PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
S 0002-9939(02)06395-5
Article electronically published on January 23, 2002

THE DISTRIBUTION OF SEQUENCES IN RESIDUE CLASSES

CHRISTIAN ELSHOLTZ

(Communicated by David E. Rohrlich)

ABSTRACT. We prove that any set of integers $\mathcal{A} \subset [1,x]$ with $|\mathcal{A}| \gg (\log x)^r$ lies in at least $\nu_{\mathcal{A}}(p) \gg p^{\frac{r}{r+1}}$ many residue classes modulo most primes $p \ll (\log x)^{r+1}$. (Here r is a positive constant.) This generalizes a result of Erdős and Ram Murty, who proved in connection with Artin's conjecture on primitive roots that the integers below x which are multiplicatively generated by the coprime integers $a_1, \ldots, a_r$ (i.e. whose counting function is also $c(\log x)^r$) lie in at least $p^{\frac{r}{r+1}+\varepsilon(p)}$ residue classes, modulo most small primes p, where $\varepsilon(p) \to 0$, as $p \to \infty$.

Let $\mathrm{ord}_p(a)$ denote the order of a modulo p, where $(a,p) = 1$. A quantitative version of Artin's conjecture on primitive roots states that for a fixed integer a, not a square, and not -1, there is a positive proportion of primes such that $\mathrm{ord}_p(a) = p-1$. (See [7] for a survey.) In favour of this conjecture, Erdős proved in [2] that for all but $o(\frac{y}{\log y})$ of the primes $p \leq y$ one has

$$\mathrm{ord}_p(2) > p^{\frac{1}{2}}.$$

This improved upon the lower bound of $\mathrm{ord}_p(2) > p^{\delta}$ for all $\delta < \frac{1}{2}$, proved by Bundschuh; see [1]. It is also implicit in section 3 of Hooley's work on Artin's conjecture (see [5]) that for all but $O(\frac{y}{(\log y)^3})$ primes $p \leq y$ one has $\mathrm{ord}_p(a) \gg \frac{\sqrt{p}}{\log p}$. Erdős announced at the end of his paper that the lower bound can be slightly sharpened to

$$\mathrm{ord}_p(2) \geq p^{\frac{1}{2}+\varepsilon(p)},$$

where ε is any real function with $\lim_{p\to\infty} \varepsilon(p) = 0$. The details of this were provided by Erdős and Ram Murty in [3]. For related results see also Pappalardi [8].

For a more general situation, they implicitly consider the following. Let $a_1, \ldots, a_r$ be mutually coprime positive integers and let p be a prime with $(p, a_1 a_2 \cdots a_r) = 1$. Let $\mathcal{A}_1$ be the semigroup of positive integers multiplicatively generated by the a_i and let $\mathcal{A} = \mathcal{A}_1 \cap [1,x]$. Then the elements in $\mathcal{A}$ have the form $a_1^{\beta_1} a_2^{\beta_2} \cdots a_r^{\beta_r} \leq x$, where the β_i are nonnegative integers. Let $f(p, a_1, \ldots, a_r)$ denote the number of distinct residue classes modulo p which are needed to cover all elements of $a \in \mathcal{A}$.

Note that the number of powers of a below x is asymptotically $c_a \log x$, and that there are about $c_{a_1,\ldots,a_r}(\log x)^r$ many integers below x which are generated

Received by the editors March 9, 2001.
1991 *Mathematics Subject Classification.* Primary 11N69, 11N36; Secondary 11B50, 11A07.
Key words and phrases. Distribution of sequences in residue classes, Gallagher's larger sieve, primitive roots, Artin's conjecture.

multiplicatively by the a_i. Here and in the following, the c with various indices stand for positive constants.

In this situation,[1] Erdős and Ram Murty prove that, for all but $o(\frac{y}{\log y})$ many primes $p \le y$ with $(p, a_1 \cdots a_r) = 1$ one has

$$f(p, a_1, \dots, a_r) \ge p^{\frac{r}{r+1}+\varepsilon(p)},$$

where ε is an arbitrary real function with $\lim_{p\to\infty} \varepsilon(p) = 0$.

Giving a more quantitative version of this statement one might consider the sequence up to x. It is then implicitly understood that $y \ll (\log x)^{r+1}$, since otherwise the sequence $\mathcal{A}$ does not have $\gg y^{\frac{r}{r+1}}$ elements below x.

In this note we generalize these results to arbitrary integer sequences. Therefore, the fact that the powers of some element a lie in many residue classes modulo many primes is not necessarily an argument in favour of Artin's conjecture. However, for special sequences like the powers of a the result by Erdős and Ram Murty is stronger by the $\varepsilon(p)$ refinement. We prove the following theorem:

Theorem. *Let $x > x_0$ and let $\mathcal{A} \subseteq [1, x]$ be a set of positive integers with $|\mathcal{A}| \ge c_1(\log x)^r$. Let $\nu_{\mathcal{A}}(p)$ denote the number of distinct residue classes modulo p which are necessary to cover $\mathcal{A}$. Let $y = c_4(\log x)^{r+1}$. Let*

$$\mathcal{S} = \{p \in \mathcal{P} \cap [1, y] : \nu_{\mathcal{A}}(p) \le c_2 p^{\frac{r}{r+1}}\}$$

and $c_3 = \frac{|\mathcal{S}|}{\pi(y)}$. Let $\beta = \frac{1}{r+1}$ and $C = \frac{1}{\beta}(1 - (1 - c_3)^\beta)c_4^\beta$. If $C > c_2$, then

$$\frac{c_2 c_3 c_4}{C - c_2} \ge c_1.$$

In typical applications, the counting function $A(x)$, i.e. c_1 and r, might be known. Suppose one wants to make the proportion c_3 of 'bad primes' very small so that one knows for essentially all primes $p \le y$, that $\nu_{\mathcal{A}}(p)$ is large. Then one can make an admissible choice of c_2 and c_4 as follows: Choose a small c_3, choose $c_4 \ge \dfrac{c_1}{c_3}$, and put $c_2 = \frac{C}{2}$. Then trivially $C > c_2$ and

$$\frac{c_2 c_3 c_4}{C - c_2} = \frac{c_2 c_3 c_4}{c_2} = c_3 c_4 \ge c_1.$$

This implies the following corollary.

Corollary. *Let $\mathcal{A}$ be an infinite set of positive integers with counting function $A(x) \gg (\log x)^r$. Let $\nu_{\mathcal{A}}(p)$ denote the number of distinct residue classes modulo p which are necessary to cover $\mathcal{A} \cap [1, x]$. Then for all $c_3 > 0$ one can find positive c_2 and c_4 such that for all but at most $\frac{c_3 y}{\log y}$ primes $p \le y$, where $y = c_4(\log x)^{r+1}$, one has $\nu_{\mathcal{A}}(p) \ge c_2 p^{\frac{r}{r+1}}$.*

Unfortunately, it appears, if one allows at most $o(\frac{y}{\log y})$ exceptional primes, that is if one requires that $c_3 \to 0$ as $x \to \infty$, then one has to allow that c_2 and c_4 vary accordingly.

[1] Strictly speaking, their theorem is stated in a more general form for rational numbers. Let us take the opportunity to mention that there is a slight inaccuracy in the description of the ε in Theorem 4 and part 3 of Theorem 5 of their results (and also in the abstracts in the Math. Reviews and the Zentralblatt): Obviously, one should either replace $p/\varepsilon(p)$ by $p\varepsilon(p)$ or one should take $p/\varepsilon(p)$ with $\lim_{p\to\infty} \varepsilon(p) = \infty$.

Our main tool is Gallagher's larger sieve, which we state for completeness.

Lemma (Gallagher's larger sieve; see [4]). *Let $\mathcal{A} \subseteq [1,x]$ be a set that lies in at most $\nu_{\mathcal{A}}(p)$ residue classes modulo p, for $p \in \mathcal{S}$. Then*

$$|\mathcal{A}| \leq \frac{-\log x + \sum_{p\in\mathcal{S}} \log p}{-\log x + \sum_{p\in\mathcal{S}} \frac{\log p}{\nu_{\mathcal{A}}(p)}},$$

provided the denominator is positive.

Proof of the Theorem. Since we deal with upper bounds and since $\log p$ and $\frac{\log p}{p^{\frac{r}{r+1}}}$ are monotonic functions for $p > p_0$, the worst case distribution of the primes in $\mathcal{S}$ is that these primes are as large as possible. If x tends to infinity, then the intervals $[0, c\,y]$ and $[(1-c)y, y]$ contain asymptotically the same number of primes, $\frac{cy}{\log y}$. The worst case distribution is determined by the primes in $[(1-c_3+o(1))y, y]$. For simplicity, we omit $o(1)$ expressions and write $\lesssim$ instead of $\leq$. Moreover, recall that it follows from $\sum_{p\leq z} \log p \sim z$ by partial summation that for $0 < \alpha < 1$ one has

$$\sum_{p\leq z} \frac{\log p}{p^\alpha} \sim \frac{z^{1-\alpha}}{1-\alpha}.$$

With $\alpha = \frac{r}{r+1}$, so that $1-\alpha = \frac{1}{r+1} = \beta$, we find that

$$\begin{aligned} |\mathcal{A}| &\lesssim \frac{-\log x + \sum_{(1-c_3)y\leq p\leq y} \log p}{-\log x + \sum_{(1-c_3)y\leq p\leq y} \frac{\log p}{c_2 p^{\frac{r}{r+1}}}} \lesssim \frac{c_3 y}{-\log x + \frac{1}{c_2\beta}\left(y^\beta - (1-c_3)^\beta y^\beta\right)} \\ &= \frac{c_3 c_4 (\log x)^{r+1}}{-\log x + \frac{C}{c_2}\log x} = \frac{c_2 c_3 c_4}{C - c_2}(\log x)^r. \end{aligned}$$

Suppose that we have $C > c_2$ but $\frac{c_2c_3c_4}{C-c_2} < c_1$. This is, for sufficiently large x, a contradiction to our assumption $|\mathcal{A}| \geq c_1(\log x)^r$. $\square$

Remark. Matthews (see [6]) considered questions related to that of Erdős and Ram Murty in a more general context of algebraic groups and abelian varieties. For the classical case of Artin's conjecture he proved that for almost all primes and for all positive ε one has $\nu(p) > p^{\frac{1}{2}-\varepsilon}$. (Apparently he was unaware of [1] and [2].) He mentions further applications to nilpotent groups and to manifolds due to Milnor, Tits, and Wolf.

References

[1] Bundschuh, P., Solution of problem 618. Elemente der Mathematik 26 (1971), 43–44.

[2] Erdős, P., Bemerkungen zu einer Aufgabe in den Elementen. Arch. Math. 27 (1976), 159-163. MR **53:**7969

[3] Erdős, P.; Murty, M. Ram, On the order of $a \pmod p$. Number theory (Ottawa, 1996), 87–97, CRM Proc. Lecture Notes, 19. MR **2000c:**11152

[4] Gallagher, P.X., A larger sieve. Acta Arith. 18 (1971), 77–81. MR **45:**214

[5] Hooley, C., On Artin's conjecture. J. Reine Angew. Math. 225 (1967), 209–220. MR **34:**7445

[6] Matthews, C.R., Counting points modulo p for some finitely generated subgroups of algebraic groups. Bull. London Math. Soc. 14 (1982), 149–154. MR **83c:**10067

[7] Murty, M. Ram, Artin's conjecture for primitive roots. Math. Intelligencer 10 (1988), 59–67. MR **89k:**11085

[8] Pappalardi, F., On the order of finitely generated subgroups of $Q^*(\bmod p)$ and divisors of $p-1$. J. Number Theory 57 (1996), 207–222. MR **97d:**11141

Institut für Mathematik, Technische Universität Clausthal, Erzstrasse 1, D-38678 Clausthal-Zellerfeld, Germany

E-mail address: `elsholtz@math.tu-clausthal.de`