Analytic number theory in function fields: The distribution of squarefrees in short intervals

Konstantz, July 2015

Zeev Rudnick, TAU

European Research Council
Established by the European Commission

Plan

An integer n is **squarefree** if it is not divisible by d^2 for any $|d|>1$

Solve over $\mathbf{F}_q[t]$ a number of open problems in analytic number theory concerning squarefree integers, in the limit $q\to\infty$

- The asymptotic number of squarefrees in short intervals
- variance of the number of squarefrees in short intervals

The density of square-free integers

The density of squarefrees is $1/\zeta(2)=6/\pi^2$

$$Q(x) := \#\{n \le x : n \quad \text{square-free}\} = \frac{x}{\zeta(2)} + O(x^{1/2})$$

Remainder term is conjectured to be $O(x^{1/4+o(1)})$.

Assuming the Riemann Hypothesis, exponent improved from 1/2 :

- Axer (1911): 2/5 ….. Jia (1993): 17/54= 0.314815

The indicator function of squarefrees

Mobius function $$\mu(n)=\begin{cases}(-1)^k, & n=p_1\cdot\ldots\cdot p_k \quad \text{squarefree}\\ 0, & \text{otherwise}\end{cases}$$

$\Rightarrow$ $$\mu(n)^2=\begin{cases}1, & n \quad \text{squarefree}\\ 0, & \text{otherwise}\end{cases}$$

Mobius inversion formula $$\sum_{d\mid n}\mu(d)=\begin{cases}1, & n=1\\ 0, & n>1\end{cases}$$

Lemma: $$\mu^2(n)=\sum_{d^2\mid n}\mu(d)$$

Proof: 1) Every integer can be uniquely written as n=sm^2, with s squarefree

2) $d^2\mid n \quad \Leftrightarrow \quad d\mid m \quad \Rightarrow \quad \sum_{d^2\mid n}\mu(d)=\sum_{d\mid m}\mu(d)=\begin{cases}1, & m=1\Leftrightarrow n=s \text{ squarefree}\\ 0, & \text{otherwise}\end{cases}$

Proof of $Q(x) = \frac{x}{\zeta(2)} + o(\sqrt{x})$

$$Q(x) = \sum_{n \le x} \mu^2(n) = \sum_{n \le x} \sum_{d^2 | n} \mu(d) = \sum_{d \le \sqrt{x}} \mu(d) \sum_{\substack{n \le x \\ d^2 | n}} 1$$

Counting the number of multiples in an interval:

$$\sum_{\substack{n \le x \\ D | n}} 1 = \lfloor \frac{x}{D} \rfloor = \frac{x}{D} + O(1)$$

$$Q(x) = \sum_{d \le \sqrt{x}} \mu(d) \Big(\frac{x}{d^2} + O(1) \Big) = x \sum_{d \le \sqrt{x}} \frac{\mu(d)}{d^2} + O\Big(\sum_{d \le \sqrt{x}} |\mu(d)| \Big)$$

$$= x \cdot \Big(\frac{1}{\zeta(2)} + O\big(\frac{1}{\sqrt{x}}\big) \Big) + O(\sqrt{x}) = \frac{x}{\zeta(2)} + O(\sqrt{x})$$

QED

Squarefree polynomials

An polynomial is **squarefree** if it is not divisible by d^2 for any polynomial d, deg(d)>0.

The number of squarefree polynomials of degree n: If n>1 then

$$Q(n) := \#\{f \in \mathbb{F}_q[t] \text{ monic}, \deg f = n, \text{squarefree}\} = \frac{q^n}{\zeta_q(2)}$$

$$\zeta_q(s) := \sum_{f \text{ monic}} \frac{1}{||f||^s}$$

Norm: $||f|| := \#\mathbf{F}_q[t]/(f) = q^{\deg(f)}$

- no remainder term !

$$\#\{f \in \mathbb{F}_q[t] \text{ monic}, \deg f = n\} = q^n$$

The zeta function for $F_q[x]$

Riemann ζ- function $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\left(1-p^{-s}\right)^{-1}$

$$\zeta_q(s):=\sum_{f\text{ monic}}\frac{1}{\|f\|^s}=\prod_{P\text{ monic irreducible}}\left(1-\|P\|^{-s}\right)^{-1}$$

Norm of a polynomial: $\|f\|:=\mathbf{F}_q[x]/(f)=q^{\deg(f)}$

Here zeta is very simple:

(no zeros!)

$$\boxed{\zeta_q(s)=\frac{1}{1-q^{1-s}}}$$

Proof of $Q(n) = q^n/\zeta(2)$

Use generating function of squarefrees

$$\sum_{n=0}^{\infty} \frac{Q(n)}{q^{ns}} = \sum_{n=0}^{\infty} \frac{1}{q^{ns}} \sum_{\deg f = n} \mu^2(f) = \sum_{\substack{f \\ \text{monic}}} \frac{\mu^2(f)}{|f|^s} =$$

$$= \frac{\zeta_q(s)}{\zeta_q(2s)} = \frac{1-q^{1-2s}}{1-q^{1-s}} = 1 - q \bullet q^{-s} + \sum_{n \geq 2} (q^n - q^{n-1}) q^{-ns}$$

$$\Rightarrow \quad Q(n) = q^n - q^{n-1} = q^n(1-q^{-1}) = \frac{q^n}{\zeta_q(2)}$$

for n≥2

Squarefrees in short intervals

$$Q(x;H) = Q(x+H) - Q(x) = \#\{\, x < n \le x+H,\, n \text{ square-free} \,\}$$

Want: for $1 \ll H \ll X$

$$Q(x;H) \sim \frac{H}{\zeta(2)}$$

OK for H > $x^{1/2}$ because of $Q(x) - x/\zeta(2) = o(x^{1/2})$

Roth (1951): OK for H > $x^{1/3}$

improvements: Roth (1951) 3/13, Richert (1954) 2/9, Tolev (2006) 1/5

Conjecture: $Q(x;H) \sim H/\zeta(2)$ for any $H \gg x^{\varepsilon}$

Moreover the fluctuations are of order $H^{1/4}$

Entin 2014: OK assuming the ABC conjecture

Erdos: False for $H \approx \log x / \log\log x$

Variance – Hall's theorem

$$\mathrm{Var}Q(\bullet;H) := \frac{1}{N}\sum_{n<N}\left|Q(n;H) - \frac{H}{\zeta(2)}\right|^2$$

R. Hall (1982): If $H \ll N^{2/9}$, $H\to\infty$ with N (very short intervals) then

$$\mathrm{Var}\,Q \sim A_{\mathrm{Hall}}\sqrt{H} \qquad A_{\mathrm{Hall}} = \frac{\zeta(3/2)}{\pi}\prod_p\left(1-\frac{3}{p^2}+\frac{2}{p^3}\right)$$

Corollary: In this case, **almost all** short intervals (n,n+H] contain ~H/ζ(2) squarefrees.

moreover the fluctuations are typically of order $H^{1/4}$.

Unknown: Behaviour of the variance Var(Q) for **longer** intervals.

Ideas for Hall’s theorem

1. The autocorrelation function of squarefrees (Carlitz 1932, Mirsky 1949): uniformly in J<x,

$$\sum_{n\le x}\mu^2(n)\mu^2(n+J)=\mathfrak{S}(J)x+O(x^{2/3})$$

$$\mathfrak{S}(J):=\prod_p\left(1-\frac{\nu(J;p^2)}{p^2}\right),\qquad \nu(J;p^2)=\begin{cases}1, & J=0 \mod p^2\\ 2, & J\neq 0 \mod p^2\end{cases}$$

2. A subtle cancelation in sums of the “singular series”

$$\sum_{I=1}^{H}\sum_{J=1}^{H}\mathfrak{S}(I-J)=\left(\frac{H}{\zeta(2)}\right)^2+A_{\text{Hall}}\sqrt{H}+O(H^{1/3})$$

$$A_{\text{Hall}}=\frac{\zeta(3/2)}{\pi}\prod_p\left(1-\frac{3}{p^2}+\frac{2}{p^3}\right)$$

Squarefree polynomials in short intervals

Norm of a polynomial: $\| f \| := \#\mathbf{F}_q[t]/(f) = q^{\deg(f)}$

A short interval around f_0: $I(f_0;h) := \{f : \| f - f_0 \| \le q^h\} = \{f : \deg(f - f_0) \le h\}$

e.g. $f_0 = t^n, h = 2: \quad \| f - t^n \| \le q^2 \Leftrightarrow f = t^n + a_2 t^2 + a_1 t + a_0$

If deg f_0 >h then $H := \#\{f : \|f - f_0\| \le q^h\} = q^{h+1}$ ↔ "length" of interval

Squarefrees in short intervals:

For a polynomial A of degree n, we count the number of squarefree polynomials in an "interval" about A:

$$Q(A;h) := \#\{ f \text{ squarefree}, \| f - A \| \le q^h \}$$

Goals: In the limit $q \to \infty$,

1. Asymptotic of Q(A;h)
2. Variance

Asymptotics of squarefrees in short intervals

$$Q(A;h) := \#\{f \text{ squarefree}, \|f - A\| \le q^h\}$$

Thm (ZR 2012): Fix 0<h<n. Then for any A with deg(A)=n, as $q\to\infty$,

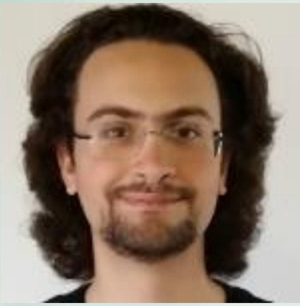
$$Q(A;h) = H + O_n\left(\frac{H}{q}\right) \sim \frac{H}{\zeta_q(2)}$$

- analogous to $x^\varepsilon < H < x$

Dan Carmon (June 2015): Can do the $n\to\infty$ limit, for intervals I(A,h) of "length"

$$H = q^{h+1} > |A|^\varepsilon = q^{n\varepsilon}, \ \forall \varepsilon > 0$$

$$Q(A;h) \sim \frac{H}{\zeta_q(2)}$$



Method

- $f \in I(A;h) \Leftrightarrow f = A + a$ with deg(a)≤h
- Want to know the proportion of substitutions a, deg(a)=m, with F(a):=A+a squarefree
- **<u>THM (ZR, 2014)</u>**: $F(X) \in \mathbb{F}_q[t][X]$ separable, with squarefree content, then as q→∞

$$\frac{1}{q^n}\#\{a \text{ monic}, \deg a = n, F(a) \text{ squarefree}\} = 1 + O_{n,Ht(F)}\left(\frac{1}{q}\right)$$

i.e. almost all substitutions give square-free values

Example: $F(X) = A(t) + cX$

Variance

$$\mathrm{Var}(Q) := \frac{1}{q^n} \sum_{degA=n} |Q(A;h) - H|^2$$

Theorem (J. Keating & ZR, 2014): Fix n, h<n-5. As q→∞ with gcd(q,6)=1,

$$\mathrm{Var}\, Q \sim \begin{cases} q^{h/2} \int_{U(n-h-2)} \left|\mathrm{trace}(\mathrm{Sym}^{h/2+1} U)\right|^2 dU, & h \text{ even} \\ q^{(h-1)/2} \int_{U(n-h-2)} \left|\mathrm{trace} V\right|^2 dV \int_{U(n-h-2)} \left|\mathrm{trace}\mathrm{Sym}^{(h+3)/2} U\right|^2 dU, & h \text{ odd} \end{cases}$$

$$= \begin{cases} \dfrac{\sqrt{H}}{\sqrt{q}}, & h \text{ even} \\ \dfrac{\sqrt{H}}{q}, & h \text{ odd} \end{cases}$$

no restriction on length of interval ;
for the integers we need $H<X^{2/9}$ (short)

comparison

Hall (1982): For $H<N^{2/9}$ $\operatorname{Var} Q \sim A_{\text{Hall}} \sqrt{H}$

Keating & ZR (2014): For $\mathbf{F}_q[t]$, in **limit $q \to \infty$** , $\operatorname{Var} Q \sim \begin{cases} \frac{\sqrt{H}}{\sqrt{q}} \\ \frac{\sqrt{H}}{q} \end{cases}$

– so smaller than over **Z** !!!

- no restriction on length of interval

Method: i) reduce to zeros of L-functions
ii) equidistribution + independence of Frobenius matrices (N. Katz 2014)

Dirichlet characters & L-functions for $F_q[t]$

Let $Q(t) \varepsilon\ \mathbf{F}_q[t]$ be a polynomial of positive degree.
A Dirichlet character modulo Q is a function $\chi : \mathbf{F}_q[t] \to \mathbf{C}^\times$ satisfying

- $\chi(AB)= \chi(A)\, \chi(B)$
- $\chi(A+CQ) = \chi(A)$
- $\chi(1)=1$

- χ is <u>**"even"**</u> if it is trivial on scalars $\mathbf{F}_q$: $\chi(cf) = \chi(f),\ \forall c \in \mathbf{F}_q^*$

The L-function associated to χ :
for Re(s)>1

$$L(s,\chi) := \sum_{f \text{ monic}} \frac{\chi(f)}{\| f \|^s} = \prod_{P \text{ prime}} \left(1 - \frac{\chi(P)}{\| P \|^s}\right)^{-1}$$

Norm of a polynomial: $||f||:=\#\mathbf{F}_q[x]/(f)=q^{\deg(f)}$

(analogy: for $0 \neq n \varepsilon \mathbf{Z}$, $|n|=\#\mathbf{Z}/n\mathbf{Z}$)

L(s, χ) and the Frobenius class

If χ is nontrivial ("primitive") then

$$L(s,\chi) := \sum_{f \text{ monic}} \frac{\chi(f)}{\| f \|^s} = \prod_{P \text{ prime}} \left(1 - \frac{\chi(P)}{\| P \|^s}\right)^{-1}$$

- L(s, χ) is a polynomial in $u{:=}q^{-s}$ of degree deg(Q)-1
- functional equation L(s, χ) ↔ L(1-s, χ^{-1})
- RH (Weil, 1940's): All non-trivial zeros lie on Re(s)=1/2
- If χ is "even" then there is a trivial zero at s=0

the Frobenius conjugacy class:

If χ is even and primitive mod Q, then can write

$$\Theta(\chi) \approx \begin{pmatrix} e^{i\theta_1} & & & & \\ & e^{i\theta_2} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & e^{i\theta_N} \end{pmatrix}$$

$$L(s,\chi) = (1-u)\det(I - uq^{1/2}\Theta(\chi)), \qquad u := q^{-s}$$

Θ(χ) = unitary mxm matrix, m=deg Q-2, called the **"unitarized Frobenius matrix"**

Definition of equidistribution

Let G be a compact metric space, with associated volume measure dm.

A sequence of subsets $\{X_n\}$ of G becomes **equidistributed** in G if for any nice subset $A \subset G$,

$$\lim_{n\to\infty} \frac{1}{\# X_n} \#\{X_n \cap A\} = \frac{m(A)}{m(G)}$$

Equivalently for any continuous function F on G,

$$\lim_{n\to\infty} \frac{1}{\# X_n} \sum_{x \in X_n} F(x) = \frac{1}{\mathrm{vol}(G)} \int_G F(x)\, dm(x)$$

For us,

- G=set of conjugacy classes in projective) unitary group PU(N-2),
- the sets X_N are the Frobenii $\Theta(\chi)$, χ all even primitive characters mod t^N

Equidistribution & independence of Frobenii

$$L(s,\chi) = (1-q^{-s})\det(I - q^{\frac{1}{2}-s}\Theta(\chi))$$

i) **<u>N. Katz, (2012)</u>** As χ varies over all "even" primitive characters mod t^N, the Frobeniius classes $\Theta(\chi)$ become **<u>equidistributed</u>** in the projective unitary group PU(N-2) as $q\to\infty$. (N>4)

i.e. for any nice function F on $PU(N-2)^{\#}$,

$$\lim_{q\to\infty} \frac{1}{\#\{\chi\}} \sum_{\substack{\chi \bmod t^N \\ \text{even primitive}}} F(\Theta(\chi)) = \int_{PU(N-2)} F(U)\,dU$$

ii) **<u>N. Katz (2014</u>**): the pairs $(\Theta(\chi),\Theta(\chi^2))$ are equidistributed in PU(N-2) x PU(N-2)

(N>5, gcd(q,6)=1) - **<u>independence</u>** of $\Theta(\chi)$ and $\Theta(\chi^2)$

i.e. for any nice function F on $PU(N-2)^{\#}$ x $PU(N-2)^{\#}$,

$$\lim_{q\to\infty} \frac{1}{\#\{\chi\}} \sum_{\substack{\chi \bmod t^N \\ \text{even primitive}}} F(\Theta(\chi),\Theta(\chi^2)) = \iint_{PU(N-2)\, x\, PU(N-2)} F(U,U')\,dU\,dU'$$

Var Q in terms of zeros of L-functions

Expression for Var(Q) via zeros of Dirichlet L-functions mod t^{n-h}

as $q \to \infty$

$$\mathrm{Var}\, Q \sim \sqrt{H} \times \frac{1}{\#\{\chi\}} \sum_{\substack{\chi \bmod t^{n-h} \\ \text{even primitive}}} F(\chi)$$

$$F(\chi) = \begin{cases} \dfrac{1}{\sqrt{q}} \left| \mathrm{traceSym}^{(h+2)/2} \Theta\left(\chi^2\right) \right|^2, & h \text{ even} \\ \dfrac{1}{q} \left| \mathrm{trace}(\Theta(\chi)) \times \mathrm{traceSym}^{(h+3)/2} \Theta\left(\chi^2\right) \right|^2, & h \text{ odd} \end{cases}$$

Using equidistribution

Equidistribution $\Rightarrow$

$$\lim_{q\to\infty}\frac{1}{\#\{\chi\}}\sum_{\substack{\chi \bmod t^{n-h}\\ \text{even primitive}}} |\operatorname{trace}\mathrm{Sym}^n\Theta(\chi^2)|^2 = \int_{U(n-h-2)} \left|\operatorname{trace}\mathrm{Sym}^n U\right|^2 dU = 1$$

Equidistribution + independence $\Rightarrow$

$$\lim_{q\to\infty}\frac{1}{\#\{\chi\}}\sum_{\substack{\chi \bmod t^{n-h}\\ \text{even primitive}}} |\operatorname{trace}\Theta(\chi)|^2 \times |\operatorname{trace}\mathrm{Sym}^n\Theta(\chi^2)|^2$$

$$= \int_{U(n-h-2)} \left|\operatorname{trace} U\right|^2 dU \times \int_{U(n-h-2)} \left|\operatorname{trace}\mathrm{Sym}^n U\right|^2 dU = 1\times 1 = 1$$

$\Rightarrow$

$$Var\,Q \sim \begin{cases} \dfrac{\sqrt{H}}{\sqrt{q}}, & h \text{ even} \\[2ex] \dfrac{\sqrt{H}}{q}, & h \text{ odd} \end{cases}$$

Summary

Solved a number of problems in $\mathbf{F}_q[t]$, in the limit $q \to \infty$, which are open for Z:

- Squarefrees in short intervals
- variance of the number of squarefrees in short intervals

These and other problems give insight as to what should be true over the integers.

Thank you !