International Mathematical Forum, Vol. 7, 2012, no. 38, 1877 - 1884

A Note on Bilharz's Example Regarding Nonexistence of Natural Density

Cherng-tiao Perng

Department of Mathematics
Norfolk State University
700 Park Avenue, Norfolk, VA 23504, USA
ctperng@nsu.edu

Abstract

In a 1937 paper (See [2] or Chapter 10 of [3] for an exposition), Bilharz proved Artin's conjecture for primitive roots for the function field case. In the same paper, it was mentioned an example concerning a set of primes M_x in the rational function field $F = \mathbb{F}_p(x)$, where $\mathbb{F}_p$ is the finite field of p elements and M_x is the set of prime divisors $\mathfrak{p}$ of F such that x is a primitive root mod $\mathfrak{p}$. Then Bilharz claimed that M_x does not have a natural density. However the proof provided by Bilharz was not clear at some points and it contained a small typo. The goal of this note is to fix the typo, and indicate an elementary proof of the above claim for the cases when p satisfies some inequality.

Mathematics Subject Classification: 11A07, 11N05, 11N56

Keywords: natural density, Bilharz's example, Artin's conjecture for primitive roots

1 Explanation of the Example

According to the footnote of Bilharz's paper ([2]), Bilharz acknowledged that the short proof of the example came from H. Davenport by a written communication in September 1936. Since we have no knowledge whether this example was from Davenport, or whether the proof was the exact proof that Davenport gave, we simply mention it as Bilharz's example.

Consider the rational function field $F = \mathbb{F}_p(x)$, where p is a rational prime. Take $a \in F$ for the original Artin's problem to be x. Define M_x to be the set of prime divisors $\mathfrak{p}$ of F such that x is a primitive root mod $\mathfrak{p}$. Then M_x does not have a natural density.

The natural density is defined to be the limit (which of course may not exist) of the quotient $\frac{\pi_x(n)}{\pi(n)}$ as n goes to infinity, where $\pi_x(n)$ denotes the number of prime divisors $\mathfrak{p}$ of F with norm $\leq p^n$ such that $\mathfrak{p} \in M_x$, and $\pi(n)$ is the number of all prime divisors of F with norm $\leq p^n$.

It was shown by algebra in 4.2 of [2] that

$$\pi_x(n) = \sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1),$$

where ϕ is the Euler function. And by prime number theorem for function fields, it can be shown that

$$\pi(n) = \sum_{\nu=1}^{n} \frac{1}{\nu}p^\nu + O(p^{\frac{n}{2}+\varepsilon}), \tag{1}$$

which can be proved to be

$$\frac{p^n}{n}\left(1 - \frac{1}{p}\right)^{-1} + o\left(\frac{p^n}{n}\right).$$

Remark. In 4.3.I of [2], the above sum was estimated as

$$\frac{p^n}{n}\left(1 - \frac{1}{p}\right) + o\left(\frac{p^n}{n}\right), \tag{2}$$

which is obviously false. Though this small typo does not affect the validity of his arguments, we will include some elementary arguments below to prove the correct estimate.

To prove the nonexistence of natural density, it remains to estimate $\pi_x(n)$, compared to $\frac{p^n}{n}$. The main idea of the argument given in [2, 4.3.II.a, 4.3.II.b] is to find two subsets S_1 and S_2 of natural numbers $\mathbb{N}$ such that, on the one hand, for $n \in S_1$ and $n \to \infty$, one has

$$\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1) = o\left(\frac{p^n}{n}\right),$$

and on the other hand, for $n \in S_2$ and $n \to \infty$, one has

$$\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1) = O\left(\frac{p^n}{n}\right), \text{ but } \neq o\left(\frac{p^n}{n}\right).$$

Unfortunately the arguments for both of the above two cases don't seem to be clear. For example, in the argument for the first set S_1, we know only that the contribution of the leading term $\frac{1}{n}\phi(p^n - 1)$ can be made arbitrarily small compared to $\frac{p^n}{n}$, but we don't know much about the other summands in $\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1)$; in the argument for S_2, it was mentioned that by applying Romanoff's Theorem (see e.g. [3] for the statement and proof), one could get

$$\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1) = O\left(\frac{p^n}{n}\right), \text{ but } \neq o\left(\frac{p^n}{n}\right),$$

which is not very clear either.

We will give an elementary argument to justify the nonexistence of natural density of the above example, valid for all primes p satisfying some inequality. First let's correct the typo mentioned above.

2 Correction of a Typo

Namely the estimate in 4.3.I of [2] for $\pi(n)$ should read

$$\frac{p^n}{n}\left(1 - \frac{1}{p}\right)^{-1} + o\left(\frac{p^n}{n}\right),$$

instead of (2) of section 1.

Note that if

$$\sum_{\nu=1}^{n} \frac{1}{\nu}p^\nu = \frac{p^n}{n}\left(1 - \frac{1}{p}\right)^{-1} + o\left(\frac{p^n}{n}\right), \tag{3}$$

then by (1) of section 1,

$$\pi(n) = \frac{p^n}{n}\left(1 - \frac{1}{p}\right)^{-1} + o\left(\frac{p^n}{n}\right). \tag{4}$$

Therefore to prove (4), it suffices to show (3), which is equivalent to the statement $\lim_{n\to\infty} A_n = \left(1 - \frac{1}{p}\right)^{-1} = \frac{p}{p-1}$, where $A_n := \frac{\sum_{\nu=1}^{n} \frac{1}{\nu}p^n}{\frac{p^n}{n}}$. Note that A_n satisfies the recursive relation $A_{n+1} = \frac{n+1}{pn}A_n + 1$. Setting $B_n = A_n - \frac{p}{p-1}$, B_n satisfies in turn the recursive relation $B_{n+1} = \frac{n+1}{pn}B_n + \frac{1}{n(p-1)}$. It remains to show that $\lim_{n\to\infty} B_n = 0$, which is a consequence of the following

Lemma 2.1 *Let $\{B_n\}$ be a sequence satisfying $B_{n+1} = \alpha_n B_n + \varepsilon_n$ with*

$$|\alpha_n| \leq r < 1 \text{ and } \lim_{n\to\infty} \varepsilon_n = 0.$$

Then $\lim_{n\to\infty} B_n = 0$.

Proof. **Step 1.** $|B_n|$ is bounded. First choose $\epsilon > 0$ such that $r + \epsilon \leq 1$. By assumption on ε_n, there exists n_0 such that $|\varepsilon_n| < \epsilon$ if $n \geq n_0$.
Case 1: $|B_{n_0}| \leq 1$. Then $|B_{n_0+1}| \leq r|B_{n_0}| + |\varepsilon_{n_0}| \leq r + \epsilon \leq 1$. Inductively, one shows that $|B_n| \leq 1$ for all $n \geq n_0$. Therefore $|B_n|$ is bounded.
Case 2: $|B_{n_0}| > 1$. Consider $\{C_n\}$ defined by $C_n = \frac{B_n}{|B_{n_0}|}$. Then C_n satisfies a recursive formula of the form $C_{n+1} = \alpha_n C_n + \varepsilon'_n$, where α_n is as above and $\varepsilon'_n = \frac{\varepsilon_n}{|B_{n_0}|}$. Clearly $\lim_{n\to\infty} \varepsilon'_n = 0$ and $|\varepsilon'_n| < \epsilon$ for all $n \geq n_0$. By Case 1, $|C_n|$ is bounded, hence $|B_n|$ is bounded as well.
Step 2. $\underline{\lim}_{n\to\infty}|B_n| = 0$. If $\underline{\lim}_{n\to\infty}|B_n| = \delta > 0$, choose $\epsilon > 0$ such that $\delta_0 := r(\delta + \epsilon) + \epsilon < \delta$, which is possible since $r < 1$.
Since $\lim_{n\to\infty} \varepsilon_n = 0$, there exists n_0 such that $|\varepsilon_n| < \epsilon, \forall n \geq n_0$. Similarly, by assumption of δ, there exists $n_1 \geq n_0$ such that $|B_{n_1}| < \delta + \epsilon$. Therefore, we have

$$|B_{n_1+1}| \leq r|B_{n_1}| + |\varepsilon_n| \leq r(\delta + \epsilon) + \epsilon = \delta_0 < \delta,$$

from which inductively

$$|B_n| \leq \delta_0, \ \forall n \geq n_1 + 1,$$

a contradiction.
Step 3. $\lim_{n\to\infty} B_n = 0$. Given $\epsilon > 0$, there exists $\epsilon_1 > 0$ such that $r\epsilon + \epsilon_1 < \epsilon$, since $r < 1$. By assumption on ε_n, there exists n_0 such that $|\varepsilon_n| < \epsilon_1$ for $n \geq n_0$. Similarly, by Step 2, there exists $n_1 \geq n_0$ such that $|B_{n_1}| < \epsilon$. Therefore $|B_{n_1+1}| \leq r|B_{n_1}| + |\varepsilon_{n_1}| < r\epsilon + \epsilon_1 < \epsilon$, from which inductively, we obtain $|B_n| < \epsilon$, for $n \geq n_1 + 1$. This shows that $\lim_{n\to\infty} B_n = 0$, as required.

□

Remark. In the above lemma, the condition $|\alpha_n| \leq r < 1$ for all n can be replaced by $|\alpha_n| \leq r < 1$ for all $n \geq N$. This is used to deal with the case $p = 2$.

3 Main Result

We will show that, for some specific choices of primes p's, the natural density of M_x does not exist. We assume from now on that p is odd.

3.1 Basic Strategy.

We use the subsets S_1 and S_2 described in Section 1.

We will find below an upper bound $U(p)$ for the supremum of $\frac{\pi_x(n)}{\frac{p^n}{n}}$ when we restrict n to S_1 and let $n \to \infty$, and also the lower bound $L(p)$ of the infimum of $\frac{\pi_x(n)}{\frac{p^n}{n}}$ when we restrict n to S_2 and let $n \to \infty$. For the natural density to exist, the necessary condition is that $U(p) \geq L(p)$. However for some choice of p's, we have $U(p) < L(p)$. This shows that at least for these p's, the natural density in question doesn't exist.

3.2 The Case $n \in S_1$.

Let's record the following result mentioned in the first section without proof.

Lemma 3.1 (Davenport) *There exists a subset S_1 of $\mathbb{N}$ such that $\frac{\phi(p^n-1)}{n} = o(\frac{p^n}{n})$ if $n \in S_1$ and $n \to \infty$.*

Now instead of showing

$$\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1) = o\left(\frac{p^n}{n}\right)$$

for $n \in S_1$ and $n \to \infty$, we will show that the ratio $\frac{\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu-1)}{\frac{p^n}{n}}$ has an upper limit for $n \in S_1$.

For $n \in S_1$, we have $\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1) = \sum_{\nu=1}^{n-1} \frac{1}{\nu}\phi(p^\nu - 1) + o(\frac{p^n}{n})$ (since the highest term is $o(\frac{p^n}{n})) \leq \sum_{\nu=1}^{n-1} \frac{1}{2\nu}p^\nu + o(\frac{p^n}{n}) = \frac{1}{2}\frac{p^{n-1}}{n-1}(1-\frac{1}{p})^{-1} + o(\frac{p^n}{n})$ (using the estimate of $\pi(n)$ with a correction of typo as above and the fact that $\phi(p^\nu - 1) \leq \frac{p^\nu - 1}{2} \leq \frac{p^\nu}{2}$, since we assume p to be odd.) Since the last expression is equal to

$$\frac{1}{2}\frac{n}{n-1}\frac{1}{p}\left(1-\frac{1}{p}\right)^{-1} \cdot \frac{p^n}{n} + o\left(\frac{p^n}{n}\right),$$

we have

$$\overline{\lim}_{n\to\infty} \frac{\sum \frac{1}{\nu}\phi(p^\nu - 1)}{\frac{p^n}{n}} \leq \frac{1}{2p}\left(1-\frac{1}{p}\right)^{-1} = \frac{1}{2(p-1)} := U(p).$$

3.3 The Case $n \in S_2$.

As in the paper, let n run through the prime numbers, which are the choice for S_2. Without using Romanoff's Theorem, we will show that for $n \in S_2$

$$\sum_{\nu=1}^{n} \frac{1}{\nu}\phi(p^\nu - 1) = O\left(\frac{p^n}{n}\right), \text{ but } \neq o\left(\frac{p^n}{n}\right),$$

and in fact we will give a more precise lower estimate.

In the following lemma, for a prime number $q \neq p$, we define $f(q)$ to be the order of p in the finite field $\mathbb{F}_q$.

Lemma 3.2 *Let $n > 2$ be a prime. Then there exists a $C > 0$ such that*

$$\prod_{f(q)=n}\left(1-\frac{1}{q}\right) \geq \prod_{2n+1\leq q\leq p^n-1,q|p^n-1}\left(1-\frac{1}{q}\right) \geq C.$$

Remark. The first inequality of the above lemma is clear, since by Fermat's lemma, $n|q-1$, so that $n|\frac{q-1}{2}$, hence $2n+1 \leq q$. In fact it is an equality if we assume that $n > \frac{p-2}{2}$.

Proof of Remark. We need to show that if $2n+1 \leq q \leq p^n-1$ and $q|p^n-1$, then $f(q) = n$. But $q|p^n-1 \Longrightarrow f(q)|n \Longrightarrow f(q) = 1$ or $f(q) = n$. If $f(q) = 1$, then $q|p-1 \Longrightarrow 2n+1 \leq q \leq p-1 \Longrightarrow n \leq \frac{p-2}{2}$, a contradiction.

Claim. $\sum_{2n+1\leq q\leq p^n-1,q|p^n-1}\frac{1}{q} \leq \frac{n\log(p)}{2n+1}$. Here, as in what follows, we follow the convention of number theory to use log as natural logarithm.

Proof of Claim. It suffices to note that each $\frac{1}{q}$ is less than or equal to $\frac{1}{2n+1}$ and there are at most $\log(p^n-1) \leq \log(p^n)$ terms. (By an easy estimate, the number of odd prime factors of m is $\leq \log(m)$.)

Sublemma. $\log(1-x) \geq -2\log(2)x$ for $0 \leq x \leq \frac{1}{2}$.

Proof. E.g. use $\frac{d^2}{dx^2}\log(1-x) < 0$.

Proof of Lemma. Combining the sublemma and the claim, we have

$$\prod_{2n+1\leq q\leq p^n-1,q|p^n-1}\left(1-\frac{1}{q}\right) \geq e^{-2\log(2)\sum_{2n+1\leq q\leq p^n-1,q|p^n-1}\frac{1}{q}} \geq e^{-2\log(2)\cdot\frac{n\log(p)}{2n+1}}.$$

Hence we may let $C = e^{-\log(2)\log(p)}$.

□

By the remark following Lemma 3.2 and the proof of Lemma 3.2, if $n > 2$ is a prime and $n > \frac{p-2}{2}$, then

$$\begin{aligned}\phi(p^n-1) &= (p^n-1)\prod_{f(q)=1}\left(1-\frac{1}{q}\right)\prod_{f(q)=n}\left(1-\frac{1}{q}\right)\\ &= (p^n-1)\prod_{q|p-1}\left(1-\frac{1}{q}\right)\cdot\prod_{2n+1\leq q\leq p^n-1,q|p^n-1}\left(1-\frac{1}{q}\right)\\ &= \frac{p^n-1}{p-1}\phi(p-1)\cdot\prod_{2n+1\leq q\leq p^n-1,q|p^n-1}\left(1-\frac{1}{q}\right)\end{aligned}$$

$$\geq \frac{p^n - 1}{p - 1}\phi(p-1) \cdot e^{-\log(2)\cdot\log(p)}.$$

Hence

$$\frac{\phi(p^n - 1)}{n} \geq \frac{p^n - 1}{n} \cdot \frac{\phi(p-1)}{p-1} \cdot e^{-\log(2)\log(p)}.$$

Therefore

$$\sum_{\nu=1}^{n} \frac{\phi(p^\nu - 1)}{\nu} \geq \frac{\phi(p^n - 1)}{n} \geq \left(\frac{\phi(p-1)}{p-1} \cdot e^{-\log(2)\log(p)} - \epsilon_n\right) \cdot \frac{p^n}{n},$$

where $\epsilon_n \to 0$ as $n \to \infty$.

Put in another way, we have

$$\underline{\lim}_{n\to\infty} \frac{\sum_{\nu=1}^{n} \frac{\phi(p^\nu - 1)}{\nu}}{\frac{p^n}{n}} \geq \frac{\phi(p-1)}{p-1} \cdot e^{-\log(2)\log(p)} = \frac{\phi(p-1)}{p-1} \cdot \frac{1}{p^{\log(2)}} := L(p).$$

Conclusion. Combining 3.2 and 3.3, we can find two subsequences $\{n_\alpha\}, \{n_\beta\}$ respectively, such that

$$\overline{\lim}_{n_\alpha\to\infty} \frac{\sum_{\nu=1}^{n_\alpha} \frac{1}{\nu}\phi(p^\nu - 1)}{\frac{p^{n_\alpha}}{n_\alpha}} \leq \frac{1}{2(p-1)}$$

and

$$\underline{\lim}_{n_\beta\to\infty} \frac{\sum_{\nu=1}^{n_\beta} \frac{1}{\nu}\phi(p^\nu - 1)}{\frac{p^{n_\beta}}{n_\beta}} \geq \frac{\phi(p-1)}{p-1} \cdot \frac{1}{p^{\log(2)}}.$$

But we can specify many p's such that $U(p) = \frac{1}{2(p-1)} < \frac{\phi(p-1)}{p-1} \cdot \frac{1}{p^{\log(2)}} = L(p)$. Therefore by 3.1, for these p's, the natural density doesn't exist.

□

Addendum. Continuing from the above setting, in fact, we can show the following

Strengthened Statement. Except possibly for $p = 2$ or $p = 3$, the natural density in question does not exist.

To prove the statement, we note that we have to show that for every odd prime p other than 3, the condition $\phi(p-1) > \frac{p^{\log(2)}}{2}$ is satisfied. For the proof, we need the following

Lemma 3.3 $\phi(n) > \frac{n}{e^\gamma \log\log(n) + \frac{3}{\log\log(n)}}$ *for* $n > 2$, *where* γ *is Euler's constant.*

Proof. See the reference of Theorem 8.8.7 of [1].

Proof of the Strengthened Statement. Let

$$g(p) = \frac{p-1}{e^{\gamma}\log\log(p-1) + \frac{3}{\log\log(p-1)}} - \frac{p^{\log(2)}}{2}.$$

Then as a function of a real variable p, $g(p)$ can be shown to satisfy $g(p) > 0$ for all $p \geq 20$.

Therefore by Lemma 3.3,

$$\phi(p-1) > \frac{p-1}{e^{\gamma}\log\log(p-1) + \frac{3}{\log\log(p-1)}} > \frac{p^{\log(2)}}{2} \text{ for all primes } p \geq 23.$$

Moreover we can verify directly that $\phi(p-1) > \frac{p^{\log(2)}}{2}$ for every prime p such that $3 < p < 23$. Consequently, the condition $\phi(p-1) > \frac{p^{\log(2)}}{2}$ is satisfied for every prime $p > 3$. This shows that for all primes other than $p = 2$ and $p = 3$, the natural density in question does not exist.

□

ACKNOWLEDGEMENTS. This article forms part of the author's thesis. The research of this particular result was done during the author's 5-month stay at NCTS of Taiwan in 2004. The author would like to thank his advisor, Professor C.-L. Chai for his encouragement, and Professor J. Yu of NCTS for his hospitality.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory (Vol I: Efficient Algorithms),* The MIT Press, Cambridge, Massachusetts, 1996.

[2] H. Bilharz, Primdivisoren mit vorgegebener Primitivwurzel, *Math. Ann.,* **114** (1937), 476 - 492.

[3] M. Rosen, *Number theory in function fields,* Graduate Texts in Math. **210**, Springer-Verlag, 2002.

Received: February, 2012