今日のテーマ

ゼータ関数の例、前回レポートの解答

命題 11.1. p **は奇素数であるとし、** $q = p^s$ (s **は正の整数**) **であるとする。**$\mathbb{F}_q$ **上の二変数の方程式系** $V = V(X^2 + Y^2 - 1)$ **に対して、**$Z(V/\mathbb{F}_q, t)$ **は** $\mathbb{F}_q$ **のなかで** -1 **の平方根があるか否かによって二通りの答えがある。**

$$Z(V/\mathbb{F}_q, t) = \begin{cases} \frac{1-t}{1-qt} & -1 \text{ が } \mathbb{F}_q \text{ の中で平方根をもつとき} \\ \frac{1+t}{1-qt} & \text{そうでないとき} \end{cases}$$

No.9 **のレポート問題の正答率がよくなかったので、解説をつける。**

例題 11.1. $p = 11$ **のとき、**$\mathbb{F}_p$ **上の多項式** $X^6 - a$ $(a \in \mathbb{F}_p)$ **は既約になり得ないことを示しなさい。**

[**解答**]

11 **個しか可能性がないから、個別に見てももちろんよい。が、もっと簡明なのは、写像**

$$\mathbb{F}_{11} \ni c \to c^3 \in \mathbb{F}_{11}$$

が全射であることを用いることである。つまり、$a = c^3$ **となる** c **が存在する。**$X^6 - c^3$ $(c \in \mathbb{F}_{11})$ **は、もちろん既約ではない。**

例題 11.2. $p = 17$ **のとき、**$\mathbb{F}_p$ **上の** 6 **次既約多項式の例を見つけ、それが既約であることを示しなさい。**

素朴にやるには膨大な計算が必要である。以下に mupad **で計算するための** program **を書いておこう。**

```
Fp:=Dom::IntegerMod(17);            // Fp=Z/17 Z
f:=poly(x^6-x-4,[x],Fp);            // 変数と係数を明示
g:=poly(x^(17^2)-x,[x],Fp);
h:=poly(x^(17^3)-x,[x],Fp);
gcd (f,g);                          // f と g の GCD を求める。

gcd(f,h);                           // f と h の GCD を求める。
```

膨大な計算をせずにすます方法はないか? **実はある。** $\mathbb{F}_{17}$ **上の既約な** 2 **次式** a **と** 3 **次式** b **をとろう。(これは諸君にも容易であろう。) ここでは、例えば** $a(X) = X^2 - 3, b(X) = X^3 - X - 2$ **とする。**a **の根** α **と** b **の根** β **の和** γ **を考える。**γ **の満たすべき** 6 **次式は比較的容易に書き下せる。それが既約であることを言えばよい。すなわち、**$\mathbb{F}_{17}(\gamma)$ **が** $\mathbb{F}_{17}$ **の** 6 **次拡大であることを言えばよい。フロベニウス写像** F **の言葉で言えば、これは** $F^i(\gamma)$ $(i = 0, 1, 2, 3, 4, 5)$ **が全て異なることを示すと言っても同じである。あとは** $F(\alpha) = -\alpha$ **と、**$F^3(\beta) = \beta$ **とに注意すればよい。**

問題 11.1. 二変数の方程式系 $V(X^2 - Y^2 - 1)$ **の合同ゼータ関数** $Z(V, t)$ **を求めよ。**