# 「ガウスの数論世界をゆく」p.106 の計算について

第 5 章 4 次のガウス周期　5.5 節 4 次曲線の有理点の個数 p.106〜107 では、次で定義される 4 次曲線の $\mathbb{F}_p-$ 有理点で $x,\, y \neq \overline{0}$ であるもの

$$S(i,\, j) := \{(x,\, y) : \overline{g}^j y^4 = \overline{g}^i x^4 + \overline{1} \quad x,\, y \in \mathbb{F}_p^{\times}\}$$

の個数 $n(i,\, j)$ について計算している。

$p \equiv 1 \pmod 8$ のときは、

$n(0,\, 0) = \alpha_0, \quad n(1,\, 0) = \alpha, \quad n(2,\, 0) = \beta, \quad n(3,\, 0) = \gamma, \quad n(1,\, 2) = \delta$

とおく。

2 次曲線に関して種々の計算を行って

$$\alpha_0 + \alpha + \beta + \gamma = 4(p-5) \qquad \cdots \qquad (5.7)$$
$$\alpha + \gamma + 2\delta = 4(p-1) \qquad \cdots \qquad (5.8)$$
$$\beta + \delta = 2(p-1) \qquad \cdots \qquad (5.9)$$

を得る。

さらに、これらの式から

$$\beta = \tfrac{\alpha+\gamma}{2} \qquad \cdots \qquad (5.10)$$
$$\alpha_0 = -\beta + 2\delta - 16 \qquad \cdots \qquad (5.11)$$

と整理しておく。

5 つの未知数 $\alpha_0,\, \alpha,\, \beta,\, \gamma,\, \delta$ に対して、方程式は $(5.7),\ (5.8),\ (5.9)$ の 3 つしかない。

そこで、4 次曲面

$$\mathcal{S} : x^4 + \overline{g}y^4 + \overline{g}^2 z^4 + \overline{1} = \overline{0}$$

を導入し、$x,\, y,\, z \in \mathbb{F}_p^{\times}$ であるものの個数を $n(i,\, j)$ に結びつける 2 通りの見方で計算し、次の等式を得る。

$$\alpha_0\delta + \alpha^2 + \beta\gamma + \gamma\delta = \alpha\beta + \gamma\delta + \delta\beta + \delta^2$$

この式に $(5.\ 11)$ を代入して整理すると

$$\delta^2 - (2\beta + 16)\delta + \alpha^2 + \beta(\alpha - \gamma) = 0 \qquad \cdots \qquad ①$$

さらに、$(5.\ 10)$ を代入し、また、$(5.\ 9)$ をうまく使っていくと、

$$\left(\frac{\beta-\delta}{4} + 1\right)^2 + \left(\frac{\alpha-\gamma}{8}\right)^2 = p \qquad \cdots \qquad (5.15)$$

を得る。すると、

$$p = a^2 + b^2 \qquad (a \equiv 1 \pmod 4, b \text{ は正の偶数})$$

の解に結びつく。

問題なのは、①から式 $(5.15)$ への変形である。テキストに書いてある指示通り計算を進めていくと到達するが、どうしてそうするのか理由がわかりにくい。そこで、自分なりに考えた計算方法を以下に述べる。

$\beta + \delta = 2(p-1) \quad \cdots \quad (5.9)$ に加えて $\beta - \delta$ の値がわかれば $\beta,\, \delta$ の値がわかる。（テキストにもそう述べられている。）

そのため、$\beta-\delta=2X,\ p-1=q$ とおいて、$\beta=q+X,\ \delta=q-X$
また、$\alpha+\gamma=2\beta \quad \cdots \quad (5.10)'$ に対して、$\alpha-\gamma=2Y$ とおいて、
$\alpha=\beta+Y=q+X+Y,\ \gamma=q+X-Y$ となる。
これらを① に代入して、

$$(q-X)^2-(2q+2X+16)(q-X)+(q+X+Y)^2+(q+X)\cdot(-2Y)=0$$

$$(X^2-2qX+q^2)-(2q^2-2X^2+16q-16X)$$
$$+(X^2+Y^2+q^2+2XY+2qX+2qY)-(2XY+2qY)=0$$

$$4X^2+Y^2+16X-16q=0 \qquad 4(X+2)^2+Y^2=16(q+1)$$

$$\left(\frac{X}{2}+1\right)^2+\left(\frac{Y}{4}\right)^2=q+1$$

従って、

$$\left(\frac{\beta-\delta}{4}+1\right)^2+\left(\frac{\alpha-\gamma}{8}\right)^2=p \qquad \cdots \qquad (5.15)$$

が成り立つ。
なお、5 つの未知数に対して方程式は 4 つであるが、最後の方程式の整数解で所定の条件を満たすものがただ 1 つ存在することから、5 つの未知数の値が決まる。

$p\equiv 5 \pmod 8$ のときは、
$n(0,\,2)=\alpha_0, \quad n(0,\,3)=\alpha, \quad n(0,\,0)=\beta, \quad n(0,\,1)=\gamma, \quad n(1,\,0)=\delta$
とおく。
2 次曲線に関して種々の計算を行って

$$\beta+\delta=2(p-5) \qquad \cdots \qquad (5.21)$$
$$\alpha_0=-\beta+2\delta \qquad \cdots \qquad (5.22)$$
$$\alpha+\gamma=2(\beta+8) \qquad \cdots \qquad (5.23)$$

を得る。
また、4 次曲面

$$\mathcal{S}:\ x^4+\overline{g}y^4+\overline{g}^2z^4+\overline{1}=\overline{0}$$

上の点で、$x,\,y,\,z\in\mathbb{F}_p^{\times}$ であるものの個数を $n(i,\,j)$ に結びつける 2 通りの見方で計算し、次の等式を得る。

$$\beta\delta+\gamma\alpha+\alpha_0\gamma+\alpha\delta=\delta\beta+\delta^2+\alpha\beta+\gamma\delta$$

この式に (5. 22) を代入して整理すると

$$\delta^2+(\beta-\delta)(\alpha-\gamma)-\alpha\gamma=0 \qquad \cdots \qquad ②$$

$\beta+\delta=2(p-5)$ に対して、$\beta-\delta=2X,\ p-5=q$ とおいて、$\beta=q+X,\ \delta=q-X$
また、$\alpha+\gamma=2\beta+16=2q+2X+16 \quad \cdots \quad (5.23)'$
に対して、$\alpha-\gamma=2Y$ とおいて、
$\alpha=q+X+8+Y,\ \gamma=q+X+8-Y$ となる。
これらを② に代入して、

$$(q-X)^2-2X(2q+2X+16)-(q+X+18+Y)(q+X+18-+Y)=0$$

$$(X^2-2qX+q^2)-\left\{4X^2+4(q+8)X\right\}-\left\{(q+X+8)^2-Y^2\right\}=0$$

$$(X^2-2qX+q^2)-\left\{4X^2+4(q+8)X\right\}-\left\{X^2+q^2+64+2(q+8)X+16q-Y^2\right\}=0$$

$$4X^2+Y^2+16X-16(q+4)=0 \qquad 4(X+2)^2+Y^2=16(q+5)$$

$$\left(\frac{X}{2}+1\right)^2+\left(\frac{Y}{4}\right)^2=q+5$$

従って、

$$\left(\frac{\beta-\delta}{4}+1\right)^2+\left(\frac{\alpha-\gamma}{8}\right)^2=p \qquad \cdots \qquad (5.25)$$

が成り立つ。

すると、

$$p=a^2+b^2 \qquad (a\equiv 3 \pmod 4, b\text{は正の偶数})$$

の解に結びつく。

それにしても、こんなにうまく結びつくということを式を眺めていて思いつくものなのだろうか？背景に何かがあり、結びつくのがもっともだとわかるのではないかと思われる。