Journal de Théorie des Nombres
de Bordeaux **16** (2004), 233–239

On some subgroups of the multiplicative group of finite rings

par José Felipe VOLOCH

Résumé. Soit S un sous-ensemble de $\mathbf{F}_q$, le corps à q éléments et $h \in \mathbf{F}_q[x]$ un polynôme de degré $d > 1$ sans racines dans S. On considère le groupe généré par l'image de $\{x - s \mid s \in S\}$ dans le groupe des unités de l'anneau $\mathbf{F}_q[x]/(h)$. Dans cet article nous présentons les bornes inférieures pour le cardinal de ce groupe. Notre motivation principale est une application au nouvel algorithme polynomial pour tester la primalité [AKS]. Ces bornes ont également des applications à la théorie des graphes et pour majorer le nombre de points rationnels sur les revètement abeliens de la droite projective sur les corps finis.

Abstract. Let S be a subset of $\mathbf{F}_q$, the field of q elements and $h \in \mathbf{F}_q[x]$ a polynomial of degree $d > 1$ with no roots in S. Consider the group generated by the image of $\{x - s \mid s \in S\}$ in the group of units of the ring $\mathbf{F}_q[x]/(h)$. In this paper we present a number of lower bounds for the size of this group. Our main motivation is an application to the recent polynomial time primality testing algorithm [AKS]. The bounds have also applications to graph theory and to the bounding of the number of rational points on abelian covers of the projective line over finite fields.

Introduction

Let S be a subset of $\mathbf{F}_q$, the field of q elements and $h \in \mathbf{F}_q[x]$ a polynomial of degree $d > 1$ with no roots in S. Consider the group G generated by the image of $\{x - s \mid s \in S\}$ in the group of units U of the ring $R = \mathbf{F}_q[x]/(h)$. In this paper we present a number of lower bounds for the size of G. We retain the above notation throughout the paper.

Our main motivation is the recent polynomial time primality testing algorithm [AKS]. A lower bound for the size of G features essentially in their argument and improvements on this bound lead to improvements to the running time of their algorithm. We will discuss some of these improvements in the last section.

Manuscrit reçu le 25 septembre 2002.

Such groups occur in many other contexts. For instance, Chung [C], showed that when q is sufficiently large and $S = \mathbf{F}_q$, then G is the whole group of units of R and the Cayley graph of G with the above generators is a graph with good expander properties. See also [Co], [K]. The group G and similar groups also appear in the index calculus method of computing discrete logarithms in finite fields.

We use different techniques according to whether $|S|$ is large or small.

1. Small $|S|$

In [AKS] they notice that, with notation as in the introduction, $|G| \geq \binom{d+|S|-1}{|S|}$ since the polynomials in the set $\{\prod_{s\in S}(x-s)^{a_s} \mid \sum_{s\in S} a_s < d\}$ are all distinct modulo h. The following result improves this when $|S| < d$.

Theorem 1. *With notation as in the introduction, assume further that q is prime and that $q > (7d - 2|S|)/5$. Then G has cardinality at least*

$$\frac{1}{2}\binom{[(6d+4|S|)/5]}{|S|}.$$

Proof. Consider the set $\{\prod_{s\in S}(x-s)^{a_s} \mid \sum_{s\in S} a_s \leq (6d-|S|)/5\} \subset \mathbf{F}_q[x]$. We claim that at most two elements of this set can lie in the same congruence class modulo h. It is clear that the claim implies the theorem.

To prove the claim, let A, B, C be polynomials of the form $\prod_{s\in S}(x-s)^{a_s}$ such that $A \equiv B \equiv C \pmod h$, with $\max\{\deg A, \deg B, \deg C\} = d+\delta$ with δ as small as possible (note that, clearly, $\delta \geq 0$). Write $A-B = fh$, $A-C = gh$, where $f, g \in \mathbf{F}_q[x], \deg f, \deg g \leq \delta$. We have then $(g-f)A - gB + fC = 0$. Let D be the greatest common divisor of $(g-f)A, gB, fC$. Let us prove that $D|fg(f-g)$. Indeed, let r be an irreducible polynomial with $r^n||D$. If r^n divides either f or g, we are done. Otherwise, r divides B and C and by the minimality of δ it cannot divide A, so r^n must divide $f-g$ and this proves that $D|fg(f-g)$ which entails that $\deg D \leq 3\delta$.

We now apply the ABC theorem to $(g-f)A/D - gB/D + fC/D = 0$. (Note that we may assume $d+\delta < q$ for otherwise the claim will follow from the hypothesis that $q > (7d-2|S|)/5$). One of the summands has degree at least $\max\{\deg A, \deg B, \deg C\} - \deg D \geq d - 2\delta$. On the other hand, the conductor of the product of the summands divides $fg(f-g)\prod_{s\in S}(x-s)$, therefore $d - 2\delta < |S| + 3\delta$. It follows that $d + \delta > (6d - |S|)/5$, proving the claim and the theorem. □

Remark. D. Bernstein pointed out that, with a bit more care, one can replace $[(6d + 4|S|)/5]$ with $[(3d + |S|)/2]$ in the theorem. He has also improved the result by allowing multiple congruences. See [B2].

Theorem 2. *If* $|S| \geq d/2$ *then*

$$|G| \geq \binom{|S| + d/2 - 1}{|S|}\binom{|S| - 1}{|S| - d/2}.$$

Proof. Consider the set of rational functions

$$\{\prod_{s\in S}(x-s)^{a_s} \mid a_s \in \mathbf{Z}, \sum_{a_s>0} a_s, \sum_{a_s<0} -a_s < d/2\}.$$

They are all distinct, for distinct choices of the a_s and moreover they are distinct mod h, by the conditions on the degrees. To count the number of elements of this set, notice that there are $\binom{|S|+d/2-1}{|S|}$ choices of $a_s \geq 0$ with $\sum a_s < d/2$. Having chosen those, note that the number of s with $a_s > 0$ is at most $d/2$ and therefore there are at least $|S| - d/2$ elements s in S with $a_s = 0$. For those s, we repick the a_s, this time choosing them non-positive and satisfying $\sum -a_s < d/2$. We have $\binom{|S|-1}{|S|-d/2}$ choices for these, proving the theorem. □

Remarks. (i) One can generalize the argument of the previous theorem by allowing

$$\sum_{a_s>0} a_s < \lambda d, \sum_{a_s<0} -a_s < (1-\lambda)d, 0 \leq \lambda \leq 1$$

and moreover, it is possible to combine the arguments of theorems 1 and 2 and thereby obtain small improvements on them when $|S| < (1+\epsilon)d$ for small ϵ.

(ii) J. Vaaler pointed out that one can improve the lower bound in the previous theorem as follows. Pick $u \leq |S|, v \leq |S| - u$, for each choice of disjoint subsets U, V of S, $|U| = u, |V| = v$, pick a_s such that $a_s > 0, s \in U, a_s < 0, s \in V, a_s = 0$, otherwise, subject to $\sum_{s\in U} a_s, \sum_{s\in V}(-a_s) < d/2$. The number of choices is $\binom{|S|}{u}\binom{|S|-u}{v}\binom{d/2}{u}\binom{d/2}{v}$. He also computed the optimal choice of u, v in terms of $|S|/d$.

(iii) I. Shparlinski pointed out that the above bounds improve the best known lower bound for the order t of a root of $x^p - x - 1$ in the multiplicative group of $\mathbf{F}_{p^p}$ (see [LPS]) to $t > 2^{2.54p}$, which in turn is significant for the arithmetic of Bell numbers (see [S]).

2. Large $|S|$

Theorem 3. *If* $|S| > (d-1)q^{1/2}$, *then*

$$|G| > |U|(|S| - (d-1)q^{1/2})/(q - (d-1)q^{1/2}).$$

Proof. Consider the group scheme $\mathcal{G}$ representing the functor $k \mapsto (k[x]/(h))^\times$ for $\mathbf{F}_q$-algebras k, which is a linear torus. We also have a

morphism $X \to \mathcal{G}, t \mapsto x - t$ where $X = \mathbf{A}^1 - \{h = 0\}$. Under these definitions, the group G is the group generated by the image of $S \subset \mathbf{A}^1(\mathbf{F}_q)$ in $\mathcal{G}$, so G is a subgroup of $\mathcal{G}(\mathbf{F}_q)$. Let m be index of the former group in the latter. There is another linear torus $\mathcal{H}$ together with an isogeny $\phi : \mathcal{H} \to \mathcal{G}$ of degree m with $\phi(\mathcal{H}(\mathbf{F}_q)) = G$ (see [V] where a similar situation is studied in the context of abelian varieties and the proofs carry over to the present context). The pull-back of the image of X in $\mathcal{G}$ under ϕ is a curve Y which is étale over X and therefore defines an abelian cover of $\mathbf{P}^1$ of degree m ramified above $\{h = 0\}$ and infinity. Moreover, the conductor of the cover is a factor of $h\infty$. Therefore, the genus of the compactification of Y is therefore at most $(d-1)(m-1)/2$ by the Hurwitz formula. Now the elements of S give points in X which split completely in Y, since S generates G, so counting points on the compactification of Y gives $m|S|+1 \leq q+1+(d-1)(m-1)q^{1/2}$, i.e., $m \leq (q - (d-1)q^{1/2})/(|S| - (d-1)q^{1/2})$. As $|G| = |U|/m$, the result follows. □

Remarks. (i) It follows immediately from the theorem that G is the whole of U if $|S| > (q + (d-1)q^{1/2})/2$.

(ii) I owe to M. Zieve the remark that the above argument works for an arbitrary h and not just separable ones.

(iii) The order of U is $\prod_{i=1}^{r}(q^{d_i} - 1)q^{d_i(n_i-1)}$ if $h = \prod_{i=1}^{r} h_i^{n_i}$, where the h_i are irreducible of degree d_i.

(iv) We can combine the bounds of section 1 with the above arguments by, say using the crude bound $|G| = |U|/m < q^d/m$, to get bounds on the number of rational points of $\mathbf{P}^1$ splitting completely in an abelian extension in terms of the degree and ramification of the extension. These bounds are sometimes better than the Riemann hypothesis and other known bounds such as the one in [FPS].

3. Large p and small $|S|$

The bounds of section 1 are independent of q and one might wonder if the size of G grows with q if $|S|$ and $\deg h$ are held fixed. We show that this is the case under special circumstances.

Theorem 4. *Let p be a prime number, r a positive integer and $h \in \mathbf{F}_p[x]$, the r-th cyclotomic polynomial and assume that h is irreducible of degree $d > 1$. Let $S = \{-2, 2, 3, \ldots, L\}$. The group G generated by the image of $\{x - s \mid s \in S\}$ in $\mathbf{F}_p[x]/(h)$ has cardinality at least $(\log p)^L/L!(\log(L+2))^L$.*

Proof. Let ζ be a root of h in $\mathbf{F}_p[x]/(h)$. Consider the lattice $\Lambda \subset \mathbf{Z}^L$ of vectors $(a_1, \ldots, a_L)$ satisfying $\prod_{s \in S}(\zeta - s)^{a_s} = 1$. This is a lattice of discriminant $|G|$ and therefore, by Minkowski's convex body theorem, there exists an $a \in \Lambda, a \neq 0$ satisfying $\|a\|_1 := \sum_{s \in S} |a_s| \leq (L!|G|)^{1/L}$. Let ξ be a primitive r-th root of unity in characteristic zero and consider the map

$\mathbf{Z}[\xi] \to \mathbf{F}_p[\zeta], \xi \mapsto \zeta$, with kernel $\wp = (p)$. Then $\gamma = \prod_{s\in S}(\xi - s)^{a_s}$ satisfies $\gamma - 1 \in \wp$ so $|N_{\mathbf{Q}(\xi)/\mathbf{Q}}(\gamma - 1)| \geq p^d$. On the other hand, for each archimedian absolute value $|.|$ on $\mathbf{Q}(\xi)$, $|\gamma - 1| \leq |\gamma| + 1 \leq 1 + \prod_{s\in S} |\xi - s|^{a_s}$. We have that $|\xi - s| \leq L + 1$ and that $|\xi - s| \geq 1$ so $\prod_{s\in S} |\xi - s|^{a_s} \leq (L+1)^{\|a\|_1}$ so $|\gamma - 1| \leq (L+2)^{\|a\|_1}$ and finally $|N_{\mathbf{Q}(\xi)/\mathbf{Q}}(\gamma - 1)| \leq (L+2)^{\|a\|_1 d}$. Comparing the upper and lower bounds for $|N_{\mathbf{Q}(\xi)/\mathbf{Q}}(\gamma - 1)|$ gives $\|a\|_1 \log(L+2) \geq \log p$ and the upper bound on $\|a\|_1$ obtained by construction above gives the result. □

4. Applications to AKS

A version of a fundamental result in [AKS] with improvements by Lenstra [L] (see also [B]) yields the following criterion:

Theorem. *Let n be a positive integer, let r be a prime such that n is a primitive root modulo r. Let h be the r-th cyclotomic polynomial. Let S be a set of integers such that, for $b \in S$, $(x - b)^n = x^n - b$ holds in the ring $(\mathbf{Z}/n\mathbf{Z})[x]/(h)$. If p is a prime dividing n such that S injects into $\mathbf{F}_p$ and the corresponding group $G \subset \mathbf{F}_p[x]/(h)$ satisfies $|G| \geq n^{\sqrt{r}}$ then n is a power of p.*

An obvious way to apply the theorem is to check the congruence for $b = 1, \ldots, B$ and take $S = \{1, \ldots, B\}$ but in fact we can take S to be a larger set, as we proceed to show. Assume $B > 1$ and suppose that $(x-b)^n = x^n - b$ in $\mathbf{Z}/n\mathbf{Z}[x]/(x^r - 1)$ for $b = 1, \ldots, B$. Assume that n does not have any prime factor smaller than B^2 and, in particular, n is odd. By projecting to $\mathbf{Z}/n\mathbf{Z}[x]/(x - 1)$ we get $b^n \equiv b (\mathrm{mod}\, n), b = 1, \ldots, B - 1$. We may replace x by $1/x$ in the above equality and still obtain a valid identity which can be rewritten as $(x - b^{-1})^n = x^n - b^{-1}$ for $b = 1, \ldots, B - 1$. If p is a prime dividing n, we claim that $b^{-1} \neq b' (\mathrm{mod}\, p), 1 < b, b' \leq B$, for otherwise $p \leq bb' - 1 \leq B^2$. Of course the identity is also valid for $b = 0$, so verifying the identity for $b = 1, \ldots, B$ automatically gives its validity for a set of $2B$ elements. One could further replace x by x^2 and take $b = a^2, a < \sqrt{B}$, to obtain that $(x + a)^n = x^n + a$ in $\mathbf{Z}/n\mathbf{Z}[x]/(x^r - 1)$ for $0 < a < \sqrt{B}$.

To apply the above to test primality one needs to choose r and S and then the cost of verifying the congruences is $O(|S|r(\log n)^2)$ approximately. Thus one wishes to minimize $|S|r$ under the condition that $|G| \geq n^{\sqrt{r}}$. The following argument is due to Bernstein: If we use the lower bound $|G| \geq \binom{d+|S|-1}{|S|}$ and we can take $d = r - 1$ and we put $|S| = tr$ where t is a parameter, then $\log \binom{d+|S|-1}{|S|}$ is approximately $H(t)r$, where $H(t) = (t + 1)\log(t + 1) - t \log(t)$. We must have $H(t)r > \sqrt{r} \log n$, which gives $r > (\log n)^2/H(t)^2$ and $|S|r > t(\log n)^4/H(t)^4$. The minimum of $t/H(t)^4$

is approximately 0.076 and occurs at t near 17.49. So theorem 1 is not useful, for it only applies for $t < 1$. However, theorem 2 can be used and one can go through the same argument with a different function $H(t) = (t+1/2)\log(t+1/2)-(t-1/2)\log(t-1/2)+\log 2$ which now has a minimum approximately 0.039 occurring at t near 10.28. This leads to choosing r near $0.061(\log n)^2$ and $|S|$ near $0.62(\log n)^2$, so B near $0.31(\log n)^2$. In the event that an optimal choice of r cannot be made, one has to choose a smaller $|S|$ and perhaps theorem 1 becomes relevant.

The applications to AKS remain in flux. To see a list of all improvements to date and a global survey of how they enter the picture, see [B].

We conclude by mentioning the results of a numerical experiment. We checked for primes p, r, with $5 \leq r \leq 19, r < p < 50, p \not\equiv 1 (\mathrm{mod}\, r)$ for the smallest value of B such that taking $S = \{1, \ldots, B\}$ and h an irreducible factor of the r-th cyclotomic polynomial, we have $G = (\mathbf{F}_p[x]/(h))^\times$. In all but a few cases, we found $B \leq 4$. For $r = 19, p = 31$ we found $B = 10$, but already for $B = 4$, G had index two in $(\mathbf{F}_p[x]/(h))^\times$. For those cases we even looked at the maximal subset S of $\mathbf{F}_p$ with $x - s, s \in S$ being in a given subgroup of G. None of our bounds were anywhere close to the true size of $|G|$. We expect that our bounds can be vastly improved.

Acknowledgements

The author would like to thank D. Bernstein, H. Lenstra, J. Vaaler, D. Zagier, M. Zieve and the referee for comments.

References

[AKS] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*. http://www.cse.iitk.ac.in/news/primality.html.

[B] D. Bernstein, *Proving primality after Agrawal-Kayal-Saxena*. http://cr.yp.to/papers.html.

[B2] D. Bernstein, *Sharper ABC-based bounds for congruent polynomials*. http://cr.yp.to/ntheory.html.

[C] F. Chung, *Diameters and Eigenvalues*. JAMS **2** (1989), 187–196.

[Co] S.D. Cohen, *Polynomial factorisation and an application to regular directed graphs*. Finite Fields and Appl. **4** (1998), 316–346.

[FPS] G. Frey, M. Perret, H. Stichtenoth, *On the different of abelian extensions of global fields*. Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math. **1518**, 26–32. Springer, Berlin, 1992.

[K] N.M. Katz, *Factoring polynomials in finite fields: An application of Lang-Weil to a problem of graph theory*. Math. Annalen **286** (1990), 625–637.

[L] H.W. Lenstra Jr., *Primality testing with cyclotomic rings*.

[LPS] W.F. Lunnon, P.A.B. Pleasants, N.M. Stephens, *Arithmetic properties of Bell numbers to a composite modulus I*. Acta Arith. **35** (1979), 1–16.

[S] I. Shparlinski, *The number of different prime divisors of recurrent sequences*. Mat. Zametki **42** (1987), 494–507.

[V] J.F. Voloch, *Jacobians of curves over finite fields*. Rocky Mountain Journal of Math. **30** (2000), 755–759.

José Felipe Voloch
Department of Mathematics
The University of Texas at Austin
1 University Station C1200
Austin, TX 78712-0257 USA
E-mail : voloch@math.utexas.edu