THE CIRCLE METHOD

PROBLEMS:

- **Waring:** Is there an s st all pos ints (or all suff large pos ints) are a sum of at most s k-th powers?
  ↳ $x_1^k + \dots + x_s^k = n$
- **Goldbach:** $p_1 + p_2 + p_3 = N$
  $p_1 + p_2 = N$
- **Germain Twin:** p st p, $p \cdot \frac{p-1}{2}$ prime or p, $p+2$ prime

How to solve? Especially Goldbach
↳ primes are multiplicative, These sumset questions

NEEDED INPUT: Number Theory

See section 13.2.6

PRIME NUMBER THM (PNT): $\sum_{p \le x} \log p = x + O\left(x \exp\left(-c\sqrt{\log x}\right)\right)$

for some $c > 1$. By Partial Sum, $\sum_{p \le x} 1 = \mathrm{Li}(x) + O\left(x \exp\left(-\frac{c\sqrt{\log x}}{2}\right)\right)$

↳ See Section 2.2.2
↳ $\mathrm{Li}(x) \approx \frac{x}{\log x}$

SIEGEL-WALFISZ: $\forall C, B > 0$ and $(a, q) = 1$

$$\sum_{\substack{p \le x \\ p \equiv a (q)}} \log p = \frac{x}{\varphi(q)} + O\left(\frac{x}{\log^C x}\right) \quad \forall q \le \log^B x$$

↳ wish could do $q \le x^\delta$
↳ Main term $\gg$ error term if C suff large
↳ $\varphi(q)$ Euler's φ-function: See Section 2.1

Need basic relation from Fourier Analysis:

$$\int_0^1 e(nx)\, e(-mx)\, dx = \begin{cases} 1 & n = m \\ 0 & \text{otherwise} \end{cases}$$

ASIDE: PNT and Siegel-Walfisz

Counting Primes

① Euclid: $P_1 \cdots P_n + 1$
↳ investigate on OEIS where q_ℓ is ℓ^{th} prime generated by this
↳ can generalize to some but not all arithm prog
$p \equiv 4n+1$ no $p \equiv 4n+3$ yes (see Exe 2.3.5)

② See "Proofs from THE BOOK"
↳ Two favorites: $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s = \prod_{p \text{ prime}} (1 - 1/p^s)^{-1}$ $\mathrm{Re}(s) > 1$
$\lim_{s \to 1^+} \zeta(s) = +\infty \Rightarrow$ ∞ many primes
$\zeta(2) = \pi^2/6$ and $\pi^2 \notin \mathbb{Q} \Rightarrow$ ∞ many primes (See also § 11.3.4)

③ Chebyshev's Thm (Thm 2.3.9) $\exists A, B$ with $0 < A < 1 < B < \infty$ s.t.
$\forall X \geq 30$ $\frac{AX}{\log X} \leq \pi(X) \leq \frac{BX}{\log X}$
↳ many proofs, one in book uses nice approx technique and telescoping sums
↳ Corr: Bertrand's Postulate: $\forall n \geq 1$ $\exists p \in [n, 2n]$!
Questions on primes in short gaps
Good Exercise: Exe 2.3.15 (Prime Deserts)
↳ also Exe 2.3.16, 2.3.17

④ Dirichlet's Thm (Section 3.3): $(a, m) = 1$. Then
$\pi_{m,a}(X) = \frac{1}{\varphi(m)} \frac{X}{\log X} + O_a\left(\frac{1}{\varphi(m)} \frac{X}{\log X}\right)$
↳ Siegel-Walfisz is controlling error

THE CIRCLE METHOD

ORIGINS / BASIC PROBLEMS

"Cookie Problem": N cookies, p people: $\binom{N+p-1}{p-1}$

↳ equiv to $x_1 + \cdots + x_p = N$

(note: easy add conds such as $x_i \geq a_i$)

↳ solving by combinatorics; doesn't generalize to higher powers such as $x_1^k + \cdots + x_s^k = N$

Generating Functions

↳ look at $x_1 + \cdots + x_s = N$ again

$$f(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

$$f(x)^s = \left(\sum_{m_1} x^{m_1}\right) \cdots \left(\sum_{m_s} x^{m_s}\right) = \sum_{n=0}^{\infty} r_{1,s}(n) x^n$$

↳ Thus $r_{1,s}(n)$ is answer, but how to recover?

BUT $f(x)^s = \left(\frac{1}{1-x}\right)^s = \frac{1}{(s-1)!} \frac{d^{s-1}}{dx^{s-1}} \frac{1}{1-x}$

$$\Rightarrow f(x)^s = \frac{1}{(s-1)!} \frac{d^{s-1}}{dx^{s-1}} \left(\sum_{n=0}^{\infty} x^n\right) = \sum_{n=0}^{\infty} \binom{n+s-1}{s-1} x^n$$

$$\Rightarrow r_{1,s}(n) = \binom{n+s-1}{s-1}$$

WARING: $f_{k,N}(x) = \sum_{n=0}^{N} x^{n^k}$, $f_{k,N}^s(x) = \cdots$

Goldbach: $f_N(x) = \sum_{p \leq N} e(px)$, $f_N^s(x) = \cdots$ $\quad e(u) = e^{2\pi i u}$

↳ technically easier to do finite sums and exponentials

↳ get say $r_{N,s}(m) = r_s(m)$ if $m \leq N$

ASIDE: Differentiating identities POWERFUL technique, especially for calculating moments in prob / generating identities. See handout

THE CIRCLE METHOD

Write $n = p_1 + \cdots + p_s$

$$F_N(x) = \sum_{p \le N} \log p \cdot e(px)$$

↳ $\log p$ is to simplify some sums

technically easier to count primes @ log weight

ASIDE: Section 2.3.4 and 3.2.2 for why we count primes with $\log p$ weight

$$F_N^s(x) = \sum_{m=0}^{\infty} R_{N,s}(m)\, e(mx)$$

where $R_{N,s}(m)$ is # ways write m as a sum of s primes at most N. Note $R_{N,s}(m) = R_s(m)$ for $m \le N$

Basic Fourier analysis

$$R_{N,s}(n) = \langle F_N^s, e(-nx) \rangle = \int_0^1 F_N^s(x)\, e(-nx)\, dx$$

↳ Note: we have "solved" our problem!

Unfortunately, not very illuminating

Goal: Show $R_{N,s}(N) > 1$ → at least one way

↳ amazing that can often only prove one item exists by showing as many do

↳ ex: general q, ℓ rel prime: to show $\exists p \equiv a \pmod{\ell}$ with p prime requires proving Dirichlet's Thm ($\tilde{\pi}_{a,\ell}(x) \sim \frac{1}{\varphi(\ell)} \pi(x)$)

The Circle Method: Size of $F_N(x)$

$$F_N(x) = \sum_{p \le N} \log p \cdot e(px)$$

Trivial: $|F_N(x)| \le \sum_{p \le N} \log p = N + o(N)$

Average: On average $|F_N(x)|^2$ is like $N \log N + o(N \log N)$

↳ Proof: VERY IMPORTANT TECHNIQUE
works for L^2 norm, not others...

$$\int_0^1 |F_N(x)|^2 dx = \int_0^1 F_N(x) F_N(-x)\, dx \cdots$$

Gives $\sum_{p \le N} \log^2 p = N \log N + o(N \log N)$

↳ could see by $p \le \frac{N}{\log^2 N}$ and $\frac{N}{\log^2 N} \le p \le N$

Aside: Philosophy of square root cancellation

Special Values: $F_N(0) = F_N(1) = N + o(N)$

$F_N(1/2) = -N + o(N)$

↳ much larger than ave value

Idea:
- F_N "large" at x near a/q with q "small" and F_N "small" otherwise
- Split $\int_0^1 F_N(x)\, e(-nx)\, dx$ into two integrals, one where F_N "large", other "small"

↳ technicalities galore!

The Circle Method: Size of $F_N(x)$ (cont.)

Thm: Fix B, set $Q = \log^B N$, take a, q rel prime with $q \le Q$.
Then $\forall C$ have $F_N\left(\frac{a}{q}\right) = \frac{N}{\varphi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right) + O\left(\frac{N}{\log^{C-B} N}\right)$

Proof: $F_N\left(\frac{a}{q}\right) = \sum_{p \le N} \log p \cdot e\left(p\frac{a}{q}\right)$

($e\left(p\frac{a}{q}\right)$ only depends on $p \bmod q$)

$$= \sum_{r=1}^{q} \log p \; e\left(\frac{ar}{q}\right) \sum_{\substack{p \equiv r (q) \\ p \le N}} \log p$$

trivial estimation + Siegel–Walfisz

Major Arcs: $\mathfrak{M} = \bigcup_{q=1}^{Q} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}_{a,q}$

where $\mathfrak{M}_{a,q} = \left\{ x \in (0,1] : \left|x - \frac{a}{q}\right| < \frac{Q}{N} \right\}$

and $\mathfrak{M}_{1,1} = \left[0, \frac{Q}{N}\right) \cup \left(1 - \frac{Q}{N}, 1\right]$

Minor Arcs: $\mathfrak{m} = (0,1] - \mathfrak{M}$

Trivially have $|\mathfrak{M}| \le \sum_{q=1}^{Q} q \cdot \frac{2Q}{N} \le \frac{2Q^3}{N}$

as $Q = \log^B N$, see $\lim_{N \to \infty} |\mathfrak{M}| = 0$, $\lim_{N \to \infty} |\mathfrak{m}| = 1$

↳ Discuss terminology for major/minor arcs.

13.3.5. The Major Arcs and the Singular Series

Major Arc Contribution (Heuristic)

Lets do $s=3$ and $n=N$ (ie, $P_1+P_2+P_3=N$)

$$\int_0^1 F_N(x)^3 \mathcal{A}\mathcal{A} e(-Nx)\,dx = \sum_{\substack{P_1,P_2,P_3 \le N \\ P_1+P_2+P_3=N}} (\log P_1 \log P_2 \log P_3$$

Major arcs

$$\int_{\mathfrak{M}} F_N(x)^3 e(-Nx)\,dx = \sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}_{a,q}} F_N(x)^3 e(-Nx)\,dx$$

↳ estimate $F_N(x)$ by $F_N(\frac{a}{q})$

ignore all lower order terms, note $|\mathfrak{M}_{a,q}| = 2Q/N$

yields $$\frac{2Q}{N} \sum_{q=1}^{Q} \sum_{(a,q)=1} \left(\frac{N}{\varphi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right) \right)^3 e\left(-\frac{Na}{q}\right)$$

$$= \mathfrak{S}(N) \cdot \left(N^2 \cdot 2Q\right) \quad \text{with } Q = \log^B N$$

where $$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \frac{1}{\varphi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right) \right)^3 e\left(-N\frac{a}{q}\right)$$

↳ More careful analysis (see Chap 14) gives $\mathfrak{S}(N) \cdot \frac{N^2}{2}$

Comments: ① Close: correct power of N, missed by a few logarithms which could matter

② not surprising, as doing a zeroth order Taylor Expansion.

↳ surprisingly, do much better (ie, easier) NOT to Taylor Expand $F_N(x)$ but to find a fn $U_N(x)$ st $U_N(a/q) = F_N(a/q)$ and U_N easily integrated

③ Main term is from this (we hope!), but tough to look at $\mathfrak{S}(N)$ and "see" its behavior: ie: $\mathfrak{S}(1776) = 0$!

THE SINGULAR SERIES

$$\mathfrak{G}(N) = \sum_{q=1}^{\infty} \frac{1}{\varphi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right) \right)^3 e\left(-N\frac{a}{q}\right)$$

Using methods of Chapter 14:

$$\mathfrak{G}(N) = \prod_p \left(1 - \frac{c_p(N)}{\varphi(p)^3}\right) \quad \text{with} \quad c_p(N) = \begin{cases} p-1 & \text{if } p \mid N \\ 0 & \text{otherwise} \end{cases}$$

↳ very important

says $\mathfrak{G}(N)$ is a multiplicative function (see Defn 2.1.2)

view as $\mathfrak{G}(N) = \prod_p \delta_p(N)$, each $\delta_p(N)$ a "local density", measuring obstructions

↳ if $2 \mid N$ then $\delta_2(N) = 0$ and main term $\mathfrak{G}(N)\frac{N^2}{2} = 0$!

↳ What does this mean?

Circle Method knows Goldbach ($p_1 + p_2 = 2n$) hard

Say $p_1 + p_2 + p_3 = 2N = 2n+2$

Then wlog $p_3 = 2$ and writing $2n$ as sum of two primes!

ASIDE ON OBSTRUCTIONS: Hasse Principle, Section 4.4

Exe 13.3.16: Important

N odd $\to \exists\, c_1, c_2 > 0$ (and indep of N) s.t. $c_1 < \mathfrak{G}(N) < c_2$

Minor Arcs Contribution

Know $|F_N(x)|$, on average, is about $\sqrt{N \log N}$ and at most N

Can be as large as order N near a/q with $q \ll N$

Vinogradov: $\max_{x \in \mathfrak{m}} |F_N(x)| \ll \frac{N}{\log^D N}$ $\quad D = D(B,C) > 1$

$$\left| \int_{\mathfrak{m}} F_N^3(x) e(-Nx)\, dx \right| \le \int_{\mathfrak{m}} |F_N(x)|^2 \cdot |F_N(x)|\, dx$$

$$\le \max_{x \in \mathfrak{m}} |F_N(x)| \cdot \int_{\mathfrak{m}} |F_N(x)|^2 dx$$

$$\ll \frac{N}{\log^D N} \cdot \int_0^1 |F_N(x)|^2 dx$$

$$= \frac{N}{\log^D N} \cdot N \log N = \frac{N^2}{\log^{D-1} N}$$

Thus a "small" cancellation is enough to win when $s = 3$

Aside: Very common/important technique

easy to evaluate $\int_0^1 |F_N(x)|^2 dx$, and

need slight savings in an $|F_N(x)|$ for $x \in \mathfrak{m}$

WHY IS GOLDBACH HARD?

Cauchy-Schwarz (ver 6): $\left|\int_0^1 fg\right| \le \left(\int_0^1 f^2\right)^{\frac{1}{2}} \left(\int_0^1 g^2\right)^{\frac{1}{2}}$

↳ Proof: Lemma A.6.9

When $s=2$ ($P_1+P_2=N$) Major arcs give $\sim \mathfrak{S}_2(N)\cdot N$

Estimate minor arcs: insert abs values (lose all oscillation)

↳ $\int_m |F_N(x)|^2\,dx \sim N\log N$ too big

↳ pull at $|F_N(x)|$: $\max_{x\in m}|F_N(x)| \cdot \int_m^1 |F_N(x)|\,dx$

↳ real bad: even if $|F_N(x)|$ is always its average value, $\sqrt{N\log N}$
we get at least $N\log N$ again

↳ what if "most" of the time $|F_N(x)|$ small?

Using Cauchy-Schwarz:

$$\int_m |F_N(x)|^{\text{"a"}}\,dx \le \left(\int_m |F_N(x)|^2\,dx\right)^{1/2}\left(\int_m 1^2\,dx\right)^{1/2}$$
$$\le (N\log N)^{1/2}\cdot 1$$

(note: applying Cauchy-Schwarz good on finite intervals)

↳ still need more than average value cancellation!

ASIDE: Littlewood Problem (includes results of Paul Cohen)

Remark: Is Goldbach hopeless?

↳ This is too crude of a method: moving absolute value inside the integration loses all oscillation.

ASIDE: Research projects / detailed calculations in Chapter 14 for German Primes