Cyclic Group Orders

Steven Finch

April 28, 2006

Let $\mathbb{Z}_n$ denote the cyclic group (under addition) of integers modulo n. Given $m \in \mathbb{Z}^+$ and $x \in \mathbb{Z}_n$, define mx to be $\sum_{k=1}^{m} x$. The **order** of $x \in \mathbb{Z}_n$ is the least $m > 0$ such that $mx = 0$. Clearly $\operatorname{ord}(x)$ divides n and, for each divisor d of n, there are precisely $\varphi(d)$ elements in $\mathbb{Z}_n$ of order d. Define the **average order** in $\mathbb{Z}_n$ to be [1]

$$\alpha(n) = \frac{1}{n} \sum_{x \in \mathbb{Z}_n} \operatorname{ord}(x) = \frac{1}{n} \sum_{d|n} d\, \varphi(d).$$

Asymptotically, we have

$$\sum_{n \leq N} \alpha(n) \sim \frac{\zeta(3)}{2\zeta(2)} N^2 = \frac{3\zeta(3)}{\pi^2} N^2 = (0.3653814847...)N^2$$

as $N \to \infty$. Variations of this result include [1, 2]

$$\sum_{n \leq N} \frac{\alpha(n)}{n} \sim \frac{\zeta(3)}{\zeta(2)} N = \frac{6\zeta(3)}{\pi^2} N = (0.7307629694...)N,$$

$$\sum_{n \leq N} \frac{\alpha(n)}{\varphi(n)} \sim \frac{\zeta(3)\zeta(4)}{\zeta(8)} N = \frac{105\zeta(3)}{\pi^4} N = (1.2957309578...)N,$$

$$\sum_{n \leq N} \frac{n}{\alpha(n)} \sim C_1 N, \qquad \sum_{n \leq N} \frac{\varphi(n)}{\alpha(n)} \sim C_2 N$$

where

$$C_1 = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \left(1 + \frac{1}{p}\right) \sum_{k=1}^{\infty} \frac{1}{p^k + p^{-k-1}}\right) = 1.4438675...,$$

$$C_2 = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \left(1 - \frac{1}{p^2}\right) \sum_{k=1}^{\infty} \frac{1}{p^k + p^{-k-1}}\right) = 0.8014696934...,$$

Let $\mathbb{F}_q^*$ denote the cyclic group (under multiplication) of nonzero elements of $\mathbb{F}_q$, the field of size q. It is well-known that q must be a prime power. The order of $x \in \mathbb{F}_q^*$ is the least $m > 0$ such that $x^m = 1$ and the average order in $\mathbb{F}_q^*$ is

$$\alpha(q-1) = \frac{1}{q-1} \sum_{x \in \mathbb{F}_q^*} \operatorname{ord}(x) = \frac{1}{q-1} \sum_{d \mid q-1} d\, \varphi(d).$$

We examine two cases: the first when q is actually a prime [2, 3]:

$$\sum_{q \le Q} \frac{\alpha(q-1)}{q-1} \sim C_3 \frac{Q}{\ln(Q)}, \qquad \sum_{q \le Q} \frac{\alpha(q-1)}{\varphi(q-1)} \sim C_4 \frac{Q}{\ln(Q)}$$

where

$$C_3 = \prod_p \left(1 - \frac{p}{p^3-1}\right) = 0.5759599688...$$

is Stephens' constant [4, 5],

$$C_4 = \prod_p \left(1 + \frac{p+1}{(p-1)^2(p^2+p+1)}\right) = 1.5664205124...;$$

and the second when $q = 2^k$ for some $k \ge 1$ [2, 3]:

$$\sum_{k \le K} \frac{\alpha(2^k-1)}{2^k-1} \sim C_5 K, \qquad \sum_{k \le K} \frac{\alpha(2^k-1)}{\varphi(2^k-1)} \sim C_6 K$$

where

$$C_5 = \sum_{\substack{n \ge 1, \\ n \text{ odd}}} \frac{f(n)}{t(n)} = 0.786125..., \qquad C_6 = \sum_{\substack{n \ge 1, \\ n \text{ odd}}} \frac{g(n)}{t(n)} = 1.102488....$$

In the preceding formulas, f and g are multiplicative functions with

$$f(p^r) = -\frac{p-1}{p^{2r}}, \qquad g(p^r) = \begin{cases} \dfrac{1}{p(p-1)} & \text{if } r = 1, \\ -\dfrac{1}{p^{2r-1}} & \text{if } r \ge 2 \end{cases}$$

and $t(n)$ is the order of the element 2 in $\mathbb{Z}_n^*$, the group (under multiplication) of integers relatively prime to n [6]. If we replace α by φ, the following emerge [1, 4]:

$$\sum_{q \le Q} \frac{\varphi(q-1)}{q-1} \sim C_7 \frac{Q}{\ln(Q)}, \qquad \sum_{k \le K} \frac{\varphi(2^k-1)}{2^k-1} \sim C_8 K$$

where

$$C_7 = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136...$$

is Artin's constant [5],

$$C_8 = \sum_{\substack{n\geq 1,\\ n \text{ odd}}} \frac{\mu(n)}{n\,t(n)} = 0.73192...,$$

and μ is the Möbius mu function. Also, we have extreme results [1, 7]:

$$1 = \liminf_{n\to\infty} \frac{\alpha(n)}{\varphi(n)} < \limsup_{n\to\infty} \frac{\alpha(n)}{\varphi(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} = \frac{315}{2\pi^4}\zeta(3) = 1.9435964368....$$

The study of the average order $\xi(n)$ in $\mathbb{Z}_n^*$ was initiated in [8]. We have extreme results

$$\liminf_{n\to\infty} \frac{\xi(n)\ln(\ln(n))}{\lambda(n)} = \frac{e^{-\gamma}\pi^2}{6}, \qquad \limsup_{n\to\infty} \frac{\xi(n)}{\lambda(n)} = 1$$

where $\lambda(n)$ is the **reduced totient** or **Carmichael function** [9]:

$$\lambda(n) = \begin{cases} \varphi(n) & \text{if } n = 1, 2, 4 \text{ or } q^j, \text{ where } q \text{ is an odd prime and } j \geq 1, \\ \varphi(n)/2 & \text{if } n = 2^k, \text{ where } k \geq 3, \\ \operatorname{lcm}\left\{\lambda(p_j^{e_j}) : 1 \leq j \leq l\right\} & \text{if } n = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}, \text{ where } 2 \leq p_1 < p_2 < \ldots \text{ and } l \geq 2. \end{cases}$$

Observe that $\lambda(n)$ is the size of the largest cyclic subgroup of $\mathbb{Z}_n^*$. A mean result [8, 9]:

$$\frac{1}{N}\sum_{n\leq N} \xi(n) = \frac{N}{\ln(N)} \exp\left[\frac{C_9 \ln(\ln(N))}{\ln(\ln(\ln(N)))}\left(1 + o(1)\right)\right]$$

holds as $N \to \infty$, where

$$C_9 = e^{-\gamma} \prod_p \left(1 - \frac{1}{(p-1)^2(p+1)}\right) = 0.3453720641....$$

There is a set S of positive integers of asymptotic density 1 such that, for $n \in S$,

$$\xi(n) = \frac{n}{(\ln(n))^{\ln(\ln(\ln(n))) + C_{10} + o(1)}}$$

and

$$C_{10} = -1 + \sum_p \frac{\ln(p)}{(p-1)^2} = 0.2269688056...;$$

it is not known whether $S = \mathbb{Z}^+$ is possible.

A different study of periodicity properties of $\{x^k\}_{k=0}^{\infty}$ for each $x \in \mathbb{Z}_n$ (including $\mathbb{Z}_n^*$ and more) has also been undertaken [10, 11]. The constants C_3 and C_9 moreover appear in theorems proved [12, 13, 14] assuming the Generalized Riemann Hypothesis.

References

[1] J. von zur Gathen, A. Knopfmacher, F. Luca, L. G. Lucht and I. E. Shparlinski, Average order in cyclic groups, *J. Théor. Nombres Bordeaux* 16 (2004) 107–123; MR2145575 (2006d:11111).

[2] K.-H. Indlekofer, S. Wehmeier and L. G. Lucht, Mean behaviour and distribution properties of multiplicative functions, *Comput. Math. Appl.* 48 (2004) 1947–1971; MR2116969 (2005m:11168).

[3] F. Luca, Some mean values related to average multiplicative orders of elements in finite fields, *Ramanujan J.* 9 (2005) 33–44; MR2166376.

[4] P. J. Stephens, An average result for Artin's conjecture, *Mathematika* 16 (1969) 178–188; MR0498449 (58 #16565).

[5] S. R. Finch, Artin's constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 104–109.

[6] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A002326.

[7] S. R. Finch, Euler totient constants, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 115–118.

[8] F. Luca and I. E. Shparlinski, Average multiplicative orders of elements modulo n, *Acta Arith.* 109 (2003) 387–411; MR2009051 (2004i:11113).

[9] P. Erdös, C. Pomerance and E. Schmutz, Carmichael's lambda function, *Acta Arith.* 58 (1991) 363–385; MR1121092 (92g:11093).

[10] S. Finch and P. Sebah, Squares and cubes modulo n, math.NT/0604465.

[11] S. Finch, Idempotents and nilpotents modulo n, math.NT/0605019.

[12] P. Kurlberg and C. Pomerance, On a problem of Arnold: The average multiplicative order of a given integer, *Algebra Number Theory* 7 (2013) 981–999; arXiv:1108.5209; MR3095233.

[13] S. Kim, Average results on the order of a modulo p, arXiv:1509.01752.

[14] S. Kim, An average result on the order of a modulo n, arXiv:1509.03768.