ACTA ARITHMETICA
172.3 (2016)

On Grosswald's conjecture on primitive roots

by

Stephen D. Cohen (Glasgow), Tomás Oliveira e Silva (Aveiro)
and Tim Trudgian (Canberra)

1. Introduction. Let $g(p)$ denote the least primitive root of a prime p. Burgess [4] showed that $g(p) \ll p^{1/4+\epsilon}$ for any $\epsilon > 0$. This remains the best known bound in general—see [12] for an insightful survey of related problems. Grosswald [7] conjectured that

$$g(p) < \sqrt{p} - 2 \tag{1.1}$$

for all primes $p > 409$. This has implications for the generators of $\Gamma(p)$, the principal congruence subgroup modulo p of the modular group Γ—see [7, §8]. Grosswald verified numerically that (1.1) is true for all $409 < p \le 10{,}000$. He also gave an explicit version of Burgess' bound, thereby proving that $g(p) \le p^{0.499}$ for all $p > 1 + \exp(\exp(24)) \approx 10^{10^{10}}$.

Using computational and theoretical arguments we improve on Grosswald's estimate in the following theorem.

Theorem 1.1. *Let $g(p)$ denote the least primitive root modulo p. Then $g(p) \le \sqrt{p} - 2$ for all $409 < p < 2.5 \times 10^{15}$ and for all $p > 3.38 \times 10^{71}$.*

The 'gap' in Theorem 1.1 between the ranges of p seems difficult to bridge. The trivial bound $g(p) \le p$ when combined with the results in Theorem 1.1 gives the following corollary.

Corollary 1.2. *$g(p) \le 5.2p^{0.99}$ for all p.*

The bound in Corollary 1.2, while weak, appears to be the first bound that holds for all p.

The remainder of the paper is organised as follows. In §2 we make use of an explicit version of Burgess' bound. This gives a substantial improvement on the upper bound $\exp(\exp(24)) + 1$ given by Grosswald. We introduce a

2010 *Mathematics Subject Classification*: Primary 11L40; Secondary 11A07.
Key words and phrases: character sums, primitive roots, Burgess' bound, prime sieves.
Received 16 March 2015; revised 28 August 2015.
Published online 16 December 2015.

DOI: 10.4064/aa8109-12-2015

sieving inequality in §3 which enables us to reduce this further. Finally, in §4 we present some computations that complete the proof of Theorem 1.1, and present some data on two related problems involving primitive roots.

2. Explicit versions of Burgess' bounds. Burgess' bounds on the character sum

$$S_H(N) = \sum_{m=N+1}^{N+H} \chi(m)$$

were first made explicit by Grosswald [7], and were later refined by Booker [3], McGown [10], and, most recently, by Treviño [16]. The following is Theorem 1.7 in [16].

THEOREM 2.1 (Treviño). *Suppose χ is a non-principal Dirichlet character modulo p where $p \geq 10^{20}$. Let $N, H \in \mathbb{Z}$ with $H \geq 1$. Fix a positive integer $r \geq 2$. Then there exists a computable constant $C(r)$ such that whenever $H \leq 2p^{1/2+1/4r}$ we have*

$$\big|S_H(N)\big| \leq C(r) H^{1-1/r} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}}. \tag{2.1}$$

We follow Burgess who in [4, §6] considers

$$f(x) = \frac{\phi(p-1)}{p-1}\bigg\{1 + \sum_{d|p-1,\, d>1} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(x)\bigg\}, \tag{2.2}$$

whence it follows that $f(x) = 1$ if x is a primitive root, and $f(x) = 0$ otherwise, provided that $p \nmid x$. Thus, if $N(H)$ denotes the number of primitive roots in the interval $1 \leq x \leq H$ we have

$$N(H) = \sum_{x=1,\, x \not\equiv 0 \,(\mathrm{mod}\, p)}^{H} f(x).$$

We can estimate the sum of $f(x)$ using (2.1) with $H = (1 - 2/p_0^{1/2})p^{1/2}$. This choice of H guarantees that $H < \sqrt{p} - 2$ for $p > p_0$.

Since we need only consider square-free divisors d in the outer sum in (2.2), and since there are $\phi(d)$ characters χ_d, we arrive at the following theorem.

THEOREM 2.2. *We have $g(p) < \sqrt{p} - 2$ for $p > p_0$ provided that*

$$p^{\frac{r-1}{4r^2}} > C(r)\bigg(1 - \frac{2}{p_0^{1/2}}\bigg)^{-1/r} (\log p)^{1/2r}\{2^{\omega(p-1)} - 1\}. \tag{2.3}$$

The exponent on the left side of (2.3) is maximised when $r = 2$. We rearrange (2.3) accordingly to show that we require

$$\frac{p}{(\log p)^4} > C(2)^{16}(0.99)^{-8}\{2^{\omega(p-1)} - 1\}^{16}, \quad p > 10^{20}. \tag{2.4}$$

With $C(2) = 3.5751$ as in [16, Table 3], a quick computation shows that (2.4) is true for $17984 \le \omega(p-1) \le 18300$. For larger values of $\omega(p-1)$ we make use of the bound

$$\omega(n) \le \frac{\log n}{\log\log n}\left(1 + \frac{1}{\log\log n} + \frac{2.8973}{(\log\log n)^2}\right), \quad n \ge 3, \tag{2.5}$$

proved by Robin [15, Theorem 16]. Since the bound on the right of (2.5) is increasing for all $n > e^{e^2} > 1619$ and since $p-1 \ge p_1 \cdots p_{18301} > 5.9 \times 10^{88331}$, we have

$$2^{\omega(p-1)} \le p^{\frac{\log 2}{\log\log p}\left(1+\frac{1}{\log\log p}+\frac{2.8973}{(\log\log p)^2}\right)} \le p^{0.06245},$$

whence it follows that (2.4) is true for all p with $\omega(p-1) \ge 18301$.

Hence we need only consider $\omega(p-1) \le 17983$. Solving for p in (2.4) we find we need only consider $p < 10^{86650}$, which is much less than $10^{10^{10}}$. We reduce this upper bound substantially by introducing a sieving inequality in the next section.

3. A sieving inequality. Let e be an even divisor of $p-1$. Let $\mathrm{Rad}(n)$ denote the product of the distinct prime divisors of n. If $\mathrm{Rad}(e) = \mathrm{Rad}(p-1)$, then set $s = 0$ and $\delta = 1$. Otherwise, if $\mathrm{Rad}(e) < \mathrm{Rad}(p-1)$, let $p_1, \ldots, p_s$, $s \ge 1$, be the primes dividing $p-1$ but not e, and set $\delta = 1 - \sum_{i=1}^{s} p_i^{-1}$. In practice, it is essential to choose e so that $\delta > 0$.

Again let e be an even divisor of $p-1$. An integer x (indivisible by p) will be called *e-free* if, for any divisor d of e (with $d > 1$), the congruence $x \equiv y^d \pmod p$ is insoluble. With this terminology, x is a primitive root iff it is $(p-1)$-free. Given H let $N_e(H)$ be the number of integers x in the range $1 \le x \le H$ that are indivisible by p and such that x is e-free. Hereafter we write $\theta(n) = \phi(n)/n$.

LEMMA 3.1. *Suppose e is an even divisor of $p-1$. Then, in the above notation,*

$$N_{p-1}(H) \ge \sum_{i=1}^{s} N_{p_i e}(H) - (s-1)N_e(H). \tag{3.1}$$

Hence

$$N_{p-1}(H) \ge \sum_{i=1}^{s} [N_{p_i e}(H) - \theta(p_i)N_e(H)] + \delta N_e(H). \tag{3.2}$$

Proof. For a given e-free integer x, the right side of (3.1) contributes 1 if x is additionally p_i-free, and otherwise contributes a non-positive quantity. We deduce (3.2) by rearranging (3.1) bearing in mind the definitions of $\theta(p_i)$ and δ. ∎

Given the divisor e of $p-1$, we extend the definition of $f(x)$ to $f_e(x)$, where

$$f_e(x) = \theta(e)\Big\{1 + \sum_{d|e,\, d>1} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(x)\Big\}.$$

Hence $f_e(x) = 1$ if x is e-free, and $f_e(x) = 0$ otherwise, provided that $p \nmid x$. Thus,

$$N_e(H) = \sum_{x=1,\, x\not\equiv 0 \,(\mathrm{mod}\, p)}^{H} f_e(x).$$

It follows from Theorem 2.1 that, under the constraints of that theorem,

$$N_e(H) \ge \theta(e)\big(H - (W(e)-1)C(r)H^{1-1/r}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}}\big), \tag{3.3}$$

where $W(e) = 2^{\omega(e)}$ is the number of square-free divisors of e.

Similarly, for any prime divisor l of $p-1$ not dividing e,

$$\begin{aligned}\Big|N_{le}(H) - \Big(1 - \frac{1}{l}\Big)N_e(H)\Big| \\ \le \theta(e)\theta(l)W(e)C(r)H^{1-1/r}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}},\end{aligned} \tag{3.4}$$

where the factor $W(e)$ arises from the expression $W(le) - W(e)$.

Now apply (3.3) and (3.4) to (3.2) to obtain

$$N_{p-1}(H) \ge \delta\theta(e)H - C(r)H^{1-1/r}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}}\theta(e)W(e)\Big(\delta + \sum_{i=1}^{s}\theta(p_i)\Big).$$

Since $\sum_{i=1}^{s}\theta(p_i) = s - 1 + \delta$, this yields

$$N_{p-1}(H) \ge \delta\theta(e)\Big\{H - W(e)C(r)H^{1-1/r}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}}\Big(\frac{s-1}{\delta} + 2\Big)\Big\}. \tag{3.5}$$

As in §2, we take $H = (1 - 2/p_0^{1/2})p^{1/2}$ and $r = 2$ in (3.5). After some rearranging this proves the following refinement of Theorem 2.2.

Theorem 3.2. *Let e be an even divisor of $p-1$ and s, δ as in Lemma 3.1 with $\delta > 0$. Then $g(p) < \sqrt{p} - 2$ for $p > p_0$ provided that*

$$\frac{p}{\log^4 p} > C(2)^{16}\Big(1 - \frac{2}{p_0^{1/2}}\Big)^{-8}\Big\{\Big(\frac{s-1}{\delta} + 2\Big)2^{n-s}\Big\}^{16}. \tag{3.6}$$

We consider (3.6) for $\omega(p-1) = n \le 17983$. By making the choice of s for n given in Table 1, we obtain bounds on δ and p_0 that enable us to verify (3.6) for all $n \ge 42$. For example, when $n = 42$, choosing $s = 38$ shows that

$$\delta > 1 - \frac{1}{11} - \cdots - \frac{1}{181} > 0.2476, \qquad p - 1 \ge p_1 \cdots p_{42} := p_0 > 5.39 \times 10^{72}.$$

This verifies (3.6) since the left-hand side is greater than $p_0/\log^4 p_0 > 6.8 \times 10^{63}$ whereas the right-hand side is less than 1.01×10^{63}.

Table 1. Choices of s for various ranges of $\omega(p-1) = n$ such that (3.6) holds

Range of $\omega(p-1) = n$	s
$[800, 17983]$	750
$[400, 799]$	300
$[198, 399]$	180
$[108, 197]$	104
$[72, 107]$	68
$[55, 71]$	52
$[47, 54]$	44
$[43, 46]$	40
42	38

We are left with those p satisfying $\omega(p-1) \le 41$. When $\omega(p-1) = n = 41$ we choose $s = 37$ to minimise the right side of (3.6). This shows that Grosswald's conjecture is satisfied provided that

$$\frac{p}{\log^4 p} > 4.59 \times 10^{62}. \tag{3.7}$$

Solving (3.7) for p gives $p > 3.38 \times 10^{71}$. It is tempting to try to remove the $\omega(p-1) = 41$ case by enumerating possible primes as in [5]. Since $p - 1 > p_1 \cdots p_{41}$ we seek the number of solutions of

$$2.98 \times 10^{70} \le p \le 3.38 \times 10^{71}, \quad p \text{ prime}, \omega(p-1) = 41. \tag{3.8}$$

A quick computer check shows that there are 307 different primes that could appear in the factorisation of $p-1$. While it may be possible to enumerate all such products satisfying (3.8), this would, at best, eliminate the $n = 41$ case only. We have not pursued such an enumeration.

4. Computational results. The computational part of Theorem 1.1 was proved in the following way. The interval $[2, 2.5 \times 10^{15}]$ was subdivided into consecutive subintervals of manageable size (each with 2^{20} integers). An efficient segmented Eratosthenes sieve (see [2] and [13, §1.1]) was then used to identify all primes in each interval. For each prime p that was found, a second Eratosthenes sieve, modified to yield complete factorisations [6, §3.2.4], was used to find the factorisation of $(p-1)/2$. Since the least primitive root modulo p cannot be of the form a^b with $a > 0$ and $b > 1$, i.e., it cannot be a perfect power, the integers $2, 3, 5, 6, 7, 10, \ldots$ were tried one at a time until a primitive root was found.

With c as a candidate primitive root, the first test was to check if $c^{(p-1)/2} \equiv -1 \pmod p$. This was efficiently done using the quadratic reci-

procity law data from known tables. If this test failed the next c candidate was tried. Otherwise, for each odd prime factor q of $(p-1)/2$ it was checked whether $c^{(p-1)/q} \not\equiv 1 \pmod{p}$. The next c candidate was tried if one of these tests failed. These tests were efficiently done by performing all modular arithmetic using the Montgomery method [11]. Since the "probability" of failure of an individual test is $1/q$, the odd factors q were sorted in increasing order before performing these tests. Note that $g(p)$ is equal to the first c that passes all tests.

Instead of checking (1.1) directly for each prime up to 2.5×10^{15}, the record-holder values of $g(p)$, i.e., the values of $g(p)$ such that $g(p') < g(p)$ for all $p' < p$, were computed, as these are of independent interest [1] and can be used to check (1.1) indirectly. The computation required a total time of about three one-core years, and took about one month to finish on nine computers (each with four cores) of one computer lab of the Electronics, Telecommunications, and Informatics Department of the University of Aveiro. Table 2 presents all $g(p)$ record holders that were found up to 2.5×10^{15}. It extends and corrects one entry of Table 2 of [14], which is a summary of computations up to 4×10^{10}.

Table 2. $g(p)$ record holders with $p < 2.5 \times 10^{15}$

$g(p)$	p	$g(p)$	p	$g(p)$	p
2	3	69	110881	179	6064561441
3	7	73	760321	194	7111268641
5	23	94	5109721	197	9470788801
6	41	97	17551561	227	28725635761
7	71	101	29418841	229	108709927561
19	191	107	33358081	263	386681163961
21	409	111	45024841	281	1990614824641
23	2161	113	90441961	293	44384069747161
31	5881	127	184254841	335	89637484042681
37	36721	137	324013369	347	358973066123281
38	55441	151	831143041	359	2069304073407481
44	71761	164	1685283601		

The largest $g(p)$ record holder in Table 2 that does not satisfy (1.1) is 21, corresponding to $p = 409$. Thus, up to 2.5×10^{15}, the largest p for which (1.1) is possibly false satisfies $\sqrt{p}-2 < 21$, i.e., $p < 529$. This is covered by Grosswald's computations, which showed that there are no exceptions to (1.1) for $409 < p \le 10{,}000$.

An analysis similar to the one described above was also performed for least prime primitive roots $\hat{g}(p)$, and for least negative primitive roots $h(p)$.

The least negative primitive root modulo p is equal to the negative integer, least in absolute value, that is a primitive root modulo p. It cannot be of the form $-a^b$ with $a > 0$ and $b > 1$, and is equal to $-g(p)$ if $p \equiv 1 \pmod 4$. It was found that $\hat{g}(p) < \sqrt{p} - 2$ for $2791 < p < 2.5 \times 10^{15}$, and that $-h(p) < \sqrt{p} - 2$ for $409 < p < 10^{15}$. We remark that little is known about either $\hat{g}(p)$ or $h(p)$—the reader may consult [9] for more details.

5. Conclusion. It appears difficult to resolve Grosswald's conjecture completely. Table 3 in [16] indicates that one may hope to reduce the size of $C(2)$ further by taking a larger value of p_0. However, this appears at present not to give an improvement for our purposes.

An alternative approach would be to use a smoothed version of Burgess' bounds, in the same way that a smoothed Pólya–Vinogradov inequality was used in [8].

Acknowledgements. We should like to thank the referee for a thorough reading of the manuscript and for many helpful suggestions.

Some of this work was completed when the third author visited the first author. This visit was supported by the Royal Society of Edinburgh and the Edinburgh Mathematical Society; the authors are grateful for this support and for the hospitality of the School of Mathematics and Statistics at the University of Glasgow.

The third author is supported by Australian Research Council DECRA Grant DE120100173.

References

[1] E. Bach, *Comments on search procedures for primitive roots*, Math. Comp. 66 (1997), 1719–1727.

[2] C. Bays and R. H. Hudson, *The segmented sieve of Eratosthenes and primes in arithmetic progressions to* 10^{12}, Nordisk Tidskr. Informationsbehandling (BIT) 17 (1997), 121–127.

[3] A. R. Booker, *Quadratic class numbers and character sums*, Math. Comp. 75 (2006), 1481–1492.

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

[5] S. D. Cohen, T. Oliveira e Silva, and T. Trudgian, *A proof of the conjecture of Cohen and Mullen on sums of primitive roots*, Math. Comp. 84 (2015), 2979–2986.

[6] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd ed., Springer, New York, 2005.

[7] E. Grosswald, *On Burgess' bound for primitive roots modulo primes and an application to* $\Gamma(p)$, Amer. J. Math. 103 (1981), 1171–1183.

[8] M. Levin, C. Pomerance, and K. Soundararajan, *Fixed points for discrete logarithms*, in: Lecture Notes in Comput. Sci. 6197, Springer, Berlin, 2010, 6–15.

[9] G. Martin, *The least prime primitive root and the shifted sieve*, Acta Arith. 80 (1997), 277–288.
[10] K. J. McGown, *Norm-Euclidean cyclic fields of prime degree*, Int. J. Number Theory 8 (2012), 227–254.
[11] P. L. Montgomery, *Modular multiplication without trial division*, Math. Comp. 44 (1985), 519–521.
[12] P. Moree, *Artin's primitive root conjecture—a survey*, Integers 12 (2012), 1305–1416.
[13] T. Oliveira e Silva, S. Herzog, and S. Pardi, *Empirical verification of the even Goldbach conjecture and computation of prime gaps up to* $4 \cdot 10^{18}$, Math. Comp. 83 (2014), 2033–2060.
[14] A. Paszkiewicz and A. Schinzel, *Numerical calculation of the density of prime numbers with a given least primitive root*, Math. Comp. 71 (2002), 1781–1797.
[15] G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le* k*-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de* n, Acta Arith. 42 (1983), 367–389.
[16] E. Treviño, *The Burgess inequality and the least* k*th power non-residue*, Int. J. Number Theory 11 (2015), 1653–1678.

Stephen D. Cohen
School of Mathematics and Statistics
University of Glasgow
Glasgow G12 8QW, Scotland
E-mail: Stephen.Cohen@glasgow.ac.uk

Tim Trudgian
Mathematical Sciences Institute
The Australian National University
Canberra, ACT 2601, Australia
E-mail: timothy.trudgian@anu.edu.au

Tomás Oliveira e Silva
Departamento de Electrónica,
Telecomunicações e Informática
Universidade de Aveiro
3810-193 Aveiro, Portugal
E-mail: tos@ua.pt