How many smooth numbers and smooth polynomials are there?
ViBrANT Seminar, May 2, 2023

Ofir Gorodetsky

1 Definition and motivation

A positive integer n is said to be y-smooth if its primes factors do not exceed y: $p \mid n \implies p \le y$. The talk will be concerned with the counting function

$$\Psi(x,y) := \#\{n \le x : n \text{ is } y\text{-smooth}\}.$$

Note $\Psi(x,x) = \lfloor x \rfloor$, $\Psi(x,1) = 1$ and $\Psi(x,2) = 1 + \lfloor \log_2 x \rfloor$, and that the indicator function of y-smooth numbers is completely multiplicative.

One can define an analogous quantity in the polynomial setting. A polynomial $f \in \mathbb{F}_q[T]$ is said to be m-smooth if its irreducible factors have degrees bounded by m: $P \mid f \implies \deg(P) \le m$. The talk will be focused today mostly on $\Psi(x,y)$.

Smooth numbers play an important role in cryptography. Pomerance, in the 80s, devised his Quadratic Sieve, an algorithm that (heuristically) factors integers in subexponential time, namely n is factored in $\exp((\log n)^{1/2+o(1)})$ time. We describe it (in a loose way) below.

For $i = 1, 2, \ldots$ we do the following. We take $x_i := \lfloor \sqrt{n} \rfloor + i$, square it and reduce it modulo n to obtain a number y_i in $[0, n-1]$:

$$x_i^2 \equiv y_i \bmod n.$$

We then check whether y_i is T-smooth – this can be done in $O(T)$ operations obviously, but happens quite rarely: with probability $(\Psi(N,T)/N)^{-1}$ the number y_i will be T-smooth (heuristically). When it is T-smooth, we obtain a relation of the form

$$x_i^2 \equiv \prod_{p \le T} p^{e_{i,p}} \bmod n.$$

We want to obtain T such relations, which takes $T^2 \times (\Psi(N,T)/N)^{-1}$ operations. Then we can perform Gaussian elimination on the T **binary** vectors $\{(e_{i,p2} \bmod 2)_{p \le T}\}_{i \in S}$ where S corresponds to y_i that are T-smooth. The complexity of Gaussian elimination is T^3. It finds subset(s) $S' \subseteq S$ such that

$$\sum_{i \in S'} (e_{i,p})_{p \le T} \equiv 0 \bmod 2$$

as vectors in $\prod_{p \le T} \mathbb{F}_2$. This means

$$\prod_{i \in S'} x_i^2 \equiv \prod_{p \le T} p^{2b_p} \bmod n$$

for $b_p = \sum_{i \in S'} e_{i,p}/2$. Given a relation $A^2 \equiv B^2 \bmod n$ we can compute $\gcd(A-B, n)$ and hope to find one the factors of n.

The complexity of this algorithm is $T^2 \times (\Psi(N,T)/N)^{-1} + T^3$, and is minimized when

$$T \approx N/\Psi(N,T)$$

which turn out to be solved for

$$T = \exp((\log N)^{1/2+o(1)})$$

which is also the total complexity.

This uses the relation $\Psi(N,T) \sim N\rho(\log N/\log T)$ which was established in a wide range by Hildebrand, where ρ is the Dickman function, which we discuss next.

2 The Dickman function

The function $\rho\colon [0,\infty) \to (0,\infty)$ was introduced by Dickman. It has initial conditions $\rho(u) = 1$ for $u \in [0,1]$. For larger u it is defined via delay-differential equation:

$$u\rho'(u) + \rho(u-1) = 0, \text{ or}$$
$$\rho(u) = u^{-1}\int_0^1 \rho(u-t)dt.$$

It is decreasing, and in fact we see it decreases rapidly:

$$\rho(u) \le u^{-1}\rho(u-1) \implies \rho(u) \le \Gamma(u+1)^{-1} = u^{-u(1+o(1))}.$$

Dickman proved (30s) that $\Psi(x,y) \sim x\rho(\log x/\log y)$ for $x \ge y \ge x^{\varepsilon}$.

De Bruijn (50s) worked out precise asymptotics for $\rho(u)$. To explain them we need to introduce the Laplace transform of ρ:

$$\hat{\rho}(s) := \int_0^\infty e^{-st}\rho(t)dt.$$

De Bruijn showed

$$\hat{\rho}(s) = \exp\left(\gamma + \int_0^{-s} \frac{e^t - 1}{t}dt\right).$$

A short proof of this follows from differentiating $\hat{\rho}(s)$ under the integral sign:

$$\hat{\rho}'(s) = -\int_0^\infty te^{-st}\rho(t)dt = -\int_0^1 te^{-st}dt - \int_1^\infty (\int_{t-1}^t \rho(v)dv)e^{-st}dt$$
$$= -\int_0^\infty \rho(v)(\int_v^{v+1} e^{-st}dt)dv = \frac{e^{-s}-1}{s}\hat{\rho}(s).$$

(This determines $\hat{\rho}$ up to a multiplicative constant; see de Bruijn's work for working out the constant.) For any $c \in \mathbb{R}$ we have

$$\rho(u) = \frac{1}{2\pi i}\int_{(-c)} e^{su}\hat{\rho}(s)ds.$$

We choose c so that $e^{-cu}\hat{\rho}(-c)$ is minimized, i.e. c is the minimizer of

$$c \mapsto -cu + \gamma + \int_0^c \frac{e^t-1}{t}dt.$$

Differentiating (with respect to c) we find

$$-u + \frac{e^c - 1}{c} = 0$$

So the optimal c is $\xi(u)$ (a function of u) where $\xi(u) \sim \log u$ is defined implicitly via

$$\frac{e^{\xi}-1}{\xi} = u.$$

Let us write

$$\rho(u) = \frac{1}{2\pi i}\int_{(-\xi(u))} e^{su}\hat{\rho}(s)ds = e^{-\xi(u)u}\hat{\rho}(-\xi(u))\frac{1}{2\pi}\int_{\mathbb{R}} G(t)dt$$

for

$$G(t) = e^{itu}\hat{\rho}(-\xi(u)+it)/\hat{\rho}(-\xi(u)).$$

By construction $G(0) = 1$. By definition of ξ, $G'(0) = 0$. It is not hard to approximate $G(t)$ as $e^{-ut^2(1+o(1))/2}$ for small t (details omitted; $u(1+o(1))$ arises from $(\log G)''(0)$). We expect

$$\rho(u) = \frac{1}{2\pi i}\int_{(-\xi(u))} e^{su}\hat{\rho}(s)ds \sim e^{-\xi(u)u}\hat{\rho}(-\xi(u))\frac{1}{2\pi}\int_{\mathbb{R}} e^{-ut^2/2}dt \sim \frac{e^{-\xi(u)u}\hat{\rho}(-\xi(u))}{\sqrt{2\pi u}}$$

and this asymptotic relation was established rigorously by de Bruijn. The quantity $-\xi(u)$ is called the *saddle point* for $\rho(u)$.

3 Hildebrand's work

Let

$$u = \frac{\log x}{\log y}.$$

Hildebrand (80s) proved the following:

$$\Psi(x,y) = x\rho(u)\left(1 + O\left(\frac{\log(u+1)}{\log y}\right)\right)$$

holds for $x \geq y \geq \exp((\log\log x)^{5/3+\varepsilon})$. Under RH he showed that

$$\Psi(x,y) = x\rho(u)\exp\left(O\left(\frac{\log(u+1)}{\log y}\right)\right) \tag{3.1}$$

holds for $y \geq (\log x)^{2+\varepsilon}$. Note this does not give an asymptotic formula for $y = (\log x)^C$.

These two results admit alternative proofs due to Saias (80s). Hildebrand used a physical space argument while Saias used Dirichlet series and complex analysis.

Two questions that were asked:

1. (Hildebrand) Can one show the asymptotic relation (3.1) fails for $y \leq (\log x)^{2-\varepsilon}$?
2. (Pomerance) Is it true that $\Psi(x,y) \geq x\rho(u)$ for all $x/2 \geq y \geq 2$? (Intuition: for very large y, there is a lower order term in $\Psi(x,y) - x\rho(u)$, found by de Bruijn, which is positive. Moreover, $x\rho(u) \leq \Psi(x,y)$ for $y \leq \log x$ trivially since $\Psi(x,y) \geq 1$, $x\rho(u) < 1$.)

Theorem 3.1 (G., 2022)**.** *Fix $\varepsilon > 0$. Unconditionally, there are sequences $x_n, y_n \to \infty$ such that*

$$y_n = (\log x_n)^{2-\varepsilon+o(1)}$$

and

$$\frac{\Psi(x_n,y_n)}{x_n\rho(\log x_n/\log y_n)} = \exp((\log x_n)^{\varepsilon+o(1)}).$$

Theorem 3.2 (G., 2022)**.** *Under RH, for $(\log x)^{1+\varepsilon} \leq y \leq (\log x)^{2-\varepsilon}$ we have*

$$\frac{\Psi(x,y)}{x\rho(\log x/\log y)} = \exp\left(\Theta\left(\frac{(\log x)^2}{y\log y}\right)\right).$$

An analogue of Theorem 3.2 holds unconditionally for polynomials. Here $\Theta(f)$ stands for a function g such that $C \geq g/f \geq c > 0$ for some positive constants C, c.

Theorem 3.3 (G., 2022)**.** *1. Unconditionally, $\Psi(x,y) \geq x\rho(u)$ holds outside of*

$$y \in [\log x \exp((\log\log x)^{3/5-\varepsilon}), \exp((\log\log x)^{5/3+\varepsilon})].$$

2. Under RH, $\Psi(x,y) \geq x\rho(u)$ holds outside of

$$y \in [(\log x)^{2-\varepsilon}, (\log x)^{2+\varepsilon}].$$

3. Assume RH. If $\psi(y) := \sum_{n\leq y}\Lambda(n) \sim y$ satisfies $\psi(y) - y = o(\sqrt{y}\log y)$ then $\Psi(x,y) \geq x\rho(u)$ holds for $y \in [(\log x)^{2-\varepsilon}, (\log x)^{2+\varepsilon}]$. Some intuition comes from the relation

$$\Psi(x,y) \sim x\rho(u)(-\zeta(1/2)\sqrt{2})\exp\left(\frac{\psi(y)-y}{\sqrt{y}\log y}\right)$$

for $y = (1 + (\log x)/2)^2$ (RH is used in the derivation of this relation as well).

4. If RH fails, and $\Theta > 1/2$ is the supremum of the real parts of zeros of ζ, then for any $\beta \in (1-\Theta, \Theta)$ there are sequences x_n, y_n with $y_n = (\log x_n)^{1/(1-\beta)+o(1)}$ such that

$$\Psi(x_n,y_n) < x_n\rho(\log x_n/\log y_n)\exp(-y_n^{\Theta-\beta-\varepsilon}).$$

4 First oscillation result

The rest of the talk will concentrate on Theorem 3.1 and the last part of Theorem 3.3.

Let us start with the last part of Theorem 3.3.[1] Rankin (30s) observed that

$$\Psi(x,y) \le x^c \zeta(c,y)$$

for any $c > 0$, where $\zeta(c,y) = \prod_{p\le y}(1-p^{-c})^{-1}$ is the partial zeta function. The optimal c, that minimizes the RHS, is denoted $\alpha = \alpha(x,y)$:

$$\Psi(x,y) \le x^\alpha \zeta(\alpha,y) = \min_{c>0} x^c \zeta(c,y).$$

Recall also that

$$\rho(u) \sim \frac{e^{-\xi(u)u}\hat{\rho}(-\xi(u))}{\sqrt{2\pi u}}.$$

Our aim is to 'marry' two classical ideas: saddle point analysis and Landau's Oscillation result (the same result that allows one to deduce $\psi(y) - y = \Omega_\pm(y^{\Theta-\varepsilon})$).

We introduce

$$\beta = \beta(x,y) := 1 - \xi(u)/\log y$$

where $u = \log x/\log y$, which allows us to rewrite

$$x\rho(u) \sim \frac{x^\beta \hat{\rho}(\log y(\beta-1))}{\sqrt{2\pi u}}.$$

Now let's divide $\Psi(x,y)$ by $x\rho(u)$:

$$\frac{\Psi(x,y)}{x\rho(u)} \ll \sqrt{u}\frac{x^\alpha \zeta(\alpha,y)}{x^\beta \hat{\rho}(\log y(\beta-1))}.$$

Here is a trivial (but new) observation. Since α minimizes the numerator we trivially have

$$\frac{\Psi(x,y)}{x\rho(u)} \ll \sqrt{u}\frac{x^\beta \zeta(\beta,y)}{x^\beta \hat{\rho}(-\xi(u))} = \sqrt{u}\frac{\zeta(\beta,y)}{\hat{\rho}(-\xi(u))}.$$

Letting

$$F(s,y) := \log\zeta(s,y) - \log\hat{\rho}(\log y(s-1)),$$

we see

$$\frac{\Psi(x,y)}{x\rho(u)} \ll \sqrt{u}e^{F(\beta,y)}.$$

By an earlier computation,

$$\log\hat{\rho}(\log y(s-1)) = \gamma + I((1-s)\log y).$$

As for $\log\zeta(s,y)$, we find

$$\log\zeta(s,y) = \sum_{p\le y} -\log(1-p^{-s}) = \sum_{n\le y}\frac{\Lambda(n)}{n^s\log n} + o(1)$$

if $s \ge 1/2+\varepsilon$. The $o(1)$ terms come from proper prime powers. Since $\beta = 1 - \xi(u)/\log y \approx 1 - \log u/\log y$, we certainly have $s \ge 1/2+\varepsilon$ if $y \ge (\log x)^{2+\varepsilon}$.

In summary: we want to show

$$\sum_{n\le y}\frac{\Lambda(n)}{n^\beta\log n} - I((1-\beta)\log y)$$

[1] For simplicity we shall assume $\sigma \in (1/2,\Theta)$ (instead of $\sigma \in (1-\Theta,\Theta)$), and concentrate on $y \ge (\log x)^{2+\varepsilon}$.

can be 'very' negative if RH fails. Strategy: we fix $\beta \in (1/2, 1)$, namely require $1 - \xi(u)/\log y = \beta$, which is easy to solve:

$$\xi(u) = \log y(1-\beta) \implies$$
$$e^{\xi(u)} = 1 + u\xi(u) = y^{1-\beta}$$

and

$$1 + u\xi(u) = 1 + u \log y(1-\beta)$$

so

$$1 + \log x(1-\beta) = y^{1-\beta}$$

i.e.

$$y = (1 + \log(1-\beta))^{1/(1-\beta)}.$$

Given a function $A(x)$ on $x \geq 1$, its Mellin transform is

$$\mathcal{M}A(s) := \int_1^\infty A(x) x^{-s} ds.$$

Landau proved the following.

Theorem 4.1. *Suppose $A(x)$ is a bounded integrable function on every interval $[1, X]$, which is eventually non-negative. Let σ_c be the infimum of σ such that $\mathcal{M}A(\sigma)$ converges. Then $\mathcal{M}A(s)$ is analytic in $\Re(s) > \sigma_c$ but not at $s = \sigma_c$.*

To illustrate, let us revisit the proof that $\psi(x) - x < -x^{\Theta-\varepsilon}$ holds infinitely often, where Θ is as before. Consider $A(x) = \sum_{n \leq x} \Lambda(n) - x + x^{\Theta-\varepsilon}$. Let us suppose $A(x)$ is eventually positive. Not hard to show

$$\mathcal{M}A(s) = -\frac{\zeta'(s-1)}{(s-1)\zeta(s-1)} - \frac{1}{s-2} + \frac{1}{s-1-\Theta+\varepsilon}.$$

This function is analytic for real $s > 1 + \Theta - \varepsilon$, but is not analytic at $s = 1 + \Theta - \varepsilon$. Hence, by Landau, $\mathcal{M}A(s)$ is analytic in the half-plane $\Re(s) > 1 + \Theta - \varepsilon$. But this is false – it is only analytic in $\Re(s) > 1 + \Theta$ due to zeros with real part $> \Theta - \varepsilon$ for any $\varepsilon > 0$; contradiction.

Another example: Diamond and Pintz (2009) showed

$$\sum_{n \leq x} \frac{\Lambda(n)}{n \log n} - \log \log x - \gamma < -\frac{C}{\sqrt{x} \log x}$$

holds infinitely often for any given $C > 0$, and same with $> C/(\sqrt{x} \log x)$. This shows that $\sqrt{x}(\prod_{p \leq x}(1 - 1/p)^{-1} - e^\gamma \log x)$ exhibits arbitrarily large positive and negative values as $x \to \infty$. They studied the Mellin transform of the LHS.

An almost identical argument works for showing

$$y \mapsto \sum_{n \leq y} \frac{\Lambda(n)}{n^\beta \log n} - I((1-\beta)\log y) \leq -y^{\Theta-\beta-\varepsilon}$$

holds infinitely often.

We conclude that if RH fails, and $\Theta > 1/2$ is the supremum of the real parts of zeros of ζ, then for any $\beta \in (1/2, \Theta)$ there are sequences x_n, y_n with $y_n = (\log x_n)^{1/(1-\beta)+o(1)}$ such that

$$\Psi(x_n, y_n) < x_n \rho(\log x_n / \log y_n) \exp(-y_n^{\Theta-\beta-\varepsilon}).$$

If RH holds, $\Theta - \beta = 1/2 - \beta < 0$ so this is useless.

Remark 4.1. *Under RH we can show that $\Psi(x, y) \sim x\rho(u)F(\beta, y)$ holds for $y \geq (\log x)^{3/2+\varepsilon}$ and this range is optimal. A similar result holds for polynomials over finite fields, unconditionally.*

5 Second oscillation result

Finally, let us turn to Theorem 3.1. We assume $y \leq (\log x)^{2-\varepsilon}$, so that $\beta \leq 1/2 - \varepsilon$ (and also $\alpha \leq 1/2 - \varepsilon$: it is known that $\alpha = \beta + O(1/\log y)$).

We have seen

$$\frac{\Psi(x,y)}{x\rho(u)} \ll \sqrt{u}\frac{x^\alpha \zeta(\alpha,y)}{x^\beta \hat{\rho}(-\xi(u))} \ll \sqrt{u}\frac{x^\beta \zeta(\beta,y)}{x^\beta \hat{\rho}(-\xi(u))} = \sqrt{u}\frac{\zeta(\beta,y)}{\hat{\rho}(-\xi(u))}.$$

This used $\Psi(x,y) \leq x^\alpha \zeta(\alpha,y)$. We also have $\Psi(x,y) \gg x^\alpha \zeta(\alpha,y)/(\sqrt{u}\log y)$ (Hildebrand and Tenenbaum, 80s) if $y \geq (\log x)^{1+\varepsilon}$, so

$$\frac{\Psi(x,y)}{x\rho(u)} \gg \frac{x^\alpha \zeta(\alpha,y)}{x^\beta \hat{\rho}(-\xi(u))\log y} \geq \frac{x^\alpha \zeta(\alpha,y)}{x^\alpha \hat{\rho}((1-\alpha)\log y)\log y} = \frac{\zeta(\alpha,y)}{\hat{\rho}((1-\alpha)\log y)\log y}.$$

The second inequality is trivial (but new): it uses the fact that β minimizes $s \mapsto x^s \hat{\rho}((1-s)\log y)$. Recall

$$F(s,y) = \log\zeta(s,y) - \log\hat{\rho}(\log y(s-1)).$$

We have just shown

$$\frac{\Psi(x,y)}{x\rho(u)} \gg e^{F(\alpha,y)}/\log y.$$

Unconditionally, Landau's Theorem shows that, if we fix $\alpha > 0$,

$$y \mapsto \sum_{n\leq y} \frac{\Lambda(n)}{n^\alpha \log n} - I((1-\alpha)\log y)$$

is non-negative. When $y \leq (\log x)^{2-\varepsilon}$ we have that $\log F(\alpha,y)$ is larger than $\sum_{n\leq y} \frac{\Lambda(n)}{n^\alpha \log n}$ by a very large quantity, leading to large values of $\Psi(x,y)/(x\rho(u))$. Indeed,

$$\log\zeta(s,y) = \sum_{p\leq y} -\log(1-p^{-s}) = \sum_{n\leq y}\frac{\Lambda(n)}{n^s \log n} + \sum_{k\geq 2}\sum_{y^{1/k}<p\leq y} p^{-ks}/k.$$

The k-sum can easily be shown to tend to infinity when $s \leq 1/2 - \varepsilon$ (this uses nothing more than the Prime Number Theorem), which is the case when $s = \alpha$ and $y \leq (\log x)^{2-\varepsilon}$.