Annales Univ. Sci. Budapest., Sect. Comp. 32 (2010) 95-101

SOME REMARKS ON THE AVERAGE ORDER IN CYCLIC GROUPS

I. Kátai (Budapest, Hungary)

Dedicated to Dr. János Fehér on his 70th anniversary

Abstract. The mean value of some arithmetical functions on thin sequences is investigated.

1. Notations. $\mathcal{P}$ = set of primes, p denotes a general prime number, $\pi(x) = \#\{p \leq x \mid p \in \mathcal{P}\}$, $\pi(x,k,l) = \#\{p \leq x \mid p \in \mathcal{P},\quad p \equiv l \pmod{k}\}$. $\varphi(n)$ = Euler's totient function. Let $\tau(n)$ = number of divisors of n. Let

$$\alpha(n) = \frac{1}{n}\sum_{d|n} d\varphi(d), \tag{1.1}$$

$$\beta(n) = \frac{\alpha(n)}{\varphi(n)}, \quad \gamma(n) = \frac{1}{\beta(n)}. \tag{1.2}$$

I just read an interesting paper written by J. von zur Gathen, A. Knopfmacher, F. Luca, L. G. Lucht, I. Shparlinski [1]. They estimate the mean value of $\alpha(n)$, $\beta(n)$, $\gamma(n)$. First they observe that

$$\alpha(p^k) = \frac{p^{k+1}}{p+1} + \frac{1}{p^k(p+1)}, \quad \beta(p^k) = 1 + \frac{1}{p^2-1}\left(1 + \frac{1}{p^{2k-1}}\right) \tag{1.3}$$

if p^k is a prime power, and that α and β are multiplicative functions. Then they deduce that

$$\frac{1}{x}\sum_{n\leq x} \alpha(n) - C_\alpha x = \mathcal{O}\left((\log x)^{\frac{2}{3}}(\log\log x)^{\frac{4}{3}}\right), \tag{1.4}$$

if $x \geq 3$,

$$C_\alpha = \frac{3\xi(3)}{\pi^2},$$

and that

$$\left| \frac{1}{x} \sum_{n \leq x} \beta(n) - C_\beta \right| < \frac{1}{x} \prod_{p \in \mathcal{P}} \left(1 + \frac{p+2}{p^3 - p} \right), \tag{1.5}$$

if $x \geq 1$,

$$C_\beta = \frac{105\xi(3)}{\pi^4},$$

$$\left| \frac{1}{x} \sum_{n \leq x} \gamma(n) - C_\gamma \right| \leq \frac{D}{x} \quad (x \geq 1), \tag{1.6}$$

the positive constants C_γ, D are given explicitly.

In the second half of the paper they formulate some open questions, namely the existence of the asymptotic of

$$\sum_{k \leq x} \frac{\alpha(2^k - 1)}{2^k - 1}, \quad \sum_{k \leq x} \beta(2^k - 1), \quad \sum_{p \leq x} \frac{\alpha(p-1)}{p-1}, \quad \sum_{p \leq x} \beta(p-1).$$

We shall show that this is true.

2. Let $f(n) := \frac{\alpha(n)}{n}$. Then f is multiplicative, $f(p^k) = \frac{p}{p+1} + \frac{1}{p^{2k}(p+1)}$. Let h be defined by $f(n) = \sum_{d|n} h(d)$. Then

$$h(p^k) = -\frac{p-1}{p^{2k}} \quad (k = 1, 2, \ldots),$$

consequently

$$|h(n)| \leq \frac{1}{n}.$$

We have

$$\sum_{p \leq x} f(p-1) = \sum_{d \leq x} h(d) \pi(x, d, -1) = \Sigma_1 + \Sigma_2 + \Sigma_3,$$

where in $\Sigma_1:\ d \le (\log x)^A$, in $\Sigma_2:\ (\log x)^A < d \le x^{\frac{2}{3}}$, in $\Sigma_3:\ x^{\frac{2}{3}} < d \le x$. From the Siegel-Walfisz theorem (see [1])

$$\pi(x,k,l) = \frac{1}{\varphi(k)}\mathrm{li}\ x + \mathcal{O}(xe^{-c\sqrt{\log x}})$$

uniformly as $(l,k)=1, \quad k \le (\log x)^A$, we deduce that

$$\Sigma_1 = (\mathrm{li}\ x)\sum_{d \le (\log x)^A} \frac{h(d)}{\varphi(d)} + \mathcal{O}(xe^{-c_1\sqrt{\log x}}).$$

Since $\pi(x,k,l) \le \frac{c\mathrm{li}\ x}{\varphi(k)}$ if $(l,k)=1,\ k \le x^{\frac{2}{3}}$, see [1], we have

$$\Sigma_2 \ll \sum_{d \ge (\log x)^A} \frac{h(d)}{\varphi(d)}\mathrm{li}\ x \ll (\mathrm{li}\ x)\sum_{d \ge (\log x)^A} \frac{1}{d\varphi(d)} \ll \frac{\mathrm{li}\ x}{(\log x)^A}.$$

Finally, since $\pi(x,d,1) \le \frac{x}{d}$, therefore $\Sigma_3 = \mathcal{O}(\sqrt{x})$, say. We proved:

(2.1) $$\frac{1}{\mathrm{li}\ x}\sum_{p \le x} \frac{\alpha(p-1)}{p-1} = C + \mathcal{O}\left(\frac{1}{(\log x)^A}\right),$$

(2.2) $$C = \sum_{d=1}^{\infty} \frac{h(d)}{d\varphi(d)}.$$

On the same way we can deduce that

(2.3) $$\frac{1}{\mathrm{li}\ x}\sum_{p \le x} \frac{\beta(p-1)}{p-1} = E + \mathcal{O}\left(\frac{1}{(\log x)^A}\right),$$

where

(2.4) $$E = \sum_{d=1}^{\infty} \frac{g(d)}{\varphi(d)},$$

and g is defined by $\beta(n) = \sum_{d|n} g(d)$. g is multiplicative,

$$g(p) = \beta(p) - 1 = \frac{1}{p(p-1)}, \quad g(p^k) = -\frac{1}{p^{2k-1}} \quad \text{if} \quad k \ge 2.$$

3. Let $P(x)$ be a primitive, squarefree polynomial over $\mathbb{Z}[x]$, $P(x) = c_k x^k + \cdots + c_0$, $c_0 \neq 0$, $c_k > 0$. Let D =discriminant of P. Then $D \neq 0$. Let $\rho(d)$ be the number of those residues $m \pmod d$, for which $P(m) \equiv 0 \pmod d$. Let furthermore $\tau(d)$ be those $m \pmod d$, for which $P(m) \equiv 0 \pmod d$, and $(m,d)=1$.

If is known, that ρ and τ are multiplicative, $\rho(p^\alpha) = \rho(p) \leq k$ if $p \nmid D$, and $\rho(p^\alpha) \leq C_1 D^2$, if $p \nmid D$ (see [3], and for a sharper estimate by Huxley, [4]). Furthermore, if $p \nmid Dc_0$, $(c_0 = P(0)$, then $\rho(p^\alpha) = \tau(p^\alpha)$. Let

$$U_x(d) := \#\{p \leq x \mid P(p) \equiv 0 \pmod d\}.$$

By using the Siegel-Walfisz theorem, and sieve estimates, we obtain that

$$U_x(d) = \frac{\kappa(d) \mathrm{li}\, x}{\varphi(d)} + \mathcal{O}\left(\kappa(d) e^{-c\sqrt{\log x}}\right) \tag{3.1}$$

uniformly as $d \leq (\log x)^A$, and

$$U_x(d) \ll \frac{\kappa(d) \mathrm{li}\, x}{\varphi(d)} \quad \text{if} \quad d \leq x^{\frac{4}{5}}. \tag{3.2}$$

We have

$$f(P(p)) = \frac{\alpha(P(p))}{P(p)} = \sum_{d \mid P(p)} h(d) = f_1(P(p)) + f_2(P(p)),$$

where

$$f_1(P(p)) = \sum_{\substack{d \leq x^{\frac{4}{5}} \\ d \mid P(p)}} h(d), \quad \text{and} \quad f_2 := f - f_1.$$

Since $|h(d)| \leq \frac{1}{d}$, therefore $|f_2(P(p))| \leq \frac{\tau(P(p))}{x^{\frac{4}{5}}}$. Since $\tau(P(p)) \ll x^\varepsilon$, we may assume that $f_2(P(p)) \ll x^{-\frac{1}{2}}$, say.

We have

$$\sum_{p \leq x} f(P(p)) = \sum_{p \leq x} f_1(P(p)) + \mathcal{O}(\sqrt{x}) = \\ = \sum_{d \leq x^{\frac{4}{5}}} h(d) U_x(d) + \mathcal{O}(\sqrt{x}).$$

From (3.1), (3.2), similarly as in Section 2 we deduce

Theorem 1. *Let P be as above. Then*

$$\sum_{p\le x}\frac{\alpha(P(p))}{P(p)} = A_p \mathrm{li}\, x + \mathcal{O}\left(\frac{x}{(\log x)^A}\right),$$

where

$$A_p = \sum_{d=1}^{\infty}\frac{\kappa(d)}{\varphi(d)}.$$

Similar theorems can be proved for $\sum_{n\le x}\frac{\alpha(P(n))}{P(n)}$, $\sum_{n\le x}\beta(P(n))$, $\sum_{p\le x}\beta(P(p))$.

4. Now we consider $\sum_{k\le x} f(2^k-1)$. Let $e(d)$ be the smallest k for which $2^k-1\equiv 0 \pmod d$. It is clear that finite k exists only if d is *odd*. According to a theorem of Romanov [5], and Erdős-Turán

$$\sum_{(d,2)=1}\frac{|\mu(d)|}{de(d)} < \infty \tag{4.1}$$

(see Prachar [2], Ch. V., Lemma 8.3).

Since $d_1 \mid d_2$ implies that $e(d_1)\mid e(d_2)$, therefore (4.1) implies that

$$\sum_{(d,2)=1}\frac{1}{de(d)} < \infty. \tag{4.2}$$

We have

$$\sum_{k\le x} f(2^k-1) = \sum_{\substack{d\le 2^x\\(d,2)=1}} h(d)\#\{2^k-1\equiv 0 \pmod d,\quad k\le x\} =$$

$$= \sum_{d\le x} h(d)\left(\frac{x}{e(d)}+\mathcal{O}(1)\right) + \mathcal{O}\left(\sum_{\substack{x\le d\le 2^x\\ e(d)\le x}} |h(d)|\frac{2x}{d}\right) =$$

$$= x\sum_{d\le x}\frac{h(d)}{e(d)} + \mathcal{O}\left(\sum_{d\le x}|h(d)|\right) + \mathcal{O}\left(x\sum_{d\ge x}\frac{|h(d)|}{d}\right) =$$

$$= Bx + \mathcal{O}\left(x\sum_{d>x}\frac{|h(d)|}{e(d)}\right) + \mathcal{O}(\log x),$$

where

$$B=\sum_{(d,2)=1}\frac{h(d)}{e(d)}. \tag{4.3}$$

From (4.2) and $|h(d)|=\frac{1}{d}$ we obtain that B is convergent. If we use the estimate

$$\#\{d\le x\mid e(d)\le(\log d)^2\}\ll\frac{x}{(\log x)^2} \tag{4.4}$$

due to Erdős and Turán (see Prachar, [2] Ch. V. (8.12)) we obtain that

$$\sum_{2^jx<d<2^{j+1}x}\frac{|h(d)|}{e(d)}\ll\frac{1}{2^jx(\log 2^jx)}\frac{2^{j+1}x}{(\log 2^jx)^2}+\frac{1}{\log^2 2^jx}$$

and so

$$\sum_{d>x}\frac{|h(d)|}{e(d)}\ll\sum_{j=0}^{\infty}\frac{1}{(\log x+j\log 2)^2}\ll\frac{1}{\log x}.$$

Consequently the following assertion holds.

Theorem 2. *We have*

$$\sum_{k\le x}f(2^k-1)=Bx+\mathcal{O}\left(\frac{x}{\log x}\right).$$

Similarly we can prove that

$$\sum_{k\le x}\beta(2^k-1)=\mathcal{S}x+\mathcal{O}\left(\frac{x}{\log x}\right),$$

$$\mathcal{S}=\sum_{(d,2)=1}\frac{g(d)}{e(d)}.$$

References

[1] **von zur Gathen J., Knopfmacher A., Luca F., Lucht L.G. and Shparlinski I.,** Average order in cyclic groups, *J. Theor. Nombres Bordeaux,* **16** (2004), 107-123.

[2] **Prachar K.,** *Primzahlverteilung,* Springer Verlag, Berlin, 1957.

[3] **Nagell T.,** *An introduction to number theory,* Chelsea, New York, 1964.

[4] **Huxley M.N.,** A note on polynomial congruences, *Recent progress in analytic number theory, Vol. I., Durham, 1979,* Academic Press, 1981, 193-196.

[5] **Romanov N.P.,** Über einzige Sätze der additiven Zahlentheorie, *Math. Ann.,* **109** (1934), 668-678

[6] **Erdős P. and Turán P.,** Ein zahlentheoretischer Satz, *Mitt. Forsch. Inst. Math. u. Mech. Univ. Tomsk,* **1** (1935), 101-103.

(Received March 14, 2008)

I. Kátai
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter sét. 1/C
H-1117 Budapest, Hungary
katai@compalg.inf.elte.hu