Primality testing with Gaussian periods

H. W. Lenstra, Jr. and Carl Pomerance

This draft is preliminary, comments welcome.

1. Introduction

The problem of quickly determining whether a given large integer is prime or composite has been of interest for centuries, if not longer. The past 30 years has seen a great deal of progress, leading up to the recent deterministic, polynomial-time algorithm of Agrawal, Kayal, and Saxena [2]. This new "AKS test" for the primality of n involves verifying the polynomial congruence

$$(x+a)^n \equiv x^n + a \bmod (n, f(x)) \tag{1.1}$$

for varying choices of the integer a, where $f(x)$ is a particular integer monic polynomial that has a loose connection to n. The test then is to first construct an appropriate polynomial $f(x)$ and then verify (1.1) for every integer a in a certain, relatively small interval. If, in addition, n has no small prime factors and n is not a power, then n is prime. Note too that if n is prime, then (1.1) holds for every integer a and for every $f(x) \in \mathbf{Z}[x]$.

In particular, the AKS test for primality is based on the following beautiful theorem. Let φ denote Euler's function and $\log_2$ the base-2 logarithm.

Theorem AKS [2]. *Suppose n is an integer with $n > 1$, and q is an integer coprime to n with the multiplicative order of n mod q exceeding $(\log_2 n)^2$. With $f(x)$ the q-th cyclotomic polynomial, suppose (1.1) holds for every integer a with $1 \le a \le \sqrt{\varphi(q)}\log_2 n$. Then n either has a prime factor below $\sqrt{\varphi(q)}\log_2 n$ or n is a power of a prime.*

To use this result as a primality test, after a suitable value of q is found and n has been checked for proper prime factors below $\sqrt{\varphi(q)}\log_2 n$ and for being a power higher than the first power, one proceeds to check the congruences (1.1) for the requisite values of a. These congruences all hold if and only if such a number n is prime.

If the degree of $f(x)$ in (1.1) is d, the number of elementary operations to verify this congruence is $\tilde{O}(d(\log n)^2)$, assuming that $|a| < n$. (The notation $\tilde{O}(X)$ signifies a bound $c_1 X(\log X)^{c_2}$ for suitable positive constants c_1, c_2.) To achieve this time bound, one uses various fast arithmetic subroutines, see [14]. Thus the time to test n for primality using Theorem AKS is $\tilde{O}(q^{3/2}(\log n)^3)$.

It is not hard to show that for most numbers n (and for most prime numbers n), a valid choice for q may be found that satisfies $O((\log n)^2)$, and so the time bound $\tilde{O}((\log n)^6)$ is achieved. Further, it is conjectured in [2] that *every* $n > 1$ has such a valid choice for q. Two results are presented in [2] concerning the choice for q. The first, which is entirely elementary, shows that $q = O((\log n)^5)$, leading to the time bound $\tilde{O}((\log n)^{10.5})$ in the primality test. The second result in [2] is short, but uses a "big gun" in analytic number theory, namely the theorem of Fouvry [13] that a positive proportion of primes q have a prime factor $r \mid q-1$ with $r > q^{2/3}$. Using this tool, it is shown that there is a choice for q with $q = O((\log n)^3)$, leading to the time bound $\tilde{O}((\log n)^{7.5})$ for the primality test.

It should be noted that the proof of Fouvry's theorem depends ultimately on Siegel's theorem, a result that without a major breakthrough in the direction of the Extended Riemann Hypothesis (ERH) for Dirichlet L-functions, is numerically ineffective. Thus, there is no way to specify the implied constants in the time bound $\tilde{O}((\log n)^{7.5})$. (Actually, it is possible to specify numerical constants, but then the bound is proved to hold only for numbers n that are "sufficiently large" and we know no way to specify exactly how large.)

In contrast, the elementary bound for q of $O((\log n)^5)$ in [2] can actually be shown to be $(\log_2 n)^5$ for every $n \geq 3$, see [7], Theorem 4.5.3. And so with the complexity-$\tilde{O}((\log n)^{10.5})$-version of the AKS primality test, there is no mystery about implied constants or "sufficiently large."

In this paper we show how one may replace the choice of $f(x)$ as a cyclotomic polynomial in Theorem AKS with an arbitrary integer monic polynomial $f(x)$ of degree $d > (\log_2 n)^2$ that "behaves" as if it is irreducible in $(\mathbf{Z}/n\mathbf{Z})[x]$. Further, we show how such a polynomial may be chosen with $d = O((\log n)^2)$, and so obtain a deterministic primality test that achieves the complexity $\tilde{O}((\log n)^6)$. Though our arguments are not simple, they avoid the use of Siegel's theorem and other ineffective tools and arguments.

Theorem A. *There is a deterministic algorithm to determine if a given number $n > 1$ is prime or composite which runs within the effective time bound $\tilde{O}((\log n)^6)$.*

Apart from primality testing, one can raise the problem of constructing an irreducible polynomial $f(x)$ over the prime finite field $\mathbf{F}_p$ of a given degree d. This problem can be viewed as "constructing" the finite field $\mathbf{F}_{p^d}$. Even for $d = 2$, it is considered a hard problem, since it is equivalent to finding a quadratic nonresidue for the prime p. There is a trivially correct, deterministic algorithm to find a quadratic nonresidue, namely choose consecutive integers a starting at $a = 2$ until one is found. Assuming the ERH, this trivial algorithm can be proved to terminate before a reaches $2(\log p)^2$, and so runs in polynomial time. However, without assuming the ERH, we know no deterministic method for finding a quadratic nonresidue for p that takes subexponential time. (A better method for finding a quadratic nonresidue is to choose random numbers a until one is found. The expected number of trials is just 2, but this search is not deterministic.)

Adleman and Lenstra [1] showed more generally that assuming the ERH, there is a deterministic polynomial-time algorithm for constructing an irreducible polynomial over $\mathbf{F}_p$ of degree d. (The running time is polynomial in d and $\log p$.) Moreover, without assuming any unproved hypotheses, they presented a deterministic algorithm that given d and p, discovers an irreducible polynomial over $\mathbf{F}_p$ of degree d', where $d \leq d' < cd \log p$ for some absolute, effectively computable positive number c. They obtain their polynomials as the polynomials for certain cyclic extensions of the rationals which remain irreducible when considered over $\mathbf{F}_p$.

We improve on the unconditional algorithm from [1] for d large.

Theorem B. *There is a deterministic algorithm and an effectively computable number B, such that, given a prime $p > B$ and an integer $d > (\log p)^{1.84}$, produces an irreducible polynomial over $\mathbf{F}_p$ of degree d', where $d \leq d' \leq 4d$. Moreover the running time is $\tilde{O}(d^{1.6} \log p)$, with effective constants.*

Our paper is organized as follows. In section 2 we present the following primality criterion that is similar in spirit to Theorem AKS, but does not need to use cyclotomic polynomials.

Theorem C. *Suppose $n > 1$ is an integer and that $f(x)$ is an integer monic polynomial of degree $d > (\log_2 n)^2$. Suppose too that the following three conditions hold: both $f(x^n)$ and $x^{n^d} - x$ are congruent to 0 in the ring $\mathbf{Z}[x]/(n, f(x))$, and for each prime $l \mid d$, $x^{n^{d/l}} - x$ is a unit in this ring. If (1.1) holds for each integer a with $1 \leq a \leq d^{1/2} \log_2 n$, then n either has all of its prime factors at most $d^{1/2} \log_2 n$ or n is a power of a prime.*

As with Theorem AKS, it is a simple matter to distinguish primes from composites in the restricted set of integers which have a small prime factor or are a power of a prime. Thus, Theorem C may be used as the backbone of a primality test once one has a method to produce polynomials $f(x)$ of suitable degrees that satisfy the initial hypotheses.

Note that if n is prime and $f(x)$ is irreducible over $\mathbf{F}_n$, then the three conditions about $f(x)$ in Theorem C all hold. In section 3, we describe how polynomials $f(x)$ may be constructed that are guaranteed to be irreducible modulo n if n is prime. These are the polynomials that we use to prove Theorem B and are the polynomials we use in the primality test of Theorem A. In the primality criterion, we do not know that n is prime, but the three conditions of Theorem C may be tested. If one of these conditions should fail, we have proved that n is composite. If they all hold, we can then proceed to use Theorem C to decide if n is prime or composite. The polynomials discussed in section 3 are related to Gaussian periods, certain sums of roots of unity that Gauss employed in his famous proof that for $n \geq 3$, a regular n-gon is constructible with straight-edge and compass provided $\varphi(n)$ is a power of 2.

In section 4 we state our main technical result that allows us to construct our polynomials of near-prescribed degree, and present some useful elementary lemmas. This technical result corresponds to the argument in [2] that an integer q exists as in Theorem AKS that is not too large, and in fact, we use some similar devices in our introductory lemmas. Proved over the subsequent 4 sections, a statement of this technical result is as follows.

Theorem D. *There is a deterministic algorithm such that for all integers n beyond an effectively computable bound, and any integer $D > (\log n)^{1.84}$, the algorithm finds a finite collection of integer pairs $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$ such that each r_i is prime and $r_i < D^{6/11}$, and each q_i satisfies $1 < q_i < D^{3/11}$, $q_i \mid r_i - 1$, and the multiplicative order of*

$n^{(r_i-1)/q_i}$ modulo r_i is q_i. Further, the integers $q_1, q_2, \ldots, q_k$ are pairwise coprime and satisfy $D \le q_1 q_2 \cdots q_k \le 4D$. The number k is $O((\log\log D)^2)$, and the running time of the algorithm is $\tilde{O}(D^{12/11})$, with both of these estimates having effective implied constants.

Theorem D is proved with tools from analytic number theory. In section 5 we review some results concerning the distribution of primes in residue classes, and give a somewhat weaker, but effective version of the Bombieri–Vinogradov inequality. (See [19] for a similar result.) We also introduce our major tool, a theorem of Deshouillers and Iwaniec [10]. This result is a "prequel" to Fouvry's theorem, and is interesting to us not only for its strength, but because it is effective in prinicple.

In section 6 we show that there are many primes r with certain stringent constraints on the primes in $r-1$. For this we follow closely a paper of Balog [4]. This paper uses the same theorem of Fouvry as in [2], and also the Bombieri–Vinogradov theorem. To achieve effectively computable estimates, we use instead the Deshouillers–Iwaniec result and the effective Bombieri–Vinogradov inequality from section 5.

The famous Frobenius postage problem asks for the largest number which is not in the additive semigroup generated by a set of coprime positive integers. Section 7 presents a new result of Bleichenbacher [6] that might be considered a continuous version of this problem. It is proved that $1/M(S)$ is a strict upper bound for the set of numbers not in the additive semigroup generated by the open subset S of the interval $(0,1)$, where $M(S)$ is the logarithmic measure $\int_S dx/x$. Similar results were also recently obtained by Lev [16].

In section 8 we tie together the results of the previous two sections to give a proof of Theorem C.

Section 9 presents an algorithm for constructing suitable polynomials as mentioned above. With $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$ as in Theorem D, the polynomial constructed is the minimum polynomial over $\mathbf{Q}$ of the product of the Gaussian periods η_{r_j,q_j}, the degree-q_j period in the cyclotomic field $Q(e^{2\pi i/r_j})$. The degree of this polynomial is the product $q_1 q_2 \cdots q_k$.

Finally in section 10 we present our primality test and analyze its complexity.

2. A primality criterion

In this section we consider the main theorem behind our primality test. The reader will readily note many similarities with the results of Agrawal, Kayal and Saxena. The principal difference here is that the auxiliary polynomial that one uses is allowed to be any monic polynomial in $\mathbf{Z}[x]$ that "behaves" as if it is irreducible over the "finite field" $\mathbf{Z}/n\mathbf{Z}$. This concept is made precise shortly.

We begin first with a general result about commutative rings.

Easy Fact. *Suppose that $\mathcal{R}$ is a commutative ring with unit, $f \in \mathcal{R}[x]$, $\beta_1, \beta_2, \ldots, \beta_k \in \mathcal{R}$ with $f(\beta_i) = 0$ for $1 \leq i \leq k$ and $\beta_j - \beta_i \in \mathcal{R}^*$ for $1 \leq i < j \leq k$. Then $\prod(x - \beta_i) \mid f(x)$.*

To prove the Easy Fact, one first notes that it is true for $k = 1$ since there is some $q \in \mathcal{R}[x]$ and some $\rho \in \mathcal{R}$ with $f(x) = (x - \beta_1)q(x) + \rho$, so that upon letting $x = \beta_1$ we see that $\rho = 0$. The general case now follows by induction since if $f(x) = h(x)(x-\beta_1)\cdots(x-\beta_{j-1})$, upon letting $x = \beta_j$ and using the hypotheses, we see that $h(\beta_j) = 0$, so that $x - \beta_j \mid h(x)$.

We now introduce the main ideas of this section. Suppose $f \in \mathbf{Z}[x]$ is monic of degree $d > 0$, n is an integer with $n > 1$, and

$$A \;=\; \mathbf{Z}[x]/(n, f).$$

Let $\alpha = x + (n, f) \in A$. Suppose that

$$f(\alpha^n) = 0, \tag{2.1}$$

$$\alpha^{n^d} = \alpha, \tag{2.2}$$

$$\alpha^{n^{d/l}} - \alpha \in A^* \quad \text{for all primes} \quad l \mid d. \tag{2.3}$$

Note that if n is prime, then (2.1) holds. Further, if n is prime, then (2.2) and (2.3) hold if and only if f is irreducible modulo n.

Whether or not n is prime, we shall first see what properties may be deduced from the above assumptions. First note that A is a free $\mathbf{Z}/n\mathbf{Z}$-module with basis $1, \alpha, \ldots, \alpha^{d-1}$. Also note that the ring homomorphism from $\mathbf{Z}[x]$ to $\mathbf{Z}[x]$ which takes x to x^n induces a ring homomorphism from A to A which takes α to α^n. Indeed this follows immediately

from (2.1). We denote this ring endomorphism of A by σ. Note that (2.2) implies that σ^d is the identity map on A, so that σ is an automorphism of A and has order dividing d. Further, (2.3) implies that σ has exactly order d.

Lemma 2.1. *In $A[y]$ we have $f(y) = \prod_{i=0}^{d-1}(y - \sigma^i\alpha)$.*

Proof. This lemma will follow from the Easy Fact if we show that each $f(\sigma^i\alpha) = 0$ and that

$$\sigma^i\alpha - \sigma^j\alpha \in A^* \text{ for } 0 \leq j < i < d. \tag{2.4}$$

Indeed, both $f(y)$ and $\prod(y - \sigma^i\alpha)$ are monic of degree d, so if the product divides $f(y)$, they are equal. Since σ is an automorphism of A it follows instantly that each $f(\sigma^i\alpha) = 0$. To show (2.4), it suffices to consider the case $j = 0$ (since σ is an automorphism). Note that d does not divide i so that there is some prime $l \mid d$ with $(i, d) \mid d/l$. Hence there are integers u, v with $ui + vd = d/l$. Since σ has order d it then follows that $\sigma^{ui}\alpha = \sigma^{d/l}\alpha$. Hence by (2.3), $\sigma^{ui}\alpha - \alpha \in A^*$. But $n^i - 1 \mid n^{ui} - 1$ so that $\alpha^{n^i-1} - 1 \mid \alpha^{n^{ui}-1} - 1$, and so

$$\sigma^i\alpha - \alpha \;=\; \alpha^{n^i} - \alpha \;\mid \alpha^{n^{ui}} - \alpha \;=\; \sigma^{ui}\alpha - \alpha.$$

But a divisor of a unit is a unit, so we are done.

Let p denote a prime factor of n, and let $R = A/pA \cong \mathbf{Z}[x]/(p, f)$. We identify members of A with their image in R, so in particular the coset $x + (p, f)$ is denoted by α. The ring R is a vector space over $\mathbf{Z}/p\mathbf{Z}$ with basis $1, \alpha, \ldots, \alpha^{d-1}$. Note that R is not necessarily a field since the polynomial f is not necessarily irreducible modulo p. Our automorphism σ of A naturally induces an automorphism of R, which we will continue to denote as σ. Further, (2.3) implies that in R we have that $\sigma^{d/l}(\alpha) \neq \alpha$ for all primes l dividing d, so that σ has order d as well when considered as an R-automorphism. Among the automorphisms of R is the Frobenius automorphism ϕ which sends every element to its p-th power.

Lemma 2.2. *Viewing σ as an automorphism of R, there is some integer i with $\sigma^i = \phi$.*

Proof. It suffices to show that for some integer i we have $\sigma^i\alpha = \alpha^p$, since if two automorphisms agree on a generator of the ring, they are the same automorphism. As ϕ is an

automorphism of R it follows that $f(\phi\alpha) = 0$, and so it follows from Lemma 2.1 taken over to R that

$$\prod_{i=0}^{d-1}(\alpha^p - \sigma^i\alpha) = 0. \tag{2.5}$$

To see that a factor in this product must be 0 we prove the following for $\beta \in R$:

$$\text{if } \sigma\beta \in \beta R \text{ then } \beta = 0 \text{ or } \beta \in R^*. \tag{2.6}$$

(Note that the converse of (2.6) is trivially true.) Indeed, if we know (2.6), it remains to note that for any integers i, j we have

$$\sigma(\alpha^i - \alpha^j) = \alpha^{in} - \alpha^{jn} = \left(\alpha^i - \alpha^j\right)\left(\alpha^{i(n-1)} + \alpha^{i(n-2)+j} + \cdots + \alpha^{j(n-1)}\right) \in (\alpha^i - \alpha^j)R,$$

so that $\alpha^i - \alpha^j$ is either 0 or a unit. But not all of the factors in (2.5) can be units, so one must be 0.

We now prove (2.6). Assume that $\sigma\beta \in \beta R$ and that β is not 0 and not a unit. Write $\beta = g(\alpha)$ where $g \in (\mathbf{Z}/p\mathbf{Z})[y]$, $\deg g < d$. Since $\beta R \neq R$, we have that the projection $R \to R/\beta R$ takes units to units. The ring $R/\beta R$ also contains $\mathbf{Z}/p\mathbf{Z}$ so that if we use an overbar to denote the image of an R-element in $R/\beta R$, then $\overline{g(\gamma)} = g(\overline{\gamma})$ for all $\gamma \in R$. The assumption that $\sigma\beta \in \beta R$ immediately implies that each $\sigma^i\beta \in \beta R$, so that

$$0 \;=\; \overline{\sigma^i\beta} \;=\; \overline{g(\sigma^i\alpha)} \;=\; g(\overline{\sigma^i\alpha}).$$

It now follows from (2.4) and the Easy Fact applied to the ring $R/\beta R$ that the degree of g is at least d, a contradiction. We now have the lemma.

Let

$$G \;=\; \{\beta \in R : \beta \neq 0,\ \sigma\beta = \beta^n\}.$$

Note that $1, \alpha \in G$ and $\sigma G \subset G$.

Lemma 2.3. *G is a cyclic subgroup of R^*.*

Proof. It is clear from the definition of G and (2.6) that G is a subgroup of R^*. It remains to show that G is cyclic. Let f_1 be an irreducible factor of f considered over $\mathbf{Z}/p\mathbf{Z}$, and

let K denote the finite field $\mathbf{Z}[x]/(p, f_1)$. There is a natural projection ψ from R to K. We shall show that the restriction of ψ to G is injective, so that G is isomorphic to a subgroup of K^*. Since K^* is itself cyclic, the lemma will follow.

Say $\beta \in G$ and $\psi\beta = 1$. Write $\beta = g(\alpha)$ where $g \in (\mathbf{Z}/p\mathbf{Z})[y]$ has degree $< d$. Since $\beta \in G$ we have $\sigma^i\beta = \beta^{n^i}$ for each i, so that

$$g(\psi\sigma^i\alpha) \;=\; \psi\sigma^i g(\alpha) \;=\; \psi\sigma^i\beta \;=\; \psi(\beta^{n^i}) \;=\; (\psi\beta)^{n^i} \;=\; 1.$$

It then follows from (2.4) and the Easy Fact applied to K that either $g(y) - 1$ is the 0-polynomial or has degree at least d. Hence it is 0, so that $1 = g(\alpha) = \beta$. Thus, $\psi|_G$ is injective, which completes the proof of the lemma.

Lemma 2.4. *Among the ordered pairs of integers (i, j) with $0 \le i, j \le \sqrt{d}$ there are two different pairs $(i_0, j_0), (i_1, j_1)$ with $p^{i_0}(n/p)^{j_0} \equiv p^{i_1}(n/p)^{j_1} \pmod{\#G}$.*

Proof. We consider the automorphism group of G. For any finite cyclic group G under multiplication, the automorphism group is naturally isomorphic to $(\mathbf{Z}/(\#G)\mathbf{Z})^*$ where a residue m corresponds to π_m, the map which takes elements of G to their m-th powers. By the definition of G, our ring automorphism σ acts as well as a group automorphism of G and is identified with π_n. We consider the order-d subgroup $\langle\sigma\rangle = \langle\pi_n\rangle$ of $\operatorname{Aut} G$. By Lemma 2.2, the Frobenius map ϕ is in this subgroup; it is identified with π_p. So, $\sigma\phi^{-1}$, which is identified with $\pi_{n/p}$, is in the subgroup as well.

Consider the automorphisms $\pi_p^i\pi_{n/p}^j$ for integers i, j with $0 \le i, j \le \sqrt{d}$. There are more than d of these expressions, and they all lie in a subgroup of order d, so two of them must be equal: say

$$\pi_p^{i_0}\pi_{n/p}^{j_0} \;=\; \pi_p^{i_1}\pi_{n/p}^{j_1},$$

where $(i_0, j_0), (i_1, j_1)$ are different pairs. Then

$$p^{i_0}(n/p)^{j_0} \;\equiv\; p^{i_1}(n/p)^{j_1} \pmod{\#G},$$

as claimed.

For a pair (i, j) considered in Lemma 2.4, note that $p^i(n/p)^j \le p^{\sqrt{d}}(n/p)^{\sqrt{d}} = n^{\sqrt{d}}$. Our goal now is show that under a certain easily checkable hypothesis we have $\#G > n^{\sqrt{d}} - 1$, which will allow us to turn the congruence of Lemma 2.4 into an equality.

We say a positive integer is B-smooth if it is not divisible by any prime exceeding B.

Theorem 2.5. *Let $f \in \mathbf{Z}[x]$ be a monic polynomial of degree d, let $n > 1$ be an integer, let $A = \mathbf{Z}[x]/(n, f)$, and let $\alpha = x + (n, f) \in A$. Assume that (2.1), (2.2), and (2.3) hold, and in addition, suppose that*

$$d > (\log_2 n)^2, \tag{2.7}$$

$$(\alpha + a)^n = \alpha^n + a \quad \text{for each integer} \quad a,\ 1 \le a \le B := \lfloor \sqrt{d} \log_2 n \rfloor. \tag{2.8}$$

Then n is B-smooth or a prime power.

Proof. Suppose that n is not B-smooth so that n has a prime factor $p > B$. Let R be the ring $A/pA \cong \mathbf{Z}[x]/(p, f)$. Let σ be the automorphism of R that takes α to α^n. Our first task is to show that the cyclic group G considered in Lemma 2.3 is large. For each proper subset S of $\{0, 1, \ldots, B\}$, we assert that

$$\prod_{a \in S} (\alpha + a)$$

is a member of G and that different choices for S give rise to different members of G. Indeed, by (2.8), $\sigma(\alpha + a) = \alpha^n + a = (\alpha + a)^n$ for $1 \le a \le B$ and the same is true trivially for $a = 0$. Thus, it is clear that each product is in $G \cup \{0\}$. Corresponding to S consider the polynomial $\prod_{a \in S}(x + a)$. Since $d > B$ and $p > B$ it follows that these polynomials over $\mathbf{Z}/p\mathbf{Z}$ are distinct, nonzero and have degrees $< d$. So evaluating these polynomials at α gives rise to distinct nonzero members of R, which proves our assertion. Thus $\#G$ is at least as big as the number of such sets S, that is,

$$\#G \ \ge\ 2^{B+1} - 1 \ >\ 2^{\sqrt{d} \log_2 n} - 1 \ =\ n^{\sqrt{d}} - 1. \tag{2.9}$$

As we noted above, for $0 \le i, j \le \sqrt{d}$, we have

$$1 \ \le\ p^i (n/p)^j \ \le\ p^{\sqrt{d}} (n/p)^{\sqrt{d}} \ =\ n^{\sqrt{d}}.$$

Thus, if we have two different pairs (i, j) in this range, the gap between the two expressions $p^i (n/p)^j$ is at most $n^{\sqrt{d}} - 1$. So consider the two different pairs $(i_0, j_0), (i_1, j_1)$ guaranteed for us by Lemma 2.4. Thus, by that lemma and (2.9) we have

$$p^{i_0} (n/p)^{j_0} \ =\ p^{i_1} (n/p)^{j_1}.$$

Since $(i_0, j_0), (i_1, j_1)$ are different pairs, we have $j_0 \neq j_1$, so that by unique factorization, n is a power of p. This completes the proof of the theorem.

3. Gaussian periods

If m is a positive integer and a is an integer coprime to m, we let $\mathrm{ord}\,(a \bmod m)$ denote the multiplicative order of a modulo m.

For prime r, let $\zeta_r = e^{2\pi i/r}$. If q is a positive integer with $q \mid r-1$, we can consider the *Gaussian period* $\eta_{r,q}$. This is the trace of ζ_r to the unique subfield of $\mathbf{Q}(\zeta_r)$ of degree q over $\mathbf{Q}$. Thus, if

$$S \;=\; \{s \bmod r : s^{(r-1)/q} \equiv 1 \pmod r\}$$

is the subgroup of q-th powers in $(\mathbf{Z}/r\mathbf{Z})^*$, then

$$\eta_{r,q} \;=\; \sum_{s \in S} \zeta_r^s.$$

Let w be a residue modulo r such that $\mathrm{ord}\,(w^{(r-1)/q} \bmod r) = q$ (in particular, any primitive root modulo r has this property). Then the q cosets of S in $(\mathbf{Z}/r\mathbf{Z})^*$ are $w^j S$ for $j = 0, 1, \ldots, q-1$. Let $g_{r,q}$ be the minimum polynomial for $\eta_{r,q}$ over $\mathbf{Q}$, so that

$$g_{r,q}(x) \;=\; \prod_{j=0}^{q-1} \left(x - \sum_{s \in S} \zeta_r^{w^j s} \right).$$

The polynomial $g_{r,q}(x)$ is integer monic and irreducible in $\mathbf{Q}[x]$. For prime p we may ask if $g_{r,q}(x)$, when considered in $\mathbf{F}_p[x]$, is irreducible. The following theorem of Kummer gives a criterion for this event.

Lemma 3.1. *Suppose that p is a prime number. For r prime and q a positive divisor of $r-1$, the polynomial $g_{r,q}(x)$ is irreducible when considered in $\mathbf{F}_p[x]$ provided that* $\mathrm{ord}\,(p^{(r-1)/q} \bmod r) = q$.

Proof. A proof of this result is given in [1]; here is another proof. We may assume that $q > 1$ and that $\mathrm{ord}\,(p^{(r-1)/q} \bmod r) = q$. Let K be the field of rq-th roots of unity over $\mathbf{F}_p$. There is a natural projection ψ of $\mathbf{Z}[\zeta_r, \zeta_q]$ to K. Let $\eta = \psi(\eta_{r,q})$. Since $g_{r,q}(\eta) = 0$, and the degree of $g_{r,q}(x)$ is q, it suffices to show that the degree d of η over $\mathbf{F}_p$ is q. Let

ϕ be the Frobenius p-th power automorphism of K, so the degree d of an element α of K over $\mathbf{F}_p$ is the least positive integer d such that $\phi^d(\alpha) = \alpha$. We have

$$\phi^j(\eta) \;=\; \eta^{p^j} \;=\; \sum_{s\in S} \zeta^{p^j s}, \qquad (\,\zeta = \psi(\zeta_r)\,)$$

where S is defined above as the group of q-th powers modulo r. Since $p^q \bmod r$ is a member of S, it follows that $\phi^q(\eta) = \eta$, and so we have $d \mid q$.

Let χ be the Dirichlet character modulo r which sends S to 1 and p to ζ_q. (Since $S, pS, \ldots, p^{q-1}S$ are the q cosets of S in $(\mathbf{Z}/r\mathbf{Z})^*$, the two conditions are sufficient to define χ.) Since $q > 1$ and q is the order of χ, we have that χ is non-principal, and since r is prime, it follows that χ is primitive. Thus, if $\tau(\chi)$ is the Gauss sum $\sum_{j \bmod r} \chi(j)\zeta_r^j$, we have $|\tau(\chi)|^2 = r$. In particular, $\psi(\tau(\chi)) \neq 0$. Letting $\omega = \psi(\zeta_q)$, we have

$$\psi(\tau(\chi)) \;=\; \sum_{j=1}^{r-1} \psi(\chi(j))\zeta^j \;=\; \sum_{i=0}^{q-1} \omega^i \sum_{j\in p^i S} \zeta^j \;=\; \sum_{i=0}^{q-1} \omega^i \eta^{p^i}.$$

We reorganize this last sum by writing $i = m + ld$, with $0 \le m \le d-1$, $0 \le l \le q/d - 1$, getting

$$\psi(\tau(\chi)) \;=\; \sum_{m=0}^{d-1} \eta^{p^m} \sum_{l=0}^{q/d-1} \omega^{m+ld} \;=\; \sum_{m=0}^{d-1} \eta^{p^m}\omega^m \sum_{l=0}^{q/d-1} \omega^{ld}.$$

But if d is a proper divisor of q, this last inner sum is 0, so that $\psi(\tau(\chi)) = 0$, a contradiction. Thus, $d = q$, which proves the lemma.

Remark. It is not hard to prove that the condition $\operatorname{ord}(p^{(r-1)/q} \bmod r) = q$ is necessary for $g_{r,q}$ to be irreducible over $\mathbf{F}_p$.

Corollary 3.2. *Suppose $r_1, r_2, \ldots, r_k$ are primes, $q_1, q_2, \ldots, q_k$ are pairwise coprime positive integers, with each $q_i \mid r_i - 1$, and p is a prime with each* $\operatorname{ord}(p^{(r_i-1)/q_i} \bmod r_i) = q_i$. *If η is the product of the Gaussian periods η_{r_i,q_i} and f is the minimum polynomial for η over $\mathbf{Q}$, then f is irreducible when considered in $\mathbf{F}_p[x]$.*

Proof. By Lemma 3.1, each η_{r_i,q_i}, when considered in an appropriate extension of $\mathbf{F}_p$, has degree q_i over $\mathbf{F}_p$. But in general, if $\alpha_1, \alpha_2, \ldots, \alpha_k$ all lie in an extension of $\mathbf{F}_p$ and have pairwise coprime degrees, their product α has degree $q = q_1 q_2 \cdots q_k$ over $\mathbf{F}_p$. Indeed, if ϕ

is the Frobenius p-th power automorphism, and l is a prime factor of q, say $l \mid q_i$, then $\phi^{q/l}(\alpha_j) = \alpha_j$ for $j \neq i$ and $\phi^{q/l}(\alpha_i) \neq \alpha_i$, so that $\phi^{q/l}(\alpha) \neq \alpha$.

4. Period systems

In this and subsequent sections, all labeled and implied constants are absolute (in that they do not depend on any parameters) unless otherwise stated, and they are all effective. In addition if a variable is to be taken "sufficiently large," either absolutely or depending on other variables, such a sufficiently large bound may be effectively computed.

For a positive integer n, we say a sequence $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$ of ordered pairs of positive integers is a *period system* for n if

(a) $r_1, r_2, \ldots, r_k$ are primes,

(b) for $i = 1, 2, \ldots, k$ we have $q_i \mid r_i - 1$, $q_i > 1$, and $\operatorname{ord}\,(n^{(r_i-1)/q_i} \bmod r_i) = q_i$,

(c) $q_1, q_2, \ldots, q_k$ are pairwise coprime.

Theorem 4.1. *There is a deterministic algorithm such that for each integer $m > 0$ the algorithm produces an integer D_m and further, for each integer $n > 1$, and each integer D with $D > D_m$ and $D > (\log n)^{11/6+1/m}$, the algorithm finds a period system $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$ for n with each $r_i < D^{6/11}$ and each $q_i < D^{3/11}$, with $D \leq q_1 q_2 \cdots q_k < 4D$, and with $k = O((\log\log D)^2)$. The running time of this algorithm is $\tilde{O}(D^{12/11})$. The implied constants may depend on the choice of m.*

Remarks. We will be applying Theorem 4.1 in the case $D = (\log_2 n)^2$, so that m may be taken as 6. There is nothing special about the number "4" in the theorem, it is only a convenient choice which may be replaced with any number larger than 1. Further, we can show that the interval $[D, 4D]$ contains more than $D/e^{c(\log\log D)^3}$ integers of the form $q_1 q_1 \cdots q_k$ as in the theorem. If we do not insist on effectivity, this last result can be improved to $D/(\log D)^c$ integers of the form $q_1 q_2 \cdots q_k$ in $[D, 4D]$ corresponding to period systems for n. Further, k may then be taken as $O(1)$, and the range for D may be widened to $D > (\log n)^{1+\epsilon}$.

It will be convenient for us to prove Theorem 4.1 with $q_1, q_2, \ldots, q_k$ being distinct primes. In the sequel we will denote $1/m$ by ϵ.

Recall the definition of a B-smooth number from section 2. It is known from work of Hildebrand and Maier that the number of B-smooth numbers in the interval $[1, x]$ is $\sim \rho(\log x/\log B)x$ as $x \to \infty$ with $B > \exp((\log\log x)^{5/3+\epsilon})$. Here $\rho(u)$ denotes the Dickman–de Bruijn function. This continuous function is identically 1 for $0 \le u \le 1$ and satisfies the differential-delay equation $u\rho'(u) = -\rho(u-1)$ for $u > 1$. We have $\log\rho(u) = -u\log(u\log u) + O(u)$ for $u \ge 2$. The result of Hildebrand and Maier will not be used in the sequel, but the function $\rho(u)$ does play a role.

We begin with a result concerning the ord function which will allow us to have in play many pairs (r, q) with which to construct a period system. First we cite a result from [18]. The methods used there, though not explicitly stated as such, are effective. Let $\pi(x)$ denote the number of primes in the interval $[1, x]$.

Lemma 4.2. *There is an absolute and effectively computable positive number c_0 with the following property. Let α be a number with $0 < \alpha < 1$, and let x be so large that $\log x/\log\log x > 1/\alpha^4$. The number of primes $r \le x$ such that $r-1$ has a divisor m with $m > x^\alpha$ and with m being x^{α^2}-smooth is at most $D(\alpha)\pi(x)$, where*

$$D(\alpha) \;=\; \frac{c_0}{\alpha^2}\left(\frac{\rho(1/\alpha)}{\log(2/\alpha)} + \rho(1/\alpha^2)\right).$$

Proposition 4.3. *Let $n > 20$ be a natural number, let x be a number such that $x \ge (\log n)^{1+3/\log\log\log n}$, and let $\alpha = \alpha(x) = 1/\log\log x$. Let $R(x, n)$ denote the number of primes $r \le x$ such that $r-1$ has a prime divisor $q > x^{\alpha^2}$ with $\operatorname{ord}(n^{(r-1)/q} \bmod r) = q$. For n larger than an effectively computable bound, we have*

$$R(x, n) \;\ge\; (1 - D(\alpha))\pi(x) - x^{1-\alpha^2} - x^{1-\alpha/4}.$$

Proof. The number of primes r which divide n or some $n^j - 1$ for $j \le x^\alpha$ is less than

$$\log_2 n + \sum_{j \le x^\alpha} j\log_2 n \;<\; x^{2\alpha}\log_2 n \;<\; x^{1-\alpha/4}$$

if n is so large that $\log_2 n < x^{1-9\alpha/4}$. Thus, there are at least $\pi(x) - x^{1-\alpha/4}$ primes $r \le x$ not dividing n, and not dividing any $n^j - 1$ as above. For such a prime r we have $\operatorname{ord}(n \bmod r) > x^\alpha$. Let q_r denote the greatest prime factor of $\operatorname{ord}(n \bmod r)$. If n is so

large that $\log x/\log\log x > 1/\alpha^4$, Lemma 4.2 is applicable, and we have $q_r > x^{\alpha^2}$, but for at most $D(\alpha)\pi(x)$ exceptional primes $r \le x$. Note that the number of integers $r \le x$ with $r-1$ divisible by some l^2 with l prime and $l > x^{\alpha^2}$ is at most

$$\sum_{\substack{l \text{ prime} \\ l > x^{\alpha^2}}} \frac{x}{l^2} \;<\; x^{1-\alpha^2}.$$

Hence, there are at least $(1-D(\alpha))\pi(x) - x^{1-\alpha^2} - x^{1-\alpha/4}$ primes $r \le x$ with $q_r > x^{\alpha^2}$ and q_r^2 does not divide $r-1$. For such a prime r we have $\operatorname{ord}(n^{(r-1)/q_r} \bmod r) = q_r$. This completes the proof of the proposition.

Remark. Proposition 4.3 implies that for n, x as given, we have

$$\pi(x) - R(x,n) = O\left(x/(\log x)^{\log\log\log x}\right).$$

5. The distribution of primes in residue classes

For a natural number q, an integer a coprime to q, and a real number x, let $\pi(x,q,a)$ denote the number of primes $p \le x$ with $p \equiv a \bmod q$. Also, let

$$\psi(x,q,a) \;=\; \sum_{\substack{n \le x \\ n \equiv a \bmod q}} \Lambda(n), \quad \theta(x,q,a) \;=\; \sum_{\substack{p \le x,\ p \text{ prime} \\ p \equiv a \bmod q}} \log p,$$

where $\Lambda(n)$ is von Mangoldt's function. (We have $\Lambda(n) = \log p$ if $n = p^j$ for some prime p and some positive integer j, and $\Lambda(n) = 0$ if n is not a power of a prime.)

Dirichlet proved in 1837 that if q is a positive integer coprime to the integer a, then $\pi(x,q,a)$ is unbounded, in fact, he showed that the sum of the reciprocals of the primes $p \equiv a \bmod q$ diverges. In 1896, de la Vallée Poussin proved the prime number theorem for arithmetic progressions. This result asserts that for q, a as in Dirichlet's theorem, we have $\pi(x,q,a) \sim \pi(x)/\varphi(q)$ as $x \to \infty$. In the last 100+ years people have been trying to improve on this result, by allowing $q \to \infty$ as well. Clearly q cannot be as large as x, since then the assertion loses meaning. We know that if the ERH is assumed then we can take q up to nearly $x^{1/2}$. But rigorously, we only have asymptotics for each individual $\pi(x,q,a)$, with effective error estimates, for $q < (\log x)^{2-\epsilon}$, see [8], page 123. Allowing the ineffective

theorem of Siegel allows us to extend this range to $q < (\log x)^A$ for any fixed A, giving us the Page–Siegel–Walfisz theorem. However, since our goal is to use only effective tools, we will bypass this result.

Other ways that the prime number theorem for arithmetic progressions has been extended is to allow for a few exceptional moduli, and then to prove results about the remaining unexceptional moduli. One such theorem is found in [3]. Another type of theorem is to show that the exceptional moduli *in toto* do not contribute too much to the error on average. An example of such a result is the Bombieri–Vinogradov theorem, which we discuss below. As it stands, this result uses Siegel's theorem to show that the contribution from exceptional moduli is small. We give a result that instead just ignores the exceptional moduli, if there are any.

Finally, barring asymptotics, or asymptotics on average, we have inequalities. In particular, the Brun–Titchmarsh inequality gives useful upper bounds for $\pi(x, q, a)$. However, this inequality degrades as q grows larger, so people have tried to get results that do not degrade so rapidly or are at least better on average. A culmination of these efforts is found in the series of papers of Bombieri–Friedlander–Iwaniec. However, these papers and many others, use Siegel's theorem. Further, unlike with the Bombieri–Vinogradov theorem, it does not seem so simple to disentangle Siegel's theorem from the result. As it turns out, we do not need a great improvement on the Brun–Titchmarsh inequality, just a small improvement. And a result of Deshouillers–Iwaniec from 1981 fills the bill: it is effective, and strong enough for our needs.

In this section we collect the main results we shall use on $\pi(x, q, a)$, including a proof-sketch of a version of the Bombieri–Vinogradov theorem that is effective.

Lemma 5.1. [Brun–Titchmarsh inequality] *If $x > q$ we have*

$$\pi(x, q, a) \ \leq \ \frac{2x}{\varphi(q)\log(x/q)}.$$

The lemma in this form is due to Montgomery and Vaughan [17]. Note that the inequality gives an upper bound for $\pi(x, q, a)$ that is of the expected order of magnitude, namely $x/(\varphi(q)\log x)$, if $q < x^{1-\epsilon}$. When q is of order of magnitude x^α, the upper bound provided by the lemma is presumably too large by a factor $2/(1-\alpha)$.

A result similar to the following lemma can be found in Timofeev [19], Theorem 2.

Lemma 5.2. [effective Bombieri–Vinogradov inequality] *There are absolute, effectively computable positive numbers c_1, c_2 such that for all numbers $x \geq 3$, there is an integer set $\mathcal{S}(x) \subset [(\log x)^{1/2}, \exp\left((\log x)^{1/2}\right)]$ of cardinality 0 or 1, such that for each number $Q \in [x^{1/3}\log x,\, x^{1/2}]$,*

$$\sum_{q\leq Q}{}' \max_{2\leq y\leq x} \max_{\gcd(a,q)=1} \left|\psi(y,q,a) - \frac{y}{\varphi(q)}\right| \;\leq\; c_1 x^{1/2} Q(\log x)^5 + c_1 x \exp\left(-c_2(\log x)^{1/2}\right),$$

where the dash indicates that if $\mathcal{S}(x) = \{s_1\}$, then no q in the sum is divisible by s_1.

Proof. We follow Vaughan's proof of Bombieri's theorem, see Davenport [8, Chapter 28]. There is an effectively computable positive number C such that for any number $X > 2$, there is at most one natural number $s_1 \leq X$ for which there is a primitive (real) character χ_1 with modulus s_1, and for which the L-function $L(s,\chi_1)$ has a real zero $\beta_1 > 1 - C/\log X$. Further, if s_1 exists, it exceeds $\log X$. Let $\mathcal{S}(x)$ be the set of such integers s_1 for $X = \exp\left((\log x)^{1/2}\right)$. Thus $\mathcal{S}(x)$ is either $\{s_1\}$ or the empty set.

For a Dirichlet character χ to the modulus q, let

$$\psi(y,\chi) \;=\; \sum_{n\leq y} \Lambda(n)\chi(n).$$

Also, let $\delta(\chi) = 1$ if χ is the principal character, and otherwise let $\delta(\chi) = 0$. We consider $|\psi(y,\chi) - \delta(\chi)y|$ for $q \leq \exp\left((\log x)^{1/2}\right)$, q not divisible by s_1 if s_1 exists, and $2 \leq y \leq x$. Any real zero of the L-function $L(z,\chi)$ must be at most $1 - C/(\log x)^{1/2}$. It then follows from (8) on page 123 of [8] that

$$|\psi(y,\chi) - \delta(\chi)y| \leq 2y^{1-C/(\log x)^{1/2}} + O\left(y\exp\left(-C'(\log y)^{1/2}\right)\right),$$

where C' and the O-constant are effectively computable. We thus have uniformly for $q \leq \exp\left((\log x)^{1/2}\right)$ with q not divisible by any member of $S(x)$ that

$$\max_{2\leq y\leq x} |\psi(y,\chi) - \delta(\chi)y| \;=\; O\left(x\exp\left(-c(\log x)^{1/2}\right)\right), \tag{5.1}$$

where $c = \min\{C, C'\}$.

Let

$$E(x,q) \;=\; \max_{2\le y\le x}\ \max_{\gcd(a,q)=1}\left|\psi(y;q,a)-\frac{y}{\varphi(q)}\right|.$$

We have from the argument on page 163 of [8] that

$$\sum_{q\le Q}{}' E(x,q) \;=\; Q(\log x)^2+\log x\sum_{q\le Q}{}'\frac{1}{\varphi(q)}\sum_{\chi \bmod q}{}^{*}\max_{2\le y\le x}|\psi(y,\chi)-\delta(\chi)y|, \tag{5.2}$$

where $\sum^*$ indicates the summation is over primitive characters. Let $c_3=\min\{1,c/2\}$ and let $Q'=\exp\left(c_3(\log x)^{1/2}\right)$. Then by (5.1),

$$\sum_{q\le Q'}{}'\frac{1}{\varphi(q)}\sum_{\chi \bmod q}{}^{*}\max_{2\le y\le x}|\psi(y,\chi)-\delta(\chi)y| \;=\; O\left(x\exp\left(-c_3(\log x)^{1/2}\right)\right). \tag{5.3}$$

From (2) on page 162 of [8] (Vaughan's inequality), we have for any number U with $1\le U<x$,

$$\sum_{U<q\le 2U}\frac{1}{\varphi(q)}\sum_{\chi \bmod q}{}^{*}\max_{2\le y\le x}|\psi(y,\chi)| \;=\; O\left(\left(x/U+x^{5/6}+x^{1/2}Q\right)(\log x)^4\right).$$

(Note that since $q>1$ in the sum, any primitive $\chi \bmod q$ is nonprincipal.) Thus, as on page 164 of [8], we have

$$\sum_{Q'<q\le Q}\frac{1}{\varphi(q)}\sum_{\chi \bmod q}{}^{*}\max_{2\le y\le x}|\psi(y,\chi)| \;=\; O\left(\left(\frac{x}{Q'}+x^{5/6}\log x+x^{1/2}Q\right)(\log x)^4\right),$$

where there is no restriction on the divisibility of q by a member of $\mathcal{S}(x)$. Putting this estimate together with (5.2) and (5.3), we have

$$\sum_{q\le Q}{}' E(x,q) \;=\; O\left(x^{1/2}Q(\log x)^5+x\exp\left(-c_2(\log x)^{1/2}\right)\right)$$

for any choice of c_2 with $c_2<c_3$. This completes the proof of the lemma.

Lemma 5.3. *With the same notation and hypotheses as Lemma 5.2, we have*

$$\sum_{q\le Q}{}'\ \max_{\gcd(a,q)=1}\left|\pi(x,q,a)-\frac{\mathrm{li}(x)}{\varphi(q)}\right| \;\le\; c_4x^{1/2}Q(\log x)^5+c_4x\exp\left(-c_2(\log x)^{1/2}\right),$$

where c_2 is as in Lemma 5.2, and c_4 is an absolute, effectively computable number.

Proof. First note that one may replace the expressions $\psi(y,q,a)$ in Lemma 5.2 with $\theta(y,q,a)$, since

$$|\psi(y,q,a)-\theta(y,q,a)| \ \le \sum_{\substack{n\le y\\ n \text{ is a power}}} \log y \ = \ O\left(y^{1/2}\log y\right).$$

Thus, the result follows directly from Lemma 5.2 and the identity

$$\pi(x,q,a) \ = \ \frac{\theta(x,q,a)}{\log x}+\int_2^x \frac{\theta(y,q,a)}{y(\log y)^2}\,dy.$$

In fact, one can save a factor of $\log x$ using this identity, but this is unimportant.

Lemma 5.4. [Deshouillers–Iwaniec] *There is an effectively computable function x_ϵ, defined for positive numbers ϵ, and absolute and effectively computable positive numbers c_5, c_6 with the following property. For arbitrary numbers ϵ, x, Q with $\epsilon>0, x\ge x_\epsilon$, and $x^{1/2}\le Q\le x^{1-\epsilon}$, and for an arbitrary integer a with $0<|a|<x^\epsilon$, we have for almost all integers $q\in[Q,2Q]$ with $\gcd(q,a)=1$, the number of exceptions being less than $Qx^{-\epsilon c_6}$,*

$$\pi(x,q,a) \ \le \ \frac{(4/3+\epsilon c_5)x}{\varphi(q)\log(x/q)}.$$

This result was announced in [9], and a sketch of the proof was presented in [10]. No claim of effectivity for c_1, c_2, x_ϵ was made by these authors, but their methods are, at least in principle, effective.

6. Sieved primes

The goal of this section is to prove a result on the distribution of primes r with $r-1$ free of prime factors in some given set, our proof closely following an argument of Balog [4]. Before stating this result we first present an elementary lemma.

Lemma 6.1. *We have for any number $t>1$ that*

$$\sum_{d<t}\frac{1}{\varphi(d)} \ = \ \frac{\zeta(2)\zeta(3)}{\zeta(6)}\log t+\nu+O\left(\frac{\log(2t)}{t}\right),$$

where ζ is the Riemann zeta-function and where ν is a constant identified below

Proof. By writing

$$\frac{1}{\varphi(d)} \;=\; \frac{1}{d}\sum_{u|d}\frac{\mu^2(u)}{\varphi(u)},$$

with μ the Möbius function, we have (with γ the Euler–Mascheroni constant)

$$\begin{aligned}\sum_{d<t}\frac{1}{\varphi(d)} \;&=\; \sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}\sum_{d\le t,\ u|d}\frac{1}{d} \;=\; \sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}\frac{1}{u}\left(\log\left(\frac{t}{u}\right)+\gamma+O\left(\frac{u}{t}\right)\right)\\ &=\; \log t\sum_{u<t}\frac{\mu^2(u)}{u\varphi(u)}+\sum_{u<t}\frac{\mu^2(u)(\gamma-\log u)}{u\varphi(u)}+O\left(\frac{1}{t}\sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}\right)\\ &=\; \log t\prod_{p\ \text{prime}}\left(1+\frac{1}{p(p-1)}\right)+\sum_{u}\frac{\mu^2(u)(\gamma-\log u)}{u\varphi(u)}+O\left(\frac{\log(2t)}{t}\right)\\ &=\; \frac{\zeta(2)\zeta(3)}{\zeta(6)}\log t+\nu+O\left(\frac{\log(2t)}{t}\right),\end{aligned}$$

where $\nu=\sum_u \mu^2(u)(\gamma-\log u)/(u\varphi(u))$.

Proposition 6.2. *There are effectively computable positive functions $X_\epsilon, \delta_\epsilon$ of the positive variable ϵ satisfying the following property. If $x \ge X_\epsilon$ and $\mathcal{Q}$ is a set of primes in the interval $(1, x^{1/2}]$ with*

$$\sum_{q\in\mathcal{Q}}\frac{1}{q-1} \;\le\; \frac{3}{11}-\epsilon, \tag{6.1}$$

then there are at least $\delta_\epsilon x/(\log x)^2$ primes $r \le x$ such that every prime factor q of $r-1$ satisfies $q \le x^{1/2}$ and $q \notin \mathcal{Q}$.

Proof. Let $0<\epsilon<3/11$, let x be large and suppose we have a set of primes $\mathcal{Q}$ satisfying (6.1). Let β be a small positive number to be determined later. For a prime $r \le x$, let $g(r)$ denote the number of factorizations of $r-1$ as lh, where

$$\begin{aligned}&x^{1/2-2\beta}<l<x^{1/2-\beta},\ x^{1/2+\beta}<h<x^{1/2+2\beta},\\ &lh \ \text{ is not divisible by any member of } \ \mathcal{Q},\\ &l \ \text{ is not divisible by any member of } \ \mathcal{S}(x),\\ &h \ \text{ is not divisible by any prime larger than } \ x^{1/2},\end{aligned}$$

where $\mathcal{S}(x)$ is defined in Lemma 5.2. It may be of course that $g(r) = 0$. Let N denote the number of primes $r \le x$ with $g(r) > 0$. Our goal is to get a good lower bound for N. From Cauchy's inequality, we obtain

$$N \ \ge \ \left(\sum_{r\le x} g(r)\right)^2 \left(\sum_{r\le x} g(r)^2\right)^{-1}.$$

Our first task is to get an upper bound for $\sum_{r\le x} g(r)^2$, and to do this we shall ignore the non-divisibility requirements in the definition of $g(r)$ and use only the relatively simple Lemma 5.1. We have, with $[a, b]$ denoting the least common multiple of a, b,

$$\sum_{r\le x} g(r)^2 \ \le \ \sum_{r\le x} \sum_{\substack{l_1,l_2 | r-1 \\ x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}}} 1 \ = \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \pi(x, [l_1, l_2], 1).$$

By Lemma 5.1, we thus have

$$\begin{aligned}\sum_{r\le x} g(r)^2 \ &\le \ 2x \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{1}{\varphi([l_1, l_2]) \log(x/[l_1, l_2])} \\ &< \ \frac{x}{\beta \log x} \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{1}{\varphi([l_1, l_2])}.\end{aligned}$$

We have

$$\begin{aligned}\sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{1}{\varphi([l_1, l_2])} \ &= \ \sum_{d<x^{1/2-\beta}} \sum_{\substack{\gcd(l_1,l_2)=d \\ x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}}} \frac{1}{\varphi(l_1 l_2/d)} \\ &\le \ \sum_{d<x^{1/2-\beta}} \sum_{a,b<x^{1/2-\beta}/d} \frac{1}{\varphi(abd)} \\ &\le \ \left(\sum_{d<x} \frac{1}{\varphi(d)}\right)^3.\end{aligned}$$

By Lemma 6.1, we conclude that

$$\sum_{r\le x} g(r)^2 \ = \ O\left(\frac{1}{\beta} x (\log x)^2\right).$$

We now turn our attention to the heart of the proof, which is to obtain a good lower bound for $\sum_{r\le x} g(r)$, and for this we shall use Lemmas 5.3 and 5.4. Let $\mathcal{L}$ denote the set of integers l with $x^{1/2-2\beta} < l < x^{1/2-\beta}$ and l is not divisible by any member of $\mathcal{S}(x)$. And let $\mathcal{H}$ denote the set of integers h with $x^{1/2+\beta} < h < x^{1/2+2\beta}$. To begin, we have

$$\begin{aligned}\sum_{r\le x} g(r) \;&\ge\; \sum_{l\in\mathcal{L}} \pi(x,l,1) - \sum_{\substack{l\in\mathcal{L}\\ q|l \text{ for some } q\in\mathcal{Q}}} \pi(x,l,1)\\ &\quad - \sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some } q\in\mathcal{Q}}} \pi(x,h,1) - \sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some prime } q>x^{1/2}}} \pi(x,h,1)\\ &=\; S_1 - S_2 - S_3 - S_4, \quad \text{say.}\end{aligned}$$

For S_1 we use Lemma 5.3, getting

$$S_1 \;=\; \mathrm{li}(x)\sum_{l\in\mathcal{L}} \frac{1}{\varphi(l)} + O\left(\frac{x}{(\log x)^2}\right).$$

(Note that Lemma 5.3 supports a smaller error estimate than used here.) By the above asymptotic estimate for the sum of $1/\varphi(d)$, and using that $\mathcal{S}(x)$ is either empty or has a single member greater than $(\log x)^{1/2}$, it follows that with $\xi = \beta\zeta(2)\zeta(3)/\zeta(6)$,

$$S_1 \;=\; \xi x + O(x/(\log x)^{1/4}).$$

For S_2 we again use Lemma 5.3, getting

$$\begin{aligned}S_2 \;&\le\; \mathrm{li}(x)\sum_{q\in\mathcal{Q}}\sum_{l\in\mathcal{L},\ q|l} \frac{1}{\varphi(l)} + O\left(\frac{x}{(\log x)^2}\right)\\ &\le\; \mathrm{li}(x)\sum_{q\in\mathcal{Q}} \frac{1}{q-1}\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} + O\left(\frac{x}{(\log x)^2}\right).\end{aligned}$$

By Lemma 6.1 we have that

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} \quad \begin{cases} = \ \beta\log x + O(q\log(2x)x^{2\beta-1/2}), & \text{for } q < x^{1/2-2\beta}\\ \le \ \beta\log x + O(q\log(2x)x^{\beta-1/2}), & \text{for } x^{1/2-2\beta} \le q \le x^{1/2-\beta}\\ = \ 0, & \text{for } q > x^{1/2-\beta}.\end{cases}$$

Thus,

$$S_2 \;\le\; \xi x\sum_{q\in\mathcal{Q}} \frac{1}{q-1} + O\left(\frac{x}{\log x}\right).$$

We estimate S_3 by using Lemma 5.4 with "ϵ" chosen as β and with "Q" being various powers of 2 so that the intervals $[Q, 2Q]$ cover the interval $(x^{1/2+\beta}, x^{1/2+2\beta})$. If h is an exceptional modulus in Lemma 5.4, we use the trivial estimate $\pi(x, h, 1) \le x/h$. We thus get

$$\begin{aligned}
S_3 &= \sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some } q\in\mathcal{Q}}} \pi(x,h,1)\\
&\le (4/3+O(\beta))x \sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some } q\in\mathcal{Q}}} \frac{1}{\varphi(h)\log(x/h)} + O\left(\frac{x}{\log x}\right)\\
&\le (8/3+O(\beta))\frac{x}{\log x} \sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some } q\in\mathcal{Q}}} \frac{1}{\varphi(h)} + O\left(\frac{x}{\log x}\right)\\
&\le (8/3+O(\beta))\frac{x}{\log x} \sum_{q\in\mathcal{Q}} \frac{1}{q-1} \sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} + O\left(\frac{x}{\log x}\right)\\
&= (8/3+O(\beta))\xi x \sum_{q\in\mathcal{Q}} \frac{1}{q-1} + O\left(\frac{x}{\log x}\right).
\end{aligned}$$

For S_4 it is sufficient to use Lemma 5.1. Note that

$$\sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)} \le \sum_{\substack{x^{1/2}<q\le x^{1/2+2\beta}\\ q \text{ prime}}} \frac{1}{q-1} \sum_{t\le x^{2\beta}} \frac{1}{\varphi(t)}.$$

By Mertens' theorem, the first sum on the right is $O(\beta)$, and by our earlier estimates, the second sum is $O(\beta \log x)$. Thus the sum $\sum 1/\varphi(h)$ is $O(\beta^2 \log x)$, so that with Lemma 5.1, we have

$$\begin{aligned}
S_4 &\le 2x \sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)\log(x/h)}\\
&= O\left(\frac{x}{\log x} \sum_{\substack{h\in\mathcal{H}\\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)}\right) = O(\beta^2 x).
\end{aligned}$$

Putting together our estimates for S_1, S_2, S_3, S_4 we have that

$$\begin{aligned}\sum_{r\le x} g(r) \;&\ge\; S_1 - S_2 - S_3 - S_4 \\ &\ge\; \xi x\left(1 - (11/3 + O(\beta))\sum_{q\in\mathcal{Q}}\frac{1}{q-1}\right) + O(\beta^2 x) + O(x/(\log x)^{1/4}) \\ &\ge\; \xi x\big(1 - (11/3 + O(\beta))(3/11 - \epsilon)\big) + O(x/(\log x)^{1/4}) \\ &=\; \xi x(11\epsilon/3 + O(\beta)) + O(x/(\log x)^{1/4}).\end{aligned}$$

Thus, if β is chosen as a small absolute constant times ϵ, we have

$$\sum_{r\le x} g(r) \;\ge\; \epsilon\xi x.$$

Using this with our upper bound for $\sum_{r\le x} g(r)^2$, we get the desired estimate for N, where we may choose δ_ϵ as a small constant times ϵ^5. This completes the proof of the proposition.

Remarks. By using the results of Bombieri–Friedlander–Iwaniec instead of Lemma 5.4 one can do better. In fact, by the method of Friedlander [13] we can not only replace "3/11" with "1/2" in Proposition 6.2, but the number of primes r satisfying the condition is of order of magnitude $\pi(x)$. However, the results of Bombieri–Friedlander–Iwaniec involve constants that are not effectively computable. If one is not concerned with effective constants, this stronger form of Proposition 6.2 would support the conclusion of Theorem 4.1 for $D > (\log n)^{1+\epsilon}$.

7. The continuous Frobenius problem

Our goal in this section is to present a proof of an inequality that might be viewed as a continuous analogue of the Frobenius postage problem. Recall that in this problem one is given a finite set of positive integers with gcd 1, so that every sufficiently large integer may be written as a nonnegative integral linear combination of the given set. The problem is to find the largest integer which cannot be so represented. There is a simple formula for this largest integer in the case that the given set has just two members, but there is no known formula in the general case. In fact, the problem of determining this largest integer is known to be NP-hard. Erdős and Graham have posed extremal variants of the Frobenius

problem, such as finding how many members the given set may have in an initial interval if a given number is not representable. Many of their questions were answered in [11] and [15]. Using these results, Lev was able to get a result only a little weaker than what we present in the proposition below. The version we present is due to Bleichenbacher, and the proof does not use the earlier work on the Frobenius problem.

Proposition 7.1. (Daniel Bleichenbacher) *Suppose S is an open subset of the positive reals that is closed under addition, and such that $1 \notin S$. Then for any number $t \in (0, 1]$, the dx/x measure of $S \cap (0, t)$ is less than t.*

Proof. We actually shall prove a little more. Let M be a positive differentiable measure on the positive reals, with derivative m. Thus, if $\mathcal{S}$ is any measurable subset of the positive reals with characteristic function $\chi_{\mathcal{S}}$, we have

$$M(\mathcal{S}) \;=\; \int_0^\infty \chi_{\mathcal{S}}(x) m(x) dx.$$

Let S be as in the hypothesis of the theorem, and first suppose that $S_t := S \cap (0, t)$ is a finite union of open intervals; that is,

$$S_t \;=\; \bigcup_{i=1}^{n} (a_i, b_i),$$

where

$$t \geq b_1 \geq a_1 \geq \cdots \geq b_n \geq a_n \geq 0. \tag{7.1}$$

Let $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n)$. The condition that 1 is not in the additive semigroup generated by S_t is equivalent to the assertion that for all vectors $\mathbf{h} \in (\mathbf{N}_{\geq 0})^n$,

$$\text{either} \;\; \mathbf{h} \cdot \mathbf{a} \geq 1 \;\; \text{or} \;\; \mathbf{h} \cdot \mathbf{b} \leq 1. \tag{7.2}$$

That is, it is not the case that $\mathbf{h} \cdot \mathbf{a} < 1 < \mathbf{h} \cdot \mathbf{b}$.

Suppose now that we fix the vector $\mathbf{b}$ and assume that

$$t \geq b_1 > b_2 > \cdots > b_n > 0. \tag{7.3}$$

If $j > 1/b_n$ is an integer, then (7.2) implies that we must have $a_n \geq 1/j$. In particular, we must have $a_n \geq b_n/2$. Hence, the set of vectors $\mathbf{a}$ which, with the fixed vector $\mathbf{b}$, satisfy

(7.1) and (7.2) forms a compact subset of $(\mathbf{R}_{>0})^n$. Thus there is a choice of the vector $\mathbf{a}$ which maximizes $M(S_t)$ for the given vector $\mathbf{b}$. Call this maximum value $M_{\mathbf{b}}$ and assume that $\mathbf{a}$ is fixed at a choice which produces this maximum.

Since we allow empty intervals, that is, we allow $a_i = b_i$, it is clear that if some coordinates of $\mathbf{b}$ are deleted to form a shorter vector $\mathbf{b}'$ then $M_{\mathbf{b}'} \leq M_{\mathbf{b}}$. Thus, by possibly replacing $\mathbf{b}$ with a shorter vector, we may assume that each $a_i < b_i$. We now show that we may assume that each $a_{i-1} > b_i$ for $2 \leq i \leq n$. For suppose some $a_{i-1} = b_i$. We may then consolidate the two intervals $(a_i, b_i), (a_{i-1}, b_{i-1})$ into one interval (a_i, b_{i-1}). Indeed, if not, then now 1 is representable by a sum of members of $S_t \cup b_i$, so that b_i must be involved in the sum, say with positive integral coefficient c. If $c = 1$, then replace b_i in the sum with $b_i + \epsilon$, for a suitably small $\epsilon > 0$, and then replace another member $x \in S_t$ of the sum with $x - \epsilon$. (There must be another number in the sum since $b_i < 1$.) If ϵ is small enough, both $b_i + \epsilon$ and $x - \epsilon$ are in S_t, and we have represented 1 as a sum of members of S_t. And if $c \geq 2$, then since $b_i + \epsilon/(c-1)$ and $b_i - \epsilon$ are both in S_t for ϵ small enough, we can replace the c copies of b_i in the sum with $c-1$ copies of $b_i + \epsilon/(c-1)$ and one copy of $b_i - \epsilon$, and so represent 1 as a sum of members of S_t. Either way, we reach a contradiction, and so the consolidation of the two abutting intervals continues to enjoy the property that 1 is not in the additive semigroup generated by the intervals. Hence, we may assume that $a_{i-1} > b_i$ for $2 \leq i \leq n$. Thus, we may assume that the vector $\mathbf{a}$ satisfies

$$t \geq b_1 > a_1 > \cdots > b_n > a_n > 0. \tag{7.4}$$

Now let

$$\begin{aligned} H_0 &= \{\mathbf{h} \in (\mathbf{N}_{\geq 0})^n \ : \ \mathbf{h} \cdot \mathbf{a} < 1\}, \\ H_1 &= \{\mathbf{h} \in (\mathbf{N}_{\geq 0})^n \ : \ \mathbf{h} \cdot \mathbf{a} = 1\}, \\ H_2 &= \{\mathbf{h} \in (\mathbf{N}_{\geq 0})^n \ : \ \mathbf{h} \cdot \mathbf{a} > 1\}. \end{aligned}$$

Since each $a_i > 0$, it follows that H_0, H_1 are finite sets. We now show that H_1 is nonempty. Suppose not. Let $\mathbf{u} = (1, 1, \ldots, 1)$. We claim that if $\epsilon > 0$ is small enough, then the pair $\mathbf{a} - \epsilon\mathbf{u}, \mathbf{b}$ still satisfies (7.2) and (7.4). This would create a choice for S_t with strictly larger $M(S_t)$, a contradiction, thus showing that H_1 is nonempty. It is clear that we may choose $\epsilon > 0$ small enough so as to preserve the condition (7.4). For $\mathbf{h} \in H_0$ we have $\mathbf{h} \cdot \mathbf{b} \leq 1$, so

that the vectors in H_0 do not pose a problem for condition (7.2), and since H_1 is assumed empty, H_1 also does not pose a problem. There are only finitely many $\mathbf{h} \in H_2$ with $\mathbf{h} \cdot \mathbf{a} \leq 2$. We may choose $\epsilon > 0$ small enough so that $\mathbf{h} \cdot (\mathbf{a} - \epsilon \mathbf{u}) \geq 1$ for all such $\mathbf{h}$. But if we choose $\epsilon < a_n/2$, then if $\mathbf{h} \cdot \mathbf{a} > 2$, then $\mathbf{h} \cdot (\mathbf{a} - \epsilon \mathbf{u}) > \frac{1}{2} \mathbf{h} \cdot \mathbf{a} > 1$. Hence, as claimed, if $\epsilon > 0$ is small enough, $\mathbf{a} - \epsilon \mathbf{u}, \mathbf{b}$ still satisfy (7.2) and (7.4), providing a contradiction which shows that H_1 is nonempty.

Let $\mathbf{h} \in H_1$. For notational convenience, let $a_{n+1} = b_{n+1} = 0$. And let $\mathbf{e}_k$ be the k-th standard basis vector in $\mathbf{R}^n$. For any k, since $\mathbf{h} \cdot \mathbf{a} = 1$ and $a_k > a_{k+1}$, we have

$$\mathbf{h} \cdot \mathbf{a} - a_k + a_{k+1} < 1.$$

Suppose that $h_k > 0$. Let $\mathbf{h}' = \mathbf{h} - \mathbf{e}_k + \mathbf{e}_{k+1}$ in the case that $k < n$, and let $\mathbf{h}' = \mathbf{h} - \mathbf{e}_k$ in the case that $k = n$. Then $\mathbf{h}' \in H_0$. Hence, from (7.2), we have that $\mathbf{h}' \cdot \mathbf{b} \leq 1$. That is,

$$\mathbf{h} \cdot \mathbf{b} - b_k + b_{k+1} \leq 1.$$

Using that $\mathbf{h} \in H_1$ we get that

$$\mathbf{h} \cdot (\mathbf{b} - \mathbf{a}) \;=\; \mathbf{h} \cdot \mathbf{b} - 1 \;\leq\; b_k - b_{k+1}.$$

Thus, we have

$$h_k \mathbf{h} \cdot (\mathbf{b} - \mathbf{a}) \;\leq\; h_k (b_k - b_{k+1}), \tag{7.5}$$

an inequality that clearly continues to hold even if $h_k = 0$.

Let $\mathbf{v} \in \mathbf{R}^n$ and let

$$f_{\mathbf{v}}(x) \;=\; M \left(\bigcup_{i=1}^{n} (a_i + x v_i, b_i) \right).$$

Note that

$$f'_{\mathbf{v}}(0) \;=\; -\mathbf{v} \cdot m(\mathbf{a}),$$

where $m(\mathbf{a}) = (m(a_1), \ldots, m(a_n))$. Note too that by the maximality of $\mathbf{a}$, if the vector $\mathbf{a} + x\mathbf{v}$ satisfies (7.2) and (7.4) for all x in some interval $[0, \epsilon)$ with $\epsilon > 0$, then $f'_{\mathbf{v}}(0) \leq 0$, that is, $\mathbf{v} \cdot m(\mathbf{a}) \geq 0$. In fact, this event occurs whenever $\mathbf{h} \cdot \mathbf{v} \geq 0$ for all $\mathbf{h} \in H_1$. Indeed,

suppose so, and suppose that $\mathbf{h}' \cdot (\mathbf{a} + x\mathbf{v}) < 1 < \mathbf{h} \cdot \mathbf{b}$ for some $\mathbf{h}' \in (\mathbf{N}_{\geq 0})^n$. Since $\mathbf{h} \cdot \mathbf{b} \leq 1$ for all $\mathbf{h} \in H_0$, we have $\mathbf{h}' \notin H_0$. If $\mathbf{h} \in H_1$, then $\mathbf{h} \cdot (\mathbf{a} + x\mathbf{v}) = 1 + x\mathbf{h} \cdot \mathbf{v} \geq 1$ for all $x \geq 0$, so that $\mathbf{h}' \notin H_1$. For any given $\epsilon > 0$, there are only finitely many $\mathbf{h} \in H_2$ with $\mathbf{h} \cdot (\mathbf{a} + \epsilon\mathbf{v}) < 1 < \mathbf{h} \cdot \mathbf{a}$. Reducing the size of ϵ to a small enough positive quantity makes this set of $\mathbf{h}$ empty, and so $\mathbf{h}' \notin H_2$. It follows that for $\epsilon > 0$ small enough, if $\mathbf{h} \cdot \mathbf{v} \geq 0$ for all $\mathbf{h} \in H_1$, then $\mathbf{a} + x\mathbf{v}$ satisfies (7.2) and (7.4) for $0 \leq x < \epsilon$, and so $\mathbf{v} \cdot m(\mathbf{a}) \geq 0$.

We now apply a theorem of Farkas [13]:

Lemma. (J. Farkas) *Suppose A is an $n \times k$ real matrix and $\mathbf{m} \in \mathbf{R}^n$. Then the inequalities $A\mathbf{v} \geq \mathbf{0}, \mathbf{m} \cdot \mathbf{v} < 0$ are unsolvable for a vector $\mathbf{v} \in \mathbf{R}^n$ if and only if there is a vector $\mathbf{p} \in \mathbf{R}^k$ with $\mathbf{p} \geq \mathbf{0}$ and $\mathbf{p}^T A = \mathbf{m}$.*

(Note that we say a vector is $\geq \mathbf{0}$ when each entry of the vector is ≥ 0.) We apply this lemma to the matrix A whose rows are the u vectors in H_1 and to the vector $\mathbf{m} = m(\mathbf{a})$. We have shown that $A\mathbf{v} \geq \mathbf{0}$ implies that $\mathbf{m} \cdot \mathbf{v} \geq 0$. Thus the lemma implies there is a vector $\mathbf{p} \in \mathbf{R}^u$ with $\mathbf{p} \geq \mathbf{0}$ and $\mathbf{p}^T A = \mathbf{m}$. Say $H_1 = \{\mathbf{h}_1, \ldots, \mathbf{h}_u\}$, and let each $\mathbf{h}_j = (h_{j1}, \ldots, h_{jn})$. We have

$$\sum_{j=1}^{u} p_j h_{ji} \;=\; m(a_i) \;\text{ for }\; 1 \leq i \leq n.$$

Multiplying (7.5) applied to $\mathbf{h}_j$ by p_j and summing over j we have, when $1 \leq k \leq n$,

$$\sum_{j=1}^{u} p_j h_{jk} \sum_{i=1}^{n} h_{ji}(b_i - a_i) \;\leq\; \sum_{j=1}^{u} p_j h_{jk}(b_k - b_{k+1}) \;=\; m(a_k)(b_k - b_{k+1}).$$

Multiplying corresponding inequalities by a_k and summing over k, we get

$$\sum_{k=1}^{n} a_k \sum_{j=1}^{u} p_j h_{jk} \sum_{i=1}^{n} h_{ji}(b_i - a_i) \;\leq\; \sum_{k=1}^{n} a_k m(a_k)(b_k - b_{k+1}). \tag{7.6}$$

The left side of (7.6) is

$$\begin{aligned}
\sum_{j=1}^{u} p_j \sum_{k=1}^{n} a_k h_{jk} \sum_{i=1}^{n} h_{ji}(b_i - a_i) \;&=\; \sum_{j=1}^{u} p_j \sum_{i=1}^{n} h_{ji}(b_i - a_i) \\
&=\; \sum_{i=1}^{n} (b_i - a_i) \sum_{j=1}^{u} p_j h_{ji} \\
&=\; \sum_{i=1}^{n} (b_i - a_i) m(a_i).
\end{aligned}$$

Thus,

$$\sum_{i=1}^{n} m(a_i)(b_i - a_i) \;\le\; \sum_{k=1}^{n} a_k m(a_k)(b_k - b_{k+1}). \tag{7.7}$$

We now apply (7.7) with the measure M being dx/x. Then each $m(a_i) = 1/a_i$, so that

$$\sum_{i=1}^{n} (b_i/a_i - 1) \;\le\; \sum_{k=1}^{n} (b_k - b_{k+1}) \;\le\; t. \tag{7.8}$$

However, $M((a_i, b_i)) = \log(b_i/a_i) < b_i/a_i - 1$. Hence, by (7.8),

$$M_{\mathbf{b}} \;=\; \sum_{i=1}^{n} \log(b_i/a_i) \;<\; t.$$

Since $M_{\mathbf{b}} < t$ for each choice of $\mathbf{b}$ satisfying (7.3), it remains to handle the case of S_t being the union of infinitely many disjoint open intervals. Suppose $S_t = \bigcup_{i=1}^{\infty} (a_i, b_i)$, where the intervals are non-empty and disjoint. For each n, (7.8) implies that $\sum_{i=1}^{n} (b_i/a_i - 1) \le t$. Thus,

$$\sum_{i=1}^{\infty} (b_i/a_i - 1) \le t.$$

But

$$M(S_t) = \sum_{i=1}^{\infty} \log(b_i/a_i) < \sum_{i=1}^{\infty} (b_i/a_i - 1) \le t,$$

so $M(S_t) < t$. This concludes the proof of the theorem.

Remarks. The inequality of the theorem is best possible. Indeed, suppose S^n is the additive semigroup generated by $(1/(n+1), 1/n)$, where n is a positive integer. Then 1 is not in S^n. Further, we have

$$M(S_t^n) \ge \sum_{j=1}^{\lfloor tn \rfloor} \log(1 + 1/n) \;=\; \lfloor tn \rfloor (1/n + O(1/n^2)) \;\sim\; t \;\text{ as }\; n \to \infty.$$

We also remark that it is not difficult to obtain inequalities for $M_\alpha(S_t)$, where M_α is the dx/x^α measure and $0 \le \alpha < 1$. This may be done as a corollary of the result for the dx/x measure, or as a consequence of (7.7).

8. Proof of Theorem 4.1

Recall that $D > (\log n)^{11/6+\epsilon}$. Let $x = D^{6/11-\epsilon/4}$ so that if n is sufficiently large, we have $x \geq (\log n)^{1+3/\log\log\log n}$. Let $\alpha = \alpha(x) = 1/\log\log x$. For a prime $r \leq x$, let $Q(r)$ denote the set of prime divisors q of $r-1$ with

$$x^{\alpha^2} < q \leq x^{1/2} \text{ and } \operatorname{ord}(n^{(r-1)/q} \bmod r) = q.$$

We suppose that the sets $Q(r)$ have been computed for each prime $r \leq x$. Further, let $\mathcal{Q}$ denote the union of the sets $Q(r)$ over all primes $r \leq x$. Finally, for each $q \in \mathcal{Q}$, find the least prime r_q with $q \in Q(r_q)$. By using a modified sieve of Eratosthenes to find the prime factorizations of every integer up to x, the time to do all of these calculations is $\tilde{O}(x \log n) = \tilde{O}(D^{12/11})$.

We have, for n sufficiently large,

$$\sum_{q \in \mathcal{Q}} \frac{1}{q} > \frac{3-\epsilon}{11}. \tag{8.1}$$

Indeed, suppose not. We apply Proposition 6.2 to $\mathcal{Q}$, with the "ϵ" of that result being the current $\epsilon/11$. Thus, there is some $\delta > 0$ such that for n sufficiently large we have at least $\delta x/(\log x)^2$ primes $r \leq x$ such that every prime factor of $r-1$ is below $x^{1/2}$ and not in $\mathcal{Q}$. But, as remarked at the end of the proof of Proposition 4.1, the number of primes $r \leq x$ that are *not* counted by $R(x,n)$ is $O(x/(\log x)^{\log\log\log x})$. Thus, for n sufficiently large there is a prime $r \leq x$ such that r is counted by $R(x,n)$ and such that $r-1$ has every prime factor below $x^{1/2}$ and not in $\mathcal{Q}$. But being in $R(x,n)$ implies that there is a prime factor q of $r-1$ such that $q > x^{\alpha^2}$ and $\operatorname{ord}(n^{(r-1)/q} \bmod r) = q$. As $r-1$ has all of its prime factors below $x^{1/2}$, this prime q must be in $\mathcal{Q}$. But this contradicts the fact that $r-1$ has no prime factors from $\mathcal{Q}$. Hence (8.1) holds.

For a bounded interval I, let $|I|$ denote the length of I. Let $N = \lceil 3\alpha^{-2} \log x \rceil$, and let

$$I_i = [x^{(i-1)/N}, x^{i/N}) \text{ for } i = 1, 2, \ldots, N,$$

so that the intervals I_i partition $[1, x)$. Note that the "expected" number of primes in I_i is about $|I_i|/\log(x^{i/N})$. For each choice of i, let

$$k_i^0 = \min\{\#(I_i \cap \mathcal{Q}), \lfloor |I_i|/\log(x^{i/N}) \rfloor\},$$

and let

$$k_i \;=\; \begin{cases} 0, & \text{if } k_i^0 \le 2\alpha^{-2} \\ k_i^0, & \text{otherwise.} \end{cases}$$

Further, let

$$J_i \;=\; (x^{(i-1)/N}, x^{(i-1)/N} + k_i \log(x^{i/N})),$$

and let $\mathcal{Q}_i$ denote the set of the least k_i primes in $\mathcal{Q} \cap I_i$. Note that each $J_i \subset I_i$, and the sets $\mathcal{Q}_i$ are disjoint with their union contained in $\mathcal{Q}$. Further, $J_i = \emptyset$ for $i < \alpha^2 N$.

We now show that if n is sufficiently large we have

$$\sum_i \sum_{q \in \mathcal{Q}_i} \frac{1}{q} \;>\; \frac{3}{11} - \frac{\epsilon}{10}. \tag{8.2}$$

The difference between $\sum_i \sum_{q \in \mathcal{Q}_i} \frac{1}{q}$ and $\sum_{q \in \mathcal{Q}} \frac{1}{q}$ comes from two sources: intervals I_i with $k_i^0 \le 2\alpha^{-2}$ and intervals I_i with $\#(I_i \cap \mathcal{Q}) > \lfloor |I_i| / \log(x^{i/N}) \rfloor$. The sum of $1/q$ for primes q involved in intervals I_i with $k_i^0 \le 2\alpha^{-2}$ is at most

$$2\alpha^{-2} \sum_{i \ge \alpha^2 N} \frac{1}{x^{(i-1)/N}} \;<\; \frac{2x^{2/N}}{\alpha^2 x^{\alpha^2}(x^{1/N} - 1)} \;<\; \frac{1}{\alpha^4 x^{\alpha^2}}$$

for n sufficiently large. Thus, this contribution is negligible. The sum of $1/q$ for the largest $\#(I_i \cap \mathcal{Q}) - \lfloor |I_i| / \log(x^{i/N}) \rfloor$ primes q in an interval I_i with $\#(I_i \cap \mathcal{Q}) > \lfloor |I_i| / \log(x^{i/N}) \rfloor$ is estimated as follows. By the prime number theorem, the total number of primes in I_i is at most

$$\lfloor |I_i| / \log(x^{i/N}) \rfloor + O\left(\frac{x^{i/N}}{(\log(x^{i/N}))^2} \right).$$

Thus, the contribution to the sum of $1/q$ for the possibly extra primes that have been deleted from $I_i \cap \mathcal{Q}$ is

$$O\left(\frac{1}{(\log(x^{i/N}))^2} \right) \;=\; O\left(\frac{N^2}{i^2 (\log x)^2} \right).$$

Summing for $i \ge \alpha^2 N$, the contribution is

$$O\left(\frac{N}{\alpha^2 (\log x)^2} \right) \;=\; O\left(\frac{1}{\alpha^4 \log x} \right),$$

so that for sufficiently large n, this contribution is negligible as well. This proves (8.2).

Let S_i be the image of J_i under the natural logarithm map. That is, if $J_i = (a_i, b_i)$, then $S_i = (\log a_i, \log b_i)$. We now show that if n is sufficiently large, then

$$\sum_i \int_{S_i} \frac{du}{u} \;>\; \frac{3}{11} - \frac{\epsilon}{9}. \tag{8.3}$$

Indeed, it follows from (8.2) that

$$\sum_i \frac{k_i}{x^{(i-1)/N}} \;>\; \frac{3}{11} - \frac{\epsilon}{10}. \tag{8.4}$$

Further, if $S_i \neq \emptyset$, that is, if $k_i > 0$, then

$$\int_{S_i} \frac{du}{u} \;=\; \log\left(\frac{\log\left(x^{(i-1)/N} + k_i \log(x^{i/N})\right)}{\log\left(x^{(i-1)/N}\right)}\right).$$

Now,

$$\log\left(x^{(i-1)/N} + k_i \log(x^{i/N})\right) \;>\; \log(x^{(i-1)/N}) + \frac{k_i \log(x^{i/N})}{x^{(i-1)/N}} - \left(\frac{k_i \log(x^{i/N})}{x^{(i-1)/N}}\right)^2.$$

Hence,

$$\begin{aligned}
\int_{S_i} \frac{du}{u} \;&>\; \frac{k_i \log(x^{i/N})}{x^{(i-1)/N} \log(x^{(i-1)/N})} - \frac{2}{\log(x^{(i-1)/N})} \left(\frac{k_i \log(x^{i/N})}{x^{(i-1)/N}}\right)^2 \\
&=\; \frac{k_i \log(x^{i/N})}{x^{(i-1)/N} \log(x^{(i-1)/N})} \left(1 - \frac{2k_i \log(x^{i/N})}{x^{(i-1)/N}}\right) \\
&>\; \frac{k_i}{x^{(i-1)/N}} \left(1 - \frac{2k_i \log(x^{i/N})}{x^{(i-1)/N}}\right).
\end{aligned}$$

Note that

$$k_i \log(x^{i/N}) \;\leq\; x^{i/N} - x^{(i-1)/N} \;=\; x^{(i-1)/N}(x^{1/N} - 1) \;<\; \frac{\alpha^2}{2} x^{(i-1)/N}.$$

Thus,

$$\int_{S_i} \frac{du}{u} \;>\; \frac{k_i}{x^{(i-1)/N}}(1 - \alpha^2),$$

and so (8.3) follows from (8.4) for n sufficiently large.

Now let S be the additive semigroup generated by

$$\bigcup_i \frac{1}{\log(2D)} S_i.$$

Note that if $S_i \neq \emptyset$ we have $x^{(i-1)/N} \leq x^{1/2}$, so that

$$\frac{\log(x^{i/N})}{\log(2D)} \;\leq\; \left(\frac{1}{2}+\frac{1}{N}\right)\frac{\log x}{\log D} \;=\; \left(\frac{1}{2}+\frac{1}{N}\right)\left(\frac{6}{11}-\frac{\epsilon}{4}\right) \;<\; \frac{3}{11}-\frac{\epsilon}{9}$$

for sufficiently large n. Thus, from (8.3), if n is sufficiently large,

$$\int_0^{3/11-\epsilon/9} \frac{\chi_S(u)}{u}\,du \;=\; \sum_i \int_{S_i} \frac{du}{u} \;>\; \frac{3}{11}-\frac{\epsilon}{9}.$$

It thus follows from Proposition 7.1 that $1 \in S$. Hence, there is a finite subset F of $\bigcup_i S_i$ and positive integers κ_f for each $f \in F$ such that

$$\sum_{f\in F} \kappa_f f = \log(2D).$$

Let $F_i = F \cap S_i$ and let

$$\kappa_i \;=\; \sum_{f\in F_i} \kappa_f.$$

Then, for sufficiently large n,

$$\begin{aligned}\sum_i \kappa_i \;&=\; \sum_i \sum_{f\in F_i} \kappa_f \;\leq\; \sum_i \frac{1}{\log(x^{(i-1)/N})} \sum_{f\in F_i} \kappa_f f \\ &<\; \frac{1}{\log\left(x^{\alpha^2-N^{-1}}\right)} \sum_{f\in F_i} \kappa_f f \;=\; \frac{\log(2D)}{\log\left(x^{\alpha^2-N^{-1}}\right)} \;<\; 2\alpha^{-2},\end{aligned}$$

where for the last inequality, we assumed, as we may, that $\epsilon < 1/10$. Since for each i with $S_i \neq \emptyset$ we have $k_i > 2\alpha^{-2}$, it follows that for each i with $\kappa_i > 0$ there are more than κ_i distinct primes in $\mathcal{Q}_i$. Label the least such primes $q_{1,i}, q_{2,i}, \ldots, q_{\kappa_i,i}$. We have

$$\left|\sum_{f\in F} \kappa_f f - \sum_i \sum_{j=1}^{\kappa_i} \log(q_{j,i})\right| \;<\; \sum_i \kappa_i(\log(x^{i/N}) - \log(x^{(i-1)/N})) \;<\; \frac{2}{\alpha^2 N}\log x \;\leq\; \frac{2}{3}.$$

Since $1 < e^{2/3} < 2$, it follows that

$$D \;<\; \prod_i \prod_{j=1}^{\kappa_i} q_{j,i} \;<\; 4D.$$

We conclude that there is a squarefree integer Q in the interval $(D, 4D)$ supported solely on primes from $\mathcal{Q}$. By sieving this interval with a modified version of the sieve of Eratosthenes that produces complete prime factorizations for each integer in this interval, we may find such an integer Q and with a running time of at most $\tilde{O}(D)$. Once such an integer Q is found, the pairs (r_q, q), with q running over the prime factors of Q, form a period system for n. This completes the proof of the theorem.

We now summarize our algorithm for the construction of a period system.

Algorithm 8.1. We are given an integers $n > 1$, $D > (\log n)^{11/6}$. This algorithm produces a period system $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$ for n.

1. Using a modified sieve of Eratosthenes, compute the prime factorizations of every integer in $[1, 4D]$.
2. For each prime $r < D^{6/11}$ and prime $q \mid r-1$ with $\exp((\log D)/(\log\log(2D))^2) < q < D^{3/11}$, compute $n^{(r-1)/q} \bmod r$.
3. Compute the set $\mathcal{S}$ of ordered pairs (r, q) where r, q are as in step 2 and $n^{(r-1)/q} \not\equiv 1 \bmod r$.
4. Compute the set $\mathcal{Q}$ of primes q such that $(r, q) \in \mathcal{S}$ for some r.
5. If there is some integer in $[D, 4D]$ which is squarefree and composed solely of primes from $\mathcal{Q}$, let d be the least one. If not, replace D with $4D$ and go to step 1.
6. Using the prime factorization $q_1 q_2 \cdots q_k$ of d, find for each q_i some r_i with $(r_i, q_i) \in \mathcal{S}$.
7. Return the pairs $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$.

The time for step 1 is $\tilde{O}(D)$. The time for step 2 is $\tilde{O}(D^{6/11} \log n) = \tilde{O}(D^{12/11})$. The remaining calculations take negligible time. Note that for each pair $(r, q) \in \mathcal{S}$ we have $\operatorname{ord}(n^{(r-1)/q} \bmod r) = q$. If step 5 bounces us back to step 1 at least $\lceil \frac{1}{100} \log\log(2n) \rceil$ times, our D will be greater than $(\log n)^{11/6+1/100}$, and then at most $O(1)$ further iterations will ensure that $D > D_{100}$, the notation as in Theorem 4.1. Building this sufficiently large point

into the implied constant, we have that the running time for our algorithm is $\tilde{O}(D^{12/11})$. The implied constant is computable in principle. Further, if n is beyond some sufficiently large point that is computable in principle and if $D > (\log n)^{11/6+1/100}$, the algorithm produces a period system with d in $[D, 4D]$; that is, no iteration is required in step 5. Another consequence is that if $n > 1$ and $D > (\log n)^{11/6+1/100}$, the algorithm produces a period system with $d \geq D$ and $d = O(D)$, the O-constant being computable in principle.

9. Period polynomials

In this section we discuss the construction of the polynomial corresponding to a particular period system for n. So, we assume we are presented with an integer $n > 1$ and a period system for n, that is, a list of ordered pairs (r_i, q_i) for $i = 1, 2, \ldots, k$ satisfying (a), (b), (c) from section 4. We shall describe a deterministic procedure that either proves that n is composite or constructs a monic polynomial $f \in (\mathbf{Z}/n\mathbf{Z})[x]$ of degree $d = q_1 q_2 \cdots q_k$ for which (2.1), (2.2), and (2.3) hold. The time complexity for this procedure is

$$\tilde{O}\left(\max_{1 \leq i \leq k} \left\{ q_i r_i \log n + q_i^2 (\log n)^2 \right\} + d^3 \log n \right).$$

If we assume that the period system was produced by Algorithm 8.1, that is, we assume that $d > (\log n)^{11/6}$, each $q_i < d^{3/11}$, and each $r_i < d^{6/11}$, this time complexity estimate may be improved to $\tilde{O}(d^{8/5} \log n)$.

If $\eta_i = \eta_{r_i, q_i}$ is the Gaussian period as discussed in section 3, and if $\eta = \eta_1 \eta_2 \cdots \eta_k$, then the polynomial f that we hope to produce in this section is the reduction modulo n of the minimum polynomial for η over $\mathbf{Q}$. As η lives in the potentially very large cyclotomic field of $r_1 r_2 \cdots r_k$-th roots of unity, we shall not produce f by merely multiplying out using the various conjugates of η. We in fact do this for the minimal polynomials of the various η_i, but then use another more internal technique for the final assembly of f.

Our algorithm comes in three stages. In the first stage we compute monic polynomials $g_i \in (\mathbf{Z}/n\mathbf{Z})[x]$ for $i = 1, 2, \ldots, k$ with $\deg g_i = q_i$. These polynomials will have the property that if n is prime, then they are irreducible modulo n. In the second stage we attempt to verify (2.1), (2.2), and (2.3) for $g_1, g_2, \ldots, g_k$. If we fail to be able to verify one of these properties for one of these polynomials we declare n composite and do no

further work. (Note that failing to be able to verify a property is not exactly the same as showing the property fails. In the case of property (2.3), which is checked via Euclid's algorithm, one may be called to invert a nonzero non-unit in $\mathbf{Z}/n\mathbf{Z}$, in which case the procedure is aborted with a declaration that n is composite. However, it is possible that the property (2.3) nevertheless holds. Thus, intrinsic in the second stage is a description of the subroutines used in our attempts to verify the various properties.) Assuming the properties (2.1), (2.2), and (2.3) hold for each g_i, in the third and final stage we assemble the polynomial f of degree d. It is not necessary to then verify properties (2.1), (2.2), and (2.3) for f; we prove that f must satisfy these properties regardless of whether or not n is prime.

In the case that n is known to be prime, the second stage of the procedure of this section may be skipped. In this case, the algorithms of this section and the preceding one may be used to construct an irreducible polynomial over the finite field $\mathbf{F}_n$ of close to a given degree.

The first stage

We suppose that we have a pair (r, q) with r prime, $q \mid r-1$, $\mathrm{ord}\,(n^{(r-1)/q} \bmod r) = q$ and $q > 1$. Let z be a primitive root for r, and for $j = 0, 1, \ldots, q-1$, let

$$S_j \;=\; \left\{ z^{j+lq} \bmod r \;:\; l = 0, 1, \ldots, \frac{r-1}{q} - 1 \right\}.$$

We can build up these sets altogether by running through $z^0 \bmod r, z^1 \bmod r, \ldots$ placing each residue in its proper set. Or we can build up the sets S_j one at a time by computing $z^j \bmod r$ and $z^q \bmod r$, and then build $z^{j+lq} \bmod r$ from $z^{j+(l-1)q} \bmod r$. With either method, the time for building all of the sets S_j is $\tilde{O}(r)$. Note that the time to find a primitive root z for r is dominated by this same complexity. Indeed, the time to obtain the complete prime factorization of $r-1$ via trial division is $\tilde{O}(r^{1/2})$, and then the time to check each candidate z to see if it is a primitive root is $(\log r)^{O(1)}$.

Now we are ready to compute $g(x)$, the period polynomial for the degree q subfield of the r-th cyclotomic field. Note that we will be reducing the coefficients of g modulo n, and this reduction should be performed in all intermediate calculations. Let $\zeta_r = e^{2\pi i/r}$.

Then $g(x)$ is the product of the linear polynomials

$$x - \sum_{m \in S_j} \zeta_r^m, \quad j = 0, 1, \ldots, q-1$$

in the ring $(\mathbf{Z}[\zeta_r]/(n))[x]$. A multiplication in $\mathbf{Z}[\zeta_r]/(n)$ can be performed in time $\tilde{O}(r \log n)$. We first take our q linear polynomials in pairs with one left out if q is odd. The products of all of the pairs can be computed in time $\tilde{O}(qr \log n)$. We now take the degree 2 polynomials that we have formed and multiply them in pairs, with at most one pair left out. Again the total time is $\tilde{O}(qr \log n)$. We continue in this fashion until no more pairs of equal degree can be assembled. At the top stage we are multiplying just two polynomials of degree 2^t where 2^{t+1} is the largest power of 2 not exceeding q. At each point the time to compute all of the pair products is $\tilde{O}(qr \log n)$. Since there are $O(\log q)$ of these pair-assembly stages and $O(\log q)$ extra polynomials left over at the end, the assembly of all of the factors into one product g may be accomplished with the time complexity of $\tilde{O}(qr \log n)$.

We compute the corresponding polynomial g_i for each pair (r_i, q_i) that we have been given. Thus, the total time for the first stage is

$$\tilde{O}\left(\left(\sum_{i=1}^{k} q_i r_i\right) \log n\right).$$

Note that each g_i is in $(\mathbf{Z}/n\mathbf{Z})[x]$, though intermediate calculations occur in the larger ring $(\mathbf{Z}[\zeta_{r_i}]/(n))[x]$. The element

$$\eta_i \;=\; \sum_{m \in S_0} \zeta_{r_i}^m$$

is a Gaussian period and is a root of g_i in $\mathbf{Z}[\zeta_{r_i}]/(n)$. In subsequent stages of the procedure of this section we shall not deal with roots explicitly, but only formally as cosets.

The second stage

For (r, q) one of the pairs in the first stage and with g the polynomial in $(\mathbf{Z}/n\mathbf{Z})[x]$ that we have constructed, let $A = \mathbf{Z}[x]/(n, g)$ and let $\alpha = x + (n, g)$. The time for a multiplication in the ring A is $\tilde{O}(q \log n)$. (The principal advantage for dealing with the formal root α of g rather than the explicit root η is that there is no longer a dependence on r in the arithmetic.) Thus the time to compute α^n is $\tilde{O}(q(\log n)^2)$. And the time to evaluate $g(\alpha^n)$, and so check condition (2.1), is $\tilde{O}(q^2 \log n)$.

For (r, q) again standing for one of our pairs (r_i, q_i), and starting from α^n, which has already been computed, we compute α^{n^q} via an addition chain that also computes each $\alpha^{n^{q/s}}$ for each prime $s \mid q$. (If q is prime, then the only choice for s is q itself.) The time for this is $\tilde{O}(q^2(\log n)^2)$. We now can readily determine if condition (2.2) holds.

To check condition (2.3), let $\beta = \alpha^{n^{q/s}} - \alpha$ for one of the primes $s \mid q$. As A is a free $\mathbf{Z}/n\mathbf{Z}$-module with basis $1, \alpha, \ldots, \alpha^{q-1}$, we have $\beta = h(\alpha)$ for some $h \in (\mathbf{Z}/n\mathbf{Z})[x]$ with either $h = 0$ or $\deg h < q$. (In fact this is how we represent every element of A and is what we mean when we say that we have "computed" β—we have computed the polynomial h.) If $h = 0$, that is, $\beta = 0$, then stop, condition (2.3) fails and n cannot be prime. So assume $h \neq 0$. We perform Euclid's algorithm on $h(x), g(x)$ in $(\mathbf{Z}/n\mathbf{Z})[x]$. After each division with a nonzero remainder we multiply the remainder by the inverse in $\mathbf{Z}/n\mathbf{Z}$ of its leading coefficient so as to make it monic. If we encounter a non-unit in $\mathbf{Z}/n\mathbf{Z}$ during this procedure, we declare n composite and stop. Assuming we have not stopped, Euclid's algorithm will terminate at a nonzero monic polynomial $h_0 \in (\mathbf{Z}/n\mathbf{Z})[x]$. (In fact the ideal (h, g) is equal to (h_0).) If $\deg h_0 > 0$, then β is not a unit in A; declare n composite and stop. Otherwise $\beta \in A^*$, that is, property (2.3) holds. The total time for this attempt to determine if β is a unit is $\tilde{O}(q^2 \log n)$.

We conclude that the total time for attempting to verify (2.1), (2.2), and (2.3) for $g_1, g_2, \ldots, g_k$ is

$$\tilde{O}\left(\left(\sum_{i=1}^{k} q_i^2\right)(\log n)^2\right).$$

The third stage

Our goal is to create one polynomial f whose roots are k-fold products of the various roots of $g_1, g_2, \ldots, g_k$. The principal ideas are already seen in the combination of just 2 polynomials. Suppose f_1, f_2 are monic polynomials in $(\mathbf{Z}/n\mathbf{Z})[x]$ of degrees d_1, d_2, repsectively, where $d_1, d_2 > 1$ and $(d_1, d_2) = 1$. For $i = 1, 2$ let $A_i = \mathbf{Z}[x]/(n, f_i)$ and let $\alpha_i = x + (n, f_i)$. Assume that properties (2.1), (2.2), and (2.3) hold for the pairs f_i, α_i for $i = 1, 2$. From (2.3), $\alpha_1 \in A_1^*$. Let

$$M(f_1, f_2)(t) \;=\; \prod_{j=0}^{d_1-1} \alpha_1^{d_2 n^j} f_2(t\alpha_1^{-n^j}),$$

so that $M(f_1, f_2)$ is a polynomial in $A_1[t]$.

Proposition 9.1. *With the above assumptions, $M(f_1, f_2)$ is a polynomial in $(\mathbf{Z}/n\mathbf{Z})[t]$, monic of degree $d_1 d_2$, and satisfying properties (2.1), (2.2), and (2.3).*

Proof. Let $f = M(f_1, f_2)$, $d = d_1 d_2$. It is clear that f is monic and has degree d. Let σ be the automorphism of A_1 that takes α_1 to α_1^n as discussed in section 2. Note that σ leaves the coefficients of f invariant. If β is one of these coefficients and $\beta = h(\alpha_1) \neq 0$, where $h \in (\mathbf{Z}/n\mathbf{Z})[x]$ is 0 or has degree less than d_1, then consider the polynomial $h(x) - \beta \in A_1[x]$. It has the d_1 roots $\sigma^j \alpha_1$ for $j = 0, 1, \ldots, d_1 - 1$. From (2.4) and the Easy Fact of section 2 it follows that $h(x) - \beta$ is either 0 or has degree at least d_1. The second cannot occur, so it is 0, which implies that $\beta = h(0) \in \mathbf{Z}/n\mathbf{Z}$. Thus, $f \in (\mathbf{Z}/n\mathbf{Z})[t]$.

Let $A' = \mathbf{Z}[t]/(n, f)$, $\alpha = t + (n, f)$. We are to show that (2.1), (2,2), and (2.3) all hold for the pair f, α. We first show that these properties hold in a similar situation.

Let $A = \mathbf{Z}[x_1, x_2]/(n, f_1(x_1), f_2(x_2))$. We have natural embeddings of A_1, A_2 into A where α_i is identified with $x_i + (n, f_1(x_1), f_2(x_2))$ for $i = 1, 2$. As $f_i(\alpha_i^n) = 0$ for $i = 1, 2$, we have a well-defined endomorphism on A that sends α_i to α_i^n for $i = 1, 2$. We continue to denote this endomorphism as σ. Note that restricted to the subrings A_1, A_2, the endomorphism σ is our familiar automorphism from section 2. We now show that (2.1), (2.2), and (2.3) hold for $f, \alpha_1 \alpha_2$.

Using Lemma 2.1, we have

$$f(t) \;=\; \prod_{j=0}^{d_1-1} \prod_{l=0}^{d_2-1} \left(t - \sigma^j(\alpha_1)\sigma^l(\alpha_2)\right).$$

Thus, we have $f(\alpha_1\alpha_2) = 0$. It is clear either from this product formula for f or from the fact that σ is an endomorphism of A that $f(\sigma(\alpha_1\alpha_2)) = f((\alpha_1\alpha_2)^n) = 0$. Thus (2.1) holds. Further,

$$(\alpha_1\alpha_2)^{n^d} \;=\; \sigma^{d_1 d_2}(\alpha_1)\sigma^{d_2 d_1}(\alpha_2) \;=\; \alpha_1\alpha_2.$$

Thus, (2.2) holds. Say q is a prime factor of d. If $q \mid d_1$, we have

$$(\alpha_1\alpha_2)^{n^{d/q}} - \alpha_1\alpha_2 \;=\; \left(\alpha_1^{n^{d/q}} - \alpha_1\right)\alpha_2.$$

Note that using (2.3) for α_2 we see that $\alpha_2 \in A_2^* \subset A^*$. Now for any positive integer u we have $\alpha_1^{n^{d/q}} - \alpha_1 \mid \alpha_1^{n^{ud/q}} - \alpha_1$ in A_1. Choose $u \equiv d_2^{-1} \pmod{d_1}$, so that $\alpha_1^{n^{ud/q}} - \alpha_1 = \alpha_1^{n^{d_1/q}} - \alpha_1$, which is seen to be in A_1^* by (2.3) applied to α_1. As $A_1^* \subset A^*$ we have $(\alpha_1\alpha_2)^{n^{d/q}} - \alpha_1\alpha_2 \in A^*$. This holds as well by a parallel argument in the case that $q \mid d_2$, so that we have (2.3) for $\alpha_1\alpha_2$. Note that we have also proved that σ is an automorphism of A with order d.

To complete the proof of the proposition it will suffice to show that $A' \cong A$ with $\alpha \in A'$ corresponding to $\alpha_1\alpha_2 \in A$. Consider the mapping $\phi : A' \to A$ where $\phi(\alpha) = \alpha_1\alpha_2$. Then ϕ is well-defined, for if $g(\alpha) = h(\alpha)$ with $g, h \in (\mathbf{Z}/n\mathbf{Z})[t]$, then $g(t) = h(t) + u(t)f(t)$ for some $u \in (\mathbf{Z}/n\mathbf{Z})[t]$, so that $\phi g(\alpha) = g(\alpha_1\alpha_2) = h(\alpha_1\alpha_2) = \phi h(\alpha)$. Clearly ϕ is a homomorphism. Suppose $\phi g(\alpha) = 0$ where either g is 0 or has degree less than d. Then $g(\alpha_1\alpha_2) = 0$. As σ is an automorphism of A, we have $g(\sigma^j(\alpha_1\alpha_2)) = 0$ for $j = 0, 1, \ldots, d-1$. By the fact that (2.3) holds for $\alpha_1\alpha_2$ we have (2.4) holding as well, so that the Easy Fact of section 2 implies that $f(t) \mid g(t)$ in $A[t]$. But then g cannot have degree less than d, so that $g = 0$. We have shown that ϕ is injective. Since both A, A' have n^d elements it follows that ϕ is also surjective. Thus $A' \cong A$ as claimed. This completes the proof of Proposition 9.1.

Armed with Proposition 9.1 we are now ready to assemble our polynomial of degree $q_1 q_2 \cdots q_k$. It is the M-operator applied to $g_1, g_2, \ldots, g_k$. Since the M-operator only applies

to two polynomials at a time, we have several choices for applying it to the ensemble of g's. An appropriate choice is one where the overall time complexity is least. So we first examine the time complexity of computing $M(f_1, f_2)$ in Proposition 9.1.

The time to compute α_1^{-1} is $\tilde{O}(d_1 \log n)$. The time to compute $\alpha_1^{-n^j}$ from $\alpha_1^{-n^{j-1}}$ is $\tilde{O}(d_1(\log n)^2)$, so the time to compute all of them is $\tilde{O}(d_1^2(\log n)^2)$. We use Corollary 10.8 of [14] to evaluate f_2 at the set points $t\alpha_1^{-n^j}$. If $d_1 > d_2$ this takes $\tilde{O}(d_1)$ operations in $A_1[t]$ with polynomials of degree at most d_2, so a total of $\tilde{O}(d_1^2 d_2 \log n)$. If $d_1 < d_2$, the time complexity is $\tilde{O}(d_1 d_2^2 \log n)$. Using our prior partial results, the time to compute $\alpha_1^{d_2 n^j}$ for each j and multiply it into $f_2(t\alpha_1^{-n^j})$ is $\tilde{O}(d_1 d_2 \log n)$. Finally we assemble $M(f_1, f_2)$ by multiplying the factors in pairs as we did with the assembly of each g_i in the first stage of this section. The time for this is $\tilde{O}(d_1^2 d_2 \log n)$. Thus, the total time to assemble $M(f_1, f_2)$ is

$$\tilde{O}\left(d_1^2(\log n)^2 + d_1 d_2(d_1 + d_2)\log n\right). \tag{9.1}$$

Since our time complexity estimate for applying M to two polynomials grows significantly with the degrees of the polynomials, it will be advantageous for us to most often be applying it to polynomials of low degree. Here is our strategy. Among all sets $S \subset \{1, 2, \ldots, k\}$ with $\prod_{s\in S} q_s < d^{1/2}$ choose the one, call it S_1, with this product maximal, and let this product be denoted d_1. Let $d_2 = d/d_1$. Say $S_1 = \{s_1, s_2, \ldots, s_l\}$ and let $f_1 = M(g_{s_1}, g_{s_2}, \ldots, g_{s_l})$ built up two at a time. By (9.1), the time for this is $\tilde{O}(d_1^2(\log n)^2 + d_1^3 \log n)$. Let

$$S_2 \;=\; \{1, 2, \ldots, k\} \setminus S_1 \;=\; \{t_1, t_2, \ldots, t_{k-l}\}.$$

We build up $f_2 = M(g_{t_1}, g_{t_2}, \ldots, g_{t_{k-l}}\}$ in the same way as with f_1. Since $d_2/q_{t_i} < d_1$ for each i by our choice of d_1, the time complexity to build up f_2 is dominated by the expression in (9.1). Finally, we compute $M(f_1, f_2)$. The time complexity is given by (9.1), so that this expression stands as the total time complexity for the final stage of our procedure.

It remains now to estimate d_1, d_2. For this we shall assume that the period system $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$ was produced by Algorithm 8.1. In particular, we assume that $d > (\log n)^{11/6}$, each q_i is at most $d^{3/11}$, and each r_i is at most $d^{6/11}$. We show that $d_1 \geq d^{2/5}, d_2 \leq d^{3/5}$. If the product of the largest two q_i's is at least $d^{2/5}$ then we choose d_1

as this product or the complementary product of the remaining q_i's, whichever is smaller. This complementary product must be at least $d^{5/11}$. So now assume that the product of the largest two q_i's is smaller than $d^{2/5}$. Then every remaining q_i is smaller than $d^{1/5}$. Hence by multiplying them in one at at time to our product we may achieve a subset product that is in $(d^{2/5}, d^{3/5})$. The smaller of this product and its complementary product may be taken as d_1.

As each r_i is bounded by $d^{6/11}$, the time complexity of the first stage of this section is $\tilde{O}(d^{6/11} \log n)$. Further, the time complexity for second stage is $\tilde{O}(d^{6/11}(\log n)^2)$.

Using that $d^{2/5} \leq d_1 < d^{1/2} < d_2 \leq d^{3/5}$ and that $d > (\log n)^{11/6}$ we find that the time complexity for the entire procedure of this section is dominated by our estimate for the third stage, which reduces to

$$\tilde{O}\left(d^{8/5} \log n\right).$$

In the case of primality testing when we shall choose d of order of magnitude $(\log n)^2$, the time complexity for the procedure of this section is $\tilde{O}((\log n)^{21/5})$.

It may be useful at this point to highlight the case when we use the above methods to construct an irreducible polynomial modulo a prime.

Algorithm 9.2. Let p be a prime and let D be an integer with $D > (\log p)^{1.84}$. This deterministic algorithm constructs an irreducible polynomial $f(x) \in \mathbf{F}_p[x]$ of degree d, where $D \leq d = O(D)$. Moreover, if p is larger than an effectively computable bound, we have $d \leq 4D$.

1. Using Algorithm 8.1, find a period system $(r_1, q_1), (r_2, q_2), \ldots, (r_k, q_k)$ for $n = p$ with $d := q_1 q_2 \cdots q_k \geq D$ and $d = O(D)$. (For p beyond an effectively computable bound, this algorithm finds such a number d with $d \leq 4D$.)
2. With the algorithm of this section, but skipping stage 2, construct a monic polynomial $f(x) \in \mathbf{F}_p[x]$ of degree d.
3. Return $f(x)$.

Algorithm 9.2 fulfills the conditions of Theorem B of the Introduction, and so we have proved this theorem.

10. The primality test

In this section we summarize our primality test.

Algorithm 10.1. We are given an integer $n > 1$. This deterministic algorithm determines whether n is prime or composite.

1. Check if n is a power other than a first power. If it is, declare n composite and stop.
2. Let $D = \lceil (\log_2 n)^2 \rceil$. Using algorithm 8.1, find a period system (r_1, q_1), $(r_2, q_2), \ldots,$ (r_k, q_k) for n with $d := q_1 q_2 \cdots q_k \geq D$ and $d = O(D)$. (For n beyond an effectively computable bound, we will have $d \leq 4D$ as discussed in section 8.)
3. Let $B = \lfloor d^{1/2} \log_2 n \rfloor$. Check to see if n has a prime factor in $[1, B]$. If n has such a factor that is not equal to n, declare n composite and stop. If n itself is this prime factor, then declare n prime and stop.
4. Using the algorithm of section 9, attempt to find a monic polynomial f in $(\mathbf{Z}/n\mathbf{Z})[x]$ of degree d and for which (2.1), (2.2), (2.3) hold. It may be that the algorithm of section 9 finds n to be composite, in which case no further work is required.
5. For each integer a, $1 \leq a \leq B$, check if $(x + a)^n \equiv x^n + a \mod (n, f(x))$. If one of these congruences should fail, declare n composite and stop. Else, declare n prime and stop.

We have seen in Theorem 2.5 and Lemma 3.1 that Algorithm 10.1 is correct. The time for step 1 using a Newton iteration to approximate the k-th root of n for $2 \leq k \leq \log_2 n$ is $\tilde{O}((\log n)^3)$. As we have seen in section 8, the time for step 2 is $O((\log n)^{24/11})$, since $D = O((\log n)^2)$. The time for step 3 is $\tilde{O}((\log n)^3)$. As we have seen in section 9, the time for step 4 is $\tilde{O}((\log n)^{21/5})$. The time to verify one of the congruences in step 5 is $\tilde{O}(d(\log n)^2)$, so the total time for step 5 is bounded by $\tilde{O}(d^{3/2}(\log n)^3)$. Since $d = O(D) = O((\log n)^2)$ it follows that the time for step 5 is bounded by $\tilde{O}((\log n)^6)$. So, in total, the time for Algorithm 10.1 is $\tilde{O}((\log n)^6)$.

Acknowledgments

We wish to thank several people for their help with various aspects of this paper, in particular Daniel Bleichenbacher, Andrew Granville, Vsevolod Lev, Francesco Pappalardi, Jonathan Pila, Peter Stevenhagen, Mark Watkins, and Alessandro Zaccagnini.

References

[1] L. M. Adleman and H. W. Lenstra, Jr., *Finding irreducible polynomials over finite fields*, Proc. 18th Symp. on Theory of Comp., ACM Press, Berkeley, CA, 1986, pp. 350–355.

[2] M. Agrawal, N. Kayal, and N. Saxena, PRIMES *is in* P, Ann. of Math. **160**, 781–793.

[3] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), 703–722.

[4] A. Balog, $p + a$ *without large prime factors*, in Seminar on number theory, 1983–1984 (Talence, 1983/1984), Exp. No. 31, 5 pp., Univ. Bordeaux I, Talence, 1984.

[5] D. Bernstein, *Proving primality in essentially quartic random time*, `http://cr.yp.to/papers.html#quartic`.

[6] D. Bleichenbacher, *The continuous postage problem*, preprint, 2003.

[7] R. Crandall and C. Pomerance, *Prime numbers: a computational perspective. Second Edition*, Springer–Verlag, New York, 2005.

[8] H. Davenport, *Multiplicative number theory*, Second edition (revised by H. L. Montgomery), Graduate Texts in Mathematics, 74. Springer–Verlag, New York–Berlin, 1980.

[9] J.-M. Deshouillers and H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. Math. **70** (1982/83), 219–288.

[10] J.-M. Deshouillers and H. Iwaniec, *On the Brun-Titchmarsh theorem on average*, in Topics in classical number theory (ed. G. Halász), Vol. I, (Budapest, 1981), 319–333, Colloq. Math. Soc. János Bolyai, **34**, North-Holland, Amsterdam, 1984.

[11] J. Dixmier, *Proof of a conjecture by Erdős and Graham concerning the problem of Frobenius*, J. Number Theory **34** (1990), 198–209.

[12] J. Farkas, *Theorie der einfachen Ungleichungen*, J. Reine Angew. Math. **124** (1902), 1–27.

[13] J. B. Friedlander, *Shifted primes without large prime factors*, in Number theory and applications (R. A. Mollin, ed.), Kluwer Academic Publishers, Dordrecht, 1989, pp. 393–401.

[14] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 1999.

[15] V. F. Lev, *Structure theorems for multiple addition and the Frobenius problem*, J. Number Theory **58** (1996), 79–88.

[16] V. F. Lev, *The continuous postage stamp problem*, preprint, 2004.

[17] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.

[18] C. Pomerance and I. E. Shparlinski, *Smooth orders and cryptographic applications*, in Algorithmic Number Theory, Proceedings of ANTS-V, Sydney, Australia, July 2002 (C. Fieker and D. R. Kohel, eds.), Lecture Notes in Computer Science **2369**, Springer–Verlag, Berlin, Heidelberg, New York, 2002, pp. 338–348.

[19] N. M. Timofeev, *The Vinogradov-Bombieri theorem*, (in Russian) Mat. Zametki **38** (1985), 801–809, 956.