Perrin の数列

こもりん

2014/05/19

LaTeX の練習のため, 例会講義の内容を文書にまとめてみました.
てちてち.

1 Perrin の数列の定義

定義 1. 以下で定義される数列 $\{p_n\}_{n=1,2,\dots}$ を Perrin の数列と呼ぶ:

$$p_1 = 0, \quad p_2 = 2, \quad p_3 = 3,$$
$$p_{i+3} = p_{i+1} + p_i \quad (i = 1, 2, \dots).$$

この数列の最初から十数項は以下のようになる: 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, ...
これをよく見ると, この範囲では

$$n \text{ が } p_n \text{ を割り切る} \Leftrightarrow n \text{ が素数}$$

が成立していることがわかる.
($\Rightarrow$) は n がもっと大きい範囲で反例が存在する[*1] のだが, ($\Leftarrow$) は実は常に成立することが示せる.
しかしどのようにすればそんなことが証明できるのだろうか? 受験で出てきた数学の問題であれば, 割り切れるかどうかの問題は余りの世界に映して考えるのが定石であり, また, 線形漸化式をもつ数列の問題はとりあえず一般項を求めるのが定石である. 抽象数学の柔軟さは, これらを組み合わせることを可能にする. それによって証明ができるのである.

2 体 $\mathbb{F}_q$ とその代数閉包の導入

まずは, 定石に従って余りの世界に移ってみよう.

定義 2. q を任意の素数とする. 集合 $\{0, 1, \dots, q-1\}$ に, 加減算と乗算をそれぞれ「通常通りに演算を行った後, q でわった余りをとる」という操作で定義したものを, $\mathbb{Z}/q\mathbb{Z}$ もしくは $\mathbb{F}_q$ と呼ぶ. [*2] この集合には 0 以外の各元について, 掛け算すると 1 になるような元が存在する[*3] ので, 加減乗除が通常通り自由にできる. このような, 集合と加減乗除を併せたものを体と呼ぶ.

[*1] p_{271441} は 271441 で割り切れる一方, $271441 = 521^2$ は素数でない. Perrin pseudoprimes で各自調べられたい.

[*2] これらの記号の相違は, この体に対する見方の違いを反映している. $\mathbb{Z}/q\mathbb{Z}$ という表記は, 整数からつくられた「余りの世界」という意味があり (これを「剰余環」という), $\mathbb{F}_q$ という表記には, q 個の元を持つ体という意味がある. (実はこれは"同型を除いて"一意に定まることがわかる.) q が素数のべきのときにもこれらは両方意味を持つが, その場合もはや 2 つの対象は異なるものとなる.

[*3] なぜだろうか. 考えるなり訊くなりしてみよう.

先の定義式を $\mathbb{F}_q$ に移せば, Perrin の数列の各項を q でわった余りを表す数列が得られる. 以後 q を任意の固定した素数とし, この $\mathbb{F}_q$ 上の数列を扱うことにする.

次に, $\mathbb{F}_q$ においての p_n の一般項を導きたい. 通常の手順を模倣するなら, 特性方程式と呼ばれる代数方程式を立て, その解を用いて一般項を表す式をつくることになる. ところが, $\mathbb{F}_q$ では代数方程式が必ず解を持つとは限らない. しかし, 非常に便利な事実があり, それにより方程式の解を取って使うのに十分な「舞台」を用意することができるのである.

定義 3. 体 K は, K に係数をもついかなる代数方程式も K の中に少なくとも 1 つ解を持つとき, 代数閉体であるという. また, 体 K を含む代数閉体で, それに真に含まれかつ K を含むような代数閉体が存在しないものを, K の代数閉包と呼ぶ.

事実 4. いかなる体も代数閉包を持つ.

証明なしで身も蓋もない事実を挙げてしまったが今回は認めて先に進む. なお証明の方もまた身も蓋もないものなので, 興味があれば調べられたい. [*4]

代数閉体上では, どのような多項式も 1 次式の積に分解できる.

定義 5. $\mathbb{F}_q$ の代数閉包をひとつとって, $\overline{\mathbb{F}_q}$ と記す.

3 一般項の導出と定理の証明

準備ができたところで, 一般項の形を導こう. その形からでは一見すぐには目的の定理は導けないように感じられるが, あることを知っていれば簡単になる.

定理 6. $\overline{\mathbb{F}_q}$ 上で, 多項式 x^3-x-1 が $(x-\alpha)(x-\beta)(x-\gamma)$ と因数分解されたとする. このとき, $\overline{\mathbb{F}_q}$ において

$$p_n = \alpha^n + \beta^n + \gamma^n (n = 1, 2, \ldots)$$

が成り立つ.

証明. 数学的帰納法を用いる. まず $n = 1, 2, 3$ の場合について示す.

$x^3 - x - 1 = (x-\alpha)(x-\beta)(x-\gamma)$ を展開して次数ごとに比較すると

$$\begin{aligned} \alpha + \beta + \gamma &= 0 \\ \alpha\beta + \beta\gamma + \gamma\alpha &= -1 \\ \alpha\beta\gamma &= 1 \end{aligned}$$

[*4] すべての多項式を列挙し, それぞれについて解をでっち上げて元の体に付加する, を無限回繰り返すのが標準的な証明である. この手法は数理論理学の分野でもよく使われるようである.

がわかる. ここから

$$\begin{aligned}\alpha+\beta+\gamma &= \alpha+\beta+\gamma\\ &= 0 = p_1\\ \alpha^2+\beta^2+\gamma^2 &= (\alpha+\beta+\gamma)^2-2(\alpha\beta+\beta\gamma+\gamma\alpha)\\ &= 2 = p_2\\ \alpha^3+\beta^3+\gamma^3 &= (\alpha+\beta+\gamma)^3-3(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)+3\alpha\beta\gamma\\ &= 3 = p_3\end{aligned}$$

が成立する. 以上で $n=1,2,3$ の場合が示せた.

次に $k\geq 4$ の場合に, $n<k$ での成立を仮定して $n=k$ での成立を示す. $n<k$ では式が成立すると仮定したから, とくに $n=k-2,k-3$ のときの式が使えて,

$$\begin{aligned}p_{k-2} &= \alpha^{k-2}+\beta^{k-2}+\gamma^{k-2}\\ p_{k-3} &= \alpha^{k-3}+\beta^{k-3}+\gamma^{k-3}\end{aligned}$$

が成立する. ここから,

$$\begin{aligned}p_k &= p_{k-2}+p_{k-3}\\ &= \alpha^{k-3}(\alpha+1)+\beta^{k-3}(\beta+1)+\gamma^{k-3}(\gamma+1)\end{aligned}$$

がわかるが, α, β, γ はいずれも x についての方程式 $x^3-x-1=0$ の解であるから, $\alpha+1=\alpha^3$ 等が成立する. ここから,

$$p_k=\alpha^k+\beta^k+\gamma^k$$

が成立することがわかる. 以上で $n=k$ の場合が示せた.

数学的帰納法により, すべての n について式は成立する. □

あとは, $\alpha^q+\beta^q+\gamma^q=0$ を示せれば目的の定理が導ける. 指数部分が場合によって変化することから, これを示すのは難しいように感じられる. しかし, 実は以下の事実を知っていれば簡単に導けるのである.

定理 7. $\overline{\mathbb{F}_q}$ において, 任意の x,y について,

$$(x+y)^q=x^q+y^q$$

が成立する.

証明. 二項定理で展開し, 両端以外の係数が q で割り切れることがわかれば, q をかければどんな数も 0 になることから証明できる. □

これを用いれば $\alpha^q+\beta^q+\gamma^q=(\alpha+\beta+\gamma)^q$ がわかり, ここからすぐに以下が示せる:

定理 8. $\overline{\mathbb{F}_q}$ において, $p_q=0$. したがって, 整数として考えれば p_q は q で割り切れる.

4 まとめ

この先数学では今回の内容に登場した体や代数閉包など, 抽象的だったり何に使えるのかがわからなかったりする概念が数多く登場するだろう. そのような概念は, 比較的わかりやすい問題においてもしばしば役立つ

ということを覚えておいてほしい. そのよい例として, この題材について話したつもりである. また, 今回の代数閉包のように, さまざまな手法を用いるのに十分なように世界を広げて考える, ということは数学ではよくある[*5]. そういう視点を持つと理解しやすくなる内容もあるだろう.

参考文献

[1] 森田康夫「代数概論」, 裳華房, 1987

[2] Wikipedia 日本語版「ペラン数」
(http://ja.wikipedia.org/wiki/%E3%83%9A%E3%83%A9%E3%83%B3%E6%95%B0)

[*5] 有理数の完備化としての実数はすでに知っているかもしれない. ほかにも, 米田埋め込み等がある.