Bull. Aust. Math. Soc. **96** (2017), 177–184
doi:10.1017/S000497271700048X

ON THE MINIMAL NUMBER OF SMALL ELEMENTS GENERATING FINITE PRIME FIELDS

MARC MUNSCH

(Received 30 January 2017; accepted 1 April 2017; first published online 17 August 2017)

Abstract

In this note, we give an upper bound for the number of elements from the interval $[1, p^{1/4\sqrt{e}+\epsilon}]$ necessary to generate the finite field $\mathbb{F}_p^*$ with p an odd prime. The general result depends on the distribution of the divisors of $p-1$ and can be used to deduce results which hold for almost all primes.

2010 *Mathematics subject classification*: primary 11A07; secondary 11N36.

Keywords and phrases: finite field, generating set, primitive root, sieve theory, character sum, algorithmic number theory.

1. Introduction

In 1927, Artin conjectured that any positive integer $n > 1$, which is not a perfect square, is a primitive root modulo p for infinitely many primes p. The conjecture remains open, but was proved assuming the generalised Riemann hypothesis for some specific Dedekind zeta functions by Hooley in [11]. Using the development of large sieve theory leading to the Bombieri–Vinogradov theorem, one can show that Artin's primitive root conjecture is true for almost all primes. (See, for example, [10] or [13] for an extended survey about this conjecture.) Another related classical problem is to bound the size $g(p)$ of the smallest primitive root modulo p. The best unconditional result is $g(p) = O(p^{1/4+\epsilon})$ obtained by Burgess [3], as a consequence of his famous character sum estimate. This is very far from what we expect. Assuming the generalised Riemann hypothesis, $g(p) = O((\log p)^{6+\epsilon})$ (see [15] following [1]). As before, as a consequence of the large sieve, the upper bound $g(p) = O((\log p)^{2+\epsilon})$ is valid for almost all primes (see [4]). The problem of improving the unconditional bound for the least primitive root seems presently out of reach. For instance, we cannot directly perform the 'Vinogradov trick' to show that there exists a primitive root less than $p^{1/4\sqrt{e}+\epsilon}$, but we can reach that range for the following question.

The author is supported by the Austrian Science Fund (FWF), START-project Y-901 'Probabilistic methods in analysis and number theory', headed by Christoph Aistleitner.

Question 1.1. How large should N be (in terms of p) such that $\langle 1, \dots, N\rangle$ is a generating set of $\mathbb{F}_p^*$ (in the sense that it generates $\mathbb{F}_p^*$ multiplicatively)?

It is shown by Burthe [5] that $N = p^{1/4\sqrt{e}+\epsilon}$ is sufficient and this seems to be the lower limit of what is possible unless the Burgess character sum bound is improved. Nonetheless, in view of this result, several interesting related questions can be formulated. Harman and Shparlinski considered the problem of minimising the value of k such that for a sufficiently large prime p and for any integer $a < p$, there is always a solution to the congruence

$$n_1 \dots n_k \equiv a (\text{mod } p) \quad \text{with } 1 \le n_1, \dots, n_k \le p^{1/4\sqrt{e}+\epsilon},$$

and showed in [9] that $k = 14$ is an admissible value. If we only ask that there is a solution for almost all values of a, then $k = 7$ is admissible. From an algorithmic point of view, another interesting question is to know precisely how many elements of $\{1, \dots, N\}$ are necessary to generate the full multiplicative group. In this note, we consider the problem of bounding the size of a generating set consisting of small elements less than N to answer the following question.

Question 1.2. How many elements of $\{1, \dots, p^{1/4\sqrt{e}+\epsilon}\}$ do we need in order to generate $\mathbb{F}_p^*$?

Let p be a prime and write $\#\mathbb{F}_p^* = p - 1 = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ where q_i, $i = 1, \dots, r$, are the distinct prime factors of $p - 1$. As usual, we denote by $\omega(n)$ the number of distinct prime factors of an integer n.

The first elementary result towards answering the question is the following lemma.

Lemma 1.3. *For every $\epsilon > 0$, we need only $\omega(p - 1)$ elements among $\{1, \dots, p^{1/4\sqrt{e}+\epsilon}\}$ to generate $\mathbb{F}_p^*$.*

Proof. Using Burgess' inequality for character sums (see [3]) and the 'Vinogradov trick' (see [17, 18]), we can pick $x_1, \dots, x_r < p^{1/4\sqrt{e}+\epsilon}$ such that x_i is not a q_ith residue modulo p. Fixing g a primitive root, we have $x_i = g^{\beta_i}$ with $\gcd(\beta_i, q_i) = 1$. Thus, $\gcd(\beta_1, \dots, \beta_r)$ is coprime to $p - 1$. By Bezout's theorem, there exist integers $l_1, \dots l_r$ such that $\sum_{i=1}^r l_i\beta_i$ is coprime to $p - 1$. Hence, $x_1^{l_1} \dots x_r^{l_r}$ is a primitive root of $\mathbb{F}_p^*$ and the statement is proved. □

To improve on Lemma 1.3 and show that fewer small elements are needed to generate the full group, we need information on the distribution of small prime divisors of $p - 1$. To measure this distribution, we introduce the following definition.

Definition 1.4. Let $l \ge 1$. Set $\omega_l(n) = \#\{q \text{ prime}, q|n, q \le (\log(n + 1))l^l\}$.

In the rest of the paper, $\log_k x$ will denote the k times iterated logarithm when k is an integer. We prove the following theorem in Section 3, using a combinatorial argument and recent developments in sieve theory for nonregularly distributed sets.

Theorem 1.5. *Let $l := l(p) \ge 1$ be a parameter tending to infinity with p such that $l \le \log p/(1000 \log_2 p)$. Then $O(\omega_l(p - 1) + \omega(p - 1)/\log l)$ elements smaller than $p^{1/4\sqrt{e}+\epsilon}$ are needed to generate the multiplicative group $\mathbb{F}_p^*$, where the implied constant is effective.*

https://doi.org/10.1017/S000497271700048X Published online by Cambridge University Press

We will also give a more precise result of this type and deduce stronger results for almost all primes in Section 4. In the next section, we recall some sieve results that we will use in our argument.

2. Sieve fundamental result

In this section, we will use the notations and recall the setting of [12]. Let $\mathbb{P}$ be the set of all primes and let $\mathcal{P} \subseteq \mathbb{P}$ be a subset of the primes $\leq x$. The most basic sieving problem is to estimate

$$\Psi(x;\mathcal{P}) := \#\{n \leq x : p \mid n \implies p \in \mathcal{P}\}.$$

In other words, we sieve the integers in $[1, x]$ by the primes in $\mathcal{P}^c = (\mathbb{P} \cap [1, x]) \setminus \mathcal{P}$. A simple inclusion–exclusion argument suggests that $\Psi(x;\mathcal{P})$ should be approximated by

$$x \prod_{p\in\mathcal{P}^c}\Big(1-\frac{1}{p}\Big).$$

This is always an upper bound, up to a constant, and also a lower bound, up to a constant, if $\mathcal{P}$ contains all the primes larger than $x^{1/2-o(1)}$. On the other hand, there are examples where $\Psi(x;\mathcal{P})$ is much smaller than the expected lower bound. For instance if one fixes $u \geq 1$ and lets $\mathcal{P}$ consist of all the primes up to $x^{1/u}$, then the prediction is about x/u, whereas, by an estimate for the number of smooth numbers, we know that $\Psi(x;\mathcal{P}) = \rho(u)x$ with $\rho(u) = u^{-u(1+o(1))}$ as $u \to \infty$, which is much smaller for large u.

Granville *et al.* [6] were the first to study what happens if one also sieves out some primes from $[x^{1/2}, x]$. They conjectured that the critical issue is to understand what is the largest y such that

$$\sum_{\substack{p\in\mathcal{P}\\ y\leq p\leq x^{1/u}}} \frac{1}{p} \geq \frac{1+\varepsilon}{u}.$$

More precisely, they conjectured that when this inequality holds, the sieve works as expected. We will use the following result proved by Matomäki and Shao confirming this conjecture.

Theorem 2.1 [12, Theorem 1.1]. *Fix $\varepsilon > 0$. If x is large and $\mathcal{P}$ is a subset of the primes $\leq x$ for which there are some u, v with $1 \leq u \leq v \leq \log x/(1000 \log_2 x)$ and*

$$\sum_{\substack{p\in\mathcal{P}\\ x^{1/v}<p\leq x^{1/u}}} \frac{1}{p} \geq \frac{1+\varepsilon}{u},$$

then

$$\frac{\Psi(x;\mathcal{P})}{x} \geq A_v \prod_{p\in\mathcal{P}^c}\Big(1-\frac{1}{p}\Big),$$

where A_v is a constant with $A_v = v^{-v(1+o_\varepsilon(1))}$ as $v \to \infty$. If u is fixed, one can take $A_v = v^{-e^{-1/u}v(1+o_\varepsilon(1))}$ as $v \to \infty$.

https://doi.org/10.1017/S000497271700048X Published online by Cambridge University Press

3. Idea of the method and main results

Definition 3.1. We define $h(p)$ as the number of elements smaller than $p^{1/4\sqrt{e}+\epsilon}$ which are sufficient to generate the multiplicative group $\mathbb{F}_p^*$.

We aim to find improvements on the size of $h(p)$. The main idea is as follows. For large divisors q_1 and q_2 of $p-1$, we want to exhibit a reasonably small prime which is simultaneously a non q_1th residue and a non q_2th residue. The nonexistence of such a prime implies by a sieve argument that the set of q_1th (or q_2th) residues is large. On the other hand, due to the sparsity of powers, the set of q_1th (respectively q_2th) residues is relatively small, leading to a contradiction. Hence, we do not need to pick up a nonresidue for every power as in Lemma 1.3. We can play this game with more divisors in order to decrease the number of steps needed in the argument. In order to do that, we will use the sieve result from Section 2. The dependence on v in the lower bound of Theorem 2.1 prevents us from grouping as many divisors as we want, so we carefully split the set of prime divisors in blocks of size k with an 'optimal' value of k for the application of Theorem 2.1.

Given a parameter $l \geq 1$, we obtain a bound for $h(p)$ depending on $\omega_l(p-1)$. If for some relatively large l, $\omega_l(p-1)$ is small, this gives a significant improvement on the trivial bound $\omega(p-1)$ in Lemma 1.3.

The next result is the main tool in deriving these improvements. It shows that we can handle several large prime divisors of $p-1$ simultaneously.

Proposition 3.2 (Main proposition). *Let $l := l(p) \geq 1$ be a parameter tending to infinity with p and k an integer with $k \leq \frac{1}{4}\log l$. Moreover, assume $l \leq \log p/(1000\log_2 p)$. Suppose that $q_1, \dots, q_k$ are prime divisors of $p-1$ greater than $(\log p)l^l$. Then, if p is sufficiently large, there exists an integer $n \leq N = p^{1/4\sqrt{e}+\epsilon}$ which is a non q_ith residue for $i = 1, \dots, k$.*

Proof. Define $S = \{1 \leq n \leq N : n \text{ is a non } q_i\text{th residue modulo } p \text{ for } i = 1, \dots, k\}$ and suppose that $S = \emptyset$ which means that every integer in this interval is a q_ith residue modulo p for at least one i. Thus, in particular,

$$\mathcal{P} = \{q \text{ prime}, 1 \leq q \leq N\} = \bigcup_{i=1}^{k} \mathcal{P}_i \tag{3.1}$$

where $\mathcal{P}_i = \mathcal{P} \cap \{q_i\text{th residues modulo } p\}$. For x sufficiently large and u, v parameters to be specified later, by Mertens' theorem (see [8, Ch. 22, Theorem 427]),

$$\sum_{q \leq x} \frac{1}{q} = \log_2 x + O(1)$$

and thus

$$\sum_{\substack{q \in \mathcal{P} \\ x^{1/v} < q \leq x^{1/u}}} \frac{1}{q} \geq \frac{1}{2}\log(v/u).$$

https://doi.org/10.1017/S000497271700048X Published online by Cambridge University Press

Consequently, using (3.1), there exists $i \in \{1, \dots, k\}$ such that

$$\sum_{\substack{q \in \mathcal{P}_i \\ x^{1/v} < q \le x^{1/u}}} \frac{1}{q} \ge \frac{1}{2k} \log(v/u). \tag{3.2}$$

To apply Theorem 2.1, we need the right-hand side of (3.2) to be larger than $(1+\epsilon)/u$ under the conditions $1 \le u \le v \le \log x/(1000 \log_2 x)$. Fix u such that

$$\frac{1}{u} = \frac{1}{4\sqrt{e}} + \epsilon$$

and set $x = p$ so that $N = x^{1/u}$. The condition of Theorem 2.1 is satisfied provided $k \le \frac{1}{4} \log v$. Therefore,

$$\frac{\Psi(p; \mathcal{P}_i)}{p} \ge A_v \prod_{q \in \mathcal{P}_i^c} \Big(1 - \frac{1}{q}\Big).$$

From the third Mertens' Theorem (see [8, Ch. 22, Theorem 429]), the product is trivially bounded from below by

$$\prod_{q \le p} \Big(1 - \frac{1}{q}\Big) \ge \frac{1}{2 \log p}$$

for p large enough. Thus, we obtain $\Psi(p; \mathcal{P}_i) \gg A_v x/\log p \gg v^{-v} x/\log p$. On the other hand, we are counting integers less than p which are q_ith residues, of which there are at most p/q_i. This leads to a contradiction when $v^{-v}(\log p)^{-1} \ge 1/q_i$, or equivalently $q_i \ge (\log p)v^v$. Under this condition, the set S is nonempty. This completes the proof with the choice $v = l$ for the parameter v. □

Proposition 3.2 helps us to group the divisors in 'blocks' of size k. Using this idea in a simple way, we are able to deduce the result announced in the introduction.

Theorem 3.3. *Let $l := l(p) \ge 1$ be a parameter tending to infinity with p such that $l \le \log p/(1000 \log_2 p)$. For a sufficiently large prime p,*

$$h(p) \ll \omega_l(p-1) + \frac{\omega(p-1) - \omega_l(p-1)}{\log l}$$

where the implied constant is effective.

Proof. Consider the prime divisors of $p-1$ which are greater than $(\log p)l^l$. We can apply Proposition 3.2 with $k = \frac{1}{4} \log p$ and pick up an integer less than $p^{1/4\sqrt{e}+\epsilon}$ which is a non qth residue for k different large values of q. Regrouping the large divisors of $p-1$ in blocks of size k gives at most $(\omega(p-1) - \omega_l(p-1))/k$ blocks. The small divisors can be treated individually using Burgess' character sum inequality combined with the 'Vinogradov trick' as in Lemma 1.3. This concludes the proof. □

Remark 3.4. The value of the optimal parameter l is not so clear for a general p, it will depend heavily on the distribution of the prime divisors of $p-1$.

https://doi.org/10.1017/S000497271700048X Published online by Cambridge University Press

We can iterate the argument used to prove Theorem 3.3 and obtain the following stronger result.

THEOREM 3.5. *Let $l_n(p), n = 0, \ldots, N$, be a strictly decreasing sequence of parameters tending to infinity with p such that $(\log p)l_0^{l_0} > p$ and $l_1 \le \log p/(1000 \log_2 p)$. Then, for a sufficiently large prime p,*

$$h(p) \ll \omega_{l_N}(p-1) + \sum_{n=0}^{N-1} \frac{\omega_{l_n}(p-1) - \omega_{l_{n+1}}(p-1)}{\log(l_{n+1})}.$$

PROOF. We argue as in Theorem 3.3, regrouping the divisors of $p-1$ lying in the interval $](\log p)l_{n+1}^{l_{n+1}}, (\log p)l_n^{l_n}]$ in blocks of size $k_n \approx \log(l_{n+1})$. The contribution of the remaining small prime divisors is given by $\omega_{l_N}(p-1)$. □

4. Results for almost all primes

We can use Theorem 3.5 to obtain a result on a set of primes of density 1. We may note that stronger results about primitive roots are known for almost all primes.

The next result gives a bound on the number of small prime divisors of $p-1$ for almost all primes p.

LEMMA 4.1. *Let $A > 1$ and $\epsilon > 0$. Suppose l is such that $l^l \ll x^{1/2-\epsilon}$. Then, the set of primes $p \le x$ such that $\omega_l(p-1) \ll \log l$ is asymptotically of density* 1.

PROOF. We evaluate the average number of primes satisfying the inequality of the lemma. By the Bombieri–Vinogradov theorem (see for instance [2]),

$$\sum_{\substack{p \le x \\ p \text{ prime}}} \sum_{\substack{q \mid p-1 \\ q \le (\log p)l^l, q \text{ prime}}} 1 = \sum_{q \le (\log x)l^l} \sum_{\substack{p \equiv 1 \bmod q \\ p \le x}} 1 = \sum_{q \le (\log x)l^l} \frac{x}{(q-1)\log x} + O\Big(\frac{x}{\log^A x}\Big).$$

Thus, Mertens' theorem gives

$$\sum_{\substack{p \le x \\ p \text{ prime}}} \sum_{\substack{q \mid p-1 \\ q \le (\log p)l^l, q \text{ prime}}} 1 = \frac{x}{\log x}(\log l + \log_2 l + M) + O\Big(\frac{x}{\log^B x}\Big)$$

where M is the Meissel–Mertens constant and $B = \min\{A, 2\}$. The conclusion follows easily. □

REMARK 4.2. We could obtain the normal order of $\omega_l(p-1)$ following the method of Turán (see [16]) using the first two moments. It might even be possible to prove a more precise statement like an Erdős-Kac version of this result using the method of Granville and Soundararajan (see [7]), but we will not explore this here.

Using Theorem 3.5 to localise the divisors of $p-1$ more precisely, we derive a result for almost all primes.

COROLLARY 4.3. *For almost all primes p, we have $h(p) \ll (\log_3 p)^2$.*

Proof. Define the following special 'dyadic' parameters: $l_n = \exp(\log_2 p/(2^n \log_3 p))$ for $1 \le n \le N = (\log_3 p - 2\log_4 p)/\log 2$. It is easy to see that this sequence satisfies the hypotheses of Theorem 3.5. Thus,

$$h(p) \ll \omega_{l_N}(p-1) + \sum_{n=1}^{N-1} \frac{\omega_{l_n}(p-1) - \omega_{l_{n+1}}(p-1)}{\log(l_{n+1})} + \frac{\omega(p-1) - \omega_{l_1}(p-1)}{\log(l_1)}.$$

By Lemma 4.1, the bound $\omega_{l_n}(p) \le \log(l_n)(\log_3 p)$ holds for almost all primes $p \le x$ with an exceptional set of 'bad' primes of size at most $x/(\log x \log_3 x)$. By applying Lemma 4.1 and this argument N times, we arrive at a set of primes of density 1 satisfying $\omega_{l_n}(p-1) \le \log(l_n)(\log_3 p)$ for $1 \le n \le N$ with a negligible exceptional set of 'bad' primes. Finally, by the trivial inequality $\log(l_n)/\log(l_{n+1}) \le 2$,

$$h(p) \le \log(l_N)\log_3 p + 2N\log_3 p + \log_3 p \ll (\log_3 p)^2$$

on a set of primes of density 1. □

Remark 4.4. As an application of the large sieve, Pappalardi obtained a result of a similar flavour. More precisely, in [14], he showed that the first $\log^2 p/\log_2 p$ primes generate a primitive root modulo p for almost all primes p.

Acknowledgements

The author is grateful to Sary Drappeau and Igor E. Shparlinski for very helpful discussions and comments.

References

[1] N. C. Ankeny, 'The least quadratic non residue', *Ann. of Math. (2)* **55** (1952), 65–72.

[2] E. Bombieri, 'On the large sieve', *Mathematika* **12** (1965), 201–225.

[3] D. A. Burgess, 'On character sums and primitive roots', *Proc. Lond. Math. Soc. (3)* **12** (1962), 179–192.

[4] D. A. Burgess and P. D. T. A. Elliott, 'The average of the least primitive root', *Mathematika* **15** (1968), 39–50.

[5] R. J. Burthe Jr, 'Upper bounds for least witnesses and generating sets', *Acta Arith.* **80**(4) (1997), 311–326.

[6] A. Granville, D. Koukoulopoulos and K. Matomäki, 'When the sieve works', *Duke Math. J.* **164**(10) (2015), 1935–1969.

[7] A. Granville and K. Soundararajan, 'Sieving and the Erdös–Kac theorem', in: *Equidistribution in Number Theory, an Introduction*, NATO Science Series II: Mathematics, Physics and Chemistry, 237 (Springer, Dordrecht, 2007), 15–27.

[8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th edn (Oxford University Press, Oxford, 2008), Revised by D. R. Heath-Brown and J. H. Silverman.

[9] G. Harman and I. E. Shparlinski, 'Products of small integers in residue classes and additive properties of Fermat quotients', *Int. Math. Res. Not. IMRN* **2016**(5) (2016), 1424–1446.

[10] D. R. Heath-Brown, 'Artin's conjecture for primitive roots', *Quart. J. Math. Oxford Ser. (2)* **37**(145) (1986), 27–38.

[11] C. Hooley, 'On Artin's conjecture', *J. reine angew. Math.* **225** (1967), 209–220.

[12] K. Matomäki and X. Shao, 'When the sieve works ii'. Preprint, 2015, arXiv:1509.02371.

[13] P. Moree, 'Artin's primitive root conjecture—a survey', *Integers* **12**(6) (2012), 1305–1416.

https://doi.org/10.1017/S000497271700048X Published online by Cambridge University Press

[14] F. Pappalardi, 'On minimal sets of generators for primitive roots', *Canad. Math. Bull.* **38**(4) (1995), 465–468.

[15] V. Shoup, 'Searching for primitive roots in finite fields', *Math. Comp.* **58**(197) (1992), 369–380.

[16] P. Turán, 'On a theorem of Hardy and Ramanujan', *J. Lond. Math. Soc.* **S1-9**(4) (1934), 274–276.

[17] J. M. Vinogradov, 'On a general theorem concerning the distribution of the residues and non-residues of powers', *Trans. Amer. Math. Soc.* **29**(1) (1927), 209–217.

[18] J. M. Vinogradov, 'On the bound of the least non-residue of *n*th powers', *Trans. Amer. Math. Soc.* **29**(1) (1927), 218–226.

MARC MUNSCH, 5010 Institut für Analysis und Zahlentheorie,
8010 Graz, Steyrergasse 30, Graz, Austria
e-mail: munsch@math.tugraz.at