The sum of digits of primes in $\mathbb{Z}[i]$

Thomas Stoll (TU Wien)

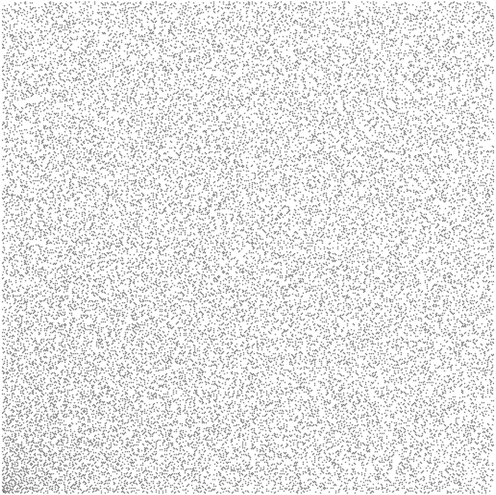
Journées de Numération, Graz 2007

April 19, 2007

(joint work with M. Drmota and J. Rivat)

Research supported by the Austrian Science Foundation, no.9604.

Pointillism: Gaussian primes in the first quadrant



Gaussian primes

Gaussian primes p:

(1) $1+\mathrm{i}$ and its associates,

(2) the rational primes $4k+3$ and their associates,

(3) the factors in $\mathbb{Z}[\mathrm{i}]$ of the rational primes $4k+1$.

Hecke prime number theorem:

$$\pi_{\mathrm{i}}(N) := \{p \in \mathbb{Z}[\mathrm{i}] \text{ non-associated : } |p|^2 \leq N\} \sim \frac{N}{\log N}.$$

Complex Von Mangoldt function Λ_{i}:

$$\Lambda_{\mathrm{i}}(n) = \begin{cases} \log|p|, & n = \varepsilon p^{\nu}, \qquad \varepsilon \text{ unit}, \ \nu \in \mathbb{Z}^{+}; \\ 0, & \text{otherwise.} \end{cases}$$

The complex sum-of-digits function

[Kátai/Kovács, Kátai/Szabó]

Let $q = -a \pm \mathrm{i}$ (choose a sign) with $a \in \mathbb{Z}^+$. Then every $n \in \mathbb{Z}[\mathrm{i}]$ has a unique finite representation

$$n = \sum_{j=0}^{\lambda-1} \varepsilon_j q^j,$$

where $\varepsilon_j \in \{0, 1, \ldots, a^2\}$ are the digits and $\varepsilon_{\lambda-1} \neq 0$.

Let $s_q(n) = \sum_{j=0}^{\lambda-1} \varepsilon_j$ be the sum-of-digits function in $\mathbb{Z}[\mathrm{i}]$.

Main results I

Recall $q = -a \pm \mathrm{i}$, $a \in \mathbb{Z}^+$ and write $\mathrm{e}(x) = \exp(2\pi \mathrm{i} x)$.

Theorem

For any $\alpha \in \mathbb{R}$ with $(a^2 + 2a + 2)\alpha \notin \mathbb{Z}$, a even, there is $\sigma_q(\alpha) > 0$ such that

$$\sum_{|n|^2 \leq N} \Lambda_{\mathrm{i}}(n)\, \mathrm{e}(\alpha s_q(n)) \ll N^{1-\sigma_q(\alpha)}.$$

Theorem

The sequence $(\alpha s_q(p))$, a even, running over Gaussian primes p is uniformly distributed modulo 1 if and only if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

Main results II

Theorem

Let $a \geq 2$, a even, $b \in \mathbb{Z}_{\geq 0}$, $m \in \mathbb{Z}^+$, $m \geq 2$ and set

$$d = (m, a^2 + 2a + 2).$$

If $(b, d) = 1$ then there exists $\sigma_{q,m} > 0$ such that

$$\#\left\{p \in \mathbb{Z}[\mathrm{i}] : \ |p|^2 \leq N, \quad s_q(p) \equiv b \mod m\right\} = \frac{d}{m\,\varphi(d)}\,\pi_{\mathrm{i}}(N) + O_{q,m}(N^{1-\sigma_{q,m}}).$$

If $(b, d) \neq 1$ then the set has cardinality $O_{q,m}(N^{1-\sigma_{q,m}})$.

Inequalities à la Vaughan and van der Corput

Lemma (Vaughan)

Let $\beta_1 \in (0, \frac{1}{3})$, $\beta_2 \in (\frac{1}{2}, 1)$. *Further suppose that for all* a_n, b_n *with* $|a_n|, |b_n| \leq 1$, $n \in \mathbb{Z}[\mathrm{i}]$ *and all* $M \leq x$ *we uniformly have (put* $Q = a^2 + 1$*)*

$$\sum_{\frac{M}{Q} < |m|^2 \leq M} \max_{\frac{x}{Q|m|^2} < t \leq \frac{x}{|m|^2}} \left| \sum_{\frac{x}{Q|m|^2} < |n|^2 \leq t} \mathrm{e}(\alpha s_q(mn)) \right| \leq U \quad \text{for} \quad M \leq x^{\beta_1},$$

$$\left| \sum_{\frac{M}{Q} < |m|^2 \leq M} \sum_{\frac{x}{Q|m|^2} < |n|^2 \leq \frac{x}{|m|^2}} a_m b_n \, \mathrm{e}(\alpha s_q(mn)) \right| \leq U \quad \text{for} \quad x^{\beta_1} \leq M \leq x^{\beta_2}.$$

Then

$$\left| \sum_{\frac{x}{Q} < |n|^2 \leq x} \Lambda_{\mathrm{i}}(n) \, \mathrm{e}(\alpha s_q(n)) \right| \ll U (\log x)^2.$$

Lemma (Van der Corput)

Let $z_n \in \mathbb{C}$ with $n \in \mathbb{Z}[\mathrm{i}]$ and $A, B \geq 0$. Then for all $R \geq 1$ we have

$$\left| \sum_{A<|n|<B} z_n \right|^2 \leq C_3 \left(\frac{B-A}{R} + 2 \right) \cdot \frac{B+A}{R} \sum_{|r|<2R} \left(1 - \frac{|r|}{2R} \right) \sum_{\substack{A<|n|<B \\ A<|n+r|<B}} z_{n+r} \overline{z_n}.$$

Now, start with

$$S = \sum_{Q^{\mu-1}<|m|^2 \leq Q^\mu} \left| \sum_{Q^{\nu-1}<|n|^2 \leq Q^\nu} b_n \, \mathrm{e}(\alpha s_q(mn)) \right|.$$

How to get the difference process:

Denote $f(n) = \alpha s_q(n)$. Then with Cauchy-Schwarz ineq.,

$$|S|^2 \leq Q^\mu \sum_{Q^{\mu-1}<|m|^2\leq Q^\mu} \left| \sum_{Q^{\nu-1}<|n|^2\leq Q^\nu} b_n \, \mathrm{e}(f(mn)) \right|^2,$$

and with Van der Corput ineq.,

$$|S|^2 \ll Q^{2(\mu+\nu)-\rho}$$

$$+ Q^{\mu+\nu} \max_{1\leq|r|<|q|^\rho} \sum_{Q^{\nu-1}<|n|^2\leq Q^\nu} \left| \sum_{Q^{\mu-1}<|m|^2\leq Q^\mu} \mathrm{e}\left(f(m(n+r)) - f(mn)\right) \right|.$$

The truncated sum-of-digits function

We introduce the truncated sum-of-digits function of $\mathbb{Z}[\mathrm{i}]$, defined by

$$f_\lambda(z) = \sum_{j=0}^{\lambda-1} f(\varepsilon_j q^j) = \alpha \sum_{j=0}^{\lambda-1} \varepsilon_j,$$

where $\lambda \in \mathbb{Z}$ and $\lambda \geq 0$.

Periodicity property: For any $d \in \mathbb{Z}[\mathrm{i}]$,

$$f_\lambda(z + dq^\lambda) = f_\lambda(z), \qquad z \in \mathbb{Z}[\mathrm{i}].$$

Reason: Let $d = x + \mathrm{i}y$.
Use the identities $\mathrm{i}q = aq + q^2$, $Q = (a-1)^2 q + (2a-1)q^2 + q^3$.

At only "small" cost: Carry propagation lemma

Put $\lambda = \mu + 2\rho$.

Lemma

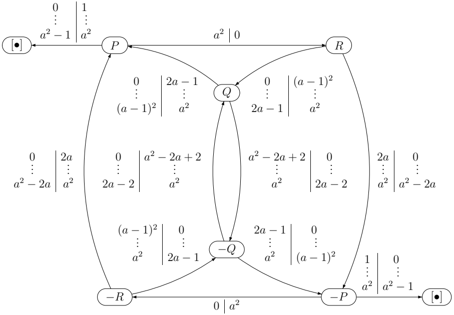
Let $a \geq 2$. For all integers $\mu > 0$, $\nu > 0$, $0 \leq \rho < \nu/2$ and $r \in \mathbb{Z}[\mathrm{i}]$ with $|r| < |q|^\rho$ denote by $E(r, \mu, \nu, \rho)$ the number of pairs $(m, n) \in \mathbb{Z}[\mathrm{i}] \times \mathbb{Z}[\mathrm{i}]$ with $Q^{\mu-1} < |m|^2 \leq Q^\mu$, $Q^{\nu-1} < |n|^2 \leq Q^\nu$ and

$$f(m(n+r)) - f(mn) \neq f_\lambda(m(n+r)) - f_\lambda(mn).$$

Then we have

$$E(r, \mu, \nu, \rho) \ll Q^{\mu+\nu-\rho}.$$

At only “small” cost II: The addition automaton



Performs addition by 1 (P), by $-a-\mathrm{i}$ (R) and by $a-1+\mathrm{i}$ (Q).
Example: Let $a=3$ and $z=58-40\mathrm{i}=(\varepsilon_0,\varepsilon_1,\varepsilon_2)=(8,2,7)$, and consider $z+2+\mathrm{i}$. The corresponding walk is

$$Q \xrightarrow{8|3} -Q \xrightarrow{2|7} Q \xrightarrow{7|2} -Q \xrightarrow{0|5} Q \xrightarrow{0|5} P \xrightarrow{0|1} [\bullet],$$

thus $z+2+\mathrm{i}=(3,7,2,5,5,1)$.

At only "small" cost III: Proof

Idea of proof of the "carry propagation lemma": Assume $mr = x + \mathrm{i}y = -y(-a-\mathrm{i}) + (x + ay)$ with $y < 0$, $x > -ay$. Write

$$\begin{aligned}
f(mn+mr) - f(mn) = \\
&f(mn+mr) - f(mn+(a+\mathrm{i})+mr) \\
&+ f(mn+(a+\mathrm{i})+mr) - f(mn+2(a+\mathrm{i})+mr) + \dots \\
&+ f(mn-(y+1)(a+\mathrm{i})+mr) - f(mn-y(a+\mathrm{i})+mr) \\
&+ f(mn-y(a+\mathrm{i})+mr) - f(mn-y(a+\mathrm{i})+mr-1) \\
&+ f(mn-y(a+\mathrm{i})+mr-1) - f(mn-y(a+\mathrm{i})+mr-2) + \dots \\
&+ f(mn-y(a+\mathrm{i})+mr-x-ay+1) - f(mn).
\end{aligned}$$

Orthogonality relation

Let $\mathcal{F}_\lambda = \{\sum_{j=0}^{\lambda-1} \varepsilon_j q^j : \varepsilon_j \in \mathcal{N}\}$ be the fundamental region of the number system, which is a complete system of residues mod q^λ with $\#\mathcal{F}_\lambda = Q^\lambda$. Hence,

$$\sum_{z \in \mathcal{F}_\lambda} \mathrm{e}\left(\mathrm{tr}\left(hzq^{-\lambda}\right)\right) = \begin{cases} Q^\lambda, & h \equiv 0 \bmod q^\lambda; \\ 0, & \text{otherwise}, \end{cases}$$

where $\mathrm{tr}\,(z) = 2\Re(z)$. Put

$$|F_\lambda(h, \alpha)| = Q^{-\lambda} \prod_{j=1}^{\lambda} \varphi_Q\left(\alpha - \mathrm{tr}\left(hq^{-j}\right)\right),$$

where

$$\varphi_Q(t) = \begin{cases} |\sin(\pi Q t)|/|\sin(\pi t)|, & t \in \mathbb{R} \setminus \mathbb{Z}; \\ Q, & t \in \mathbb{Z}. \end{cases}$$

Transformation

Let

$$S_2'(n) = \sum_{Q^{\mu-1}<|m|^2\leq Q^\mu} \mathrm{e}\left(f_\lambda(m(n+r)) - f_\lambda(mn)\right).$$

Then

$$\begin{aligned} S_2'(n) &= \frac{1}{Q^{2\lambda}} \sum_{u\in\mathcal{F}_\lambda} \sum_{v\in\mathcal{F}_\lambda} \mathrm{e}(f_\lambda(u)\cdot f_\lambda(v)) \cdot \\ &\quad \cdot \sum_{h\in\mathcal{F}_\lambda} \sum_{k\in\mathcal{F}_\lambda} \sum_{Q^{\mu-1}<|m|^2\leq Q^\mu} \mathrm{e}\left(\mathrm{tr}\,\frac{h(m(n+r)-u)}{q^\lambda} + \mathrm{tr}\,\frac{k(mn-v)}{q^\lambda}\right) \\ &= \sum_{h\in\mathcal{F}_\lambda} \sum_{k\in\mathcal{F}_\lambda} F_\lambda(h,\alpha)\overline{F_\lambda(-k,\alpha)} \sum_{Q^{\mu-1}<|m|^2\leq Q^\mu} \mathrm{e}\left(\mathrm{tr}\,\frac{(h+k)mn+hmr}{q^\lambda}\right). \end{aligned}$$

Fourier analysis of F_λ

Lemma

For all $\alpha \in \mathbb{R}$, $\xi \in \mathbb{C}$ and $a \geq 3$ we have

$$\sum_{j=0}^{\lambda-1} \left\|\alpha - \mathrm{tr}\left(\xi q^j\right)\right\|^2 \geq \frac{\lambda - 2}{2(a^2+1)^2} \left\|(a^2+2a+2)\alpha\right\|^2.$$

Corollary

There exists a constant $C_a > 0$ only depending on a such that

$$|F_\lambda(h,\alpha)| \leq \exp(-C_a \lambda \left\|(a^2+2a+2)\alpha\right\|^2)$$

uniformly for all $h \in \mathbb{Z}[\mathrm{i}]$, $\alpha \in \mathbb{R}$ and integers $\lambda \geq 0$.

Fourier analysis of G_λ

Define

$$G_\lambda(b,d,\alpha) := \sum_{\substack{h\in\mathcal{F}_\lambda \\ h\equiv b \bmod d}} |F_\lambda(h,\alpha)|, \quad G_\lambda(\alpha) = G_\lambda(0,1,\alpha) = \sum_{h\in\mathcal{F}_\lambda} |F_\lambda(h,\alpha)|.$$

Lemma

For $a\geq 2$, $b\in\mathbb{Z}[\mathrm{i}]$, $\alpha\in\mathbb{R}$, $0\leq\delta\leq\lambda$ there is $\eta_Q<\frac{1}{2}$ and

$$G_\lambda(b,q^\delta,\alpha) = \sum_{\substack{h\in\mathcal{F}_\lambda \\ h\equiv b \bmod q^\delta}} |F_\lambda(h,\alpha)| \leq Q^{\eta_Q(\lambda-\delta)}\cdot|F_\delta(b,\alpha)|.$$

In particular,

$$G_\lambda(\alpha) = G_\lambda(0,1,\alpha) \leq Q^{\eta_Q\lambda}.$$

Fourier analysis II of G_λ

Lemma

For $a \geq 2$, $b \in \mathbb{Z}[\mathrm{i}]$, $\alpha \in \mathbb{R}$, $0 \leq \delta \leq \lambda$, $k \in \mathbb{Z}[\mathrm{i}]$ and $k \mid q^{\lambda-\delta}$, $q \nmid k$ we have

$$G_\lambda(b, kq^\delta, \alpha) \leq 2|k|^{-2\eta_5} Q^{\eta_5(\lambda-\delta)} \cdot |F_\delta(b,\alpha)|.$$

Lemma

For a even we have

$$\sum_{\substack{h \in \mathcal{F}_\lambda \\ h \equiv b \bmod q^\delta}} |F_\lambda(h,\alpha)|^2 = |F_\delta(b,\alpha)|^2$$

and thus, in particular,

$$\sum_{h \in \mathcal{F}_\lambda} |F_\lambda(h,\alpha)|^2 = 1.$$