Math 80220 Algebraic Number Theory
Problem Set 11

Andrei Jorza

due Friday, May 4

1. Let $f \in \mathbb{Z}[X]$ be a nonzero polynomial such that for all but finitely many primes p the polynomial $f \mod p$ splits into linear factors in $\mathbb{F}_p[X]$.
   (a) If f is irreducible and K is the splitting field of f show that for all but finitely many primes p the element $\mathrm{Frob}_{\mathfrak{p}/p} = 1$ for $\mathfrak{p} \mid p$ prime ideal of K and conclude that $\deg f = 1$. [Hint: Chebotarev.]
   (b) Show that f splits into linear factors in $\mathbb{Z}[X]$.
2. Suppose $f \in \mathbb{Z}[X]$ is a monic irreducible polynomial such that $f \mod p$ has a root in $\mathbb{F}_p$ for all but finitely many primes p.
   (a) Let $K/\mathbb{Q}$ be the splitting field of f. If $\deg f > 1$ show that there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\alpha) \neq \alpha$ for every root α of f. (You may use the fact, contained in the problem at the end of this set, that if a group G acts faithfully and transitively on a set X with at least 2 elements then some $g \in G$ has no fixed points in X.)
   (b) Show that there exist infinitely many primes p such that Frob_p is the conjugacy class of σ.
   (c) Show that for all but finitely many p, Frob_p has a fixed point and deduce that f is linear.
3. (a) Show that $f(X) = (X^2-2)(X^2-3)(X^2-6)$ has a root in $\mathbb{F}_p$ for every prime p but no root in $\mathbb{Z}$. [Hint: $\mathbb{F}_p^\times$ is cyclic.]
   (b) Show that $f(X) = (X^3-2)(X^2+X+1)$ has a root in $\mathbb{F}_p$ for every prime p but no root in $\mathbb{Z}$. [Hint: treat $p \equiv \pm 1 \pmod 3$ separately.]
   (c) Show that if $f(X)$ has a root in $\mathbb{F}_p$ for every prime p but no root in $\mathbb{Z}$ then $\deg f \geq 5$. [Hint: Use the previous problem to reduce to a product of two quadratics and recall that $X^2 - a$ has a root mod p if and only if $\mathrm{Frob}_p = 1$ in $\mathbb{Q}(\sqrt{a})$.]
4. For a set of integer primes $\mathcal{P}$ define

$$a_{\mathcal{P}}(x) = |\{p \in \mathcal{P} \mid p \leq x\}|$$
$$b_{\mathcal{P}}(x) = \sum_{p \in \mathcal{P}, p \leq x} \frac{1}{p}$$
$$Z_{\mathcal{P}}(s) = \sum_{p \in \mathcal{P}} \frac{1}{p^s}.$$

When $\mathcal{P}$ is the set of all primes we'll drop the subscript. Let

$$\overline{\delta}_{\mathrm{nat}}(\mathcal{P}) = \limsup_{x\to\infty} \frac{a_{\mathcal{P}}(x)}{a(x)}$$
$$\overline{\delta}_{\log}(\mathcal{P}) = \limsup_{x\to\infty} \frac{b_{\mathcal{P}}(x)}{b(x)}$$
$$\overline{\delta}(\mathcal{P}) = \limsup_{s\to 1^+} \frac{Z_{\mathcal{P}}(s)}{Z(s)},$$

and analogously $\underline{\delta}_{\mathrm{nat}}(\mathcal{P})$, $\underline{\delta}_{\log}(\mathcal{P})$, and $\underline{\delta}(\mathcal{P})$ using lim inf.

(a) Show that for integers $x \geq 2$ one has

$$b_{\mathcal{P}}(x) = \frac{a_{\mathcal{P}}(x)}{x} + \sum_{n=2}^{x-1} \frac{a_{\mathcal{P}}(n)}{n(n+1)}.$$

(b) Show that for $\operatorname{Re} s > 1$ one has

$$Z_{\mathcal{P}}(s) = \sum_{n\geq 2} b_{\mathcal{P}}(n) \left(\frac{1}{n^{s-1}} - \frac{1}{(n+1)^{s-1}} \right).$$

(c) Conclude that

$$\underline{\delta}_{\mathrm{nat}}(\mathcal{P}) \leq \underline{\delta}_{\log}(\mathcal{P}) \leq \underline{\delta}(\mathcal{P}) \leq \overline{\delta}(\mathcal{P}) \leq \overline{\delta}_{\log}(\mathcal{P}) \leq \overline{\delta}_{\mathrm{nat}}(\mathcal{P}).$$

In particular, the existence of natural density implies the existence of logarithmic density, which in turn implies the existence of Dirichlet density.

(You may assume that $a(x) = O(x/\log x)$ for convergence issues.)

5. Let $p > 3$, $p \equiv 3 \pmod 4$ be a prime number and $K = \mathbb{Q}(\zeta_p)$. Recall from the first homework that $\mathbb{Q}(\sqrt{-p}) \subset K$.

(a) The group $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic and therefore so is its character group $\widehat{G}$. Denote χ a generator, taking a generator of G to ζ_{p-1}. Show that

$$\chi^{(p-1)/2}(x) = \left(\frac{x}{p}\right)$$

(b) Show that if H is the subgroup of $G \cong \mathbb{Z}/(p-1)\mathbb{Z}$ corresponding to $\{0, 2, 4, \dots, p-3\} \subset \{0, 1, 2, \dots, p-2\}$ then the fixed subfield is $K^H = \mathbb{Q}(\sqrt{-p})$. [Hint: Show that there is only one quadratic subfield of K.]

(c) Show that the characters χ^k and $\chi^{k+(p-1)/2}$ are equal on H and conclude that the characters of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-p})/\mathbb{Q})$ are 1 and $\left(\frac{\cdot}{p}\right)$. Deduce that

$$\tau\left(\left(\frac{\cdot}{p}\right)\right) = \sqrt{-p}$$

[Hint: For the Gauss sum, use the result from class.]

(d) Show that

$$L\left(\left(\frac{\cdot}{p}\right), 1\right) = \frac{\pi h_{\mathbb{Q}(\sqrt{-p})}}{\sqrt{p}}$$

and conclude that

$$B_{1,\left(\frac{\cdot}{p}\right)} = -h_{\mathbb{Q}(\sqrt{-p})}$$

and thus that

$$h_{\mathbb{Q}(\sqrt{-p})} = -\frac{1}{p} \sum_{k=1}^{p} \left(\frac{k}{p}\right) k.$$

Useful

You do not need to do these exercises.

1. Let G be a group acting faithfully (i.e., $G \to \mathrm{Aut}(X)$ is injective) and transitively (i.e., for any x, y there exists g such that $gx = y$) on a finite set X with more than one element.

   (a) If every $g \in G$ has a fixed point, i.e., $x \in X$ such that $gx = x$, show that $G = \cup_{x \in X} \mathrm{Stab}_G(x) = \cup_{g \in G} g \,\mathrm{Stab}_G(x_0) g^{-1}$ for a fixed x_0.

   (b) If H is the maximal proper subgroup of G containing $\mathrm{Stab}_G(x_0)$ show that H is not normal.

   (c) Deduce that the normalizer $N_G(H) = H$ and thus that $\{gHg^{-1} | g \in G\} = \{gHg^{-1} | g \in G/H\}$.

   (d) Deduce that $\cup gHg^{-1}$ has at most $(|H| - 1)[G : H] + 1$ elements.

   (e) Derive a contradiction and conclude that there exists $g \in G$ such that g has no fixed points.