Czechoslovak Mathematical Journal

Qichun Wang; Haibin Kan

Counting irreducible polynomials over finite fields

Czechoslovak Mathematical Journal, Vol. 60 (2010), No. 3, 881–886

Persistent URL: http://dml.cz/dmlcz/140610

Czechoslovak Mathematical Journal, 60 (135) (2010), 881–886

COUNTING IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Qichun Wang, Haibin Kan, Shanghai

(Received April 1, 2009)

Abstract. In this paper we generalize the method used to prove the Prime Number Theorem to deal with finite fields, and prove the following theorem:

$$\pi(x) = \frac{q}{q-1}\frac{x}{\log_q x} + \frac{q}{(q-1)^2}\frac{x}{\log_q^2 x} + O\Big(\frac{x}{\log_q^3 x}\Big), \quad x = q^n \to \infty$$

where $\pi(x)$ denotes the number of monic irreducible polynomials in $F_q[t]$ with norm $\leqslant x$.

Keywords: finite fields, distribution of irreducible polynomials, residue

MSC 2010: 11T55

1. Introduction

Let F_q be a finite field with character p, and $N(f)$ be the norm of f which is equal to the number of elements in the quotient ring $F_q[t]/(f(t))$. We consider the irreducible polynomials in $F_q[t]$ with norm less than or equal to x.

Let $\pi(x)$ denote the number of monic irreducible polynomials in $F_q[t]$ with norm $\leqslant x$. In 1990, M. Kruse and H. Stichtenoth (see [1]) proved that

$$\pi(x) \sim \frac{q}{q-1}\frac{x}{\log_q x}, \quad x = q^n \to \infty.$$

In this paper we generalize the method used to prove the Prime Number Theorem to deal with finite fields, and prove the following more precise result:

$$\pi(x) = \frac{q}{q-1}\frac{x}{\log_q x} + \frac{q}{(q-1)^2}\frac{x}{\log_q^2 x} + O\Big(\frac{x}{\log_q^3 x}\Big),$$

where $x = q^n \to \infty$.

The work is supported by Grants with No. 60772131, NCET08, and the Ph.D. Programs Foundation of Ministry of Education of China 2009.

2. The prime number theorem for $F_q[t]$

Let $f(t)$ be a polynomial in $F_q[t]$ with degree n. It is easily seen that $N(f) = q^n$. The zeta function of $F_q[t]$ is defined as

$$\zeta(s) = \sum_f N(f)^{-s},$$

where the sum is taken over all monic polynomials in $F_q[t]$. There are q^n monic polynomials in $F_q[t]$ with degree n. Hence

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{q^n}{q^{ns}} = \sum_{n=0}^{\infty} q^{n(1-s)}$$

converges for $\mathrm{Re}(s) > 1$. Whence

$$\zeta(s) = \frac{1}{1 - q^{1-s}}. \tag{2.1}$$

Hence we obtain an analytic continuation of $\zeta(s)$ which has poles at $s = 1 + 2k\pi\mathrm{i}/\log q$, $k \in \mathbb{Z}$ and does not vanish everywhere.

Since every monic polynomial can be factored as a product of monic irreducible polynomials uniquely, we have the Euler product formula:

$$\zeta(s) = \prod_P \left(1 - \frac{1}{N(P)^s}\right)^{-1} \quad \text{for } \mathrm{Re}(s) > 1, \tag{2.2}$$

where the product is taken over all monic irreducible polynomials in $F_q[t]$. By applying logarithms to both sides in equation (2.2), and then differentiating, we obtain

$$-\frac{\zeta'}{\zeta}(s) = \sum_P \frac{N(P)^{-s} \log N(P)}{1 - N(P)^{-s}} = \sum_P \sum_{n=1}^{\infty} N(P)^{-ns} \log N(P) = \sum_f \frac{\Lambda(f)}{N(f)^s},$$

where the sum is taken over all monic polynomials in $F_q[t]$ and

$$\Lambda(f) = \begin{cases} \log N(P) & \text{if } f \text{ is a power of some irreducible polynomial } P, \\ 0 & \text{otherwise.} \end{cases}$$

From the equation (2.1), we see that

$$-\frac{\zeta'}{\zeta}(s) = \frac{q^{1-s} \log q}{1 - q^{1-s}}, \tag{2.3}$$

which has simple poles at $s = 1 + 2k\pi\mathrm{i}/\log q$, $k \in \mathbb{Z}$, and with residue 1.

Let $\psi(x) = \sum\limits_{N(f)\leqslant x} \Lambda(f)$, where f are monic polynomials in $F_q[t]$. Beginning with the fundamental line integral

$$\frac{1}{2\pi\mathrm{i}} \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} y^s \frac{\mathrm{d}s}{s} = \begin{cases} 1 & \text{if } y > 1, \\ \dfrac{1}{2} & \text{if } y = 1, \\ 0 & \text{if } y < 1, \end{cases}$$

for any $c > 1$ we have

$$\psi_0(x) = \frac{1}{2\pi\mathrm{i}} \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} -\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,\mathrm{d}s,$$

where

$$\psi_0(x) = \begin{cases} \psi(x) - \dfrac{1}{2} \sum\limits_{N(f)=x} \Lambda(f) & \text{if } x = q^n, \ \ n \in \mathbb{N}, \\ \psi(x) & \text{otherwise.} \end{cases}$$

Then by (2.3) we get

$$\psi_0(x) = \frac{1}{2\pi\mathrm{i}} \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} \frac{q^{1-s}\log q}{1-q^{1-s}} \frac{x^s}{s}\,\mathrm{d}s.$$

As a consequence of this calculus we get

Lemma 2.1. *Let $f(s)$ be continuous on $\Gamma_R\colon\ s = c + R\mathrm{e}^{\mathrm{i}\theta}$ $(\frac{1}{2}\pi \leqslant \theta \leqslant \frac{3}{2}\pi)$, and $f(s) \to 0$ as $R \to +\infty$, then $\int_{\Gamma_R} f(s)x^s\,\mathrm{d}s \to 0$ as $R \to +\infty$, for any $x > 1$.*

Let $f(s) = (q^{1-s}\log q)/(1-q^{1-s})s$. We have

$$\text{(2.4)} \qquad \frac{1}{2\pi\mathrm{i}} \int_{c-iR}^{c+iR} f(s)x^s\,\mathrm{d}s \to \psi_0(x), \quad \text{as } R \to +\infty, \text{ where } c > 1.$$

If $R = R_0 = \sqrt{(c-1)^2 + ((2k+1)^2\pi^2)/\log^2 q}$, (2.4) holds also for $k \to +\infty$.

If $\Gamma_R\colon\ s = c + R_0\mathrm{e}^{\mathrm{i}\theta}$ $(\frac{1}{2}\pi \leqslant \theta \leqslant \frac{3}{2}\pi)$, it is easily seen that we can apply Lemma 2.1 to $f(s)$. Hence we deduce the following proposition:

Proposition 2.1.

$$\psi_0(x) = \frac{q\log q}{1-q} + x\sum_{k=-\infty}^{\infty} \frac{\cos(ky)(\log q)^2 + 2k\pi\log q\sin(ky)}{(\log q)^2 + 4k^2\pi^2},$$

for any $x > 1$, *where* $y = 2\pi\log x/\log q$.

P r o o f. By Lemma 2.1 we get $\int_{\Gamma_{R_0}} f(s)x^s\,\mathrm{d}s \to 0$, as $R_0 \to \infty$ for any $x > 1$. Hence by contour integration we have

$$\psi_0(x) = \frac{q\log q}{1-q} + \sum_{k=-\infty}^{\infty} \frac{x^{1+2k\pi\mathrm{i}/\log q}}{1+2k\pi\mathrm{i}/\log q}. \tag{2.5}$$

Indeed, this is obtained by the integral on the line $\mathrm{Re}(s) = c$ and by moving it to Γ_{R_0}. The simple poles at $s = 0$, $s = 1 + 2k\pi\mathrm{i}/\log q$ produce the corresponding terms in (2.5). Since $\psi_0(x)$ is a real valued function, imaginary part of it must be zero, and the result follows. □

Corollary 2.1.

$$\sum_{k=-\infty}^{\infty} \frac{\log^2 q}{\log^2 q + 4k^2\pi^2} = \frac{q+1}{2(q-1)}\log q.$$

P r o o f. By Proposition 1 let $x = q$. We have

$$\psi_0(q) = \frac{q\log q}{1-q} + q\sum_{k=-\infty}^{\infty} \frac{\log^2 q}{\log^2 q + 4k^2\pi^2} = \frac{q}{2}\log q,$$

and the result follows. □

Let $x = q^n$. We get

$$\psi_0(q^n) = \frac{q\log q}{1-q} + q^n\sum_{k=-\infty}^{\infty} \frac{\log^2 q}{\log^2 q + 4k^2\pi^2} = \frac{(q^{n+1}+q^n-2q)\log q}{2(q-1)} \tag{2.6}$$

and

$$\psi(q^n) = \psi_0(q^n) + \frac{1}{2}\sum_{N(f)=q^n} \Lambda(f) = 2\psi_0(q^n) - \psi(q^{n-1}), \tag{2.7}$$

$$\psi(q) = q\log q. \tag{2.8}$$

Then by (2.6), (2.7) and (2.8) we deduce that

$$\psi(q^n) = \frac{q^{n+1}-q}{q-1}\log q. \tag{2.9}$$

□

Lemma 2.2.

$$\sum_{i=1}^{n} \frac{q^i}{i} = \frac{q^{n+1}}{n(q-1)} + \frac{q^{n+1}}{n^2(q-1)^2} + O\Big(\frac{q^n}{n^2}\Big), \quad \textit{as } n \to \infty.$$

Proof. We have

$$\sum_{i=1}^{n} \frac{q^i}{i} = \frac{q^n}{n} \sum_{i=0}^{n-1} \frac{nq^{-i}}{n-i} = \frac{q^n}{n}\Big(\sum_{i=0}^{n-1}\Big(1+\frac{i}{n-i}\Big)q^{-i}\Big),$$

and

$$\sum_{i=0}^{n-1} q^{-i} = \frac{q}{q-1} + O(q^{-n}),$$

$$\sum_{i=0}^{n-1} \frac{i}{n-i} q^{-i} = q^{-n} \sum_{i=1}^{n-1} \frac{n-i}{i} q^i.$$

By Poisson's summation formula we get

$$\sum_{i=1}^{n-1} \frac{n-i}{i} q^i = \frac{qn}{n-1} \sum_{i=1}^{n-2} \frac{q^i}{i(i+1)} + \frac{q}{n-1} \frac{1-q^{n-1}}{1-q} + O(n),$$

and

$$\sum_{i=1}^{n-2} \frac{q^i}{i(i+1)} = \frac{q}{q-1} \frac{q^{n-2}-1}{(n-2)(n-1)} + O\Big(\frac{q^n}{n^3}\Big).$$

Therefore

$$\sum_{i=1}^{n-1} \frac{n-i}{i} q^i = \frac{q^{n+1}}{n(q-1)^2} + O\Big(\frac{q^n}{n^2}\Big),$$

and the result follows. □

Theorem 2.1.

$$\pi(x) = \frac{q}{q-1} \frac{x}{\log_q x} + \frac{q}{(q-1)^2} \frac{x}{\log_q^2 x} + O\Big(\frac{x}{\log_q^3 x}\Big), \quad \textit{where } x = q^n \to \infty.$$

Proof. Let

$$\pi_1(x) = \sum_{N(f)\leqslant x} \frac{\Lambda(f)}{\log N(f)}.$$

We have

$$\pi_1(x) = \sum_{N(P^m)\leqslant x} \frac{\log N(P)}{m \log N(P)} = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \dots \tag{2.10}$$

$$= \pi(x) + o(x^{1/2}) \quad \text{(see [2])}.$$

□

By (2.9) and Lemma 2.2 we have

$$\pi_1(x) = \sum_{i=1}^{n} \frac{\psi(q^i) - \psi(q^{i-1})}{i \log q} = \sum_{i=1}^{n} \frac{q^i}{i} = \frac{q^{n+1}}{n(q-1)} + \frac{q^{n+1}}{n^2(q-1)^2} + O\Big(\frac{q^n}{n^2}\Big), \tag{2.11}$$

as $x = q^n \to \infty$. By (2.10) and (2.11) we deduce the theorem. □

References

[1] *M. Kruse, H. Stichtenoth*: Ein Analogon zum Primzahlsatz fur algebraische Functionenkoper. Manuscripta Math. *69* (1990), 219–221. (In German.)

[2] *H. Davenport*: Multiplicative Number Theory. Springer-Verlag, New York, 1980.

Authors' address: Q. Wang, H. Kan, The Shanghai Key Lab of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai, 200433, P. R. China, e-mail: `032018023@fudan.edu.cn`, `hbkan@fudan.edu.cn`.