Average values of some non-multiplicative functions

Greg Martin
University of British Columbia

joint work with Paul Pollack, Ethan Smith

Canadian Number Theory Association XII Meeting
University of Lethbridge
June 22, 2012

slides can be found on my web page
www.math.ubc.ca/∼gerg/index.shtml?slides

Outline

Some constants that will appear

The following values will be the average value of some function in this talk:

1. $$\frac{2}{2}+\frac{3}{4}+\frac{5}{8}+\frac{7}{16}+\cdots=\sum_{k=1}^{\infty}\frac{p_k}{2^k}\approx 3.67464$$
2. $$\sum_{\substack{\ell \text{ prime}}}\ell^2\prod_{\substack{p\le\ell\\ p \text{ prime}}}(p+1)^{-1}\approx 2.53505$$
3. $$\sum_{\substack{\ell \text{ prime}}}\frac{5\ell^3+6\ell^2+6\ell}{6(\ell^2+\ell+1)}\prod_{\substack{p<\ell\\ p \text{ prime}}}\frac{p^2}{6(p^2+p+1)}\approx 2.12110$$
4. $$\frac{2}{3}\prod_{\substack{p>2\\ p \text{ prime}}}\left(1-\frac{1}{(p-1)^2}\right)\left(1+\frac{1}{(p-2)(p-1)(p+1)}\right)\approx 0.50517$$

Erdős's result

Definition: least quadratic nonresidue

For q prime, $n_2(q)$ is the least number n such that $\left(\frac{n}{q}\right) = -1$.

(Note that $n_2(q)$ is always a prime.)

Theorem (Erdős, 1961)

$$\lim_{x\to\infty} \left(\frac{1}{\pi(x)} \sum_{2<q\le x} n_2(q) \right) = \sum_{k=1}^{\infty} \frac{p_k}{2^k},$$

where p_k denotes the kth prime in increasing order.

The average value of the least quadratic nonresidue modulo a prime is the constant $\sum_{k=1}^{\infty} p_k/2^k \approx 3.67464$.

A surprising constant . . .

A shiny result

Time muffles the original éclat of a theorem. In 1967, in a Nottingham seminar, I did not get past the value of Erdős's limit . . . before Eduard Wirsing stopped me. "I don't believe it!", says he, looking at the expression for the constant, "I have never seen anything like it!"

Peter Elliott

Exercise

$$\sum_{k=1}^{\infty} \frac{p_k}{2^k} = \sum_{n=0}^{\infty} \frac{1}{2^{\pi(n)}}$$

. . . but a believable constant

Definition: least quadratic nonresidue

For q prime, $n_2(q)$ is the least number n such that $\left(\frac{n}{q}\right) = -1$.

Heuristic

- For a fixed prime p, asymptotically half the primes q satisfy $\left(\frac{p}{q}\right) = -1$. Using the number theorist's conceit,
$$\text{Prob}\left(\left(\tfrac{p}{q}\right) = -1\right) = \text{Prob}\left(\left(\tfrac{p}{q}\right) = 1\right) = \tfrac{1}{2}.$$
- The statement $n_2(q) = p_k$ is equivalent to
$$\left(\tfrac{p_1}{q}\right) = \left(\tfrac{p_2}{q}\right) = \cdots = \left(\tfrac{p_{k-1}}{q}\right) = 1 \text{ and } \left(\tfrac{p_k}{q}\right) = -1.$$
- These k events should be independent, so we should have $\text{Prob}(n_2(q) = p_k) = 2^{-k}$.
- So the expected value of $n_2(q)$ should be $\sum_{k=1}^{\infty} 2^{-k} p_k$.

Evaluating $\frac{1}{\pi(x)}\sum_{2<q\le x} n_2(q)$, in one slide

1. For $n_2(q)$ fixed, or small compared to x, this heuristic can be made rigorous using quadratic reciprocity and the prime number theorem for arithmetic progressions:
$$\frac{1}{\pi(x)} \sum_{\substack{2<q\le x \\ n_2(q) \text{ small}}} n_2(q) = \sum_{k=1}^{\infty} \frac{p_k}{2^k} + o(1).$$
2. For medium-sized $n_2(q)$, a similar approach using the Brun–Titchmarsh theorem gives a suitable upper bound.
3. For large $n_2(q)$, Burgess's bounds give
$$\frac{1}{\pi(x)} \sum_{\substack{2<q\le x \\ n_2(q) \text{ large}}} n_2(q) \ll \frac{1}{\pi(x)} x^{1/4\sqrt{e}+\varepsilon} \#\{2 < q \le x : n_2(q) \text{ large}\},$$
which can be shown to be $o(1)$ by the large sieve.

Considering all quadratic characters

Definition: least character nonresidue for real characters

For D a fundamental discriminant, $n_2(D)$ is the least number n such that $\left(\frac{D}{n}\right) = -1$. ($n_2(D)$ is still always a prime.)

Theorem (Pollack, 2012)

$$\lim_{x\to\infty} \left(\sum_{|D|\le x} 1\right)^{-1} \left(\sum_{|D|\le x} n_2(D)\right) = \sum_{\ell} \frac{\ell^2}{2(\ell+1)} \prod_{p<\ell} \frac{p+2}{2(p+1)},$$

where $\sum_\ell$ is over primes ℓ. The average value of the least character nonresidue for quadratic characters is ≈ 4.98085.

$$\frac{\ell^2}{2(\ell+1)} \prod_{p<\ell} \frac{p+2}{2(p+1)} = \ell \operatorname{Prob}\left(\left(\tfrac{D}{\ell}\right) = -1\right) \textstyle\prod_{p<\ell} \operatorname{Prob}\left(\left(\tfrac{D}{p}\right) \ne -1\right)$$

Considering all characters

Definition: least character nonresidue

For χ a Dirichlet character, n_χ is the least number n such that $\chi(n) \neq 1$ and $\chi(n) \neq 0$. (n_χ is still always a prime.)

Theorem (M.–Pollack, 2012+)

If we define

$$\Delta = \sum_{\ell} \frac{\ell^2}{\prod_{p \le \ell}(p+1)} \approx 2.53505,$$

where the sum and product are taken over primes ℓ and p, then

$$\lim_{x\to\infty} \left(\sum_{q\le x} \sum_{\chi \pmod q} 1 \right)^{-1} \left(\sum_{q\le x} \sum_{\chi \pmod q} n_\chi \right) = \Delta.$$

Most characters quit right away

Definition

$\ell(q)$ is the least prime *not* dividing q. Note that $n_\chi \geq \ell(q)$.

Proposition

$$0 \leq \sum_{\chi \pmod q} \bigl(n_\chi - \ell(q)\bigr) = \sum_{\chi \pmod q} n_\chi - \phi(q)\ell(q) \ll \phi(q)\frac{(\log\log q)^3}{\log q}$$

- The proof involves sorting the χ according to whether n_χ is equal to $\ell(q)$, is medium-sized, or is large.
- The structure of the group $(\mathbb{Z}/q\mathbb{Z})^\times$ comes into play, as does the multiplicative order of $\ell(q)$ modulo q.

A sum of a non-multiplicative function

$$\lim_{x\to\infty} \Bigg(\sum_{q\le x} \sum_{\chi \pmod q} 1 \Bigg)^{-1} \Bigg(\sum_{q\le x} \sum_{\chi \pmod q} n_\chi \Bigg) = \Delta = \sum_{\ell} \frac{\ell^2}{\prod_{p\le \ell}(p+1)}$$

The theorem now reduces to showing:

$$\lim_{x\to\infty} \Bigg(\sum_{q\le x} \phi(q) \Bigg)^{-1} \Bigg(\sum_{q\le x} \phi(q)\ell(q) \Bigg) = \Delta$$

- The function $\phi(q)\ell(q)$ is certainly not multiplicative.
- However, if we sort q according to $\gcd(q, Q)$ where $Q = \prod_{p\le z} p$, then both $\ell(q)$ and $\phi(q)/q$ are essentially determined as a function of $\gcd(q, Q)$.
- We sum over all divisors of Q and (after four pages or so) obtain Δ.

Considering only primitive characters

Theorem (M.–Pollack, 2012+)

If we define

$$\Delta^* = \sum_{\ell} \frac{\ell^4}{(\ell+1)^2(\ell-1)} \prod_{p<\ell} \frac{p^2-p-1}{(p+1)^2(p-1)} \approx 2.15144,$$

where the sum and product are taken over primes ℓ and p, then

$$\lim_{x\to\infty} \Bigg(\sum_{q\le x} \sum_{\substack{\chi \pmod q \\ \chi \text{ primitive}}} 1 \Bigg)^{-1} \Bigg(\sum_{q\le x} \sum_{\substack{\chi \pmod q \\ \chi \text{ primitive}}} n_\chi \Bigg) = \Delta^*.$$

I've been talking in prose all this time?

Theorem (Erdős, 1961)

$$\lim_{x\to\infty}\left(\frac{1}{\pi(x)}\sum_{2<q\le x} n_2(q)\right) = \sum_{k=1}^{\infty}\frac{p_k}{2^k}$$

Among quadratic number fields with prime conductor:

The average least inert prime is $\sum_{k=1}^{\infty}\frac{p_k}{2^k}$.

Theorem (Pollack, 2012)

$$\lim_{x\to\infty}\left(\sum_{|D|\le x} 1\right)^{-1}\left(\sum_{|D|\le x} n_2(D)\right) = \sum_{\ell}\frac{\ell^2}{2(\ell+1)}\prod_{p<\ell}\frac{p+2}{2(p+1)}$$

Among all quadratic number fields:

The average least inert prime is $\frac{\ell^2}{2(\ell+1)}\prod_{p<\ell}\frac{p+2}{2(p+1)}$.

Cubic number field result

Definition: least non-split prime

For K a number field, D_K is the discriminant of K, and n_K is the least rational prime that does not split completely in K.

Theorem (M.–Pollack, 2012+)

If we define

$$\Delta_{\text{non-split}} = \sum_{\ell} \frac{5\ell^3 + 6\ell^2 + 6\ell}{6(\ell^2+\ell+1)} \prod_{p<\ell} \frac{p^2}{6(p^2+p+1)} \approx 2.12110,$$

where the sum and product are taken over primes ℓ and p, then

$$\lim_{x\to\infty} \Bigg(\sum_{|D_K|\le x} 1 \Bigg)^{-1} \Bigg(\sum_{|D_K|\le x} n_K \Bigg) = \Delta_{\text{non-split}},$$

where the sums on the left-hand side are taken over (all isomorphism classes of) cubic fields K for which $|D_K| \le x$.

Evaluating the average of n_k, in one slide

- We need to count cubic fields K, sorted according to discriminant (Davenport–Heilbronn), but also sorted according to how several small rational primes factor into prime ideals in O_K.
- Work of Taniguchi–Thorne/Bhargava–Shankar–Tsimerman gives such estimates with uniformity; allows us to handle small n_K (whence the main term $\Delta_{\text{non-split}}$) and medium n_K.
- As before, for large n_K we need:
  - a uniform bound on n_K (uses the quadratic resolvent of K, and Burgess's bound applied to its quadratic character)
  - an estimate for the number of cubic fields K with n_K large (again uses large sieve; $D(K)$ is a square times the discriminant of K's quadratic resolvent; uses Ellenberg–Venkatesh to bound cubic fields with fixed $D(K)$)

Other factorization types

Assuming GRH for Dedekind zeta functions:

- The average least completely split prime in cubic fields is

$$\sum_{\ell} \ell \operatorname{Prob}(\ell \text{ splits completely}) \prod_{p<\ell} \operatorname{Prob}(p \text{ doesn't}) \approx 19.79522.$$

- The average least inert prime in cubic fields is

$$\sum_{\ell} \ell \operatorname{Prob}(\ell \text{ is inert}) \prod_{p<\ell} \operatorname{Prob}(p \text{ isn't}) \approx 8.54473.$$

- The average partially split prime in non-cyclic cubic fields is

$$\sum_{\ell} \ell \operatorname{Prob}(\ell \text{ is partially split}) \prod_{p<\ell} \operatorname{Prob}(p \text{ isn't}) \approx 5.36802.$$

Without GRH, we can still do a couple of other cases (for example, the least prime that is either partially split or ramified).

How many reductions of elliptic curves have N points?

Definition

For E an elliptic curve, $M_E(N)$ is the number of primes p for which $E(\mathbb{F}_p)$ has exactly N points.

Theorem (David–Smith, 2012)

Fix N, and let A and B be big enough in terms of N. The average value of $M_E(N)$, over elliptic curves $y^2 = x^3 + ax + b$ with $|a| \le A$ and $|b| \le B$, is asymptotic to $\frac{1}{\log N} K(N) \frac{N}{\phi(N)}$.

Provisos:

- conditional on primes in short intervals of arithmetic progressions (strong Barban–Davenport–Halberstam)
- only proved for N odd

Revealing the function $K(N)$

Definition

$$K(N) = \prod_{p \nmid N(N-1)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \mid (N-1)} \left(1 - \frac{1}{(p-1)^2(p+1)}\right)$$
$$\times \prod_{\substack{p^\alpha \| N \\ \alpha \text{ odd}}} \left(1 - \frac{1}{p^\alpha(p-1)}\right) \prod_{\substack{p^\alpha \| N \\ \alpha \text{ even}}} \left(1 - \frac{p - \left(\frac{-N/p^\alpha}{p}\right)}{p^{\alpha+1}(p-1)}\right),$$

where $\left(\frac{\cdot}{p}\right)$ is the Jacobi symbol.

Note: each factor is $1 + O(p^{-2})$, so $1 \ll K(N) \le 1$.

Question

What is the average value of $K(N)\frac{N}{\phi(N)}$?

What is the average value of $K(N)\frac{N}{\phi(N)}$?

The following values will be the average value of some function in this talk:

1. $\displaystyle \frac{2}{2}+\frac{3}{4}+\frac{5}{8}+\frac{7}{16}+\cdots=\sum_{k=1}^{\infty}\frac{p_k}{2^k}$ — average $n_2(q)$
2. $\displaystyle \sum_{\ell \text{ prime}} \ell^2 \prod_{\substack{p\le\ell \\ p \text{ prime}}} (p+1)^{-1}$ — average n_χ
3. $\displaystyle \sum_{\ell \text{ prime}} \frac{5\ell^3+6\ell^2+6\ell}{6(\ell^2+\ell+1)} \prod_{\substack{p<\ell \\ p \text{ prime}}} \frac{p^2}{6(p^2+p+1)}$ — average cubic n_K
4. $\displaystyle \frac{2}{3}\prod_{\substack{p>2 \\ p \text{ prime}}}\left(1-\frac{1}{(p-1)^2}\right)\left(1+\frac{1}{(p-2)(p-1)(p+1)}\right)$ — ?

What is the average value of $K(N)\frac{N}{\phi(N)}$?

The following values will be the average value of some function in this talk:

1. $\frac{2}{2}+\frac{3}{4}+\frac{5}{8}+\frac{7}{16}+\cdots=\sum_{k=1}^{\infty}\frac{p_k}{2^k}$ — average $n_2(q)$
2. $\sum_{\ell \text{ prime}} \ell^2 \prod_{\substack{p\le\ell \\ p \text{ prime}}} (p+1)^{-1}$ — average n_χ
3. $\sum_{\ell \text{ prime}} \frac{5\ell^3+6\ell^2+6\ell}{6(\ell^2+\ell+1)} \prod_{\substack{p<\ell \\ p \text{ prime}}} \frac{p^2}{6(p^2+p+1)}$ — average cubic n_K
4. $\frac{2}{3}\prod_{\substack{p>2 \\ p \text{ prime}}}\left(1-\frac{1}{(p-1)^2}\right)\left(1+\frac{1}{(p-2)(p-1)(p+1)}\right)$ — ?

One is the averagest number

Definition

$$K(N) = \prod_{p \nmid N(N-1)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \mid (N-1)} \left(1 - \frac{1}{(p-1)^2(p+1)}\right)$$
$$\times \prod_{\substack{p^\alpha \| N \\ \alpha \text{ odd}}} \left(1 - \frac{1}{p^\alpha(p-1)}\right) \prod_{\substack{p^\alpha \| N \\ \alpha \text{ even}}} \left(1 - \frac{p - \left(\frac{-N/p^\alpha}{p}\right)}{p^{\alpha+1}(p-1)}\right)$$

Theorem (M.–Pollack–Smith, 2012+)

$$\frac{1}{x} \sum_{N \le x} K(N) \frac{N}{\phi(N)} = 1 + O\left(\frac{1}{\log x}\right).$$

The answer has to be 1, since averaging the David–Smith result turns into essentially "the average number of primes per prime".

Reductions of elliptic curves that have prime order

Theorem (M.–Pollack–Smith, 2012+)

The average value of $K(q)\frac{q}{q-1}$ over primes q equals

$$\frac{2}{3}\prod_{\substack{p>2\\ p \text{ prime}}}\left(1-\frac{1}{(p-1)^2}\right)\left(1+\frac{1}{(p-2)(p-1)(p+1)}\right).$$

Koblitz conjecture

Given an elliptic curve E, there exists a constant $C(E)$ such that

$$\sum_{\substack{p\le x\\ p \text{ prime}}} M_E(p) \sim C(E)\frac{x}{(\log x)^2}.$$

Jones (2009) has shown the average value of $C(E)$ over elliptic curves E is consistent with our average value for $K(q)\frac{q}{q-1}$.

The end

These slides

www.math.ubc.ca/~gerg/index.shtml?slides

"The average least character nonresidue and further variations on a theme of Erdős", with Paul Pollack

www.math.ubc.ca/~gerg/index.shtml?abstract=ALCNFVTE

"Averages of the number of points on elliptic curves", with Paul Pollack and Ethan Smith (in preparation)

www.math.ubc.ca/~gerg/index.shtml?abstract=ANPEC