TWO-DIMENSIONAL LARGER SIEVE

Gallagher's larger sieve states that if $\mathcal{A} = \{a_1, \ldots, a_k\}$ is a finite set of k distinct integers with $1 \leqslant a_i \leqslant x$, and if, for primes p, the image of $\mathcal{A}$ under the reduction map has cardinality $\leqslant \nu(p)$, then we have for all $y \geqslant 2$

$$|\mathcal{A}| \leqslant \frac{\theta(y) - \log x}{\theta(y;\nu) - \log x},$$

provided the denominator is positive, where for any sequence $\alpha(n)$ of positive numbers and $y \geqslant 2$ we write

$$\theta(y;\alpha) = \sum_{p \leqslant y} \alpha(n)^{-1} \log(p)$$

with the convention $\theta(y) = \theta(y;1)$.

Here is a two-dimensional version:

Proposition 1. *Let $\mathcal{A} = \{(a_1, b_1), \ldots, (a_k, b_k)\}$ be a finite sequence of k distinct integral vectors with $1 \leqslant a_i, b_i \leqslant x$ for $1 \leqslant i \leqslant k$. Assume that for any prime p the cardinality of the reduction $\mathcal{A} \pmod p \subset (\mathbf{Z}/p\mathbf{Z})^2$ is $\leqslant \nu(p)$. Then we have*

$$|\mathcal{A}| \leqslant \frac{\theta(y;4,3) - (\log 2x^2)}{\theta(y;\nu,4,3) - (\log 2x^2)}$$

where

$$\theta(y;\alpha,q,a) = \sum_{\substack{p \leqslant y \\ p \equiv a \pmod q}} \alpha(p)^{-1} \log p,$$

provided the denominator is > 0.

Proof. Let

$$\Delta_2 = \prod_{1 \leqslant i \neq j \leqslant k} \big((a_i - a_j)^2 + (b_i - b_j)^2\big),$$

a positive integer. Note first that

$$|\Delta_2| \leqslant (2x^2)^{|\mathcal{A}|(|\mathcal{A}|-1)}. \tag{1}$$

On the other hand, if p is a prime number congruent to 3 modulo 4, we know that for any integers r and s we have

$$p \mid r^2 + s^2 \text{ if and only if } p \mid r \text{ and } p \mid s,$$

so for $p \leqslant y$ congruent to 3 modulo 4, we have

$$p \mid (a_i - a_j)^2 + (b_i - b_j)^2$$

if and only if $p \mid a_i - a_j$ and $p \mid b_i - b_j$. Therefore, for such p the p-adic valuation v_p of Δ_2 satisfies

$$\begin{aligned} v_p &= \sum_{\substack{i \neq j \\ (a_i,b_i) \equiv (a_j,b_j) \pmod p}} 1 \\ &= \sum_{(a_i,b_i) \equiv (a_j,b_j) \pmod p} 1 - |\mathcal{A}| \\ &= \sum_{\nu \in (\mathbf{Z}/p\mathbf{Z})^2} R(\nu)^2 - |\mathcal{A}| \end{aligned}$$

where

$$R(\nu) = |\{i \mid (a_i, b_i) \equiv \nu \,(\mathrm{mod}\, p)\}|$$

is the multiplicity of ν as reduction of an element of the sequence $\mathcal{A}$.

By Cauchy-Schwarz, we have

$$\sum_{\nu} R(\nu)^2 \geqslant \frac{\Bigl(\sum_{\nu} R(\nu)\Bigr)^2}{\nu(p)} = \frac{|\mathcal{A}|^2}{\nu(p)}.$$

Since

$$\prod_{\substack{p \leqslant y \\ p \equiv 3 \,(\mathrm{mod}\, 4)}} p^{v_p} \leqslant |\Delta_2|,$$

we obtain

$$\sum_{\substack{p \leqslant y \\ p \equiv 3 \,(\mathrm{mod}\, 4)}} v_p \log p \leqslant \log |\Delta_2| \leqslant |\mathcal{A}|(|\mathcal{A}| - 1)(\log 2x^2)$$

which translates by the above to

$$\sum_{\substack{p \leqslant y \\ p \equiv 3 \,(\mathrm{mod}\, 4)}} \Bigl\{ \frac{|\mathcal{A}|^2}{\nu(p)} - |\mathcal{A}| \Bigr\} \log p \leqslant |\mathcal{A}|(|\mathcal{A}| - 1)(\log 2x^2).$$

Simplifying by $|\mathcal{A}|$ (if non-zero...) and re-arranging gives the result. □

Remark 2. (1) This can only be interesting if the sum of $\log p/\nu(p)$ gets large; this requires $\nu(p)$ to be quite small, and more importantly this condition doesn't involve the two-dimensional nature of the situation: the total number of permitted residue classes has to be (essentially) $< p/2$, although there are p^2 possible classes now. But that's reasonable because we can get a set of δp^2 residue classes in $(\mathbf{Z}/p\mathbf{Z})^2$ simply by taking $\mathbf{Z}/p\mathbf{Z} \times \Omega_p$ where Ω_p is of size δp, and then the cardinality of the sifted set is $p|\mathcal{A}|$, where $\mathcal{A}$ is the (one-dimensional) sifted set with respect to the Ω_p.

(2) One can incorporate more primes than those $\equiv 3 \,(\mathrm{mod}\, 4)$ by using more polynomials $F(x, y)$ such that $p \mid F(x, y)$ if and only if $p \mid x$ and $p \mid y$ for some other subsets of the primes. It is probably impossible to get all primes involved in this manner, however.

(3) Similar statements hold in dimension $d \geqslant 3$, with the same restriction on $\nu(p)$ in order that they be efficient. (One can find a polynomial $F_d(X_1, \ldots, X_d)$, homogeneous of degree d, such that for some positive density of primes, $(0, \ldots, 0)$ is the only zero of F_d modulo p). For instance, if d is prime, one can take

$$F_d = X_1^d + \cdots + X_d^d,$$

and the set of primes we can take is the set of those p which are primitive roots modulo d if d is odd, or $2d$ if $d = 2$.