An interesting application:

Thm 11.4.17 (Linnik)

For any prime $p \geq 2$, let

$$k_p = \min\{ n \geq 1 : (n \bmod p) \notin \mathbb{F}_p^{\times 2} \}.$$

(quadr. nonres.)

For any $\varepsilon > 0$, for every $N \geq 1$, there are only $O_\varepsilon(1)$ primes p with $k_p > N^\varepsilon$.

~~For any $\varepsilon > 0$, there are only fin. many p with $k_p > N^\varepsilon$.~~

Rmk The GRH implies that $k_p \ll (\log p)^2$ for all p and even that there is a primite root $n \ll (\log p)^6$ modulo p.

Pf Let $N \geq 1$ be large, $z = N^{1/2}$.

For any p, define $E_p \subseteq \mathbb{Z}/p\mathbb{Z}$ as follows:

$$E_p = \begin{cases} \{a \in \mathbb{Z}/p\mathbb{Z} \text{ quadr. nonresidue}\}, & k_p > N^\varepsilon, \\ \emptyset, & k_p \leq N^\varepsilon \text{ (or } p = 2) \end{cases}$$

Let $S = \{1 \leq n \leq N : \forall p \leq z : (n \bmod p) \notin E_p\}$

$= \{1 \leq n \leq N : \forall p \leq z \text{ with } k_p > N^\varepsilon, \ n \text{ is a quadr. res. mod } p\}.$

Note: $S \supseteq \{1 \leq n \leq N^\varepsilon\}$.

In fact, since any prod. of quadr. res. is a quadr. res, $S \supseteq \{1 \leq n \leq N \mid n = p_1 \cdots p_k \text{ with } p_1, \dots, p_k \leq N^\varepsilon\}$.

~~W.l.o.g. $\varepsilon = 1/R$ with $R \in \mathbb{Z}$~~

$\cancel{\Rightarrow \# S \geq \frac{1}{R!} \#\{p \leq N^\varepsilon\}^R \gg_R \left(\frac{N^\varepsilon}{\log(N^\varepsilon)}\right)}$

$= \{1 \leq n \leq N \mid n \text{ is } N^\varepsilon\text{-smooth}\}.$

$\Rightarrow \# S \geq \#\{1 \leq n \leq N \mid n \text{ is } N^\varepsilon\text{-smooth}\} \gg_\varepsilon N.$ (skipped)

On the other hand, the large sieve shows:

$$\#S \ll \frac{N+z^2}{J} \asymp \frac{N}{J}.$$

$\geq N$

$$\Rightarrow J \ll_\varepsilon 1$$

$\geq$

$$\sum_{p\le z} \frac{\omega(p)}{p} = \sum_{\substack{p\le z:\\ k_p>N^\varepsilon}} \frac{\frac{p-1}{2}}{p} \gg \sum_{\substack{p\le z:\\ k_p>N^\varepsilon}} 1.$$

$$\omega(p) = \#E_p = \begin{cases} \frac{p-1}{2}, & k_p > N^\varepsilon, \\ 0, & \text{otherwise.} \end{cases}$$

$\Rightarrow \#\{p \le z : k_p > N^\varepsilon\} \ll_\varepsilon 1$ is bounded as $N\to\infty$ (and $z\to\infty$). $\square$

~~There's a higher dim~~

The large sieve can be generalised to higher dimension:

Thm 11.4.8 (Large sieve). Let $m \geq 1$.

Let $z \geq 1$, $N \geq 1$, $B \subset \mathbb{R}^m$ a ball of radius N.

For each p, let $E_p \subseteq (\mathbb{Z}/p\mathbb{Z})^m$ be a set of size $\omega(p)$.

Then,

$$\#\{v \in B \cap \mathbb{Z}^m : \forall p \leq z : (v \bmod p) \in E_p\} \ll_m \frac{(N + z^2)^m}{J},$$

where $$J = \sum_{\substack{d \leq z \\ \text{sqfree}}} \prod_{p \mid d} \frac{\omega(p)}{p^m - \omega(p)} \geq \sum_{p \leq z} \frac{\omega(p)}{p^m - \omega(p)} \geq \sum \frac{\omega(p)}{p^m}.$$

Some other consequences:

Thm 11.4.9

Let $V \subset \mathbb{A}^n_{\mathbb{Q}}$ be an irreducible algebraic set of dimension n, not an affine linear subspace.

Then,

$$\#\{(x_1,\dots,x_n)\in V : x_1,\dots,x_n\in\mathbb{Z},\ |x_1|,\dots,|x_n|\le T\}$$

$$\ll T^{n-\frac{1}{2}}\cdot \log T.$$

Pf cf. Thm 13.1.2 in Serre: Lectures on the Mordell-Weil Theorem. $\square$

Rmk If $f\in\mathbb{Q}[X_1,\dots,X_n]$ is a pol. of degree d, how many pts. $(x_1,\dots,x_n)\in\mathbb{Z}^n$ with $|x_1|,\dots,|x_n|\le T$ do we expect?

Naively, $\asymp_f T^{n-d}$ if $d\le n$,

$\ll_f 1$ if $d>n$.

(because $f(x_1,\dots,x_n)$ is a number $\ll T^d$ $\leadsto$ $=0$ with prob. T^{-d} for random $x_1,\dots,x_n$).

Of course, this is wrong in general.

For example, the result should be the same if we replace f by f^2. Also, $V(f) = \{x \mid f(x)=0\}$ could contain a line. Or $f=gh$. ...

Counterexamples to the naive heuristic

a) $f(X,Y,Z) = X^2+Y^2+Z^2 \rightsquigarrow N(T)=1$

b) $f(X,Y) = 2X+1$

$\rightsquigarrow N(T)=0$

c) $f = gh$

d) ~~$\{P \mid f(P)=0\}$ can contain a line for arbitrarily large d~~

$f(X,Y,Z) = X^d + Y$

$\rightsquigarrow N(T) \gg T$

$f(0,0,z)=0$

e) $f(X,Y,Z) = XY - Z$

$\rightsquigarrow N(T) \asymp T \log T$

$\vdots$

(See also Manin's conjecture.)

Thm 11.4.10 (Bombieri – Vinogradov)

Let $A > 0$. For large x and for

$\frac{x^{1/2}}{(\log x)^A} \le Q \le x^{1/2}$, we have

$$\sum_{q \le Q} \max_{\substack{y \le x \\ a \in (\mathbb{Z}/q\mathbb{Z})^\times}} \left| \sum_{\substack{n \equiv a \bmod q \\ n \le y}} \Lambda(n) - \frac{y}{\varphi(q)} \right| \ll_A Q\, x^{1/2} (\log x)^5 .$$

Rmk We have

$$\sum_{\substack{n \equiv a \bmod q \\ n \le y}} \Lambda(n) \ll \frac{x \log x}{q} \quad \text{and} \quad \frac{y}{\varphi(q)} \ll \frac{x \log x}{q}, \text{ so}$$

clearly $\text{LHS} \ll x \log x \log Q \le x (\log x)^2$.

Rmk GRH implies

$$\left| \sum \Lambda(n) - \frac{y}{\varphi(q)} \right| \ll y^{1/2} (\log y)^2$$

according to Thm 10.10, which implies

$$\text{LHS} \ll Q\, x^{1/2} (\log x)^2 .$$

12. The circle method

12.1. Introduction

Dirichlet series $D(a,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ are useful for multiplicative problems.

Power series $F(a,z) = \sum_{n=0}^{\infty} a_n z^n$ are useful for additive problems.

$$F(a,z) \cdot F(b,z) = F(a * b, z)$$

where $a * b$ is (now) the additive convolution:

$$(a * b)_k = \sum_{\substack{n,m \geq 0: \\ k = n+m}} a_n b_m .$$

Ex $F((1,1,\dots), z) = \sum z^n = \frac{1}{1-z}$

Ex For $d \geq 1$, $a_n = \begin{cases} 1, & d \mid n, \\ 0, & d \nmid n, \end{cases}$

$$F(a,z) = \sum z^{dn} = \frac{1}{1-z^d} .$$

Ex $\frac{1}{1-z} \cdot \frac{1}{1-z^d} = F(a,s)$ for $a_k = \#\{(n,m) : k = n+m,\ 2 \mid m\}$.

$\underline{\text{Ex}}$ $\prod_{d=1}^{\infty} \frac{1}{1-z^d} = F(a,z)$

$\uparrow$
formal product

for $a_k = \left\{ (n_1, n_2, \dots) \;\middle|\; \begin{array}{l} a_1, a_2, \dots \geq 0 \\ d \mid a_d \ \forall d \\ k = a_1 + a_2 + \dots \end{array} \right\}$

$= \left\{ (m_1, m_2, \dots) \;\middle|\; \begin{array}{l} m_1, m_2, \dots \geq 0 \\ k = \sum_{d=1}^{\infty} d m_d \end{array} \right\}$

$=$ # ways to write $k = s_1 + \dots + s_r$ with $1 \leq s_1 \leq \dots \leq s_r$, $r \geq 0$.

$=$ # partitions of k.

To study asymptotics of a_n for $n \to \infty$, instead of Perron's formula, use:

$\underline{\text{Rmk}}$ If $F(a,z)$ has radius of convergence R and $\mathcal{C}$ is a CCW circle centered at 0 of radius $0<r<R$, then

$$a_n = \frac{1}{2\pi i} \int_{\mathcal{C}} \frac{F(a,z)}{z^{n+1}} \, dz.$$

$\underline{\text{Rmk}}$ If $a_n = 0$ for all but finitely many n, then $R = \infty$ and we'll take $r = 1$.

$$\Rightarrow a_n = \frac{1}{2\pi i} \int_0^1 \frac{F(a, e(t))}{e(t)^{n+1}} \underbrace{e'(t)}_{2\pi i e(t)} \, dt = \int_0^1 F(a, e(t)) e(-nt) \, dt.$$