Notes for Working Seminar:
On k-free values of polynomials II *
06/09/99

Equations to Solve (in several variables):

$$D_1 z_1 - D_2 z_2 + D_3 z_3 = 0 \tag{1}$$

$$D_1 {z_1}^2 - D_2 {z_2}^2 + D_3 {z_3}^2 = D \tag{2}$$

Two Quadratics of Interest:

$$D_1 \left((D_1 + D_3) z_1 - D_2 z_2 \right)^2 - D_2 D_3 {z_2}^2 (D_1 - D_2 + D_3) = D_3 (D_1 + D_3) D \tag{3}$$

$$D_1 D_3 (z_1 - z_3)^2 - D_2 (D_1 - D_2 + D_3) {z_2}^2 = (D_1 + D_3) D \tag{4}$$

Comments: Equation (3) follows from solving for z_3 in (1), substituting into (2), and completing a square. Equation (4) appears to be more useful, however. If we set $\alpha = z_1 - z_3$ and $\beta = z_2$ so that (4) becomes a quadratic in α and β, then observe that solutions in α and β correspond to solutions in z_1, z_2, and z_3 (use the definitions of α and β together with (1) to determine unique values for z_1, z_2, and z_3). Observe that in (3) we can rewrite the first expression which is squared as follows:

$$(D_1 + D_3) z_1 - D_2 z_2 = D_3 z_1 + (D_1 z_1 - D_2 z_2).$$

From (1), the last expression in parentheses is $-D_3 z_3$. Making this substitution results in (4). On the other hand, if one uses (3) directly, one should take into account that the first expression which is squared in (3) is divisible by D_3.

Summary: We are interested in bounding the number of solutions to the quadratic

$$D_1 D_3 \alpha^2 - D_2 (D_1 - D_2 + D_3) \beta^2 = (D_1 + D_3) D. \tag{5}$$

Here, α and β each belong to the set

$$\mathcal{S} = \left\{ a_1\omega_1 + \cdots + a_n\omega_n : a_j \in \mathbb{Z}, |a_j| \le A \text{ for each } j \right\},$$

where $A = o\left(t^{1/n}\right)$ (and $\omega_1, \ldots, \omega_n$ form an integral basis for the ring R of integers in $\mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(x)$).

Background Material: We count integers $m \in (X, X+h]$ such that $f(m)$ is k-free. The polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$ and of degree n. We will want $h \approx X$. We restrict estimates to $m \in I \subseteq (X, X+h]$ with $|I| \le H$. Here, $H \ll t^{k/n}$ (note that we are mainly interested in the case when $k < n$). Of concern to us is the case when $t > T = X\sqrt{\log X}$. Recall that estimating the number of such m as above has been reduced to estimating the number of z_j as in (1) and (2). These z_j correspond to a difference of u_j's (or x_j's in Trifonov's write-ups) in a set of the type described by $\mathcal{S}$ except with A replaced by $t^{1/n}$. If we restrict to a smaller sub-hypercube (so that the u_j's are "close" to one another), then the differences z_j belong to a set of the type $\mathcal{S}$.

Recall also that the u_j's we are interested in are primary. The u_j's correspond to u satisfying an equation of the form

$$E(m - \theta) = u^k v \tag{6}$$

where E is some fixed element of R and where $v \in R$ (v depending on m and u). Taking norms of both sides of (6) (the norm of $m - \theta$ is $f(m)$ divided by the leading coefficient of $f(x)$) and using that the norm of v is at least 1 and the norm of u is $\asymp t$ (each of its conjugates being $\asymp t^{1/n}$), we deduce $X^n \gg t^k$ so that $t \ll X^{n/k}$. Observe that this implies $H \ll X \ll h$ (so the comment about $k < n$ above doesn't serve much of a purpose - the point is that if $k \ge n$, then showing $f(m)$ is k-free for some $m \in (X, 2X]$ is trivial and does not require estimating the number of u_j as above). We fix y of the form $E(m' - \theta)$ where m' is an integer in I, and consider the function $F(u) = y/u^k$. Using (6), we deduce

$$v = \frac{E(m-\theta)}{u^k} = F(u) + O(\delta),$$

where $\delta = Ht^{-k/n}$ (since $|I||u|^{-k} \ll Ht^{-k/n}$). In other words, the function $F(u)$ is within $O(\delta)$ of being an element v of R. This is nothing spectacular as the elements of R will typically be dense in the complex plane. But something more is true. Note that $F(u) = y/u^k$ is an element of the field $\mathbb{Q}(\theta)$. Not only does the difference $v - F(u)$ have a small absolute value but also the same is true of the differences $\sigma(v) - \sigma(F(u))$ for every σ in the Galois group G of $\mathbb{Q}(\theta)$ over $\mathbb{Q}$. Each of these will have absolute value $O(\delta)$.

*These are working notes and may be prone to errors.

We are considering the determinant

$$D = \det\begin{pmatrix} 1 & 1 & 1 & 1 \\ u_0 & u_1 & u_2 & u_3 \\ u_0^2 & u_1^2 & u_2^2 & u_3^2 \\ v_0 & v_1 & v_2 & v_3 \end{pmatrix} \tag{7}$$

together with D_0, D_1, D_2, and D_3 obtained by considering determinants of respective minors along the third row. For each $j \in \{0,1,2,3\}$, we have $E(m_j - \theta) = u_j^k v_j$ for some integer $m_j \in I$.

Two Preliminary Estimates:

Lemma 1. *[Recall that $A = o(t^{1/n})$.] For each $\sigma \in G$ (the Galois group),*

$$Xt^{-(k+3)/n} + O\big(HA^3 t^{-k/n}\big) \ll \sigma(D) \ll XA^6 t^{-(k+3)/n} + O\big(HA^3 t^{-k/n}\big)$$

and, for each $j \in \{0,1,2,3\}$,

$$Xt^{-(k+2)/n} + O\big(HAt^{-k/n}\big) \ll \sigma(D_j) \ll XA^3 t^{-(k+2)/n} + O\big(HAt^{-k/n}\big).$$

Lemma 2. *Suppose that for some $\sigma \in G$ that some $\sigma(D_j) \gg B$. Then there exist integers i_1 and i_2 with $0 \le i_1 < i_2 \le 3$ such that*

$$\sigma(u_{i_2} - u_{i_1}) \gg B^{1/3} t^{(k+2)/(3n)} X^{-1/3} + O\big(H^{1/3} A^{1/3} X^{-1/3} t^{2/(3n)}\big).$$

Also,

$$\sigma(D) \gg Bt^{-1/n} + O\big(HAt^{-(k+1)/n}\big) + O\big(HA^3 t^{-k/n}\big).$$

The First Case: Suppose that for some $\sigma \in G$ that some $\sigma(D_j) \gg B$. Lemma 2 implies that the u_j's cannot all lie in a sub-hypercube with edge length εL for some $\varepsilon > 0$ where L is the bound given for $\sigma(u_{i_2} - u_{i_1})$. The terminology to "lie in a sub-hypercube" requires some explanation. We consider a hypercube

$$\mathcal{C} = \{(a_1, \ldots, a_n) : a_j \in \mathbb{Z}, |a_j| \ll t^{1/n} \text{ for } 1 \le j \le n\}$$

and say u *lies in the hypercube* if there is an n-tuple $(a_1, \ldots, a_n) \in \mathcal{C}$ such that $u = a_1\omega_1 + \cdots + a_n\omega_n$. Therefore, we are saying that if u_0, u_1, u_2, and u_3 are expressed as linear combinations of the basis elements $\omega_1, \ldots, \omega_n$, then there is an ω_i such that the four coefficients of ω_i do not all lie in an interval of length εL. We deduce that there are $\ll \big(t^{1/n}/L\big)^n \ll t/L^n$ such u_j's. This expression needs to be multiplied by $h/H \asymp X/H$ (assuming $H \ll X$) to take into account the different intervals I.

Another Preliminary Estimate:

Lemma 3. *Let $G = \{\sigma_1, \ldots, \sigma_n\}$, and let $z_1, \ldots, z_n$ be n complex numbers. Let $\varepsilon_1, \ldots, \varepsilon_n$ be n positive real numbers. The number of pairs (α, β) with α and β in $\mathcal{S}$ such that, for every $j \in \{1, 2, \ldots, n\}$,*

$$|\sigma_j(\alpha/\beta) - z_j| < \varepsilon_j$$

is $\ll \prod_{j=1}^{n} \big(\varepsilon_j A^2 + 1\big)^{2n}$. If the roots of $f(x)$ are all real, then this bound can be replaced by $\ll \prod_{j=1}^{n} \big(\varepsilon_j A^2 + 1\big)^{n}$.

The Second Case: In the case that $\sigma(D_j) \ll B$ for every $\sigma \in G$ and each j, we return to the situation in the summary. We choose the $D_j = b_1^{(j)}\omega_1 + \cdots + b_n^{(j)}\omega_n$. The conditions for this case imply that each $|b_i^{(j)}|$ is $\ll B$. Thus, each D_j can be chosen in $\ll B^n$ ways. There are therefore $\ll B^{3n}$ possibilities for D_1, D_2, and D_3 in (5). From (5), we can deduce the situation in Lemma 3. Crossing our fingers, we may be able to choose $\varepsilon \ll At^{-1/n}$ (it may help to note that D/D_j has some cancellations in the differences $u_i - u_j$). Then one would get a bound in this case of (at best) $B^{3n}A^{3n}t^{-1} + O\big(t/A^n\big)$. In this case, there is no need for other factors (a solution in α and β corresponds to unique u_j which in turn can only occur $\ll 1$ times as $f(x) \equiv 0 \pmod{p^k}$ has $\ll 1$ positive solutions $\le X$ when $p > T$).