Notes for Working Seminar:
*On $k$-free values of irreducible polynomials*
05/18/99

**Halberstam & Roth (1951):** For every $\varepsilon > 0$ and $x \geq x_0(\varepsilon)$, there is a $k$-free number in the interval $(x, x + x^{1/(2k)+\varepsilon}]$.

**Nair (1976, 1979):** He extended the approach to algebraic number fields.

**Theorem (Nair, 1979):** Let $f(x) \in \mathbb{Z}[x]$ with $f(x)$ irreducible and $\gcd(f(m) : m \in \mathbb{Z}) = 1$. Let $n = \deg f$, and let $k$ be an integer $\geq n+1$. There is a constant $c$ such that for $x$ sufficiently large, there is an integer $m \in (x, x + cx^{\theta}]$, where $\theta = n/(2k - n + 1)$, such that $f(m)$ is $k$-free.

**Theorem (Huxley & Nair for $n \geq 2$ in 1980, Trifonov for $n = 1$ in 1995):** One can take $\theta = n/(2k - n + 2)$ above.

**Theorem (Filaseta, 1993):** One can take $\theta = n/(2k - n + r)$ above where $r \sim \sqrt{2n}$.

**Comment:** Similar results can be obtained for $k \leq n$ but not too small compared to $n$ (see the next theorem).

**Theorem (Nair, 1976):** Let $f(x) \in \mathbb{Z}[x]$ with $f(x)$ irreducible and $\gcd(f(m) : m \in \mathbb{Z}) = 1$. Let $n = \deg f$, and let $k$ be an integer $\geq \left(\sqrt{2} - \frac{1}{2}\right)n$. Then there are infinitely many integers $m$ such that $f(m)$ is $k$-free.

**Comment:** Previous results were obtained by Nagel (for $k \geq n$ in 1922) and Erdős (for $k \geq n-1$ in 1953). Nagel's result contained an asymptotic formula for the number of such $m \leq x$ with $f(m)$ being $k$-free; Erdős' result did not. Later Hooley (1967) established asymptotics for $k \geq n-1$. For small $n$, Hooley's result is the best known. Nair obtained his theorem above with asymptotics for the number of $m \leq x$ with $f(m)$ being $k$-free, improving on Hooley's result when $n$ is sufficiently large.

**Question 1:** Can one use differences to prove Hooley's result?

**Question 2:** Can the Swinnerton-Dyer approach be extended to number fields and, if so, what does it imply about $k$-free values of polynomials?

**Question 3:** Is $m^4 + 1$ squarefree for infinitely many integers $m$?

**Notation:** $f(x) \in \mathbb{Z}[x]$
$f(x)$ irreducible
$\gcd(f(m) : m \in \mathbb{Z}) = 1$
$n = \deg f$
$k \geq 2$
$f(\theta) = 0$
$R$ is the ring of integers in $\mathbb{Q}(\theta)$

**Basic Idea 1:** Count $m \leq x$ such that $f(m)$ is not divisible by $p^k$ where $p \leq \varepsilon \log x$. The number of such $m$ is

$$\prod_{p \leq \varepsilon \log x} \left(1 - \frac{\rho(p^k)}{p^k}\right) x + o(x).$$

**Basic Idea 2:** Let $T = x\sqrt{\log x}$. Find an upper bound for the number of $m \leq x$ such that $f(m)$ is divisible by $p^k$

where $\varepsilon \log x < p \le T$. Using that $\rho(p^k)$ is bounded for $p$ large, the number of such $m$ is

$$\ll \sum_{\varepsilon \log x < p \le T} \Big(\frac{x}{p^k} + 1\Big) \ll \frac{x}{\sqrt{\log x}}.$$

**Main Idea:** Find an upper bound for $P(x)$, the number of $m \le x$ such that $f(m)$ is divisible by $p^k$ with $p > T$. Nair shows that there are $E_1, \dots, E_r$ such that

$$P(x) \le \max_{E \in \{E_1,\dots,E_r\}} \Big| \Big\{ u \in R : |u| > T^{1/n}, u^k v = E(m-\theta) \text{ for some } m \in \mathbb{Z} \cap [1,x], v \in R, \text{ and } u \text{ primary } \Big\} \Big|.$$

Here, $u$ being "primary" means any two conjugates have the same order.

**Comment:** One should actually count pairs $(u,v)$ above. The above is correct provided that we divide $[1,x]$ into subintervals of length $H \ll T^{k/n}$ and deal with the subintervals separately.

**Notation:** $I \subseteq [1,x]$
$|I| \le H$
$S$ is the set in the bound for $P(x)$ above restricted to $m \in I$
$S(t) = \{u \in S : t^{1/n} < |u| \le (2t)^{1/n}\}$
$y = m' - \theta$ for some $m' \in I$

**Classical Use of Differences:** Observe that

$$\frac{E(m-\theta)}{u^k} = \frac{Ey}{u^k} + O\Big(\frac{H}{|u|^k}\Big).$$

Consider appropriate forms $P_s(u,\alpha)$ and $Q_s(u,\alpha)$ in $\mathbb{Z}[u,\alpha]$ of degree $s$ such that

$$\frac{E(m_1-\theta)}{u^k} P_s(u,\alpha) - \frac{E(m_2-\theta)}{(u+\alpha)^k} Q_s(u,\alpha)$$

has small absolute value (in particular, $< 1$ so that $H/|u|^{k-s} < 1$ forcing us to restrict to $H \ll t^{(k-s)/n}$). Ideally, we would like to conclude that since the expression above is an algebraic integer with absolute value $< 1$, it must be zero.

**Difficulty:** Algebraic integers (even from a fixed number field) can have arbitrarily small absolute value without being equal to 0.

**Solution:** Apply $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ to the above (to obtain a conjugate of the expression). Using that $u$ and $u+\alpha$ are primary, the conjugate obtained will still have small absolute value (in particular, $< 1$). But some conjugate of a non-zero algebraic integer MUST BE $\ge 1$. Hence, we can deduce the expression above is 0.

**Comment:** One then continues as in the classical Halberstam-Roth method.

**Additional Difficulty:** How does one count $u \in R$ with $|u| \asymp t^{1/n}$?

**Solution:** Write $u = u_1\omega_1 + \cdots + u_n\omega_n$ where $u_j \in \mathbb{Z}$ and $\omega_1, \dots, \omega_n$ form an integral basis for $R$. For $u \in S(t)$, one has each $|u_j|$ is $\ll t^{1/n}$ (and some $|u_j| \gg t^{1/n}$). Consider the hypercube

$$\{(u_1,\dots,u_n) : u_j \in \mathbb{Z}, |u_j| \ll t^{1/n} \text{ for each } j\}.$$

Divide it into sub-cubes with edge length $\ell$. One gets $\ll \big((t^{1/n}/\ell) + 1\big)^n$ such sub-cubes. One picks $\ell$ so that there are $\ll 1$ different $u$ that can lie in a sub-cube and $S(t)$ (via the Halberstam-Roth method).