invertível).

Logo o número de soluções projetivas de $(\star)$ é igual ao número de soluções projetivas de

$$X + Y + Z \equiv 0 \pmod p \qquad (I)$$

Para demonstrar isso, basta notar que podemos fazer uma bijeção entre as soluções de $(\star)$ e (I): tome $X = x^3$ mód p, $Y = y^3$ mód p e $Z = z^3$ mód p. Como a função x^3 em Z/pZ é uma bijeção, podemos recuperar os valores de x, y e z a partir de X, Y e Z, ou seja, estabelecemos uma outra bijeção entre as soluções $(x;y;z)$ de $(\star)$ e as soluções $(X;Y;Z)$ de (I).

Contar as soluções projetivas de (I). Se você conhecer resultados de planos projetivos finitos, sabe que (I) é uma equação de reta do plano projetivo baseado no corpo Z/pZ e que (I) tem $p+1$ pontos.

Mas você não precisa ser um *expert* em geometria projetiva para contar o número de soluções de (I): temos

$$(I) \iff Z \equiv -X - Y \pmod p$$

Escolhidos X e Y, temos o valor de Z. Há p escolhas para cada uma das variáveis X e Y, mas não podemos escolher $X = Y = 0$, pois isso implicaria $(X;Y;Z) = (0;0;0)$, o que contraria nossa convenção.

Assim, há p^2-1 escolhas válidas para X e Y. Mas, lembrando que $(X;Y;Z)$ e $(aX;aY;aZ)$ são projetivamente a mesma coisa e que há $p-1$ escolhas para a (você não vai escolher $a=0$, vai?), cada tripla está sendo contada $p-1$ vezes, de modo que o total de soluções projetivas de (I) (e, conseqüentemente, de $(\star)$) é $\frac{p^2-1}{p-1} = p+1$. ∎

4. Agora, vamos ao item b!

Quando $p \equiv 1 \pmod 3$, as coisas não são tão simples assim (mas são, de certo modo, mais interessantes). O conjunto dos resíduos cúbicos mód p agora não é todo o conjunto Z/pZ.

Isso levanta uma pergunta bastante natural: quantos são os resíduos cúbicos nesse caso?

4.1. Contando resíduos cúbicos

Vamos primeiro verificar quantas soluções tem a congruência

$$x^3 \equiv 1 \pmod p$$

Fatorando, obtemos

$$x \equiv 1 \pmod p \text{ ou } x^2+x+1 \equiv 0 \pmod p \iff x \equiv 1 \text{ ou } (2x+1)^2 \equiv -3 \pmod p$$

Ironicamente, vamos contar resíduos cúbicos utilizando... reciprocidade quadrática! Será que -3 é resíduo quadrático mód p? Vejamos:

$$\left(\frac{-3}{p}\right)\cdot\left(\frac{p}{-3}\right) = (-1)^{\frac{-3-1}{2}\cdot\frac{p-1}{2}} \iff \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Ou seja, -3 é resíduo quadrático mód p (por isso estamos dividindo os casos mód 3!). Assim, a congruência $x^3 \equiv 1 \pmod p$ tem três soluções distintas 1, u e u^2.

Provamos que três resíduos elevados ao cubo são congruentes a 1 mód p. Na verdade, não é difícil provar que se $a \not\equiv 0 \pmod p$ então a congruência $x^3 \equiv a^3 \pmod p$ tem três soluções distintas (que seriam a, ua e u^2a).

Isso implica uma divisão dos $p-1$ restos a não nulos em subconjuntos de três elementos (todos da forma $\{a;ua;u^2a\}$), sendo que os cubos de elementos de um mesmo subconjunto são congruentes mód p. Assim, podemos concluir que há $\frac{p-1}{3}$ subconjuntos e, portanto, $\frac{p-1}{3}$ resíduos cúbicos não nulos.

4.2. Três mundos disjuntos

Poderíamos ter contados os resíduos cúbicos de outra maneira: a existência de três soluções para $x^3 \equiv 1 \pmod p$ implica a existência de um resíduo não cúbico s (por quê?). Seja R o conjunto dos resíduos cúbicos. Seja $S = sR = \{sr \mid r \in R\}$ o conjunto obtido multiplicando mód p os elementos de R por s. Os conjuntos R e S são disjuntos: primeiro observe que se $r_1, r_2 \in R$ então $r_1r_2 \in R$; se $sr \in R$, então $sr \cdot r^{-1} = s \in R$, absurdo.

Agora, defina $T = s^2R$. Veja que s^2 não é resíduo cúbico pois se fosse o elemento $s \cdot s^2 = s^3$ de S seria resíduo cúbico, o que não pode acontecer já que R e S são disjuntos. Assim, com um argumento análogo ao do parágrafo anterior, provamos que T e R são disjuntos. Para provar que S e T são disjuntos, primeiro veja que $sT = s^3R = R$, pois s^3 é resíduo cúbico. Logo se $sr \in T$ então $s^2r \in R$, ou seja, T e R não seriam disjuntos, absurdo.

Assim, os conjuntos R, S e T são disjuntos e, o mais interessante, têm o mesmo número de elementos. Assim, $|R| = |S| = |T| = \frac{p-1}{3}$.

Veja como fica a partição nos casos $p = 7$, $p = 13$ e $p = 19$:

$p = 7$ e $s = 2$		
R	S	T
1	2	4
6	5	3

$p = 13$ e $s = 3$		
R	S	T
1	3	9
5	2	6
8	11	7
12	10	4

$p = 19$ e $s = 6$		
R	S	T
1	6	17
7	4	5
8	10	3
11	9	16
12	15	14
18	13	2

Daqui em diante, o número $\frac{p-1}{3}$ vai aparecer bastante, então vamos chamá-lo de m para simplificar.

A contagem das soluções de $(\star)$ vai se basear nesses três "mundos" R, S e T. Para o nosso trabalho ficar mais simples, estaremos (em gerundês mesmo)...

5. Introduzindo uma notação

Lembremos que estamos interessados nas soluções $(x; y; z)$ de

$$x^3 + y^3 + z^3 \equiv 0 \pmod{p} \qquad (\star)$$

Mas, assim como fizemos no item a, podemos trocar x^3, y^3 e z^3 por resíduos cúbicos. Assim, podemos pensar nos ternos $(X; Y; Z)$ de elementos de R tais que $X + Y + Z \equiv 0 \pmod{p}$.

Podemos, então, definir $[ABC] = [A, B, C]$ como o número de triplas $(x; y; z)$ tais que $x \in A$, $y \in B$ e $z \in C$ e $x + y + z \equiv 0 \pmod{p}$.

No fundo, o que queremos é $[RRR]$. Será? Vamos calcular o número de soluções M_p de $(\star)$ em função de $[RRR]$. Para cada terno $(X; Y; Z) \in R^3$ tal que $X + Y + Z \equiv 0 \pmod{p}$ correspondem, na verdade, $3^3 = 27$ soluções $(x; y; z)$ de $(\star)$, já que $x^3 \equiv X \pmod{p}$ tem três soluções. Mas como queremos soluções projetivas, ainda devemos dividir tudo por $p - 1 = 3m$. Assim, o número de soluções $(x; y; z)$ de $(\star)$ tais que nenhum dos números x, y, z é zero é $\frac{27[RRR]}{3m} = \frac{9[RRR]}{m}$.

Faltam as soluções com algum dos componentes (mas não todos!) nulos. Digamos que $z = 0$. Ficamos então com $x^3 \equiv -y^3 \equiv (-y)^3 \pmod{p}$. Já vimos que, fixado a, o número de soluções de $x^3 \equiv a^3 \pmod{p}$ é 3. Assim, para cada um dos $p-1$ valores de $-y$ (zero não pode!) há 3 soluções. Assim, há $3(p-1)$ soluções. Analogamente, há $3(p-1)$ soluções quando $x = 0$ e $y = 0$, respectivamente. Lembrando que procuramos soluções projetivas, o total de soluções com alguma das variáveis nula é $\frac{9(p-1)}{p-1} = 9$.

Deste modo,

$$M_p = \frac{9[RRR]}{m} + 9 = 9\left(\frac{[RRR] + m}{m}\right) \qquad (III)$$

Mas, para calcular $[RRR]$, precisamos dos três mundinhos R, S e T e até do solitário $\{0\}$.

A notação $[ABC]$ tem várias propriedades:

- $[AB(C \cup D)] = [ABC] + [ABD]$ se $C \cap D = \emptyset$;
- $[ABC] = [aA, aB, aC]$ para $a \not\equiv 0 \pmod{p}$;
- $[ABC] = [ACB] = [BAC] = [BCA] = [CAB] = [CBA]$.

Vamos começar a partir do fato de que $Z/pZ = \{0\} \cup R \cup S \cup T$ é uma união disjunta:

$$[Z/pZ, R, R] = [\{0\}RR] + [RRR] + [SRR] + [TRR]$$

Mas $[Z/pZ, R, R]$ e $[\{0\}RR]$ são fáceis de contar: o primeiro é o número de soluções de $x+y+z \equiv 0 \pmod{p} \iff x \equiv -y-z \pmod{p}$, com x qualquer e y e z pertencentes a R. Escolhidos y e z, encontramos x. Logo $[Z/pZ, R, R] = |R|^2 = m^2$. O segundo é o número de soluções de $y+z \equiv 0 \pmod{p} \iff y \equiv -z \pmod{p}$. Fixado z, encontramos y. Logo $[\{0\}RR] = m$. Portanto

$$m^2 = m + [RRR] + [SRR] + [TRR] \tag{1}$$

$[SRR]$ e $[TRR]$ não parecem amigáveis; falta simetria. Algo mais simpático parece ser $[RST]$. Vamos dar um jeito de fazê-lo aparecer:

$$[Z/pZ, S, T] = [\{0\}ST] + [RST] + [SST] + [TST] \tag{2}$$

$[Z/pZ, S, T]$ é igual a $[Z/pZ, R, R]$, ou seja, é igual a m^2; já $[SST] = [TSS]$ e $[TST] = [STT]$ são muito parecidos com $[SRR]$ e $[TRR]$. De fato, eles são respectivamente iguais: $[TSS] = [sS, sR, sR] = [SRR]$ e $[TRR] = [sS, sT, sT] = [STT]$. Por fim, $[\{0\}ST]$ é o número de soluções de $y+z \equiv 0 \pmod{p} \iff y \equiv -z \pmod{p}$ com $y \in S$ e $z \in T$. Como $-1 \in R$, $-z \in T$ e como S e T são disjuntos, nunca ocorre $y \equiv -z \pmod{p}$ com $y \in S$ e $-z \in T$, ou seja, $[\{0\}ST] = 0$. Subtraindo (2) de (1), obtemos

$$0 = m + [RRR] - [RST] \iff m + [RRR] = [RST]$$

Substituindo em (III), encontramos que o número de soluções de $(\star)$ é

$$M_p = \frac{9[RST]}{m}$$

Bonitinho, não? Mas como calcular $[RST]$? Aí é que entra...

5.1. Um pouco de Álgebra: raízes da unidade e somas de Gauss

Um artifício bastante utilizado em contagem é o uso de funções geratrizes (para saber um pouco mais sobre elas, veja [5]). Quando estamos trabalhando módulo um primo p, a contagem pode ser feita com o auxílio de raízes p-ésimas da unidade.

A idéia de Gauss é bastante parecida com a idéia de utilizar funções geratrizes.

Desde pequeno, Gauss foi muito bom em somas. Deste modo, ele resolveu fazer a contagem com as famosas *somas de Gauss*. Seja $\zeta = e^{\frac{i2\pi}{p}}$ uma raiz p-ésima primitiva da unidade. Defina

$$\alpha_1 = \sum_{r \in R} \zeta^r$$
$$\alpha_2 = \sum_{s \in S} \zeta^s$$
$$\alpha_3 = \sum_{t \in T} \zeta^t$$

Os números α_1, α_2 e α_3 são as *somas cúbicas de Gauss*, cada uma com m termos.

O que vamos calcular agora é um polinômio cujas raízes são α_1, α_2 e α_3. O surpreendente é que esse polinômio tem coeficientes inteiros!

Mas qual a relação entre esses complexos e a nossa contagem? Vamos calcular $\alpha_2\alpha_3$:

$$\alpha_2\alpha_3 = \sum_{s \in S} \zeta^s \sum_{t \in T} \zeta^t = \sum_{s \in S, t \in T} \zeta^{s+t} = \sum_{1 \le x \le p-1} N_x \zeta^x,$$

sendo N_x o número de pares $(s;t)$ de $S \times T$ tais que $s+t=x \iff s+t+(-x) \equiv 0 \pmod{p}$. Ou seja, $N_x = [ST\{-x\}]$.

Algo sutil: na última soma não está incluído o índice $x=0$. Por quê? Tente você mesmo responder...

Note que se $r \in R$ então $rS=S$, $rT=T$ e $-rx$ pertence ao mesmo mundo de $-x$. Logo

$$N_x = [ST\{-x\}] = [rS, rT, \{-rx\}] = [ST\{-rx\}] = N_{rx},$$

isto é, *se x_1 e x_2 pertencem a um mesmo mundo, então $N_{x_1} = N_{x_2}$, ou seja, para achar N_x só precisamos achar o mundo de x.*

Deste modo, lembrando que $-1 \in R$, "multiplicando por R dos dois lados", obtemos

$$mN_x = [S,T,Rx] = \begin{cases} [STR] & \text{se } x \in R \\ [STS] & \text{se } x \in S \\ [STT] & \text{se } x \in T \end{cases}$$

Sejam a, b e c inteiros tais que

$$[STR] = ma, \quad [STS] = mb, \quad [STT] = mc$$

Logo $M_p = 9a$ e

$$\alpha_2\alpha_3 = \sum_{1 \le x \le p-1} N_x \zeta^x = \sum_{x \in R} N_x\zeta^x + \sum_{x \in S} N_x\zeta^x + \sum_{x \in T} N_x\zeta^x = a\sum_{x \in R}\zeta^x + b\sum_{x \in S}\zeta^x + c\sum_{x \in T}\zeta^x = a\alpha_1 + b\alpha_2 + c\alpha_3$$

Podemos concluir, com duas contas análogas, que

$$\begin{aligned} \alpha_2\alpha_3 &= a\alpha_1 + b\alpha_2 + c\alpha_3 \\ \alpha_3\alpha_1 &= a\alpha_2 + b\alpha_3 + c\alpha_1 \\ \alpha_1\alpha_2 &= a\alpha_3 + b\alpha_1 + c\alpha_2 \end{aligned}$$

A partir daqui, fazemos contas. Tenha sempre em mente que, sendo $M_p = 9a$, nossa meta é encontrar a.

Vamos calcular o polinômio cujas raízes são α_1, α_2 e α_3. Para isso precisamos de

$$\alpha_1 + \alpha_2 + \alpha_3, \quad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1, \quad \alpha_1\alpha_2\alpha_3$$

A soma é até simples. Quando somamos as três somas α_1, α_2 e α_3, obtemos a soma de todas as potências de ζ, exceto ζ^0:

$$\alpha_1 + \alpha_2 + \alpha_3 = \sum_{k=1}^{p-1} \zeta^k = \zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta = \zeta \cdot \frac{\zeta^{p-1}-1}{\zeta - 1} = \frac{\zeta^p - \zeta}{\zeta - 1} = \frac{1-\zeta}{\zeta-1} = -1$$

A soma dos produtos tomados dois a dois é obtida somando as três expressões para $\alpha_i\alpha_j$:

$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = (a+b+c)(\alpha_1 + \alpha_2 + \alpha_3) = -(a+b+c)$$

Mas

$$m(a+b+c) = [STR] + [STS] + [STT] = [ST(R \cup S \cup T)] = [ST(Z/pZ - \{0\})] = [S,T,Z/pZ] - [ST\{0\}] = m^2$$

e, portanto,

$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = -m$$

Para achar o produto, fazemos

$$\begin{aligned}\alpha_1(\alpha_2\alpha_3) &= a\alpha_1^2 + b\alpha_1\alpha_2 + c\alpha_3\alpha_1\\ \alpha_2(\alpha_3\alpha_1) &= a\alpha_2^2 + b\alpha_2\alpha_3 + c\alpha_1\alpha_2\\ \alpha_3(\alpha_1\alpha_2) &= a\alpha_3^2 + b\alpha_3\alpha_1 + c\alpha_2\alpha_3\end{aligned}$$

Somando, obtemos

$$3\alpha_1\alpha_2\alpha_3 = a(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + (b+c)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)$$

Já temos $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = -m$. Além disso, a soma dos quadrados é $(\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) = 1 + 2m$. Logo

$$3\alpha_1\alpha_2\alpha_3 = a(1+2m) - (b+c)m = a + m(2a - b - c) = a + m(2a - (m-a)) = a + m(3a - m)$$

Seja $k = 3a - m$. Assim,

$$M_p = 9a = 3(m+k) = 3m + 3k = p - 1 + 3k = p + 1 + (3k - 2),$$

o que sugere que o A do teorema é $3k - 2$ (que é congruente a 1 mód 3, que coincidência!).

O nosso querido polinômio é

$$F(t) = t^3 + t^2 - mt - \frac{a + km}{3}$$

Bom, encontramos o A. Falta provar que esse A é aquele que está no enunciado do teorema, ou seja, que é o único inteiro congruente a 1 mód 3 tal que $4p = A^2 + 27B^2$, sendo B um outro inteiro.

Para a demonstração definitiva do teorema, precisamos de mais uma arma:

5.2. Discriminante de uma equação de terceiro grau

A palavra *discriminante* não deve ser estranha para você. Ela é um outro nome para o nosso famoso Δ. Ele nos diz se uma equação do segundo grau tem duas raízes reais distintas, uma raiz real dupla ou duas raízes não reais (ele *discrimina*, daí o nome *discriminante*).

Existe um discriminante para equações do terceiro grau. Como deve ser a sua fórmula?

Antes de responder, vamos escrever o nosso famoso Δ em função das raízes x_1 e x_2 de $x^2 + bx + c = 0$ (cuidado, aqui $a = 1$):

$$\Delta = b^2 - 4c = (-(x_1 + x_2))^2 - 4x_1x_2 = (x_1 - x_2)^2$$

Ou seja, Δ, nesse caso, é o quadrado da diferença das raízes. Se $\Delta = 0$ sabemos que $x_1 = x_2$, ou seja, temos raízes duplas. Para equações de terceiro grau, estamos um pouco mais interessados em raízes duplas. Por que não definir o *discriminante de uma equação de terceiro grau* de raízes α_1, α_2 e α_3 como o produto do quadrado da diferença entre duas raízes?

$$D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2$$

Se $P(x) = x^3 + bx + c$, a fórmula para o discriminante é simples: $D_P = -4b^3 - 27c^2$. Esse 27 parece familiar? Ele aparece no nosso teorema!

A aplicação no teorema vai vir a partir do uso de discriminantes e algumas transformações em $F(t)$.

Como

$$\begin{aligned}
&(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)\\
&=\alpha_2\alpha_3(\alpha_2-\alpha_3)+\alpha_3\alpha_1(\alpha_3-\alpha_1)+\alpha_1\alpha_2(\alpha_1-\alpha_2)\\
&=(a\alpha_1+b\alpha_2+c\alpha_3)(\alpha_2-\alpha_3)+(a\alpha_2+b\alpha_3+c\alpha_1)(\alpha_3-\alpha_1)+(a\alpha_3+b\alpha_1+c\alpha_2)(\alpha_1-\alpha_2)\\
&=(b-c)(\alpha_1^2+\alpha_2^2+\alpha_3^2-\alpha_1\alpha_2-\alpha_2\alpha_3-\alpha_3\alpha_1)\\
&=(b-c)(1+3m)=(b-c)p,
\end{aligned}$$

o discriminante de $F(t)$ é $D_F=(b-c)^2p^2$.

Veja que

$$F(t)=t^3+t^2-mt-\frac{a+km}{3}$$

não é da forma t^3+Mt+N. Então, vamos trocar t por outra coisa para cancelar o termo em t^2. Temos

$$\begin{aligned}
F(t+C)&=(t+C)^3+(t+C)^2-m(t+C)-\frac{a+mk}{3}\\
&=t^3+(3C+1)t^2+(3C^2+2C-m)t+C^3+C^2-mC-\frac{a+mk}{3}
\end{aligned}$$

Assim, escolhemos $C=-1/3$, obtendo

$$\begin{aligned}
F\left(t-\frac{1}{3}\right)&=t^3-\frac{1+3m}{3}t+\frac{2}{27}-\frac{a+mk-m}{3}\\
&=\frac{1}{27}((3t)^3-3p(3t)+2-9a-9mk+9m)\\
&=\frac{1}{27}((3t)^3-3p(3t)+2-3(3a-m)+6m-9mk)\\
&=\frac{1}{27}((3t)^3-3p(3t)+2-3k-3m(2-3k))\\
&=\frac{1}{27}((3t)^3-3p(3t)-(3k-2)(3m+1))\\
&=\frac{1}{27}((3t)^3-3p(3t)-Ap)
\end{aligned}$$

Parece valer a pena definirmos

$$G(x)=x^3-3px-Ap$$

Note que $G(x)=G(3t)=27F\left(t-\frac{1}{3}\right)=27F\left(\frac{x-1}{3}\right)$ e, portanto, $F(x)=G(3x+1)/27$. Ou seja, as raízes de $G(x)$ são $\beta_1=3\alpha_1+1$, $\beta_2=3\alpha_2+1$ e $\beta_3=3\alpha_3+1$. Considerando que $\beta_i-\beta_j=3(\alpha_i-\alpha_j)$, o discriminante de G é

$$D_G=27^2D_F$$

Utilizando a fórmula para o discriminante de $x^3+bx+c=0$, obtemos

$$-4(-3p)^3-27(-Ap)^2=27^2(b-c)^2p^2\iff 4p=A^2+27(b-c)^2$$

Tome $B=b-c$ e chegamos, finalmente, em

$$4p=A^2+27B^2$$

Só falta provar que...

5.3. A representação na forma $4p = A^2 + 27B^2$ é única

Aqui, mais contas! Suponha que haja alguma outra representação $4p = A_1^2 + 27B_1^2$. Igualar as duas representações não parece ser muito sensato, já que perdemos o primo p. Vamos utilizar a seguinte fatoração "esperta":

$$4p(B^2 - B_1^2) = (A_1^2 + 27B_1^2)B^2 - (A^2 + 27B^2)B_1^2 = (AB_1 + A_1B)(AB_1 - A_1B)$$

Isso implica que p divide $AB_1 + A_1B$ ou $AB_1 - A_1B$. Suponha, sem perda de generalidade, que divide $AB_1 - A_1B$ (se não, é só trocar o sinal de A_1, por exemplo).

Multiplicando as duas representações, obtemos

$$\begin{aligned} 16p^2 &= A^2A_1^2 + 27B^2A_1 + 27B_1^2A^2 + 27^2B^2B_1^2 \\ &= (AA_1 + 27BB_1)^2 + 27(B^2A_1^2 - 2BA_1 \cdot B_1A + B_1^2A^2) \\ &= (AA_1 + 27BB_1)^2 + 27(BA_1 - B_1A)^2 \end{aligned}$$

Como p divide $BA_1 - B_1A$, divide também $AA_1 + 27BB_1$. Assim,

$$16 - \left(\frac{AA_1 + 27BB_1}{p}\right)^2 = 27\left(\frac{BA_1 - B_1A}{p}\right)^2$$

O lado esquerdo é menor ou igual a 16 e é igual a um múltiplo não negativo de 27. Esse múltiplo só pode ser zero. Portanto

$$BA_1 - B_1A = 0 \iff \frac{A_1}{A} = \frac{B_1}{B} = \lambda$$

Substituindo $A_1 = \lambda A$ e $B_1 = \lambda B$ em $A^2+27B^2 = A_1^2+27B_1^2$, obtemos $\lambda = \pm 1$. Ou seja, a representação é única, a não ser de sinal. Como $A = 3k - 2$, k inteiro, $A \equiv 1 \pmod 3$, de modo que só há um valor possível para A. ∎

6. Curiosidades

- A curva $x^3 + y^3 = 1$ que acabamos de estudar é um caso particular de curva elíptica. Pode-se provar (e isso é bastante difícil) que se M_p é a quantidade de pontos projetivos (em Z/pZ) de uma curva elíptica homogenizada então
$$|M_p - p - 1| \leq 2\sqrt{p}$$
(caso particular – isso mesmo! – do teorema de Hasse-Weil)
- Os números α_1, α_2 e α_3 são na verdade reais! Podemos nos perguntar: qual é a menor de todas? A resposta é que depende do primo $p \equiv 1 \pmod 3$. E tudo que se sabe é que os primos desses três tipos são igualmente distribuídos!
- Para resolver algumas equações diofantinas, podemos vê-la módulo algum número inteiro. De fato, para equações do tipo
$$aX^2 + bY^2 = cZ^2, \qquad (**)$$
sendo a, b e c números inteiros, existe um inteiro m, que depende de a, b e c tal que a equação admite solução diferente de $(0;0;0)$ se, e somente se, a congruência
$$aX^2 + bY^2 \equiv cZ^2 \pmod m$$
admite soluções com X, Y e Z primos com m (esse é um teorema demonstrado por Legendre, o mesmo do símbolo de Legendre, que usamos no artigo).

Como a maioria das cônicas pode ser reduzida, na sua forma projetiva, a $(**)$, o problema de encontrar pontos de coordenadas racionais em cônicas é relativamente simples.

Todavia, não existe nenhum critério parecido para cúbicas. Na verdade, Selmer deu o seguinte contra-exemplo: a equação

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

não admite soluções diferentes de $(0;0;0)$ mas a congruência

$$3X^3 + 4Y^3 + 5Z^3 \equiv 0 \pmod{m}$$

admite soluções com X, Y e Z primos entre si para todo inteiro m.

A cúbica que estudamos nesse arquivo é "quase" um outro exemplo. Tirando $p = 2, 7, 13$, a congruência $X^3 + Y^3 + Z^3 \equiv 0 \pmod{p}$ admite soluções não triviais.

Exercícios

01. Seja p um número primo ímpar. Prove que o número de soluções projetivas da congruência

$$x^2 + y^2 + z^2 \equiv 0 \pmod{p}$$

é $p + 1$.

Observação: o argumento que conheço para provar isso usa Álgebra Linear.

02. Prove que o número de resíduos quadráticos não nulos módulo p primo ímpar positivo é $\frac{p-1}{2}$.

03. Verifique que se $p \equiv 1 \pmod{3}$ então a congruência $x^3 \equiv a^3 \pmod{p}$ tem três soluções.

04. Prove as propriedades

- $[AB(C \cup D)] = [ABC] + [ABD]$ se $C \cap D = \emptyset$;
- $[ABC] = [aA, aB, aC]$ para $a \not\equiv 0 \pmod{p}$;
- $[ABC] = [ACB] = [BAC] = [BCA] = [CAB] = [CBA]$.

05. Prove que se $r \in R$, $s \in S$ e $t \in T$, então

$$\begin{array}{lll} rR = R & rS = S & rT = T \\ sR = S & sS = T & sT = R \\ tR = T & tS = R & tT = S \end{array}$$

06. Aqui vamos resolver o problema 6 da IMO 1995 (Canadá) com o auxílio de funções geratrizes.

O enunciado do problema é:

Seja p um número primo ímpar. Determine o número de subconjuntos de $\{1;2;3;\ldots;2p\}$, com p elementos cuja soma é divisível por p.

(a) Considere o polinômio em duas variáveis

$$f(y,z) = (1+yz)(1+yz^2)(1+yz^3)\cdots(1+yz^{2p})$$

Prove que o termo em $y^k z^s$ em $f(y,z)$ é igual ao número de subconjuntos de $\{1,2,\ldots,2p\}$ de k elementos cuja soma é s.

(b) Utilizando a raiz p-ésima da unidade $\zeta_p = e^{\frac{i2\pi}{p}}$, calcule $f(y,\zeta_p)$.

(c) A partir da sua resposta do item anterior, que tipo de polinômio (em z) deve ser o termo em y^p em $f(y,z)$?

(d) Resolva o problema 6 da IMO 1995.

07. Prove que o discriminante da equação $x^3 + bx + c = 0$ é $D = -4b^3 - 27c^2$.

08. Existem somas quadráticas de Gauss, também. Seja p um primo ímpar e $\zeta_p = e^{\frac{i2\pi}{p}}$ uma raiz p-ésima primitiva da unidade. Seja R o conjunto dos resíduos quadráticos não nulos mód p e N o conjunto dos não resíduos quadráticos.

(a) Prove que $-1 \in R$ se, e somente se, $p \equiv 1 \pmod 4$, ou seja, que -1 é resíduo quadrático se, e somente se, p é da forma $4k + 1$, k inteiro.

(b) Defina as somas quadráticas de Gauss como

$$\alpha = \sum_{r \in R} \zeta^r, \qquad \beta = \sum_{n \in N} \zeta^n$$

Prove que $\alpha + \beta = -1$ e

$$\alpha\beta = \begin{cases} -\frac{p-1}{4} & \text{se } p \equiv 1 \pmod 4 \\ \frac{p+1}{4} & \text{se } p \equiv 3 \pmod 4 \end{cases}$$

(c) Encontre os possíveis valores de α. Se possível (essa é a parte mais difícil!!), encontre o valor certo de α. Bom, com alguns casos pequenos, você encontra, mas provar é outra história...

09. Prove que o teorema de Hasse-Weil é verdadeiro para a curva que estudamos.

10. Prove que os números α_1, α_2 e α_3 são reais.

11. Prove que para todo p primo exceto 2, 7 e 13, a congruência

$$X^3 + Y^3 + Z^3 \equiv 0 \pmod p$$

admite soluções não triviais, ou seja, com $XYZ \not\equiv 0 \pmod p$.

7. Referências Bibliográficas

[1] Uma biografia de Gauss pode ser encontrada no site

`http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Gauss.html`

[2] O teorema e a sua demonstração foram extraídas e adaptadas do livro *Rational Points on Elliptic Curves*, de Joseph H. Silverman e John Tate. Esse livro é uma pequena introdução à fascinante geometria algébrica, tratando somente de curvas elípticas. Uma *curva elíptica* é uma curva da forma $y^2 = f(x) = x^3 + bx^2 + cx + d$. O nome "elíptico" vem do fato de que para calcular o comprimento de um arco de elipse aparecem integrais envolvendo funções do tipo $y = \sqrt{f(x)}$.

[3] Mas, como as demonstrações da referência [2] eram todas baseadas em fatos da teoria dos grupos, resolvi fazer algumas "traduções" para fatos de teoria dos números e combinatória. Alguns resultados de teoria dos números podem ser encontrados em diversos artigos da Eureka!, como *Divisibilidade, Congruências* e *Aritmética Módulo n*, do meu amigo flamenguista Carlos Gustavo T. de A. Moreira, o Gugu, e *A Lei da Reciprocidade Quadrática*, do Gugu e do outro grande matemático Nicolau Corção Saldanha.

[4] O exercício 1 na verdade está em um dos capítulo de um dos meus livros favoritos, o *Proofs From The Book*, de Martin Aigner e Gunter M. Ziegler. Pode ser qualquer uma das duas edições. A segunda, inclusive, pode ser encontrada em português, sob o título *As Provas Estão n'O Livro*, traduzido por Marcos Botelho (ITA) e revisado por Elza Gomide (IME-USP).

[5] Um artigo de funções geratrizes, na Eureka!: Eduardo Tengan, Séries Formais. Artigo da Revista Eureka! 11.

[6] Outras técnicas em Combinatória podem ser encontradas no treinamento para a IMO, no site

`http://www.teorema.mat.br/imo/`

Veja, em particular, o artigo *Combinatória: um Conjunto de Técnicas*, de minha autoria, em

`http://www.teorema.mat.br/imo/combinatoria.ps`

Lá está resolvido, de duas maneiras, o problema 6 da IMO 1995.