ある合同式の解の個数

高校 2 年 2 組 49 番　三谷庸

1　はじめに

本日は数学研究部にお越しいただきありがとうございます。

この記事では、合同方程式

$$\sum_{k=1}^{n} x_i^m \equiv 0 \pmod{p} \tag{1}$$

の解がいくつあるかについて書いていきます。ここで、$A \equiv B \pmod{p}$ とは、$A - B$ が p で割り切れることを意味します。

高校生までの知識があれば読めるようになっています。

2　初等的考察

(1) の解の個数を N_p とかきます。

m, p がある条件を満たす場合は解の個数は簡単に決定できます。

準備として定理を 2 つ挙げておきます。

定理 1. 素数 p について、ある g が存在して、 $\bmod p$ で

$$1, 2, \ldots, p-1 = 1, g, g^2, \ldots, g^{p-2}$$

が成り立つ。これを原始根という

定理 2 (フェルマーの小定理)**.** p が素数で a が p に互いに素なとき、

$$a^{p-1} \equiv 1 \pmod{p}$$

どちらも有名な定理なので証明は省略します。初等整数論の本を見ると書いてあると思います。

これを使って、次のことがわかります。

定理 3. $(p-1,m)=1$ のとき、$N_p=p^{n-1}$ となる。

証明. mod p の原始根 g をとる。任意の k に対して、$ml\equiv k \pmod{p-1}$ となる l が取れる。

よって、任意の $x_1,x_2,\dots x_{n-1}$ に対して、$g^k=-(x_1^m+x_2^m+\cdots+x_{n-1}^m)$ となる k をとり、上のような l に対して $x_n=g^l$ とすれば 1 を満たす。よって、N_p は $x_1,x_2,\dots x_{n-1}$ の選び方に等しく、p^{n-1} となる。 □

よって、以下 $p\equiv 1 \pmod{m}$ とします。この場合も $N_{p,m}$ の値はが p^{n-1} に近くなることが期待されます。このことを示していきます。

3 一般の場合

この章では、次の主張を示します。

N_p は、

$$|N_p-p^{n-1}|\le (d-1)^n(p-1)p^{\frac{n}{2}-1}$$

を満たす。(d は $p-1$ と m の最大公約数)

以下、「$x_1^m+x_2^m+\dots x_n^m$ が mod p で 0 ならば値が 1、そうでないならば値が 0 となるような関数」をうまく作り、その大きさを評価することで N_p の大きさを決定していきます。

定義 1. 実数 t に対して、

$$\mathbf{e}(t)=\cos 2\pi t+i\sin 2\pi t$$

と定める。($\mathbf{e}(t)=e^{2\pi it}$ である)

この関数は、普通の指数関数と同様の性質をもちます (指数法則が成り立ちます)。この関数の性質で必要なものを準備しておきます。

定理 4. *1.* 実数 t に対して、$|\mathbf{e}(t)|=1$

2. t が整数 $\Leftrightarrow \mathbf{e}(t)=1$

定理 5. a,d が整数で $d>0$ のとき、

$$\sum_{x=0}^{d-1}\mathbf{e}(\frac{ax}{d})\begin{cases}=d & (d|a)\\ =0 & (d\not|a)\end{cases}$$

ここで、$d|a$ とは、a が d で割り切れることを意味する。

証明. $d|a$ のときは各項の値が全て 1 になるので良い。

$d \not| a$ のとき、$\mathbf{e}(a/d) \neq 1 m, \mathbf{e}(ad/d) = 1$ なので、等比数列の和の公式を使うと (左辺)$=\dfrac{\mathbf{e}(ad/d)-1}{\mathbf{e}(a/d)-1} = 0$ となる。

□

定義 2. 素数 p に対して、二つの記号 $\mathbb{F}_p, \mathbb{F}_p^*$ を、

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}, \mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$$

を $\mod p$ でみたものとする。

定義 3. 整数 t に対して、

$$f(t) = \sum_{x \in \mathbb{F}_p} \mathbf{e}(\frac{x^m t}{p})$$

とする。

定理 6.

$$N_p = \frac{1}{p} \sum_{t \in \mathbb{F}_p} f(t)^n$$

証明.

$$\begin{aligned}\sum_{t \in \mathbb{F}_p} f(t)^n &= \sum_{t \in \mathbb{F}_p} \sum_{x_i \in \mathbb{F}_p} \mathbf{e}(\frac{x_1^m t}{p}) \ldots \mathbf{e}(\frac{x_n^m t}{p}) \\ &= \sum_{t \in \mathbb{F}_p} \sum_{x_i \in \mathbb{F}_p} \mathbf{e}(\frac{(x_1^m + x_2^m + \ldots x_n^m)t}{p}) \\ &= pN_p\end{aligned}$$

最後の等式で定理 3 を用いた。 □

あとは関数 f の大きさを評価すればよいことになります。定理 6 の式で、$t = 0$ の部分を別に計算すると、

$$N_p = p^{n-1} + \frac{1}{p} \sum_{t \in \mathbb{F}_p^*} f(t)^n$$

がわかります。この式の第二項の大きさについてみていきます。

$p-1$ と m の最大公約数を d とします。ここでは、$d \neq 1$ とします。(最初の仮定)

定義 4. 集合 A を F_p^* での m 乗数全体の集合とする。

まず、A の性質について見ていきます。

原始根 g をとると、$A = \{g^m, g^{2m}, \ldots, g^{(p-1)m}\}$ となります。$e \equiv f \pmod{p-1}$ のとき $g^e \equiv g^f \pmod{p}$ が成り立つことから (フェルマーの小定理)、次のことがわかります。

- A は $\dfrac{p-1}{d}(= k$ とする) 個の元からなる集合である
- 任意の A の元 a に対して、$x^m \equiv a \pmod{p}$ となる x は d 個ある。

このことから、

$$f(t) = 1 + d\sum_{x\in A} \mathbf{e}(\frac{xt}{p})$$

となります。

さらに扱いやすい形に書き換えます。

定義 5. 原始根 g を固定し、$i = 1, 2, \ldots, d-1$ に対して、F_p^* から $\mathbb{C}$ への写像 (関数)χ_i を、

$$\chi_i(g^l) = \mathbf{e}(\frac{li}{d})$$

により定める。

$g^{l_1} \equiv g^{l_2} \pmod{p}$ すなわち $l_1 \equiv l_2 \pmod{p-1}$ のとき、$l_1 - l_2 \equiv 0 \pmod{d}$ なので、$\mathbf{e}(\dfrac{l_1 i}{d})$ と $\mathbf{e}(\dfrac{l_2 i}{d})$ の値は等しい。

よってこのように定めてよい。

定義 6. $i = 1, 2, \ldots d-1$ と $t \in \mathbb{F}_p^*$ に対して、

$$\tau(i,t) = \sum_{x\in\mathbb{F}_p^*} \chi_i(x)\mathbf{e}(\frac{xt}{p})$$

と定める。

定理 7.

$$f(t) = 1 + \sum_{i=0}^{d-1} \tau(i,t)$$

が成り立つ。

証明.

$$\sum_{i=0}^{d-1} \tau(i,t) = \sum_{i=0}^{d-1}\sum_{x\in\mathbb{F}_p} \chi_i(x)\mathbf{e}(\frac{xt}{p}) = \sum_{x\in\mathbb{F}_p}\sum_{i=0}^{d-1} \mathbf{e}(\frac{li}{d})\mathbf{e}(\frac{xt}{p})$$

ここで、

$$\sum_{i=0}^{d-1} \mathbf{e}(\frac{li}{d})$$

の値は x が d 乗数 ($\Leftrightarrow$ l が g の倍数) のとき d、そうでないとき 0 となる。よって、上の式の値は

$$d\sum_{i=0}^{d-1} \mathbf{e}(\frac{xt}{p})$$

となるので、定理が成り立つことがわかる。 □

あとは $\tau(i,t)$ の値の大きさを評価すれば N_p の大きさがわかります。

定理 8.
- $i=0$ のとき、$\tau(i,t)=-1$ が成り立つ。
- 上記以外のとき、$|\tau(i,t)|=\sqrt{p}$ が成り立つ。

証明. $i=0$ のときは、定理 3 より、

$$\begin{aligned}\tau(0,t) &= \sum_{x\in\mathbb{F}_p^*} \mathbf{e}(\frac{xt}{p}) \\ &= -1 + \sum_{x\in\mathbb{F}_p} \mathbf{e}(\frac{xt}{p}) \\ &= -1\end{aligned}$$

となるので成り立つ。

そうでないとき、χ_i を単に χ と書くことにすると、

$$|\tau(i,t)|^2 = \tau(i,t)\overline{\tau(i,t)} = \sum_{x,y\in\mathbb{F}_p^*} \chi(x)\mathbf{e}(\frac{xt}{p})\overline{\chi(y)\mathbf{e}(\frac{yt}{p})} =$$

ここで、$x=yz$ とすると、

$$\chi(x)\overline{\chi(y)} = \chi(yz)\overline{\chi(y)} = \chi(y)\chi(z)\overline{\chi(y)} = \chi(z)$$

および

$$\mathbf{e}(\frac{yzt}{p})\overline{\mathbf{e}(\frac{yt}{p})} = \mathbf{e}(\frac{yt(z-1)}{p})$$

が成り立つので、

$$|\tau(i,t)|^2 = \sum_{y,z\in\mathbb{F}_p^*} \chi(z)\mathbf{e}(\frac{yt(z-1)}{p})$$

$$= \sum_{z\in\mathbb{F}_p^*} \chi(z)(-1+\sum_{y\in\mathbb{F}_p} \mathbf{e}(\frac{yt(z-1)}{p}))$$

$$= -\sum_{z\in\mathbb{F}_p^*} \chi(z) + \sum_{z\in\mathbb{F}_p^*} \chi(z) \sum_{y\in\mathbb{F}_p} \mathbf{e}(\frac{yt(z-1)}{p})$$

となる。ここで定理 3 を用いると、($\tau(i,t)$ は $t\in\mathbb{F}_p^*$ で定義されることに注意)

$$\sum_{y\in\mathbb{F}_p} \mathbf{e}(\frac{yt(z-1)}{p})$$

は $z=1$ のとき p、それ以外のとき 0 となる。同じく定理 3 より、$\sum_{z\in\mathbb{F}_p} \chi(z) = 0$ となるので、結局 $|\tau(i,t)|^2 = p$ となり、示された。

□

ここまで来ると、もう N_p の大きさの評価は簡単です。

前の章で示した内容とともにまとめます。

定理 9. $\sum_{i=1}^{n} x_i^m \equiv 0 \pmod p$ の解の個数を N_p とする。$d=(p-1,m)$ とおくと、次が成り立つ。

N_p は、

$$|N_p - p^{n-1}| \le (d-1)^n (p-1) p^{\frac{n}{2}-1}$$

を満たす。とくに、$d=1$ のとき、$N_p = p^{n-1}$

証明. $N_p = p^{n-1} + \frac{1}{p}\sum_{t\in\mathbb{F}_p^*} f(t)^n$ であったので、

$$|N_p - p^{n-1}| = \frac{1}{p}\sum_{t\in\mathbb{F}_p} f(t)^n$$

である。また、

$$f(t) = 1 + \sum_{i=0}^{d-1} \tau(i,t)$$

$$= \sum_{i=1}^{d-1} \tau(i,t)$$

$$< (d-1)\sqrt{p}$$

となるので、

$$|N_p - p^{n-1}| < \frac{1}{p}((d-1)\sqrt{p})^n$$

となり、結論が得られる。 □

4 おわりに

参考文献は数学オリンピック申込者に配られる小冊子です。(申込者以外でも入手できるようです) この記事は、その小冊子に書いてあった今回の内容の特殊な場合 ($m = n = 3$ の場合) の一般化です。

記事を書くのは、なかなかうまくいかないなあという感じでしたが、楽しかったです。

これを読んで、少しでも数学に興味をもってもらえればうれしいです。お読みいただきありがとうございました。

参考文献

[1] “math OLYMPIAN October”