IJMMS 2004:42, 2265–2268
PII. S0161171204312056
http://ijmms.hindawi.com
© Hindawi Publishing Corp.

ON THE RANGES OF DISCRETE EXPONENTIALS

FLORIN CARAGIU and MIHAI CARAGIU

Received 3 December 2003

Let $a > 1$ be a fixed integer. We prove that there is no first-order formula $\phi(X)$ in one free variable X, written in the language of rings, such that for any prime p with $\gcd(a,p) = 1$ the set of all elements in the finite prime field F_p satisfying ϕ coincides with the range of the discrete exponential function $t \mapsto a^t \,(\mathrm{mod}\, p)$.

2000 Mathematics Subject Classification: 11T30, 11U09.

1. Introduction. Let $\phi(X)$ be a formula in one free variable X, written in the first-order language of rings. Then for every ring R with identity, $\phi(X)$ defines a subset of R consisting of all elements of R satisfying $\phi(X)$. For example, the formula $(\exists Y)(X = Y^2)$ will define in every ring R the set of perfect squares in R (for an introduction to the basic concepts arising in model theory of first-order languages, we refer to [5]).

The value sets (ranges) of polynomials over finite fields have been studied by various authors, and many interesting results have been proved (see [3, pages 379–381]). Note that if $f(X)$ is a polynomial with integer coefficients, the formula $(\exists Y)(X = f(Y))$ will define in every finite field F_q the value set of the function from F_q to F_q induced by f. The value sets of the discrete exponentials are no less interesting. For example, if $a > 1$ is an integer that is not a square, Artin's conjecture for primitive roots [4] implies that the range of the function $t \to a^t (\mathrm{mod} p)$ has $p - 1$ elements for infinitely many primes p. In the present note, we investigate the ranges of exponential functions

$$\exp_a : Z \longrightarrow F_p, \qquad \exp_a(t) = a^t (\mathrm{mod} p), \tag{1.1}$$

from the point of view of definability. Note that the range of $\exp_a : Z \to F_p$ coincides with $\langle a \rangle$, the cyclic subgroup of F_p^* generated by a (modulo p). Our main result will be the following.

Theorem 1.1. *Let $a > 1$ be a fixed integer. Then there is no formula $\phi(X)$ in one free variable X, written in the first-order language of rings, such that for any prime p with $\gcd(a,p) = 1$, the set of all elements in the finite prime field F_p satisfying ϕ coincides with the range of the discrete exponential $\exp_a : Z \to F_p$.*

Here is a brief outline of the proof. We will first prove a result (Theorem 2.1) concerning the existence of primes with respect to which a fixed integer $a > 1$ has sufficiently small orders. This, in conjunction with a seminal result of Chatzidakis et al. [1] on definable subsets over finite fields, will lead to the proof of Theorem 1.1.

2. Small orders modulo p. In what follows, we will prove that there exist infinitely many primes with respect to which a given integer $a > 1$ has "small order." More precisely, the following result holds true.

Theorem 2.1. *Let $a > 1$ be an integer. Then, for every $\varepsilon > 0$, there exist infinitely many primes q such that $\operatorname{ord}_q(a)$, the order of a modulo q, satisfies*

$$\operatorname{ord}_q(a) < q\varepsilon. \tag{2.1}$$

Proof. Let k be an integer satisfying

$$\frac{1}{k} < \varepsilon, \tag{2.2}$$

and let p be a prime satisfying

$$p > a, \tag{2.3}$$

$$p \equiv 1 (\operatorname{mod}(k+1)!). \tag{2.4}$$

Due to Dirichlet's theorem on primes in arithmetic progressions [2], there are infinitely many primes p satisfying (2.3) and (2.4). We select a prime q with the property

$$q \mid 1 + a + a^2 + \cdots + a^{p-1}. \tag{2.5}$$

Note that both p and q are necessarily odd. Since from (2.5) it follows that

$$a^p \equiv 1 (\operatorname{mod} q), \tag{2.6}$$

the order $\operatorname{ord}_q(a)$ can be either 1 or p. We will rule out the possibility $\operatorname{ord}_q(a) = 1$. Indeed, if $\operatorname{ord}_q(a) = 1$, then

$$q \mid a - 1. \tag{2.7}$$

On the other hand, $1 + X + X^2 + \cdots + X^{p-1} = (X-1)Q(X) + p$ with $Q(X)$ a polynomial with integer coefficients, and therefore

$$1 + a + a^2 + \cdots + a^{p-1} = (a-1)Q(a) + p. \tag{2.8}$$

From (2.5), (2.7), and (2.8) it follows $q \mid p$ and, since p, q are primes, $q = p$. This, together with (2.7), leads us to $p \mid a - 1$, and therefore $a > p$, which contradicts assumption (2.3). This leaves us with

$$\operatorname{ord}_q(a) = p. \tag{2.9}$$

From (2.9) and from $a^{q-1} \equiv 1 (\operatorname{mod} q)$ it follows that $p \mid q - 1$, so that

$$q = tp + 1 \tag{2.10}$$

for some positive integer t. We will show that $t > k$, so that

$$q > kp+1. \tag{2.11}$$

Indeed, we assume, for contradiction, that $t \le k$. From (2.4), we get $p = (k+1)!s+1$ for some positive integer s. Then

$$q = tp+1 = t\big((k+1)!s+1\big)+1 = t(k+1)!s+(t+1). \tag{2.12}$$

Note that $t+1$ is, under the assumption $t \le k$, a divisor of $(k+1)!$. Then, from (2.12), q will be a multiple of $t+1$, a contradiction, since $2 \le t+1 < q$. Thus, (2.11) holds true and, consequently, since $1/k < \varepsilon$, we get

$$\frac{\operatorname{ord}_q(a)}{q} = \frac{p}{q} < \frac{p}{kp+1} < \frac{1}{k} < \varepsilon, \tag{2.13}$$

which implies

$$\liminf \frac{\operatorname{ord}_q(a)}{q} = 0, \tag{2.14}$$

where the infimum is taken over all primes $q > a$. This completes the proof of Theorem 2.1. □

3. Proof of the main result. We now proceed to the proof of Theorem 1.1. We will use the following result which is a corollary of the main theorem in [1, page 108].

Theorem 3.1. *If $\phi(X)$ is a formula in the first-order language of rings, then there are constants $A, C > 0$, such that for every finite field K, either $|(\phi(K))| \le A$ or $|(\phi(K))| \ge C|K|$, where $\phi(K)$ is the set of elements of K satisfying ϕ.*

We are now ready to proceed to the proof of Theorem 1.1. Assume, for contradiction, that for some integer $a > 1$ there exists a first-order formula $\phi(X)$ in the language of rings such that for every prime $p \nmid a$, we have

$$\phi(F_p) = \exp_a(F_p). \tag{3.1}$$

From (3.1) we get

$$|\phi(F_p)| = \operatorname{ord}_p(a) \tag{3.2}$$

for all $p \nmid a$. Clearly,

$$\operatorname{ord}_p(a) > \log_a(p) \tag{3.3}$$

for all $p \nmid a$. From (3.2), (3.3), and Theorem 3.1, it follows that for every large enough prime p, we have

$$\operatorname{ord}_p(a) \ge Cp. \tag{3.4}$$

Clearly, (3.4) is in contradiction to Theorem 2.1 proved above, which implies that

$$\liminf \frac{\operatorname{ord}_p(a)}{p} = 0. \tag{3.5}$$

Remark 3.2. From Theorem 1.1, it follows as an immediate corollary that, if $a > 1$ is a fixed integer, then there is no first-order formula $\phi(X)$ in the first-order language of rings, such that for any prime p, the set of all elements in F_p satisfying ϕ is $\{a^t \bmod p \mid t \geq 1\}$. Indeed, assuming such a formula exists, it would define in any F_p with $\gcd(a,p) = 1$ the range of the discrete exponential $\exp_a : Z \to F_p$.

Acknowledgment. The authors wish to thank the anonymous referees for the helpful comments.

References

[1] Z. Chatzidakis, L. van den Dries, and A. Macintyre, *Definable sets over finite fields*, J. reine angew. Math. **427** (1992), 107–135.
[2] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000.
[3] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
[4] M. R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), no. 4, 59–67.
[5] P. Rothmaler, *Introduction to Model Theory*, Algebra, Logic and Applications, vol. 15, Gordon and Breach Science Publishers, Amsterdam, 2000.

Florin Caragiu: Department of Mathematics II, University Politechnica of Bucharest, Splaiul Independentei 313, 77206 Bucharest, Romania
E-mail address: f_caragiu@k.ro

Mihai Caragiu: Department of Mathematics, Ohio Northern University, Ada, OH 45810, USA
E-mail address: m-caragiu1@onu.edu