

ANALYTIC NUMBER THEORY, SPRING 2022: ANKENY'S THEOREM FOR THE RATIONAL FUNCTION FIELD

ZE'EV RUDNICK

Let $N \gg 1$ be a large integer. Ankeny's theorem (1952) shows that, assuming the Generalized Riemann Hypothesis (GRH) (for all Dirichlet L-functions), for every nontrivial subgroup G of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$, there is some small residue $a \in (\mathbb{Z}/N\mathbb{Z})^* \setminus G$ which is not contained in G ; here “small” means $a = O((\log N)^2)$. This has a number of applications:

- (1) Given a large prime p , the least non-residue is at most $O((\log p)^2)$.
- (2) Primality testing: We can test whether a large integer is prime in polynomial time.

Below we shall explain how Ankeny's theorem gives these applications, and then prove it for $\mathbb{F}_q[x]$.

1. THE LEAST NON-RESIDUE MOD p

Given a large prime p , denote by $n(p)$ the least non-residue mod p . Since $1 = 1^2$ is a quadratic residue, we always have $n(p) \geq 2$. If $p = 3, 5 \bmod 8$ then $\left(\frac{2}{p}\right) = -1$ so that $n(p) = 2$, while if $p = 1, 7 \bmod 8$ then 2 is also a quadratic residue, so $n(p) \geq 3$.

1.1. A lower bound. First of all, we claim

Proposition 1. *The least quadratic residue $n(p)$ is an unbounded function of the prime p : $\limsup_p n(p) = \infty$.*

Proof. Let $\ell_1 = 2, \ell_2 = 3, \ell_3 = 5, \dots$, be the primes enumerated in increasing order. Let $Q_M = 8 \cdot 3 \cdot 5 \cdots \ell_M = 4 \prod_{j=1}^M \ell_j$. By Dirichlet's theorem, there are (infinitely many) primes p in the arithmetic progression $p = 1 \bmod Q_M$. Denote by $p(M)$ the least such prime. We claim that $n(p(M)) > \ell_M$, which will show that $\limsup_p n(p) = \infty$.

To see this, will show that for all $1 \leq t \leq \ell_M$ we have the Legendre symbol $\left(\frac{t}{p}\right) = +1$. Indeed, factor t , noting that since $t \leq \ell_M$, the only primes which can appear are among the first M primes: $t = 2^{a(1)} 3^{a(2)} \cdots \ell_m^{a(m)}$, $a(j) \geq 0$.

Then by the multiplicativity of the Legendre symbol,

$$\left(\frac{t}{p}\right) = \left(\frac{2}{p}\right)^{a(1)} \prod_{j=2}^M \left(\frac{\ell_j}{p}\right)^{a(j)}.$$

We have $\left(\frac{2}{p}\right) = +1$ because $p = 1 \pmod 8$ since $p = 1 \pmod{Q^M}$ and $8 \mid Q_M$. Likewise $p = 1 \pmod{\ell_j}$ for $2 \leq j \leq M$ since $\ell_j \mid Q_M$ for $j \leq M$, so that $\left(\frac{\ell_j}{p}\right) = +1$. Thus $\left(\frac{t}{p}\right) = +1$. $\square$

Remark. *With further work we can show (unconditionally!) that there are arbitrarily large primes for which $n(p) \gg \log p$:*

A difficult result of Linnik guarantees that there is some $C > 1$ so that every arithmetic progression $p = A \pmod Q$ contains a prime $p \ll Q^C$ (assuming GRH we can take any $C > 2$). Applying to the progression $p = 1 \pmod{Q_M}$ gives $p(M) \ll Q_M^C$ or $\log Q_M \gg \log p(M)$. By Chebyshev (or PNT),

$$\log Q_m = \log 4 + \sum_{\ell \leq \ell_M} \log \ell \ll \ell_M$$

and so

$$\log p(M) \ll \log Q_M \ll \ell_M.$$

Since $n(p(M)) > \ell_M$ we obtain

$$n(p(M)) > \ell_M \gg \log p(M)$$

so that there are arbitrarily large primes for which $n(p) \gg \log p$.

1.2. Upper bounds. Concerning upper bounds for $n(p)$, we know that half of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ consists of quadratic residues (that is $a = x^2 \pmod p$) and half are non-residues, so that $n(p) \leq p/2$. If there were a conspiracy and all the integers $1, 2, \dots, (p-1)/2$ were quadratic residues, then this is all that we could say. But in fact much better is known. We first start with the Polya-Vinogradov inequality (1918):

Theorem 2. *Let p be a prime, and χ a nontrivial character mod p . Then there is some $C > 0$ so that for all M ,*

$$\left| \sum_{1 \leq a \leq x} \chi(a + M) \right| \leq C \sqrt{p} \log p$$

Applying to the Legendre symbol, we find that if $x \gg \sqrt{p} \log p$ then there is nontrivial cancellation in the character sum $\sum_{a \leq x} \left(\frac{a}{p}\right)$, hence there is at least one $a \leq x$ for which $\left(\frac{a}{p}\right) = -1$, so that $n(p) < x$. Thus we obtain $n(p) \ll \sqrt{p} \log p$.

We also note that for a smooth sum $\sum f(\frac{a}{x}) \chi(a)$ one can remove the log factor.

An improvement to the Polya-Vinogradov bound is due to D.A. Burgess (1962), whose work implies that for p prime, we have

$$\left| \sum_{M+1 \leq n \leq M+x} \chi(x) \right| < x^{1-\delta^2}$$

for any $x > p^{\frac{1}{4}+\delta}$, $\delta \in (0, 1/2)$.

1.3. Harmonic analysis on $\mathbb{Z}/p\mathbb{Z}$. Before proving Theorem 2, we need some background on harmonic analysis on $\mathbb{Z}/p\mathbb{Z}$. Let $L^2(\mathbb{Z}/p\mathbb{Z})$ be the space of complex valued functions on $\mathbb{Z}/p\mathbb{Z}$ equipped with the inner product

$$\langle f, g \rangle = \frac{1}{p} \sum_{t \bmod p} f(t) \overline{g(t)}.$$

An orthonormal basis of $L^2(\mathbb{Z}/p\mathbb{Z})$ is provided by the additive characters

$$e_n : t \mapsto e^{2\pi i n t / p}.$$

We can therefore expand any $f \in L^2(\mathbb{Z}/p\mathbb{Z})$ as

$$f = \sum_{n \bmod p} \hat{f}(n) e_n, \quad \hat{f}(n) = \frac{1}{p} \sum_{t \bmod p} f(t) e_n(-t).$$

We note the Parseval identity

$$\sum_{n \bmod p} |\hat{f}(n)|^2 = \langle f, f \rangle = \frac{1}{p} \sum_{t \bmod p} |f(t)|^2.$$

In particular, we may expand the nontrivial Dirichlet character in terms of this basis:

$$\chi = \sum_{n=0}^{p-1} \hat{\chi}(n) e_n.$$

We have $\hat{\chi}(0) = 0$, since by the orthogonality relation for the nontrivial character χ ,

$$\hat{\chi}(0) = \frac{1}{p} \sum_{t \bmod p} \chi(t) = 0.$$

Thus the sum is only over $1 \leq n \leq p-1$. For $n \neq 0$, we have

$$\hat{\chi}(n) = \overline{\chi(n)} \hat{\chi}(1)$$

after a change of variables:

$$\begin{aligned} \chi(n) \hat{\chi}(n) &= \chi(n) \frac{1}{p} \sum_{t \bmod p} \chi(t) e(-\frac{nt}{p}) \\ &= \frac{1}{p} \sum_{t \bmod p} \chi(nt) e(-\frac{nt}{p}) \\ &= \frac{1}{p} \sum_{z \bmod p} \chi(z) e(-\frac{z}{p}) = \hat{\chi}(1). \end{aligned}$$

In particular $|\widehat{\chi}(n)| = |\widehat{\chi}(1)|$. Using the Parseval identity gives

$$(p-1)|\widehat{\chi}(1)|^2 = \sum_{n \bmod p} |\widehat{\chi}(n)|^2 = \frac{1}{p} \sum_{t \bmod p} |\chi(t)|^2 = \frac{p-1}{p}$$

and therefore for all $n \neq 0$,

$$|\widehat{\chi}(n)| = |\widehat{\chi}(1)| = \frac{1}{\sqrt{p}}.$$

Note: The Fourier coefficient $\widehat{\chi}(-1)$ is called a (normalized) “Gauss sum”: $\widehat{\chi}(-1) = \tau(\chi)/p$, with

$$\tau(\chi) := \sum_{t \bmod p} \chi(t) e^{2\pi i t/p}$$

and we just showed that $|\tau(\chi)| = \sqrt{p}$.

Exercise 1. Show that for the quadratic character $\chi(t) = \left(\frac{t}{p}\right)$ (Legendre symbol),

$$\tau\left(\left(\frac{\bullet}{p}\right)\right)^2 = \left(\frac{-1}{p}\right) p.$$

Thus $\tau\left(\left(\frac{\bullet}{p}\right)\right) = \epsilon_p \sqrt{p}$ for a suitable 4-th root of unity, $\epsilon_p^2 = \left(\frac{-1}{p}\right)$. Gauss determined the “sign” of the Gauss sum: $\epsilon_p = +1$ for $p \equiv 1 \pmod{4}$, and $\epsilon_p = +i$ for $p \equiv 3 \pmod{4}$.

1.4. Proof of Theorem 2.

Proof. We compute the sum by using the Fourier expansion of χ :

$$\begin{aligned} \sum_{1 \leq a \leq x} \chi(a+M) &= \sum_{1 \leq a \leq x} \left(\sum_{n \bmod p} \widehat{\chi}(n) e_n(a+M) \right) \\ &= \sum_{n \bmod p} \widehat{\chi}(n) \sum_{M+1 \leq a \leq M+x} e_n(a). \end{aligned}$$

For $n \neq 0 \bmod p$, the inner sum is a geometric progression

$$\sum_{1 \leq a \leq x} e_n(a+M) = \sum_{1 \leq a \leq x} e^{2\pi i n(a+M)/p} = \frac{e_n(M+1) - e_n(M+x+1)}{1 - e_n(1)}$$

and taking absolute values gives

$$\left| \sum_{1 \leq a \leq x} e_n(a+M) \right| = \frac{1}{|\sin(\pi n/p)|} \leq \frac{1}{\|n/p\|}$$

where $\|x\| := \text{dist}(x, \mathbb{Z})$ (there is no longer any dependence on M). Thus

$$\left| \sum_{1 \leq a \leq x} \chi(a) \right| \leq \sum_{n=1}^{p-1} |\widehat{\chi}(n)| \frac{1}{\|n/p\|} = \frac{1}{\sqrt{p}} \sum_{n=1}^{p-1} \frac{1}{\|n/p\|}.$$

We have

$$\sum_{n=1}^{p-1} \frac{1}{\|n/p\|} = 2 \sum_{n=1}^{(p-1)/2} \frac{1}{n/p} \sim 2p \log p$$

and thus

$$\left| \sum_{1 \leq a \leq x} \chi(a+M) \right| \ll \sqrt{p} \log p$$

as claimed. $\square$

1.5. Vinogradov's trick.

Proposition 3. *Assume that $\chi \neq \chi_0$ is a nontrivial real character, and that $\sum_{1 \leq n \leq x} \chi(n) = o(x)$. Then there is some $n < x^{\frac{1+\epsilon}{\sqrt{e}}}$ with $\chi(n) = -1$.*

Note that $1/\sqrt{e} = 0.606\dots$

Proof. Assume on the contrary, that for $y = x^{(1+\epsilon)/\sqrt{e}}$ we have $\chi(m) = +1$ for all $m \leq y$. Since $\chi(n) = \pm 1$, we can write (assume $x \gg 1$ is an integer)

$$\sum_{1 \leq n \leq x} \chi(n) = \sum_{1 \leq n \leq x} 1 - 2 \sum_{\substack{1 \leq n \leq x \\ \chi(n) = -1}} 1 = x - 2\#\{y < n \leq x : \chi(n) = -1\}$$

where we have used $\chi(n) = +1$ for all $n \leq y$. We will show that

$$(1) \quad \#S := \#\{y < n \leq x : \chi(n) = -1\} \leq \frac{1-\epsilon}{2}x,$$

which will give

$$\sum_{1 \leq n \leq x} \chi(n) = x - 2\#\{y < n \leq x : \chi(n) = -1\} \geq \epsilon x,$$

contradicting $\sum_{1 \leq n \leq x} \chi(n) = o(x)$.

If $\chi(n) = -1$, then there must be a prime $q \mid n$ so that $\chi(q) = -1$, and necessarily $q > y$ since $\chi \equiv +1$ on $[1, y]$ by assumption. Such q is unique, since $q \leq n \leq x < y^2 < q^2$ (since $y^2 > x^{2/\sqrt{e}} > x$) or $n^{1/2} < q$. Hence we can write S as a disjoint union

$$S = \coprod_{\substack{y < q \leq x \text{ prime} \\ \chi(q) = -1}} \left\{ n = mq, \frac{y}{q} < m \leq \frac{x}{q} \right\}$$

and so

$$\#S \leq \sum_{\substack{y < q \leq x \\ \text{prime}}} \frac{x}{q} = x \sum_{\substack{y < q \leq x \\ \text{prime}}} \frac{1}{q}$$

By Mertens' theorem

$$\begin{aligned} \sum_{\substack{y < q \leq x \\ \text{prime}}} \frac{1}{q} &= (\log \log x + C + o(1)) - (\log \log y + C + o(1)) \\ &\lesssim \log \frac{\log x}{\log y} < \log \frac{\log x}{\log x^{(1+\epsilon)/\sqrt{e}}} \\ &= \frac{1}{2} - \log(1 + \epsilon) < \frac{1 - \epsilon}{2}. \end{aligned}$$

Thus $\#S < \frac{1-\epsilon}{2}x$, proving (1). $\square$

Combining the Polya-Vinogradov inequality with the combinatorial trick, Vinogradov showed $n(p) \ll p^{1/(2\sqrt{e})+\epsilon}$ for all ϵ . Using the Burgess bound this is improved to $n(p) < p^{1/(4\sqrt{e})+\epsilon}$, which is the best (unconditional) result known. However, already Vinogradov conjectured that $n(p) \ll p^\epsilon$, for all ϵ , and this was proved by Linnik (1942) assuming GRH. Ankeny's theorem improves this:

Theorem 4. *Assume GRH. Then $n(p) \ll (\log p)^2$.*

This is because the set of quadratic residues forms a proper subgroup of the multiplicative group, hence Ankeny's theorem applies directly.

2. PRIMALITY TESTING

We are given a (large) integer N and want to “quickly” test if it is prime or not. “Quick” means in polynomial time relative to the number of bits of N , that is with $O((\log N)^4)$ operations. One option is to try to factor it, but currently there is no known method to quickly factor. But this is an overkill, because there are methods that will give a yes/no answer without giving the factors!

One option is to use Fermat's little theorem: If N is prime, and a is coprime to N then $a^{N-1} = 1 \pmod{N}$. Computing $a^{N-1} \pmod{N}$ can be done “quickly” by repeated squaring, and so if we find $1 < a < N$ so that $a^{N-1} \not\equiv 1 \pmod{N}$ then we are sure that N is not a prime. Such an a is called a “witness”. So assuming that there exists a witness (this is not always the case, but the exceptions are few, and are called Carmichael numbers), the issue is how to find one. It turns out that assuming GRH for all Dirichlet L-functions, there are “small” witnesses, in fact of size $O((\log N)^2)$, in fact up to $2(\log N)^2$. Thus we can systematically go through all small residues and for each compute $a^{N-1} \pmod{N}$. If we found a single residue for which $a^{N-1} \not\equiv 1 \pmod{N}$ then we know that N is composite, while if all tests with $a < 2(\log N)^2$ give $a^{N-1} = 1 \pmod{N}$ then assuming GRH we are guaranteed that N is prime.

Our goal here is to explain why we are guaranteed to have small witnesses. To do so, we first check that the set of “liars”, that is

$$L_N := \{a \in (\mathbb{Z}/N\mathbb{Z})^* : a^{N-1} = 1 \pmod{N}\}$$

is a *subgroup* of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$. Then we use Ankeny's theorem [1] which shows that for any *proper* subgroup of the group of invertible residues modulo N , there is an invertible residue not in the subgroup of size $O((\log N)^2)$. The best result to date is due to E. Bach [2, 3] who showed that there is a residue not in the subgroup which is at most $2(\log N)^2$. Thus assuming that there is a witness, Ankeny's theorem guarantees (on GRH) that there is a small witness.

3. ANKENY'S THEOREM IN $\mathbb{F}_q[x]$

Consider the rational function field $\mathbb{F}_q(x)$ over the finite field $\mathbb{F}_q$ of q elements. Let $Q(x) \in \mathbb{F}_q[x]$ be a polynomial of positive degree. We will show an analogue of Ankeny's theorem in this setting. Let

$$||A|| := \#\mathbb{F}_q[x]/(A) = q^{\deg(A)}.$$

Theorem 5. *Let $Q \in \mathbb{F}_q[x]$ be a polynomial of positive degree, and let $G \subset (\mathbb{F}_q[x]/(Q))^\times$ be a proper subgroup of invertible residues modulo Q . Then there is a prime polynomial $P \in \mathbb{F}_q[x]$, $P \nmid Q$, with $P \notin G$ such that*

$$(2) \quad ||P|| \leq q(\deg Q)^2.$$

3.1. Preliminaries. Given a nontrivial character modulo Q (not necessarily primitive!) the L-function $\mathcal{L}(u, \chi)$ is defined by

$$(3) \quad \mathcal{L}(u, \chi) = \prod_P (1 - \chi(P)u^{\deg P})^{-1}, \quad |u| < 1/q.$$

This is a polynomial of degree at most $\deg Q - 1$ and we can write it as

$$(4) \quad \mathcal{L}(u, \chi) = \prod_{j=1}^{\deg Q - 1} (1 - \alpha_{j,\chi} u)$$

(where possibly some of the inverse roots are zero). The Riemann Hypothesis (Weil's theorem) implies

$$|\alpha_{j,\chi}| \leq \sqrt{q}.$$

Let

$$\Psi(m, \chi) = \sum_{\substack{\deg f = m \\ \text{monic}}} \Lambda(f) \chi(f) = \sum_{\substack{\deg(P) | m \\ \text{prime}}} \deg(P) \chi(P)^{m/\deg P}.$$

The Explicit Formula is the identity

$$\Psi(m, \chi) = - \sum_{j=1}^{\deg Q - 1} \alpha_{j,\chi}^m$$

proved by computing the logarithmic derivative $u \frac{\mathcal{L}'}{\mathcal{L}}$ in two different ways, either using the Euler product (3) or the zeros (4) and comparing the result. Thus for nontrivial characters mod Q , the Riemann Hypothesis gives

$$(5) \quad |\Psi(m, \chi)| \leq (\deg(Q) - 1)q^{m/2}.$$

3.2. Group theory.

Lemma 6. *Let A be a finite abelian group, and $B \subset A$ a proper subgroup $B \neq A$. Then there is a nontrivial character $\chi : A \rightarrow \mathbb{C}^*$ so that the restriction $\chi|_B$ to B is trivial.*

Proof. Consider the quotient group $\bar{A} := A/B$. This is not the trivial group since $B \neq A$, and hence has a nontrivial character $\bar{\chi} : \bar{A} \rightarrow \mathbb{C}^*$. The pullback $\chi : A \rightarrow \bar{A} \rightarrow \mathbb{C}^*$ is then trivial on B , but nontrivial on A . $\square$

3.3. Proof of Ankeney's theorem. If G is a proper subgroup, then there is a nontrivial Dirichlet character $\chi \neq \chi_0 \bmod Q$ such that $\chi|_G = 1$. So it suffices to find a prime P satisfying (2) such that $\chi(P) \neq 0, 1$. Let $n \geq 1$ be such that all primes of degree dividing (!) n are in G or divide Q . We will show that $q^n \leq (\deg Q)^2$. Indeed, by assumption on n ,

$$\begin{aligned} \Psi(n, \chi) &= \sum_{\deg(P)|n} \deg(P) \chi(P)^{n/\deg P} = \sum_{\substack{\deg P|n \\ P|Q}} \deg(P) \\ &= \Psi(n) - \sum_{\substack{\deg(P)|n \\ P|Q}} \deg P \geq \Psi(n) - \deg Q. \end{aligned}$$

Since $\Psi(n) = q^n$, we get

$$(6) \quad q^n \leq \Psi(n, \chi) + \deg Q$$

Comparing with (5) gives

$$(7) \quad q^n \leq (\deg Q - 1)q^{n/2} + \deg Q.$$

The solution of this quadratic inequality is

$$-1 \leq q^{n/2} \leq \deg Q$$

that is $q^{n/2} \leq \deg Q$. Hence our assumption forces $q^n \leq (\deg Q)^2$.

Thus if $q^\nu \leq (\deg Q)^2 < q^{\nu+1}$ then there exists a prime P with $\deg(P) \mid \nu + 1$ such that $P \notin G$, $P \nmid Q$, that is

$$\|P\| \leq q^{\nu+1} \leq q(\deg Q)^2.$$

This concludes the argument. $\square$

REFERENCES

- [1] N.C. Ankeny, *The least quadratic non residue*. Ann. of Math. (2) **55**, (1952). 65–72.
- [2] E. Bach, *Analytic methods in the analysis and design of number-theoretic algorithms*. ACM Distinguished Dissertations. MIT Press, Cambridge, MA, 1985.
- [3] E. Bach, *Explicit bounds for primality testing and related problems*. Math. Comp. **55** (1990), no. 191, 355–380.