PROBLEM 521

- $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n/m$ $\left[\underbrace{\underbrace{\mathbb{F}_p \subset \mathbb{F}_{p^n}}_{\deg n} \subset \mathbb{F}_{p^m}}_{\deg m} \Rightarrow n/m \right.$; conversely if $\alpha \in \mathbb{F}_{p^n}$ & $nk = m \Rightarrow \alpha^{p^n} = \alpha \Rightarrow (\alpha^{p^n})^{p^n} = \alpha^{p^n} = \alpha$ so $\alpha^{p^{2n}} = \alpha$ $\Rightarrow (\alpha^{p^{2n}})^{p^n} = \alpha^{p^n} = \alpha \Rightarrow$ $\Rightarrow \alpha^{p^{3n}} = \alpha$ etc till get kn]

- $f \in \mathbb{F}_p[x]$ irred of deg d & $d/n \Rightarrow f / x^{p^n} - x$

$\left[\begin{array}{l} \text{Suf: any root of } f \text{ in } \overline{\mathbb{F}}_p \text{ is a root of } x^{p^n} - x \\ \text{But } \forall \text{ root } \alpha \text{ of } f \text{ has degree } d \text{ i.e. } \mathbb{F}_p(\alpha) = \mathbb{F}_{p^d} \text{ \& conclude by 1st problem} \end{array} \right.$; i.e. $\forall$ root of f is in $\mathbb{F}_{p^n}$

- f irred in $\mathbb{F}_p[x]$ of degree d ; $f \mid x^{p^n} - x \Rightarrow d / n$. [Let $f(\alpha) = 0 \Rightarrow$ $\alpha \in \mathbb{F}_{p^n}$ But $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d} \Rightarrow d/n$]

- Cor of above $\displaystyle x^{p^n} - x = \prod_{d/n} \prod_{f \in \mathcal{F}_d} f(x)$; $\mathcal{F}_d$ = set of irr polyn of deg d

$\Uparrow$ dist. roots of $x^{p^n} - x$

- take degrees $\Rightarrow$ $\displaystyle p^n = \sum_{d/n} d \cdot N(d)$; $N(d) = \# \mathcal{F}_d$

$M(n) = n N(n) \Rightarrow p^n = \sum_{d/n} M(d)$

(by Möbius invers formula $\overset{M(n)}{n N(n)} = \sum_{d/n} \mu(d) p^{n/d}$ where $\mu(1) = 1$, $\mu(p_1 \cdots p_r) = (-1)^r$, $\mu(k) = 0$ if $\exists p^2 / k$.)

$\boxed{\text{Intro to arith fcns}}$ $f : \underset{\{1,2,3,\dots\}}{\mathbb{N}} \to \mathbb{C}$, $L_f = \sum f(n) n^{-s}$ (formal)

Def $R = \{ f : \mathbb{N} \to \mathbb{C} \}$ is a comm ring wrt usual ad & mult $(f * g)(n) = \sum_{d/n} f(d) g(n/d)$

Prop 1 $L_{f*g} = L_f L_g$ [Pf: triv] $L_{f+g} = L_f + L_g$. So $R \simeq (\{ \sum a_n n^{-s} \mid a_n \in \mathbb{C} \}, +, \cdot)$

Def f mult if $f(mn) = f(m) f(n)$ for $(m,n) = 1$ (& $f(1) \neq 0$; it then foll $f(1) = 1$)

Prop 2 f mult $\iff$ $\displaystyle L_f = \prod_p (1 + f(p) p^{-s} + f(p^2) p^{-2s} + \cdots)$ (Euler prod) [Pf triv

Prop 3 f, g mult $\Rightarrow f * g$ mult.

Examples
1) $1 \in R$, $1(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$; it is the 1-elt in R
2) $\mathbb{1} \in R$, $\mathbb{1}(n) = 1$, all n. So $L_{\mathbb{1}} = \sum n^{-s}$ Riemann zeta
3) $I \in R$, $I(n) = n$. So $L_I = \sum n^{1-s}$
4) $\mu \in R$ (see above)
5) $\phi \in R$, Euler's fcn. Multiplic bec $(\mathbb{Z}/nm)^\times \simeq (\mathbb{Z}/n \times \mathbb{Z}/m)^\times = (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$

Möbius inv formula: if $F = \mathbb{1} * f$ then $f = \mu * F$

Various identities

By multiplic enough for $n = p^k$

a) $\phi * \mathbb{1} = I$ $\left[\sum_{d/n} \phi(d) \overset{n = p^k}{=} \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^k) = 1 + (p-1) + (p^2 - p) + \cdots + p^k - p^{k-1} = p^k \right.$

b) $\mu * \mathbb{1} = 1$ [simil $\displaystyle \sum_{d/n} \mu(n) \underset{n = p^k}{=} \mu(1) + \mu(p) + \mu(p^2) + \cdots = \begin{cases} 1 - 1 = 0 & \text{if } k > 0 \\ 1 & \text{if } k = 0 \end{cases}$

c) $\phi = I * \mu$ [Cor of a & b]

PROBLEMS 521

521

- Legendre symbol for $p \geq 3$, Euler's crit., $p = a^2 + b^2$ [cf notes]
- Constr of $\mathbb{F}_{p^2}$, $p \geq 3$ via $x^2 - d = f(x)$, $\left(\frac{d}{p}\right) = -1$, ~~Constr~~
- Constr of $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{16}$ (*)
- → any elt in $\mathbb{F}_p$ is a sum of 2 squares.
- → $p \geq 3 \Rightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$ cyclic; (**) (not true for $p = 2$, $n = 3$)
- (Artin, ex 3 p. 296) $v \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$, $E \subset \overline{\mathbb{Q}}$ max s.t. $v \notin E$. Then $\forall$ fin dim ext F of E is cyclic (****)
- $\sigma \in G(\overline{\mathbb{Q}}/\mathbb{Q})$; then $\forall$ fin ext F of $E = \overline{\mathbb{Q}}^\sigma$ is cyclic. (+)
- $\forall$ # field contains only fin many roots of 1. [if not $\mathbb{Q}(\zeta_{n_k}) \subset K$, $n_k \to \infty$. But $\phi(n_k) \to \infty$]
- → $K \subset D \subset F$, F/K alg ext of fields $\Rightarrow D$ field
- → char $K = p$, $a \in K \setminus K^{p}$ $\Rightarrow x^{p^n} - a$ irred$/_K$ if $n \geq 1$ (***)
- $G(\overline{\mathbb{Q}}/\mathbb{Q})$ uncountable or at least ∞ $[\sigma_p \sqrt{p} = -\sqrt{p}]$ ← define Krull Top
- → $G(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \hat{\mathbb{Z}}$.
- no finite field K is alg closed. $\left[f(x) = 1 + \prod_{\alpha \in K}(x - \alpha)\right]$
- $k(x)^\sigma = k$ if $\sigma(x) = x + 1$. (char $k = 0$) appears if $p = 3$ (?)
- → $S := \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \zeta_p^a$. Prove $S^2 = p\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} p$. So $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p, i)$

(+) May ass F/E normal. Then $\sigma \in G(F/E)$ & $F^{\langle\sigma\rangle} = E$ so $\langle\sigma\rangle = G(F/E)$

⇒ If G not cyclic then $G = H_0$ ↯

(****) May ass F/E normal $\Rightarrow \forall$ interm field contains $E(v) \Rightarrow \forall H \overset{\neq}{<} G = G(F/E)$ is contained in $H_0 = G(F/E(v)) \Rightarrow \forall g \in G$, $\langle g \rangle \neq G$, $\langle g \rangle \subset H_0$

(***) $x^{p^n} - a$ has all roots $= \alpha$ so $x^{p^n} - a = (x - \alpha)^{p^n}$ if $g\,h \Rightarrow g = (x-\alpha)^{kp^i} = (x^{p^i} - \alpha^{p^i})^k = x^{p^i k} - k \cdot \alpha^{p^i}(x^{p^i})^{k-1} + \dots \Rightarrow \alpha^{p^i} \in K \Rightarrow x^{p^n} - a = x^{p^n} - \alpha^{p^n} = (x^{p^i} - \alpha^{p^i})^{p^{n-i}}$. $p \nmid k$

(**) $0 \to \frac{p\mathbb{Z}}{p^n\mathbb{Z}} \xrightarrow{x \mapsto \log(1+x)} \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^\times \to \frac{\mathbb{Z}}{p\mathbb{Z}} \to 0$ & (L) $0 \to A \to B \to C \to 0$, $(|B|, |C|) = 1 \Rightarrow$ split.

(*) $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$

(or $/(x^3 + x^2 + 1)$)

$\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x^3 + 1)$

Proof of irred: ass red & use fact that only deg 1 pol are x & $x+1$, — " — 2 — " — for deg 2 & 3 $\Rightarrow \exists$ root. For deg 4 div by x or by $x+1$ or $x^2 + x + 1$