

Elements of high order in some Finite fields

May 5, 2011

Abstract

1 Multiplicative generator for some finite field

Notations:

Let $\mathbb{F}_{p^p} = \mathbb{F}[x]/(x^p - x - 1)$ be the finite field with p^p elements,

Conjecture 1.1. *Is \bar{x} a multiplicative generator of the norm 1 subgroup in $\mathbb{F}_{p^p}^*$? Equivalently, this is asking if $\text{ord}(\bar{x}) = \frac{p^p-1}{p-1} = p^{p-1} + p^{p-2} + \dots + 1 =: N_p$.*

2 Attack 1: Prime Factorization

Naively, the order of $\langle \bar{x} \rangle$ is a factor of N_p . In [MNW] it is stated that the current status of factoring N_p is around the level $137 < p < 173$, with some factorization not complete. However, it is also summarized in their paper some patterns of the prime factors of N_p , we list them in the following:

1. (Euler) When p is odd, every prime factors of N_p has the form $2kp + 1$.
2. If $2p + 1$ is prime and $q \equiv 1 \pmod{4}$, then $2p + 1 | N_p$.
3. If $4p + 1$ is prime, then $4p + 1 | N_p$. In general, if p is just an odd integer, m positive s.t. $4m^2p + 1$ is prime, then $4m^2p + 1 | p^{m^2p} - 1$.
4. Heuristically, fix k and varies p . If k odd, and $2kp + 1$ is a prime, then the probability that $2kp + 1 | N_p$ is approximately $\frac{1}{k}$. For k even it is approximately $\frac{1}{2k}$. Anomalies lie in the case when $k = 2m^2$ for some m , where the probability is $\frac{4}{k}$.

For more general results of this sort see [MNW].

2.1 An analogy

I can not pass this result without mentioning it, though it does not apply to our problem:

Theorem 2.1. *([Chung]) For $\mathbb{F}_{p^d} = \mathbb{F}[x]/(f(x))$, every element in \mathbb{F}_{p^d} can be written as $(x+a_1) \cdots (x+a_m)$ for $a_i \in \mathbb{F}_p$ if $\sqrt{p} > d - 1$ and $m \geq \frac{2d+4d \log d}{\log p - 2 \log(d-1)}$.*

3 Attack 2: Permutation of cycles

Denote $\bar{a} := (a_0, a_1 \cdots, a_{p-1})$. Define the map

$$\rho : \mathbb{Z}^p \rightarrow \mathbb{Z}, \rho(\bar{a}) = a_0 + a_1p + \cdots + a_{p-1}p^{p-1}$$

Give \mathbb{Z}^p the reverse lexicographic ordering, then ρ is an order preserving map to \mathbb{Z} .
 Look at the map: $\phi : \mathbb{Z}^p \rightarrow \mathbb{F}_{p^p}$,

$$\phi(\bar{a}) := x^{\rho(\bar{a})} = x^{a_0}(x+1)^{a_1} \dots x^{a_{p-1}}$$

The kernel of ϕ is a lattice in \mathbb{Z}^p , denote it by K . We have

$$0 \rightarrow K \rightarrow \mathbb{Z}^p \rightarrow \langle \bar{x} \rangle \rightarrow 0$$

In particular, $\text{covol}(K) = \text{ord}(\bar{x})$, $(1, 1, 1 \dots, 1) \in K$. We want to know if $(1, 1, 1 \dots, 1)$ is the minimum element in K with respect to the reverse lexicographic ordering. In other words, we can ask if there is a p -tuple \bar{a} s.t. $0 \leq a_i \leq p-1$, $\bar{a} < (1, 1 \dots, 1)$, and $\sum_{i=0}^{p-1} a_i p^i$ is the order of \bar{x} . WLOG we can have $a_0 = 1$, $a_{p-1} = 0$. A priori, not every $\rho(\bar{a})$ could be the order of \bar{x} . Denote the absolute Frobenius morphism by $Fr \in \text{Gal}(\mathbb{F}_{p^p}/\mathbb{F}_p)$. $Fr(a_0, a_1 \dots a_{p-1}) = (a_1, \dots, a_{p-1}, a_0)$ cycles the coordinates around. Let's look at the linear span $\oplus c_i Fr^i(\bar{a})$, with $c_i \in \mathbb{Z}$. There is a unique nonzero minimal element in the linear space with regard to the reverse lexicographic ordering. Only such minimal element in its linear span could be a candidate to give the correct order of $\langle \bar{x} \rangle$.

4 Attack 3: A Naive restriction on the volume

In particular, if it happens that $Fr^j(\bar{a})$ generate a full dimensional sub-lattice in K , (how often does that happen?), then $\text{covol}(Fr^j(\bar{a})) \geq \text{covol}(K) = \sum_{i=0}^{p-1} a_i p^i$.

Denote the complex p -th roots of unity by ζ_p , by elementary matrix operation,

$$\text{covol}(Fr^j(\bar{a})) = \det(Fr^j(\bar{a})) = \prod_{j=0}^{p-1} (a_0 + a_1 \zeta_p^j + a_2 \zeta_p^{2j} \dots a_{p-1} \zeta_p^{j(p-1)}) =: \Pi^*$$

One can eliminate those p -tuples s.t. $\Pi^* < \sum_{i=0}^{p-1} a_i p^i$. The nice thing for this expression is that it relates our problem to describe norm of elements in a cyclotomic number field. Though it is hard to estimate it as an exponential sum.

Unfortunately, the above inequality does not hold for all interesting elements in K . Let's go back to the determinant. Before doing anything, the determinant is always a homogeneous polynomial in p variables, whereas the linear expression in $\text{rho}(\bar{a})$ only equips a_{p-1} with a coefficient with magnitude of p^{p-1} . Numerical experiment for small p suggests the above restriction doesn't rule out a big portion of \bar{a} to check. (Does it suggest if such a p -tuple is really the order of \bar{x} , a_0 should be relatively large, and a_{p-1} should be relatively small?)

Let's summarize the above:

If $Fr^j(a_0, a_1, \dots, a_{p-1})$ for $j = 0, 1, \dots, p-1$ generate a full dimension sub-lattice in K , and

$$\prod_{j=0}^{p-1} (a_0 + a_1 \zeta_p^j + a_2 \zeta_p^{2j} \dots a_{p-1} \zeta_p^{j(p-1)}) = Nm_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(a_0 + a_1 \zeta_p + a_2 \zeta_p^2 \dots a_{p-1} \zeta_p^{p-1}) < \frac{\sum_{i=0}^{p-1} a_i p^i}{\sum_i a_i}$$

Then $\sum_{i=0}^{p-1} a_i p^i$ can not be the order of \bar{x} . Here $0 \leq a_i \leq p-1$ for $i = 0, \dots, p-2$, $a_0 = 1$, $a_{p-1} = 0$. I don't know if this combined with Attack 2 will give us any interesting result.

5 Geometry of numbers and packing

It can be proved by elementary estimation that the convex symmetric region $V := \sum_i |a_i| < p$ has only trivial intersection with K . By Minkowski's bound, we have $\frac{\text{vol}(V)}{2^p \text{covol}(K)} \leq 1$. It is trivial calculus that

$$\text{vol}(V) = 2^p \int_{\sum a_i < p, a_i > 0} da_1 \dots da_{p-1} = \frac{p^p}{2^p p!}$$

Therefore $\text{covol}(K) \geq \frac{p^p}{p!} \approx e^p$.

Here V is an p -dimensional cross-polytope, dual to the p -dimension cube. If we can have a bound on the packing density $\frac{\text{vol}(V)}{2^p \text{covol}(K)} \leq \delta_p$ one could do better on the above bound. As far as I know, an upper bound for the packing density for cross-polytope is not known in dimension higher than 3. However, there do exist a lower bound (Minkowski-Hlawka) (cf [Rush],[Ro]): $\delta_n \geq 2^{-n(1+o(1))}$. Since we want δ_p to drop quickly as p increases, this gives us a limit on the best we can do for considering packing densities for corss-polytopes. Suppose the lower bound were the upper bound, we could get at best $\text{covol}(K) \geq (2(1+o(1))e)^p$, which is comparable to Voloch's bound below.

Let's look at some case when we do know the bound for a packing density, namely we can look at the inscribed spheres in V .

S is the hyper-sphere inscribed in V , it has radius \sqrt{p} .

$$\text{vol}(S) \approx \frac{(2\pi p)^{\frac{p}{2}}}{p!!} \approx (2\pi e)^{\frac{p}{2}}$$

For (lattice) sphere packing, one has $\frac{\text{vol}(S)}{2^p \text{covol}(K)} \leq \frac{p+2}{\sqrt{2^{p+2}}}$

$\text{covol} \geq (\sqrt{\pi e})^p \approx (2.92)^p$.

Note here the radius the sphere can not be any larger as the point $(1, \dots, 1)$ lies already on the boundary of the sphere.

I don't know if one can find a bigger star shaped region than V and use upper bound on packing density there.

5.1 Bounds Known in the Literature

Voloch mentioned in mathoverflow that he prove in the paper [Vo] that $\text{covol}(K) \geq 2^{2 \cdot 54p}$ using techniques from estimations for the primality testing algorithm in [AKS]. Though in his paper it is only obvious to me that he proved $\text{covol}(K) \geq 2^{2p}$. Such a result is also mentioned in [Qi].

6 Attack from Geometry

In another paper [Vo2] has another method to get elements of high order in finite field:

Theorem 6.1. *Let $f(x, y) \in \mathbb{F}_q[x, y]$ be an absolutely irreducible polynomia s.t. $f(x, 0)$ is not a monomial. Given $\epsilon > 0$, there exist $\delta_f > 0$ s.t. if $(a, b) \in \mathbb{F}_q^*$ satisfies $f(a, b) = 0$ and $d := [\mathbb{F}_q(a) : \mathbb{F}_q]$ large, but the multiplicative order of a is smaller than $d^{2-\epsilon}$, then the multiplicative order for b is at least $\exp(\delta(\log d)^2)$.*

From this theorem, it seems that if one wants to prove b has high multiplicative order, he only need to find (better fixed) $f(x, y)$ and (various) a s.t. $f(a, b) = 0$ but a has high degree and small multilicative order.

A little caution is needed when one wants to apply ths theorem. The trick here is that δ_f is related to $f(x, y)$. Suppose an absolutely irreducible $f(x, y)$ satisfying the above condition is "separable", $f(x, y) = f_1(x) + (y - 1)$, then for whichever $f_1(a) = 0$, we know $b = 1$ has multiplicative order 1.

References

- [AKS] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, Primes is in P, Annlas of math, 160(2004), 781-793.
- [Chung] F.R.K.Chung, Diameters and Eigenvalues, Journal of the AMS, Volume 2, Number 2, April 1989, page 187-196.

- [Qi] Qi Cheng, Constructing finite field extensions with large order elements, SODA '04 Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms.
- [MNW] Peter L.Montgomery, Sangil Nahm, Samuel S.Wagstaff, Jr The Period of the Bell Numbers Modulo a Prime, Mathematics of Computation, Vol 79, Number 271, July 2010, Page 1793-1800.
- [Ro] C.A.Rogers, Existence Theorems in the Geometry of Numbers, Annals of math, Vol 48, No.4, 1947, page 994-1002.
- [Rush] J.A.Rush, A Lower Bound on Packing Density, Inventiones, Vol 98, Number 3, page 499-509.
- [Vo] Jose.F.Voloch, On some subgroups of the multiplicative group of finite rings, preprint.
- [Vo2] Jose.F.Voloch, On the order of points on curves over finite fields, preprint.