代数学 II 試験略解

問題 14.1. 写像 $\mathbb{F}_p \ni x \mapsto x^k - x^2 \in \mathbb{F}_p$ が定値写像 $\mathbb{F}_p \ni x \mapsto 0 \in \mathbb{F}_p$ と等しくなるための k, p の条件を求めなさい。(わからない場合には k, p のできるだけ多くの組みに対して二つの写像が等しいかどうか判定せよ。)

(答え)$k > 0$ で、$k-2$ が $p-1$ で割り切れればよい。
(証明) 便宜上, 最初の写像を f, 次の写像を g とおく。$k = 0$ なら $f = g$ となるのは不可能なので、 $k > 0$ の場合を考える。このとき、$f(0) = g(0) = 0$ であるから, $x \in \mathbb{F}_p^\times$ のときの f と g の値が一致するかどうか調べればよい。

いま、$k-2 = (p-1)m$ なる整数 m があったとすると、フェルマの小定理により

$$x^k - x^2 = (x^{p-1})^m x^2 - x^2 = 1^m x^2 - x^2 = 0$$

となり、$f(x) = g(x)$ がすべての $x \in \mathbb{F}_p^\times$ について成り立つことがわかる。

逆に, $f = g$ と仮定しよう。$k-2$ を $p-1$ で割った商を m, あまりを r とおくと、全ての $x \in \mathbb{F}_p^\times$ にたいして,

$$f(x) = x^k - x^2 = x^2(x^r - 1)$$

であることが上と同様にしてわかる。$f(x) = g(x) = 0$ で, かつ $x^2 \neq 0$ (で、かつ $\mathbb{F}_p$ は体) だから、$x^r - 1 = 0$ がすべての $x \in \mathbb{F}_p^times$ について成り立つことになる。もし $r \neq 0$ ならば, これは $p-1$ 個の元が r 次方程式の根になることになって、矛盾。ゆえに、$r = 0$ である。

この問題に限らず、解答は証明 (とは言わないまでもなぜその答えで正しいかの説明) があってはじめて一人前である。

問題 14.2. 体 K の 2 つの元 x, y が、 $x^2 + y^2 = 0$ を満たすとき、$x = 0$ かつ $y = 0$ といえるだろうか。いえるならば証明をつけ、いえないならば反例を 3 つ以上あげなさい。(K の標数が 0 の場合と 0 でない場合の両方について議論すること.)

(答え)

これは簡単である。標数 0 なら $K = \mathbb{C}$ で

$$1^2 + (i)^2 = 0$$

などが反例となる。

標数が正のものに関しては、標数 2 の $K = \mathbb{F}_2$ で

$$1^2 + 1^2 = 0$$

標数 5 の $K = \mathbb{F}_5$ で,

$$1^2 + 2^2 = 0$$

などを反例にあげればよい。

項式 X^6-1 を一次式の積に分解しなさい。

(答え)
この問題はまちがっておった。二次式のほうは X^2+X+2 にすべきであった。X^2+X-1 は既約でないからである。
問題のままでは, X^6-1 は一次式の積に分解できない。ただし (なぜ分解できないかまで含めた) 正しい指摘は皆無であった。寂しい限りである。
本当は $(\mathbb{F}_{25})^\times$ の位数が 24 であることを用いる問題だった。

問題 14.4. 奇素数 p が与えられているとするとき、$\mathbb{F}_p$ 上の 2 変数の方程式系 $V_1=V((X^2-2Y^2-1)(Y-2))$ の合同ゼータ関数 $Z(V_1/\mathbb{F}_p,t)$ を求めよ。

$V(X^2-2Y^2-1)$ と $V(Y-2)$ の共通部分は $(3,2),(-3,2)$ の二点である。それ以外は講義で説明した通りである。念のために述べておくと、$W=V(X^2-2Y^2-1)$ とおいて, $W(\mathbb{F}_q)$ の元の数を求める必要があるのだが、
(1) 2 が $\mathbb{F}_q$ で平方根を持つときには、$W(\mathbb{F}_q)$ の元の数は $\mathbb{F}_q^\times$ の元の数と同じであって、$q-1$ である。
(2) 2 が $\mathbb{F}_q$ で平方根を持たないときには, $W(\mathbb{F}_q)$ の元のうち $(1,0)$ 以外は

$$(\frac{m^2+2}{m^2-2},\frac{2m}{m^2-2}) \qquad (m\in\mathbb{F}_q)$$

とパラメータ表示できて、$\#W(\mathbb{F}_q)=q+1$ になる.
したがって 2 が modulo p で平方剰余ならば,

$$\begin{aligned} Z(W/\mathbb{F}_p,t) &= \exp(\sum_{k=1}^{\infty}((p^k-1)/kt^k) \\ &= \frac{1-t}{1-pt} \end{aligned}$$

となり, 2 が modulo p で平方非剰余ならば $\#(W(\mathbb{F}_{p^r})=p^r+(-1)^r$ となって,

$$\begin{aligned} Z(W/\mathbb{F}_p,t) &= \exp(\sum_{k=1}^{\infty}((p^k+(-1)^k)/kt^k) \\ &= \frac{1}{(1-pt)(1+t)} \end{aligned}$$

あとは、一般に, 方程式系 W,U に対して,

$$Z(W\cup U)=Z(W)Z(U)/Z(W\cap U)$$

が成り立つ (もちろん上のようなゼータレベルでなく, 個数のレベルで同じことをしてもよい.) ことをを用いればよい。
答えは
p が平方剰余のとき (つまり p を 8 で割ったあまりが 1 または 7 のとき,

$$Z(V_1,t)=\frac{1-t}{1-pt}\frac{(1-t)^2}{1-pt}=\frac{(1-t)^3}{(1-pt)^2}$$

とき,

$$Z(V_1,t)=\frac{1}{(1-pt)(1+t)}\frac{(1-t)^2}{1-pt}=\frac{(1-t)^2}{(1-pt)^2(1+t)}$$

という具合になる.

問題 14.5. 奇素数 p が与えられているとするとき、$\mathbb{F}_p$ 上の 3 変数の方程式系 $V_2=V((X^2+Y^2-Z^2)$ の合同ゼータ関数 $Z(V_2/\mathbb{F}_p,t)$ を求めよ。

X 座標 x の値によって $V_2(\mathbb{F}_q)$ の元を分類すればよい。(これは幾何学的には円錐を平面で切ることにあたる). $x=0$ のときは、$V(Y^2-Z^2)$ の解の数だが、これは先刻承知 $(2q-1)$ のはずである。$x\neq 0$ のときは、$Y/x, Z/x$ を Y,Z と変数変換することにより, $\#(V(x^2+Y^2-Z^2)(\mathbb{F}_q))=\#(V(1+Y^2-Z^2)(\mathbb{F}_q))$ をえる。この解の数は前問同様 $q-1$ になる。あとはそれらを足せばよい。

$$\#V(X^2+Y^2-Z^2)(\mathbb{F}_q)=2q-1+(q-1)(q-1)=q^2$$

よって

$$Z(V_2/\mathbb{F}_p,t)=\exp(\sum_{k=1}^{\infty}\frac{p^{2k}}{k}t^k)=\frac{1}{1-p^2t}$$

となる。

問題 14.6. $n=123556429$ とするとき、$\mathbb{Z}/n\mathbb{Z}$ での 2^n の値を計算せよ。また、n は素数といえるかどうか、判定しなさい。計算は全部を載せる必要はないが、どのような方法を採ったかは明記すること。

(答え)

MuPAD の powermod 関数をつかえば簡単であった。答えは 84299180 である。したがって、フェルマの小定理の対偶により, n は素数でないことがわかる。念のためにいっておくと, $2^n=2$ だからと言って、n が素数であるとは限らない。

powermod なんぞ知らぬという人のほうが多いであろう。次の等式を何度も使えばよい。

$$ab^n=(ab^\epsilon)(b^2)^{[n/2]}$$

ここで $[\bullet]$ はガウス記号, $\epsilon=n-2[n/2]$ (n を 2 でわったあまり) である。計算回数は $\log n$ に比例して、n 回かけ算するのとは比較にならないぐらい速い。

いずれにせよ、計算機を活用しないと面倒な問題であった。