Problem sheet for minicourse 'Probabilistic Galois Theory'

Q1 In example 2, we considered the interval $[1, N]$ and for each odd prime $p \leq Q = [\sqrt{N}]$ removed all integers $n \in [1, N]$ such that $(\frac{n}{p}) = -1$. It is easy to see that each square survives this process, but do only the squares survive? You can first discuss this question in the easier setting where for each odd prime p (restriction $p \leq Q$ dropped) we remove all quadratic non-residues.

Q2 Show that once you established Theorem 1 (the large sieve inequality) for one M, you can deduce it for all M, i.e. it was permissible in class without loss of generality to assume that $M = [-\frac{1}{2}(N+1)]$.

Q3 By considering suitable examples, show that in Theorem 1 we indeed need a dependence on N and δ of the corresponding orders of magnitude N and $\frac{1}{\delta}$, respectively.

Q4 Show that if f is continuously differentiable on $[0, 1]$, then for all $x \in [0, 1]$ we have

$$f(x) = \int_0^1 f(u)\,du + \int_0^x uf'(u)\,du + \int_x^1 (u-1)f'(u)\,du.$$

Q5 Using the notation from class, i.e.

$$V(q) = \sum_{h=1}^{q} \left(Z(q,h) - \frac{Z}{q} \right)^2$$

and

$$S(\alpha) = \sum_{n \in \mathcal{N}} e(n\alpha),$$

show that

$$V(q) = \frac{1}{q} \sum_{a=1}^{q-1} \left| S\left(\frac{a}{q}\right) \right|^2.$$

Hint: As in the proof of Parseval's equation, first evaluate $\sum_{a=1}^{q-1} |S(a/q)|^2$ by using the orthogonality relation

$$\sum_{a=1}^{q} e\left(\frac{ab}{q}\right) = \begin{cases} q & \text{if } b \equiv 0 \pmod{q} \\ 0 & \text{if } b \not\equiv 0 \pmod{q}. \end{cases}$$

Q6 This question assumes some familiarity for example with *Gaussian sums*, which can be explicitly evaluated. Let $f(y)$ be quadratic and no square, for instance $f(y) = y^2 + 1$ to keep it simple. Show that

$$\#\{x, y \pmod{p} : x^2 \equiv f(y) \pmod{p}\} = p + O(p^{1/2}).$$

Problem sheet 2 for minicourse 'Probabilistic Galois Theory'

Q7 Let $f(X) \in \mathbb{Z}[X]$ such that $f(x)$ is a square (i.e. a square of an integer) for all $x \in \mathbb{Z}$. Show that f must be a square of an integer polynomial itself.

Q8 Let $G = \{\mathrm{id}\}$ be the one-element subgroup of S_2. In the notation of Lemma 2, work out the polynomial $\Phi_G(z; a_1, a_2)$ and verify that if $f = X^2 + a_1 X + a_2 \in \mathbb{Z}[X]$ has Galois group G, which amounts to f being reducible over $\mathbb{Q}$, then $\Phi_G(z; a_1, a_2)$ has an integer root z.

Q9 Prove Lemma 2: Let G be a subgroup of S_n,

$$f(X) = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$$

with distinct roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, and let

$$\Phi_G(z; a_1, \ldots, a_n) = \prod_{\sigma \in S_n/G} \left(z - \sum_{\tau \in G} \alpha_{\sigma(\tau(1))} \alpha_{\sigma(\tau(2))}^2 \cdots \alpha_{\sigma(\tau(n))}^n \right).$$

Then $\Phi_G(z; a_1, \ldots, a_n)$ is a polynomial in $z, a_1, \ldots, a_n$ having integer coefficients. Moreover, for fixed $a_1, \ldots, a_n$, if the splitting field of f over $\mathbb{Q}$ has Galois group G, then $\Phi_G(z) = \Phi_G(z; a_1, \ldots, a_n)$ has an integer root z.

Q10 For example using Vieta's Theorem, prove Lemma 3: If $f(X) = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{C}[X]$, then all roots $z \in \mathbb{C}$ of the equation $f(z) = 0$ satisfy the inequality

$$|z| \ll_n \max_{1 \le k \le n} \sqrt[k]{|a_k|}.$$

Q11 By considering a suitable example, show that except possibly for the ϵ, the exponent $\frac{2}{d}$ in the Corollary to Theorem 6 (projective version of Bombieri-Pila) is best possible.

Q12 Fill in the details in the proof of Lemma 6 from class: If $F(X_1, X_2, X_3) \in \mathbb{Z}[X_1, X_2, X_3]$ is homogeneous of degree d having coprime coefficients, then either

$$N(F; P) \le d^2$$

or

$$||F|| \ll P^{d(d+1)(d+2)/2}.$$

Possible projects for minicourse 'Probabilistic Galois Theory'

Project 1: Continuation of Q1: Get a good upper bound on Q (depending on N, for example $Q = \sqrt{N}$), such that if for sufficiently large N for each odd prime $p \leq Q$ you remove all quadratic non-residues modulo p from the interval $[1, N]$, then only the squares remain. Can you also find a *lower bound* on Q that needs to be satisfied to guarantee that only the squares remain?
Useful literature: For example [7], §12.4.

Project 2: Read the paper [9]. Try to improve Lemma 1 and Lemma 2 in that paper by using sharper bounds for the divisor function, for example, reducing the bound from a power with exponent ϵ to a function growing more slowly. This way also sharpen the bound for $E_3(H)$.

Project 3: Read the paper [8], which takes a somewhat different approach to Galois resolvents. Prove the statements in the examples section at the end of the paper (explicit resolvents for the groups C_n and D_n). Write a program in Mathematica, for example, to do some example calculations for Lemma 2 from class and the approach in Lefton's paper, and compare the outcomes. Find some interesting examples of polynomials where using Galois resolvents you can determine the Galois group.

References

[1] Davenport, H. Multiplicative Number Theory, Springer Verlag (2000).
[2] Dummit, D. & Foote, R. Abstract Algebra, John Wiley (2004).
[3] Dietmann, R. On the distribution of Galois groups, *Mathematika* **58** (2012), 35–44.
[4] Gallagher, P.X. The large sieve and probabilistic Galois theory, *Proceedings of Symposia in Pure Mathematics* XXIII (1973, A.M.S.), 91–101.
[5] Heath-Brown, D.R. The density of rational points on curves and surfaces, *Ann. of Math.* **155** (2002), 553–598.
[6] Heath-Brown, D.R. Counting rational points on algebraic varieties, Springer Lecture Notes **1891** (2006), 51–95.
[7] Iwaniec, H. & Kowalski, E. Analytic Number Theory, AMS (2004)
[8] Lefton, P. Galois resolvents of permutation groups, *Amer. Math. Monthly* **84** (1977), 642–644.
[9] Lefton, P. On the Galois groups of cubics and trinomials, *Acta Arith.* **XXXV** (1979), 239–246.