On multiplicative order of elements in finite field extension generated by a root of unity

Roman Popovych

A partition of an integer C is a sequence of non-negative integers $u_1, ..., u_C$ such that $\sum_{j=1}^{C} ju_j = C$. $U(C,d)$ is the number of such partitions of C, for which $u_1, ..., u_C \leq d$. Let q be a power of a prime number p, F_q a finite field with q elements, F_q^* the multiplicative group of F_q. Field extensions based on cyclotomic polynomials are considered in [**1, 5, 6**]. Let $r \geq 3$ be a prime number coprime with q, q a primitive root modulo r, that is the multiplicative order of q modulo r equals $r-1$. Set $F_q(\theta) = F_{q^{r-1}} = F_q[x]/\Phi_r(x)$, where $\Phi_r(x) = x^{r-1} + x^{r-2} + ... + 1$ is the r-th cyclotomic polynomial and θ is the coset of x modulo $\Phi_r(x)$. Clearly $\theta^r = 1$.

The problem of finding lower bounds on the order of elements in the extensions based on cyclotomic polynomials was, in particular, considered in [**1, 5, 6**]. Lower bound on the order of the Gauss period and some similar elements was given in [**1, 5**]. Voloch (see [**4, 6**]) gave lower bound on the orders for all elements in the extensions. He showed that, for $R(x) \in F_q[x]$, $R(x)$ not a monomial, $R(\theta)$ has the order at least $\exp(r^\delta)$ for some constant δ. Theorem 1 below also gives explicit lower bound on multiplicative orders of all elements in the extensions, but the bound does not depend on any unknown constant.

Theorem 1. *Let q be a power of prime number p, $r \geq 3$ a prime number coprime with q, q a primitive root modulo r, θ generates the extension $F_q(\theta)$. Let $0 \leq e \leq r-1$, $1 \leq f \leq g \leq r-2$; w_g, w_f, w_0 belong to F_q^* and $c = \lfloor (r-1)/g \rfloor - 1$. Then $\theta^e(\sum_{i=f}^{g} w_i\theta^i + w_0)$ has the order at least $U(c, p-1)$.*

Corollary 1. [**1**, theorem 1]. *The Gauss period $\theta + \theta^{-1}$ has the order at least $U((r-1)/2, p-1)$.*

Corollary 2. *Let $1 \leq f \leq g \leq r-2$; w_g, w_f, w_0 belong to F_q^*, $c = \lfloor (r-1)/g \rfloor - 1$ and $T(\theta) = \sum_{i=f}^{g} w_i\theta^i + w_0$. Then $\theta^i T(\theta^j)$ for $0 \leq i, j \leq r-1$ has the order at least $U(c, p-1)$.*

We use known estimates [**2, 3**] and Corollary 2 to derive explicit lower bound in terms of p and c (depends on r, g) in the most interesting case when c is large comparatively to p.

Corollary 3. *Let $1 \leq f \leq g \leq r-2$; w_g, w_f, w_0 belong to F_q^*, $c = \lfloor (r-1)/g \rfloor - 1$ and $T(\theta) = \sum_{i=f}^{g} w_i\theta^i + w_0$. If $c \geq p^2$, then $\theta^i T(\theta^j)$ for $0 \leq i, j \leq r-1$ has the order larger than $\left(\frac{p(p-1)}{160c}\right)^{\sqrt{p}} \exp\left(\pi\sqrt{\frac{2}{3}(1-\frac{1}{p})c}\right)$.*

References

1. O. Ahmadi, I. E. Shparlinski and J. F. Voloch, *Multiplicative order of Gauss periods*, Intern. J. Number Theory **6** (2010), no. 4, 877–882.
2. G. E. Andrews, *The Theory of Partitions*, Addison-Wesley, Reading, 1976.
3. A. Maroti, *On elementary lower bounds for the partition function*, Integers **3** (2003), A10.
4. G. L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, Boca Raton, 2013.
5. R. Popovych, *Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$*, Finite Fields Appl. **18** (2012), no. 4, 700–710.
6. J. F. Voloch, *On the order of points on curves over finite fields*, Integers **7** (2007), A49.

Contact information

Roman Popovych
Department of Specialized Computer Systems, Lviv Polytechnic National University, Lviv, Ukraine
Email address: rombp07@gmail.com

Key words and phrases. Finite field, multiplicative order, lower bound

Algebraic structures in the theory of fractals (fractal geometry and fractal analysis)

Mykola Pratsiovytyi

The fractal is a set of complete metric space that have the property of self-similarity in some sense (classic self-similarity, self-affinity or "structural similarity") or have fractional metric dimension (like a Hausdorff–Besicovitch or Minkowski dimension, entropic or box-counting dimension) as well as such that its metric and topological dimension are unequal.

The publication of Felix Hausdorff's paper "Dimension und äußeres Maß", Math. Ann. **79** (1919), 157–179, should be considered as the birth of the theory of fractals. Hausdorff introduced the definition of fractal set and initiated the study of such sets using the so-called Hausdorff measures constructed by the C. Carathéodory principle. Before this, there was some interest to various sets (figures), which are called the simplest (self-similar) fractals today. Cantor set, Sierpiński carpets and Koch snowflake are among them. Thus, 100th anniversary of the theory of fractals is celebrated this year. The results of A. S. Besicovitch, P. Billingsley, H. G. Eggleston, John E. Hutchinson and other authors were stages in the history of development of this theory. The interest to the theory of fractals has increased after publication of Benoit B. Mandelbrot's book as well as various monographs and handbooks devoted to fractals and their applications.

Today fractals appear in different fields of mathematics. Many objects of continuous mathematics have fractal properties, namely, objects such that their essential sets have fractal structure. Functions, measures, transformations of space, dynamical systems etc. are among them. Some of such objects are directly related or induced by algebraic structures in the phase space. Some representatives of groups of similarity transformations, groups of affine transformations, and linear spaces can be used for construction of systems of encoding of real numbers and for development of the corresponding analytic theory for definition and studying of fractal objects. We understand the fractality of these objects in different ways.

The talk is devoted to functions, probability measures and transformations of Euclidean space. They have sets of various peculiarities with fractal structure, supports of distribution and attractors of dynamical systems as well as transformations defined by invariants related to fractal characteristics, dimension, self-similarity, etc. Systems of self-similar representations, functions preserving frequency of digits of representation, their mean values, tails of representation etc. as well as measures with self-similar essential supports of distribution are studied in detail.

We focus on the normal properties of numbers (on the base of Lebesgue measure). For systems of representation with constant and variable alphabet, problems of probabilistic theory of numbers defined by the system of invariants of representation are also discussed.