Lecture 6: The Density of Squarefree $0, 1$-Polynomials

Conjecture (Odlyzko & Poonen): Almost all $0, 1$-polynomials are irreducible.

Theorem 1 (Konyagin): The number of irreducible $0, 1$-polynomials of degree $\le n$ is $\gg 2^n/\log n$.

Theorem 2 (F. & Konyagin): Almost all $0, 1$-polynomials are squarefree.

Consequence of the Approach (see Lemmas 2 and 3 below): There are infinitely many squarefree numbers having only the digits 0 and 1 in base 3.

Notation:
- m, n, and b are positive integers with $b \ge 3$
- $S_n = \{f(x) = \sum_{j=0}^{n} \varepsilon_j x^j : \varepsilon_j \in \{0,1\}$ for each j and $\varepsilon_0 = 1\}$
- $t(n) = t(n, m, b)$ is the number of $f(x) \in S_n$ for which m divides $f(b)$

Lemma 1: Let m and b be relatively prime integers with $m \ge 2$. Then $t(n) = \dfrac{2^n}{m}\,(1 + o(1))$.

Main Ideas of Proof:

- $$\sum_{j=0}^{m-1} e^{2\pi i a j/m} = \begin{cases} m & \text{if } m|a \\ 0 & \text{otherwise} \end{cases}$$
- $$t(n) = \frac{1}{m} \sum_{f(x)\in S_n} \sum_{j=0}^{m-1} e^{2\pi i f(b) j/m} = \frac{1}{m} \sum_{j=0}^{m-1} \sum_{f(x)\in S_n} e^{2\pi i f(b) j/m}$$
- $$\sum_{f(x)\in S_n} e^{2\pi i f(b) j/m} = e^{2\pi i j/m} \prod_{k=1}^{n} \left(1 + e^{2\pi i b^k j/m}\right)$$
- $$t(n) = \frac{2^n}{m} + E \quad \text{where} \quad E = \frac{1}{m} \sum_{j=1}^{m-1} e^{2\pi i j/m} \prod_{k=1}^{n} \left(1 + e^{2\pi i b^k j/m}\right)$$
- $$\left| \prod_{k=1}^{n} \left(1 + e^{2\pi i b^k j/m}\right) \right| = \left| \prod_{k=1}^{n} e^{\pi i b^k j/m} \right| \left| \prod_{k=1}^{n} \left(e^{\pi i b^k j/m} + e^{-\pi i b^k j/m}\right) \right| = 2^n \prod_{k=1}^{n} \left|\cos(\pi b^k j/m)\right|.$$
- $$\left|\cos(\pi b^k j/m)\right| \le \left|\cos(\pi/m)\right| \implies |E| \le 2^n \left|\cos(\pi/m)\right|^n \implies |E| = o\big(2^n\big)$$

Lemma 2: Let b be a positive integer, and let B be a real number > 0. Denote by $S(B, n)$ the number of $f(x) \in S_n$ such that $f(b)$ is not divisible by p^2 for every prime $p \le B$. Then

$$S(B, n) = 2^n \prod_{p \le B,\ p\nmid b} \left(1 - \frac{1}{p^2}\right) + o\left(2^n\right).$$

Lemma 3: Let $\varepsilon > 0$, and let B be sufficiently large. Then there are $\leq \varepsilon 2^n$ polynomials $f(x) \in S_n$ for which there exists an integer $d > B$ such that $d^2 | f(3)$.

Main Ideas of Proof:

- Fix $d > B$, and define $r \in \mathbb{Z}$ by $3^{r/2} < d \leq 3^{(r+1)/2}$ (so r is large).
- Fix $\varepsilon_r, \varepsilon_{r+1}, \ldots, \varepsilon_n \in \{0, 1\}$ arbitrarily and consider $f(x) = \displaystyle\sum_{j=0}^{n} \varepsilon_j x^j \in S_n$.
- Distinct choices of the $r-$tuple $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{r-1})$ give distinct sums $\displaystyle\sum_{j=0}^{r-1} \varepsilon_j 3^j$ in $[0, d^2)$.
- For fixed $\varepsilon_r, \varepsilon_{r+1}, \ldots, \varepsilon_n \in \{0, 1\}$, there is at most one choice of $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{r-1})$ such that $f(3)$ is divisible by d^2.
- There are at most 2^{n-r+1} choices for $f(x) \in S_n$ such that $f(3)$ is divisible by d^2.
- Since $d \leq 3^{(r+1)/2}$, we obtain $2^{-r} = (3^{r/2})^{-2\log 2/\log 3} < (3^{(r+1)/2})^{-5/4} \leq d^{-5/4}$.
- The number of $f(x) \in S_n$ such that $d^2 | f(3)$ for some integer $d > B$ is $\leq 2^{n+1} \displaystyle\sum_{d > B} d^{-5/4}$.

Main Ideas for Proof of Theorem 2:

- Fix $R \geq 1$, and consider $g(x) \in \mathbb{Z}[x]$ of degree $r \in [1, R]$. We estimate the number of $0,1$-polynomials $f(x) = \displaystyle\sum_{j=0}^{n} \varepsilon_j x^j$, with $\varepsilon_0 = 1$, that are divisible by some such $g(x)^2$.
- Each coefficient of $g(x)$ has absolute value $\leq 2^R$ (a bound on the product of any k roots of $g(x)$ with $k \leq r$) times 2^R (a bound on the number of combinations of r items taken k at a time). Thus, there are $\leq \big(2 \cdot 4^R + 1\big)^{R+1}$ different possible $g(x)$ (independent of n).
- Define $T_n(f(x))$ as the set of polynomials $w(x) = \displaystyle\sum_{j=0}^{n} \varepsilon'_j x^j$, with $\varepsilon'_0 = 1$, that differ from $f(x)$ in exactly one term. Since $f(x) - w(x) = \pm x^k$ for some $k \in [0, n]$, if $g(x)^2 | f(x)$, then $g(x)^2 \nmid w(x)$ for every $w(x) \in T_n(f(x))$.
- If $f_1(x)$ and $f_2(x)$ are different $f(x)$ as above both divisible by $g(x)^2$, then $T_n(f_1(x))$ and $T_n(f_2(x))$ are disjoint (otherwise, their difference being divisible by $g(x)^2$ would imply $x^k - x^\ell$ is).
- There are $o\big(2^n\big)$ different $f(x)$ divisible by the square of a polynomial of degree $\leq R$.
- If $f(x)$ is divisibly by some $g(x)^2$ with $\deg g > R$, then since the roots of $g(x)$ have real part < 1.5, we deduce $f(3)$ is divisible by d^2 where $d = |g(3)| \geq 1.5^R$. Apply Lemma 3.