AN APPLICATION OF THE LARGE SIEVE: COUNTING REDUCIBLE POLYNOMIALS
COURSE NOTES, 2015

We now state a higher dimensional version of the arithmetic large sieve. We start with the following situation:

- We are given a set $\mathcal{A} \subset \mathbb{Z}^n$ of integer vectors, contained in a box of size X:
$$\operatorname{diam} \mathcal{A} \leq X$$
- We are given a set $\mathcal{P}$ of primes, all satisfying $p \leq z$.
- For all $p \in \mathcal{P}$, we are given a set $\Omega(p) \subset \mathbb{Z}^n/p\mathbb{Z}^n$ of "excluded" residue classes mod p. Set
$$\omega(p) = \#\Omega(p)$$

Let

$$\mathcal{S}(\mathcal{A},\mathcal{P},\Omega) = \{\vec{a} \in \mathcal{A} : \vec{a} \mod p \notin \Omega(p), \ \forall p \in \mathcal{P}, p \leq z\}$$

be the sifted set. The arithmetic form of the large sieve gives an inequality

Theorem 0.1.

$$\#\mathcal{S}(\mathcal{A},\mathcal{P},\Omega) \ll_n \frac{X^n + z^{2n}}{L(z)} \tag{1}$$

where

$$L(z) := \sum_{\substack{m \leq z \\ \text{squarefree}}} \prod_{p|m} \frac{\#\Omega(p)}{p^n - \#\Omega(p)} \tag{2}$$

It is convenient to state a general lower bound for $L(z)$, where instead of summing over squarefree integers, one uses positivity of the summands to just sum over the primes in $\mathcal{P}$:

$$L(z) \geq \sum_{p \in \mathcal{P}} \frac{\#\Omega(p)}{p^n - \#\Omega(p)} \tag{3}$$

We now present two applications, the first quite trivial

Date: June 11, 2015.

0.1. **Counting perfect squares.** We want to count the number $\#\square[X]$ of perfect squares in the interval $[1, X]$ - the answer is clearly

$$\#\square[X] \sim \sqrt{X}, \quad X \to \infty$$

To fit this into the large sieve inequality, we let $\mathcal{A} = [1, X] \cap \mathbb{Z}$, let $\mathcal{P}$ be the set of all odd primes $2 < p \leq z$, and $\Omega(p) \subset \mathbb{Z}/p\mathbb{Z}$ to be the non-squares modulo p. Then for all $z > 2$,

$$\square[X] \subseteq \mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega)$$

and hence by Theorem 0.1,

$$\#\square[X] \leq \#\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) \ll \frac{X + z^2}{L(z)}$$

For an odd prime, the number of non-squares modulo p is exactly $\#\Omega(p) = (p-1)/2$. Hence

$$\frac{\#\Omega(p)}{p - \#\Omega(p)} = \frac{(p-1)/2}{(p+1)/2} = \frac{1 - \frac{1}{p}}{1 + \frac{1}{p}} \geq \frac{1}{2}$$

Therefore

$$\begin{aligned} L(z) &\geq \sum_{2<p<z} \frac{\#\Omega(p)}{p - \#\Omega(p)} \\ &\geq \sum_{2<p<z} \frac{1}{2} \sim \frac{1}{2} \frac{z}{\log z} \end{aligned}$$

Thus $L(z) \gg z/\log z$ and we find that

$$\#\square[X] \leq \#\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) \ll \frac{X + z^2}{z/\log z} \ll \sqrt{X} \log X$$

on taking $z = \sqrt{X}$.

0.2. **Counting reducible quadratic polynomials.** We now give an upper bound for the number of reducible monic quadratic polynomials with integer coefficients of bounded height, in particular showing that almost all monic quadratic polynomials with integer coefficients are irreducible over the rationals.

Remark: It is known (van der Waerden [2]) that this result holds for polynomials of arbitrary degree, in fact that the generic polynomial is irreducible and has Galois group the full symmetric group.

For a monic integer polynomial

$$f(t) = t^n + a_{n-1}t + \cdots + a_0$$

we define the height as

$$\mathrm{Ht}(f) = \max_j |a_j|$$

Thus for $n = 2$,

$$\mathrm{Ht}(t^2 + bt + c) := \max(|b|, |c|)$$

We define

$$\mathcal{R}_n(N) = \{f(t) = t^n + a_{n-1}t + \cdots + a_0 : \mathrm{Ht}(f) \le N; \text{reducible over } \mathbb{Q}\}$$

to be the set of reducible monic polynomial of degree n with integer coefficients. In particular for $n = 2$,

$$\begin{aligned}\mathcal{R}_2(N) &= \{f(t) = t^2 + bt + c : \mathrm{Ht}(f) \le N,\ f \text{ reducible over } \mathbb{Q}\}\\ &= \{(b, c) \in \mathbb{Z}^2, \max(|b|, |c|) \le N,\ f \text{ reducible over } \mathbb{Q}\}\ .\end{aligned}$$

Proposition 0.2. *$\#\mathcal{R}_2(N) \ll N^{3/2} \log N$.*

Note that the bound is quite weak, and we only present it as an application of the large sieve. In fact van der Waerden [2] already gives upper and lower bounds of order $\#\mathcal{R}_2(N) \asymp N \log N$, (and $\#\mathcal{R}_n(N) \asymp N^{n-1}$ for $n > 2$, see also [1]).

Observe that $t^2 + bt + c$ is reducible if and only if the discriminant $b^2 - 4c$ is a perfect square. Hence

$$\mathcal{R}_2(N) = \{(b, c) \in \mathbb{Z}^2, \max(|b|, |c|) \le N,\ b^2 - 4c = \square\}$$

and therefore for all z,

$$\mathcal{R}_2(N) \subseteq \{(b, c) \in \mathbb{Z}^2, \max(|b|, |c|) \le N,\ (b, c) \bmod p \notin \Omega(p),\ \forall p \le z\}$$

where

$$\Omega(p) = \{(b, c) \in \mathbb{Z}^2/p\mathbb{Z}^2 : b^2 - 4c \ne \square \bmod p\}$$

Therefore $\#\mathcal{R}_2(N) \le \#\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega)$ where

$$\mathcal{A} = [-N, N]^2 \cap \mathbb{Z}^2$$

which has diameter $X = 2N$. By the large sieve inequality,

$$\#\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) \ll \frac{N^2 + z^4}{L(z)}$$

so we need to give a lower bound for $L(z)$.

Lemma 0.3. *For an odd prime p, $\#\Omega(p) = (p^2 - p)/2$.*

Proof. We take $p \ne 2$ odd. Let $\mathbf{1}_{\mathrm{NR}}$ be the indicator function of the squares mod p. Then

$$\#\Omega(p) = \sum_{b \bmod p} \sum_{c \bmod p} \mathbf{1}_{\mathrm{NR}}(b^2 - 4c)$$

For each fixed b, we change variables $c \mapsto c' = b^2 - 4c$ which is a bijection of $\mathbb{Z}/p\mathbb{Z}$ if p is odd. This shows that the inner sums all coincide, to be the number of non-squares $\bmod p$, which is $(p - 1)/2$. Summing over all p possibilities for b gives the Lemma. □

From Lemma 0.3 we find

$$L(z) \geq \sum_{2<p\leq z} \frac{(p^2-p)/2}{(p^2+p)/2} = \sum_{2<p<z} \frac{1-\frac{1}{p}}{1+\frac{1}{p}}$$

which is exactly the sum that appeared when bounding squares. Hence

$$L(z) \gg z/\log z$$

giving

$$\#\mathcal{S}(\mathcal{A},\mathcal{P},\Omega) \ll \frac{N^2+z^4}{L(z)} \ll (\frac{N^2}{z}+z^3)\log z \ll N^{3/2}\log N$$

on choosing $z=\sqrt{N}$. This proves Proposition 0.2.

0.3. **Counting reducible polynomials of higher degree.**

Exercise 1. Show that for $n>2$,

$$\#\mathcal{R}_n(N) \ll_n N^{n-\frac{1}{2}}\log N\ .$$

Hint: Use the large sieve with

$$\Omega_p = \{f\in\mathbb{F}_p[t], \deg f = n,\ \text{monic irreducible over } \mathbb{F}_p\}\ .$$

References

[1] R. Chela, *Reducible polynomials.* J. London Math. Soc. 38 1963 183–188.

[2] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt.* Monatsh. Math. Phys. 43 (1936), no. 1, 133–147.