JEMS

H. W. Lenstra Jr. · Carl Pomerance

Primality testing with Gaussian periods

Abstract. We exhibit a deterministic algorithm that, for some effectively computable real number c, decides whether a given integer $n > 1$ is prime within time $(\log n)^6 \cdot (2 + \log \log n)^c$. The same result, with $21/2$ in place of 6, was proved by Agrawal, Kayal, and Saxena. Our algorithm follows the same pattern as theirs, performing computations in an auxiliary ring extension of $\mathbb{Z}/n\mathbb{Z}$. We allow our rings to be generated by Gaussian periods rather than by roots of unity, which leaves us greater freedom in the selection of the auxiliary parameters and enables us to obtain a better run time estimate. The proof depends on results in analytic number theory and on the following theorem from additive number theory, which was provided by D. Bleichenbacher: if t is a real number with $0 < t \le 1$, and S is an open subset of the interval $(0, t)$ with $\int_S dx/x > t$, then each real number greater than or equal to 1 is in the additive semigroup generated by S. A byproduct of our main result is an improved algorithm for constructing finite fields of given characteristic and approximately given degree.

Keywords. Primality testing, constructing finite fields, Frobenius problem

Contents

H. W. Lenstra Jr.: Mathematisch Instituut, Universiteit Leiden,
Postbus 9512, 2300 RA Leiden, The Netherlands; e-mail: hwl@math.leidenuniv.nl

C. Pomerance: Department of Mathematics, Dartmouth College,
Hanover, NH 03755, USA; e-mail: carl.pomerance@dartmouth.edu

1. Introduction

Our main result reads as follows.

Theorem 1. *There exists, for some effectively computable real number c_0, a deterministic algorithm that, given an integer n with $n > 1$, decides whether or not n is prime, and does so in time at most $(\log n)^6 \cdot (2 + \log \log n)^{c_0}$.*

We shall exhibit an algorithm with the stated properties. Its run time is measured in bit operations. The constant c_0 is effectively computable in the sense that our proof of the existence of c_0, combined with the proofs in the papers to which we refer, implicitly contains an algorithm for computing c_0.

  The same result, but with the run time exponent 6 replaced by 21/2, was obtained by Agrawal, Kayal, and Saxena [2]. They also prove a result with run time exponent 15/2 (in which "c_0" is not effectively computable), and they argue that the true run time exponent of their algorithm may reasonably be conjectured to equal 6. We achieve the exponent 6 not by proving their conjecture, but by modifying their algorithm.

  A fundamentally new idea would be required to obtain a deterministic primality testing algorithm with run time exponent smaller than 6. For *probabilistic* primality tests the situation is different. Bernstein [6], also elaborating on [2] and building on an idea of Berrizbeitia [9], exhibited a probabilistic algorithm that, for some effectively computable constant c_1, has the following property. Given any integer $n > 1$, the algorithm correctly decides whether or not n is prime, and it does so in expected time at most $(\log n)^4 \cdot (2 + \log \log n)^{c_1 \log \log \log(22 \log n)}$. See [4] for a similar result.

  Like [2], the present paper has an algebraic and an analytic component, addressing the correctness and the efficiency of the algorithm, respectively. By working harder on the algebra, we leave the algorithm greater freedom in the selection of auxiliary parameters, thus simplifying the analytic problem of obtaining a good run time estimate. Specifically, both the algorithm of [2] and our own algorithm perform computations in a suitable ring extension of the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n; if d denotes the "degree" of the extension, then the run time estimate becomes $d^{3/2} \cdot (\log n)^3$ times a lower order factor, and the problem of obtaining a small run time exponent boils down to proving a good upper bound for the smallest d that can be used. Agrawal et al. use the ring $(\mathbb{Z}/n\mathbb{Z})[X]/(X^d - 1)$, and find that the problem of accurately estimating the least usable value for d leads to an unsolved problem in analytic number theory. We select our ring extension from a much wider class, for which estimating d becomes feasible.

  The ring extensions of $\mathbb{Z}/n\mathbb{Z}$ that we use will be referred to as *pseudofields*. If n is a prime number, then these pseudofields are in fact *finite fields*, and our construction of pseudofields is inspired by a construction of finite fields proposed by Adleman and Lenstra [1]. They describe a deterministic algorithm that, for certain effectively computable constants c_2 and c_3, has the following properties: given a prime number p and a positive integer D, it computes an irreducible polynomial f in $(\mathbb{Z}/p\mathbb{Z})[X]$ satisfying $D \leq \deg f \leq c_2 D \log p$, and it does so within time $(D + \log p)^{c_3}$. The ring $(\mathbb{Z}/p\mathbb{Z})[X]/(f)$ is then a finite field of given characteristic p of degree "close" to a given number D. Our construction improves upon this result when D is not too small.

Theorem 2. *There exist an effectively computable positive integer c_4 and a deterministic algorithm such that the following holds. Given a prime number p and a positive integer D with $D > (\log p)^{46/25}$, the algorithm computes an irreducible polynomial f in $(\mathbb{Z}/p\mathbb{Z})[X]$ with $D \le \deg f < 2D$ and has run time at most $(D \log p) \cdot (2 + \log D + \log \log p)^{c_4}$.*

Note that the run time of our algorithm is essentially linear in terms of the length of the output. Under mild restrictions we may narrow the interval $[D, 2D)$ to $[D, (1 + \epsilon)D)$ for small positive values of ϵ (see Theorem 4.4). There is a deterministic algorithm that produces an irreducible polynomial in $\mathbb{F}_p[X]$ of exact degree D and that runs in polynomial time assuming the Generalized Riemann Hypothesis (see [1]). In addition, there is a probabilistic algorithm to do the same that runs in expected time $\tilde{O}(D^2 \log p + D \log^2 p)$ (see [29]), where the notation $\tilde{O}$ is defined below.

Adleman and Lenstra [1] construct the finite field $(\mathbb{Z}/p\mathbb{Z})[X]/(f)$ by adjoining to $\mathbb{Z}/p\mathbb{Z}$ a certain set of *Gaussian periods* parametrized by what we call a *period system*. For Theorem 2, we use almost exactly the same construction, but we are much more careful in selecting the period system, so that we are able to narrow the interval $[D, c_2 D \log p]$ for the degree down to $[D, 2D)$, and even narrower, in a large range.

The proof that an appropriate period system can be found is the major technical hurdle we have to take; our desire that the constants in Theorems 1 and 2 be effectively computable has added to the difficulties.

An auxiliary result, which has independent interest, was provided by D. Bleichenbacher [10], who kindly allowed us to include his result and its proof. The Frobenius postage problem asks for the largest number which is not in the additive semigroup generated by a given set of coprime positive integers. Bleichenbacher's theorem considers a continuous version of this problem. A similar result was obtained by Lev [25].

Theorem 3. *Suppose S is an open subset of the set of positive real numbers that is closed under addition and for which $1 \notin S$. Then for each real number $t \in (0, 1]$ one has $\int_{S \cap (0,t)} \mathrm{d}x/x \le t$.*

We give a number-theoretic application of Theorem 3, a simplified version of which is the following.

Theorem 4. *For every real number α with $0 < \alpha \le 1/2$, there is a positive integer x_0, effectively computable when α is rational, with the following property. If x, u are real numbers with*

$$x > x_0, \quad 1/\alpha < u < (\log x)^{1/10}$$

and $\mathcal{Q}$ is a set of primes contained in $(x^{1/u}, x^{1/2}]$ with

$$\sum_{q \in \mathcal{Q}} \frac{1}{q} \ge \alpha,$$

then there is a squarefree number in $[x^{1/\alpha}, 2x^{1/\alpha})$ composed solely of primes in $\mathcal{Q}$.

Our proofs of Theorems 1 and 2 depend on the existence of many primes r where $r - 1$ has certain multiplicative constraints. It has been known since Erdős [18] that there is a

positive constant E such that for a positive proportion of all primes r the number $r - 1$ is composed solely of primes in $(1, r^{1-E}]$; and he conjectured that this holds for each choice of E less than 1. Since then many people have worked on this problem, with the current record being any number $E < 1 - 1/(2\sqrt{e})$. The proof (in Friedlander [20]) is modeled on a similar result of Balog [5], who obtained the slightly weaker assertion that the number of primes in $(1, x]$ with the desired property is at least proportional to $x/(\log x)^2$. We follow Balog's approach to prove the following theorem.

Theorem 5. *If $x > 1$ is a real number and $\mathcal{Q}$ is a set of primes in the interval $(1, x^{1/2}]$, let $R(x, \mathcal{Q})$ denote the number of primes $r \le x$ with $r - 1$ composed solely of primes in $(1, x^{1/2}] \setminus \mathcal{Q}$. There are effectively computable positive numbers X_0, δ, with X_0, δ^{-1} integers, such that if $x \ge X_0$ and $R(x, \mathcal{Q}) < \delta x/(\log x)^2$, then*

$$\sum_{q \in \mathcal{Q}} \frac{1}{q - 1} > 0.2727.$$

That the numbers X_0, δ in Theorem 5 are effectively computable has us forgo certain standard tools, such as the prime-number estimates of Bombieri, Friedlander, and Iwaniec. In addition we need to modify another tool, namely the Bombieri–Vinogradov theorem. The major "off-the-shelf" tool that we do employ is a result of Deshouillers and Iwaniec [17] on the Brun–Titchmarsh theorem on average.

The connection of Theorems 4 and 5 to our problem is as follows. Our pseudofields are built up to have their degrees as close as possible to a given target degree. We construct a certain set of primes $\mathcal{Q}$, showing that we can attain degrees equal to subset products of $\mathcal{Q}$. Our set $\mathcal{Q}$ is constructed to satisfy the hypotheses of Theorem 5. Theorem 4 is then used to show that there are indeed squarefree numbers close to a given target which are built solely from primes in $\mathcal{Q}$.

In Section 2 we define pseudofields and period systems, and we state all properties of these concepts that go into our proofs. Taking these results for granted, we prove Theorem 1 in Section 3 and Theorem 2 in Section 4. In Sections 5–8 we prove the properties of pseudofields stated in Section 2. A proof of Theorem 3 is found in Section 9. In Section 10 we apply Theorem 3 to prove a somewhat stronger version of Theorem 4. In Sections 11–12 we use analytic number theory to prove Theorem 5. In Section 13, we use the result of Section 10 plus Theorem 5 to show the existence result for period systems stated in Section 2.

In this paper, we write simply *ring* for *commutative ring*. As in [3, 24], a ring is required to have a unit element, a ring homomorphism is required to preserve the unit element, and a subring is required to contain the unit element. The ring of integers is denoted by $\mathbb{Z}$, and, for a prime number p, we write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$. For a ring R, we write R^* for the group of units of R, the *characteristic* char R is the non-negative integer n for which $n\mathbb{Z}$ is the kernel of the unique ring homomorphism $\mathbb{Z} \to R$, and we write $R[X]$ for the polynomial ring in one variable X over R. An element of $R[X]$ is *monic* if it has leading coefficient 1, the unit element of R.

Let S be a set, and let $f, g \colon S \to \mathbb{R}$ be two functions from S to the field $\mathbb{R}$ of real numbers such that for all $x \in S$ one has $g(x) \ge 0$. By the statement $f = O(g)$

we mean that there exists $c \in \mathbb{R}$ such that for all $x \in S$ one has $|f(x)| \leq c \cdot g(x)$, and by $f = \tilde{O}(g)$ we mean that there exists $c \in \mathbb{R}$ such that for all $x \in S$ one has $|f(x)| \leq g(x) \cdot (\log \max\{3, g(x)\})^c$. We shall often apply this with S equal to a set of inputs to an algorithm, and $f(x)$ equal to the run time of the algorithm when given x. For example, with the notation just introduced one expresses the run time estimates in Theorems 1 and 2 as $\tilde{O}((\log n)^6)$ and $\tilde{O}(D \log p)$, respectively.

Whenever we assert that a constant with certain properties exists, it will be effectively computable in the sense explained above; this is also valid for the constants implicit in our use of the O- and $\tilde{O}$-symbols. The same comment, *mutatis mutandis*, applies to the existence of algorithms. All of the algorithms that we present in this paper are deterministic.

2. Pseudofields and period systems

Pseudofields. By a *pseudofield* we mean a pair (A, α) consisting of a ring A and an element $\alpha \in A$, such that for some integer $n > 1$, some integer $d > 0$, and some ring automorphism σ of A, the following conditions are satisfied:

(2.1) $\qquad$ char $A = n$,

(2.2) $\qquad$ $\#A \leq n^d$,

(2.3) $\qquad$ $\sigma\alpha = \alpha^n$,

(2.4) $\qquad$ $\sigma^d\alpha = \alpha$,

(2.5) $\qquad$ $\sigma^{d/l}\alpha - \alpha \in A^*$ $\quad$ for each prime number l dividing d.

In Section 5 we shall prove the following result about pseudofields.

Proposition 2.6. *Let (A, α) be a pseudofield, and let n, d be as above. Then there is a unique monic polynomial $f \in (\mathbb{Z}/n\mathbb{Z})[X]$ with the property that there is a ring isomorphism $(\mathbb{Z}/n\mathbb{Z})[X]/(f) \cong A$ that maps the coset $(X \bmod f)$ to α. In addition, the degree of this polynomial equals d.*

The polynomial f from 2.6 and its degree d are called the *characteristic polynomial* and the *degree* of the pseudofield, respectively. The proposition implies that each element of A can in a unique way be written as $g(\alpha)$, where $g \in (\mathbb{Z}/n\mathbb{Z})[X]$ satisfies $\deg g < d$. This implies that equality holds in (2.2). It also implies that, as a ring, A is generated by α, so that the automorphism σ of A is uniquely determined by (2.3); we refer to it as the *Frobenius automorphism* of the pseudofield.

Example. If $n \in \mathbb{Z}_{>1}$ and $a \in \mathbb{Z}$, then the pair $(\mathbb{Z}/n\mathbb{Z}, a \bmod n)$ is a pseudofield if and only if one has $a^n \equiv a \bmod n$; for composite n, one often expresses this property by saying that n is a *pseudoprime to the base a*. In this example, the degree equals 1, the Frobenius automorphism is the identity, and the characteristic polynomial is $X - (a \bmod n)$.

Example. Let $n \in \mathbb{Z}_{>1}$, let r be a positive integer with $\gcd(r, n) = 1$, and denote by Φ_r the rth cyclotomic polynomial. Then the pair $((\mathbb{Z}/n\mathbb{Z})[X]/(\Phi_r), X \bmod \Phi_r)$ is a pseudofield if and only if $(n \bmod r)$ generates the group $(\mathbb{Z}/r\mathbb{Z})^*$. This pseudofield is closely related to the rings used in [2]. In this example, the degree equals $\varphi(r)$, where φ denotes Euler's function, the Frobenius automorphism maps each $(g \bmod \Phi_r)$ to $(g(X^n) \bmod \Phi_r)$, and Φ_r is the characteristic polynomial.

Finite fields yield pseudofields, as explained in the following result.

Proposition 2.7. *Let p be a prime number, let A be a ring of characteristic p, and let $\alpha \in A$. Then (A, α) is a pseudofield if and only if A is a finite field satisfying $A = \mathbb{F}_p(\alpha)$. In addition, if (A, α) is a pseudofield, and σ denotes its Frobenius automorphism, then for all $\beta \in A$ one has $\sigma\beta = \beta^p$.*

This proposition is proved in Section 5.

Primality testing with pseudofields. The following result shows that, for the purposes of primality testing, pseudofields can play the role that the rings $(\mathbb{Z}/n\mathbb{Z})[X]/(X^d - 1)$ play in [2].

Proposition 2.8. *Let (A, α) be a pseudofield of degree d with Frobenius automorphism σ, and let $n = \operatorname{char} A$. Suppose that for each $a = 1, \ldots, \lfloor (d/3)^{1/2}(\log n)/\log 2 \rfloor$ one has $\alpha^n + a = (\alpha + a)^n$. Suppose also that $d > (\log n)^2/(3 \cdot (\log 2)^2)$, and that n has a prime factor greater than $(d/3)^{1/2}(\log n)/\log 2$. Then n is a power of a prime number.*

The proof of Proposition 2.8 is given in Section 6.

Algorithmic aspects of pseudofields. Proposition 2.6 shows that a pseudofield is, up to isomorphism, determined by its characteristic n and its characteristic polynomial f. We shall for algorithmic purposes always assume a pseudofield to be specified by the pair (n, f), the polynomial f being represented by its vector of coefficients; this applies in particular when a pseudofield forms part of the input or output of an algorithm. The pseudofield represented by (n, f) equals $((\mathbb{Z}/n\mathbb{Z})[X]/(f), X \bmod f)$, and its elements are represented as polynomials in $(\mathbb{Z}/n\mathbb{Z})[X]$ of degree smaller than the degree d of the pseudofield. It is well-known that there are algorithms that, given n, f, and two elements of $(\mathbb{Z}/n\mathbb{Z})[X]/(f)$, compute the sum and the product of these two elements within time $\tilde{O}(d \log n)$ (see [7]). As a consequence, testing the equality $\alpha^n + a = (\alpha + a)^n$ from 2.8 for a single value of a in $\mathbb{Z}/n\mathbb{Z}$ can be done in time $\tilde{O}(d(\log n)^2)$, and for about $(d/3)^{1/2}(\log n)/\log 2$ values of a in time $\tilde{O}((d^{1/2} \log n)^3)$. This time bound will equal the time bound $\tilde{O}((\log n)^6)$ from Theorem 1 if we use a pseudofield for which the degree d is, as a function of n, not too much larger than the lower bound $(\log n)^2/(3 \cdot (\log 2)^2)$ from 2.8. Thus, we are faced with the problem of constructing a pseudofield of given characteristic and approximately given degree.

The techniques that we develop for constructing pseudofields culminate in the following result. Let $n \in \mathbb{Z}$, $n > 1$. By a *period pair* for n we mean a pair (r, q) of integers with the properties

(2.9) r is a prime number not dividing n,

(2.10) $\qquad q$ divides $r - 1$ and $q > 1$,

(2.11) $\qquad$ the multiplicative order of $n^{(r-1)/q}$ modulo r equals q.

Further, a *period system* for n is a finite set $\mathcal{P}$ of period pairs for n such that

(2.12) $\qquad \gcd(q, q') = 1 \quad$ whenever $\quad (r, q), (r', q') \in \mathcal{P}, \ (r, q) \neq (r', q')$,

and the *degree* of $\mathcal{P}$ is $\prod_{(r,q) \in \mathcal{P}} q$, denoted $\deg \mathcal{P}$.

Proposition 2.13. *There is an algorithm that, given an integer $n > 1$ and a period system $\mathcal{P}$ for n with $n > \deg \mathcal{P}$, either correctly declares n composite or constructs a pseudofield of characteristic n and degree $\deg \mathcal{P}$, and that runs in time*

$$\tilde{O}\left(\left(\deg \mathcal{P} + \sum_{(r,q) \in \mathcal{P}} q(r + \log n)\right) \log n\right).$$

The proof of Proposition 2.13 is given in Section 8.

If n is known to be prime, then the algorithm of Proposition 2.13 simplifies somewhat, and the term involving $(\log n)^2$ in the run time estimate may be omitted; in view of Proposition 2.7, this leads to the following result.

Proposition 2.14. *There is an algorithm that, given a prime number p and a period system $\mathcal{P}$ for p with $p > \deg \mathcal{P}$, constructs a monic irreducible polynomial $f \in \mathbb{F}_p[X]$ with $\deg f = \deg \mathcal{P}$, and that runs in time*

$$\tilde{O}\left(\left(\deg \mathcal{P} + \sum_{(r,q) \in \mathcal{P}} qr\right) \log p\right).$$

The proof of Proposition 2.14 is also given in Section 8.

The existence of period systems. Our final auxiliary result reads as follows.

Proposition 2.15. *There are effectively computable positive integers c_4, c_5 such that, for each integer $n > c_4$ and each integer $D > (\log n)^{46/25}$, there exists a period system $\mathcal{P}$ for n consisting of pairs (r, q) with*

(2.16) $\qquad r < D^{6/11}, \quad q < D^{3/11}, \quad q \text{ prime},$

and with $D \leq \deg \mathcal{P} < D + D^{1 - 1/(c_5 (\log \log D)^2)}$. In addition, the number of period systems $\mathcal{P}$ for n with $\deg \mathcal{P} \in [D, 2D)$ exceeds $D / \exp(5(\log \log D)^3)$.

We use Proposition 2.15 to show that the algorithms of Theorems 1 and 2 perform as stated. In particular the number c_4 of Theorem 2 is the same as in 2.15. Proposition 2.15 is proved in Section 13 using a stronger version of Theorem 4 (namely, Proposition 10.1) and using Theorem 5. In particular, we will show in Propositions 13.1 and 13.4 that it is common for primes r of a certain size to have $r - 1$ divisible by a fairly large prime divisor q with (r, q) being a period pair for n. We then use Theorem 5 to show that the primes q appearing in this way are plentiful enough for the hypothesis of Proposition 10.1 to hold, and so construct period systems for n, as in 2.15, with degrees close to a given target degree.

3. The primality test

In this section we deduce Theorem 1 from the results stated in Section 2. We begin with a straightforward transformation of 2.15 into an algorithm for constructing period systems.

Algorithm 3.1. We describe an algorithm that takes as input an integer $n > 1$ and an integer $D > 0$, and that searches for a period system $\mathcal{P}$ for n consisting of pairs (r, q) satisfying (2.16) and with $\deg \mathcal{P}$ not much larger than D.

Step 1. Using a modified version of the sieve of Eratosthenes, sieving with prime powers rather than just with primes, compute the prime factorizations of all integers in $[1, 2D)$.

Step 2. For each prime number $r < D^{6/11}$ not dividing n, in increasing order, determine the set $\mathcal{Q}(r)$ of prime factors q of $r - 1$ that satisfy

$$q < D^{3/11}, \quad n^{(r-1)/q} \not\equiv 1 \bmod r, \quad q \notin \bigcup_{r' < r} \mathcal{Q}(r').$$

Put $\mathcal{Q} = \bigcup_r \mathcal{Q}(r)$ and, for each $q \in \mathcal{Q}$, put $r_q = r$ if $q \in \mathcal{Q}(r)$.

Step 3. If there is some integer in $[D, 2D)$ that is squarefree and composed solely of primes from $\mathcal{Q}$, let d be the least such integer, let $\mathcal{P}$ be the set of all pairs (r_q, q) with q ranging over the prime factors of d, return $\mathcal{P}$ and halt. If no such integer exists, pronounce failure and halt.

This completes the description of Algorithm 3.1.

The constant c_4 in the following result is as in 2.15.

Proposition 3.2. *Algorithm* 3.1, *when given integers $n > 1$ and $D > 0$, successfully computes a period system $\mathcal{P}$ for n with the properties listed in (2.16) and with $\deg \mathcal{P} \in [D, 2D)$ if and only if such a period system exists, which is the case if $n > c_4$ and $D > (\log n)^{46/25}$; the run time of the algorithm is $\tilde{O}(D + D^{6/11} \log n)$.*

Proof. The "if and only if" statement is clear from the algorithm, the second assertion is immediate from 2.15, and proof of the run time estimate is entirely straightforward. This proves 3.2.

Primality testing. We describe an algorithm that has the properties stated in Theorem 1. We let c_4 again be as in 2.15.

Algorithm 3.3. Given an integer $n > 1$, this algorithm decides whether or not n is prime.

Step 1. If $n \leq c_4$, find by trial division the least prime p dividing n, declare n prime or composite according as $n = p$ or $n \neq p$, and halt.

Step 2. Using the algorithm of [8], determine the largest $k \in \mathbb{Z}$ for which there exists $m \in \mathbb{Z}$ with $n = m^k$. If $k > 1$, declare n composite and halt.

Step 3. Using standard algorithms for computing elementary functions (cf. [7, 12]), compute an integer D satisfying

$$D - 2 < \max\{(\log n)^2/(3 \cdot (\log 2)^2), (\log n)^{46/25}\} < D.$$

Next, using Algorithm 3.1, construct a period system $\mathcal{P}$ for n with the properties listed in (2.16) and with $\deg \mathcal{P} \in [D, 2D)$. Put $d = \deg \mathcal{P}$.

Step 4. Using standard algorithms for computing elementary functions (cf. [7, 12]), compute an integer b satisfying

$$b - 1 < (d/3)^{1/2}(\log n)/\log 2 < b + 1,$$

and test by trial division whether n has a divisor among $2, \ldots, \max\{d, b\}$. If it does, let p be the least such divisor, declare n prime or composite according as $n = p$ or $n \neq p$, and halt.

Step 5. Using the algorithm of 2.13, either declare n composite and halt, or construct a pseudofield (A, α) of characteristic n and degree d.

Step 6. For $a = 1, \ldots, b$, test the equality $\alpha^n + a = (\alpha + a)^n$ in A. If all of these are valid, declare n prime and halt. If at least one fails to be valid, declare n composite and halt.

This completes the description of Algorithm 3.3.

Proof of Theorem 1. We prove that Algorithm 3.3 has the properties claimed in Theorem 1; that is, it terminates within time $\tilde{O}((\log n)^6)$, correctly declaring n prime or composite. Step 1 runs in time $O(1)$, and by [8], Step 2 runs in time $\tilde{O}(\log n)$. If the algorithm halts during one of these two steps, it is clearly correct. Assume otherwise, so that one has $n > c_4$ and n is not a proper power. The first part of Step 3 runs in time $O(\log n)$, and from $D > (\log n)^{46/25}$ and $D = O((\log n)^2)$ it follows, by 3.2, that the second part of Step 3 successfully computes a period system in time $\tilde{O}((\log n)^{23/11})$. We have $d = O((\log n)^2)$, and from $d \geq 2^{\#\mathcal{P}}$ one obtains $\#\mathcal{P} = O(\log(2 \log n))$. Step 4 runs in time $\tilde{O}((\log n)^3)$ because $b = O((\log n)^2)$. If the algorithm halts in Step 4, it is clearly correct. Suppose otherwise. Then we have $n > d$, so by 2.13 and the inequalities in (2.16), Step 5 runs in time $\tilde{O}((\log n)^3)$. As we argued in Section 2, the test in Step 6 can be done in time $\tilde{O}((d^{1/2} \log n)^3)$, which is $\tilde{O}((\log n)^6)$. Since n passed Step 4, it has a prime divisor greater than $(d/3)^{1/2}(\log n)/\log 2$, so 2.8 implies that, if n passes the test in Step 6, it is a prime power; not being a proper power, it must be prime. If n does not pass the test in Step 6, then by 2.7 (with n in the role of p and $\alpha + a$ in the role of β) it cannot be a prime number. This concludes the proof of Theorem 1.

4. Constructing finite fields

In this section we prove Theorem 2. We begin with two lemmas that are used to deal with certain exceptional cases.

Lemma 4.1. *Let k be a finite field, r a prime number, h a non-negative integer, and $b \in k^*$ an element that is not an rth power in k^*. Assume that $\#k \equiv 1 \bmod 4$ if $r^h \equiv 0 \bmod 4$. Then $X^{r^h} - b$ is irreducible in $k[X]$.*

Proof. See [26, Theorem 3.75].

Lemma 4.2. *For any non-negative integer h, the polynomials $X^{2 \cdot 3^h} + X^{3^h} + 1$ and $X^{4 \cdot 3^h} + X^{3^h} + 1$ are irreducible in $\mathbb{F}_2[X]$. For any prime number p with $p \equiv 1 \bmod 4$, any non-negative integer h, and any $a \in \mathbb{F}_p$ satisfying $\left(\frac{a}{p}\right) = -1$, the polynomial $X^{2^h} - a$ is irreducible in $\mathbb{F}_p[X]$. For any prime number p with $p \equiv -1 \bmod 4$ there exists $a \in \mathbb{F}_p$ with $\left(\frac{a^2+4}{p}\right) = -1$, and for any such a and any non-negative integer h the polynomial $X^{2^{h+1}} - aX^{2^h} - 1$ is irreducible in $\mathbb{F}_p[X]$.*

Proof. In this proof, we denote algebraic closures by an overhead bar.

First let $p = 2$. Let $a, \alpha \in \bar{\mathbb{F}}_2$ satisfy $a^2 + a + 1 = 0$ and $\alpha^{3^h} = a$. Then $\mathbb{F}_2(\alpha)$ contains $\mathbb{F}_2(a)$, and the latter field has degree 2 over $\mathbb{F}_2$. Since the only non-zero cube in $\mathbb{F}_2(a)^*$ is 1, one sees by 4.1 that $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(a)] = 3^h$, and therefore $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2 \cdot 3^h$. Since α is a zero of $X^{2 \cdot 3^h} + X^{3^h} + 1$, this polynomial is irreducible in $\mathbb{F}_2[X]$. Now let $b, \beta \in \bar{\mathbb{F}}_2$ satisfy $b^4 + b + 1 = 0$ and $\beta^{3^h} = b$. Then $\mathbb{F}_2(\beta)$ contains $\mathbb{F}_2(b)$, a field of degree 4 over $\mathbb{F}_2$. The non-zero cubes in $\mathbb{F}_2(b)$ are roots of $X^5 - 1$, so b is not a cube. Thus, by 4.1 one has $[\mathbb{F}_2(\beta) : \mathbb{F}_2(b)] = 3^h$ and so $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 4 \cdot 3^h$. Since β is a root of $X^{4 \cdot 3^h} + X^{3^h} + 1$, this polynomial is irreducible in $\mathbb{F}_2[X]$.

Next let $p \equiv 1 \bmod 4$. In this case the lemma is immediate from 4.1.

Finally suppose $p \equiv -1 \bmod 4$. If c is the least positive integer with $\left(\frac{c}{p}\right) = -1$, then one can write $(c - 1 \bmod p) = e^2$ with $e \in \mathbb{F}_p$, and $a = 2e$ then satisfies $\left(\frac{a^2+4}{p}\right) = \left(\frac{4}{p}\right) \cdot \left(\frac{c}{p}\right) = -1$. Next let $b, \alpha \in \bar{\mathbb{F}}_p$ satisfy $b^2 - ab - 1 = 0$ and $\alpha^{2^h} = b$. From $\left(\frac{a^2+4}{p}\right) = -1$ it follows that $X^2 - aX - 1$ is irreducible in $\mathbb{F}_p[X]$, so the field $\mathbb{F}_p(b)$, which is a subfield of $\mathbb{F}_p(\alpha)$, has degree 2 over $\mathbb{F}_p$. The product of b and its conjugate equals -1, which is not a square in $\mathbb{F}_p$, so b is not a square in $\mathbb{F}_p(b)$. Since also $\#\mathbb{F}_p(b) = p^2 \equiv 1 \bmod 4$, Lemma 4.1 implies $[\mathbb{F}_p(\alpha) : \mathbb{F}_p(b)] = 2^h$ and therefore $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = 2^{h+1}$. Since α is a zero of $X^{2^{h+1}} - aX^{2^h} - 1$, the latter polynomial is irreducible in $\mathbb{F}_p[X]$.

This proves 4.2.

We describe an algorithm that has the properties stated in Theorem 2.

Algorithm 4.3. Given a prime number p and a positive integer D, this algorithm attempts to construct an irreducible polynomial $f \in \mathbb{F}_p[X]$ with $D \leq \deg f < 2D$. We let c_4 be as in 2.15.

Step 1. [This step takes care of the case in which p is too small for 2.14 or 3.2 to apply.] If $D = 1$, return $f = X$ and halt. If $p = 2$, determine the least non-negative integer h with $2 \cdot 3^h \geq D$; if $2 \cdot 3^h < 2D$, return $f = X^{2 \cdot 3^h} + X^{3^h} + 1$ and halt. Else, return $f = X^{4 \cdot 3^{h-1}} + X^{3^{h-1}} + 1$ and halt. If $p \equiv 1 \bmod 4$ and $p \leq \max\{c_4, 2D\}$,

determine the least positive integer a with $\left(\frac{a}{p}\right) = -1$ and the least non-negative integer h with $2^h \geq D$, return $f = X^{2^h} - a$ and halt. If $p \equiv -1 \bmod 4$ and $p \leq \max\{c_4, 2D\}$, determine the least positive integer a with $\left(\frac{a^2+4}{p}\right) = -1$ and the least non-negative integer h with $2^{h+1} \geq D$, return $f = X^{2^{h+1}} - aX^{2^h} - 1$ and halt.

Step 2. [In this case we have $p > c_4$ and $p > 2D$.] Apply Algorithm 3.1 to $n = p$ and D; if that algorithm pronounces failure, pronounce failure and halt. Otherwise, let $\mathcal{P}$ be the period system for p produced by Algorithm 3.1, apply the algorithm of 2.14 to $\mathcal{P}$, return the polynomial produced by the latter algorithm and halt.

This completes the description of Algorithm 4.3.

Theorem 2 is now an immediate consequence of the following somewhat stronger result.

Theorem 4.4. *Let c_4, c_5 be as in 2.15. Algorithm 4.3, when given a prime number p and a positive integer D, runs in time $\tilde{O}(D \log p)$, and if it does not pronounce failure then it computes a monic irreducible polynomial $f \in \mathbb{F}_p[X]$ satisfying $D \leq \deg f < 2D$; in addition, it does not pronounce failure if $p \leq \max\{c_4, 2D\}$ or $D > (\log p)^{46/25}$. Further, in the case $p > \max\{c_4, 2D\}$ and $D > (\log p)^{46/25}$, one has $D \leq \deg f < D + D^{1-1/(c_5(\log \log D)^2)}$.*

Proof. First suppose $p \leq \max\{c_4, 2D\}$. Then by 4.2 the algorithm halts in Step 1 and returns a polynomial f that is irreducible over $\mathbb{F}_p$ and satisfies $D \leq \deg f < 2D$. From $p = O(D)$ one readily deduces that the computation of h in Step 1 and, if p is odd, of a in Step 1 can be done in time $\tilde{O}(D)$. Next assume $p > \max\{c_4, 2D\}$. If $D > (\log p)^{46/25}$, then by 3.2 the algorithm successfully computes a period system for p, and if it successfully computes a period system, then by 2.14 it computes a polynomial f with the stated properties. The run time estimate for Step 2 is obtained in a routine manner from 3.2 and 2.14; note that the sum $\sum_{(r,q)\in\mathcal{P}} qr$ occurring in 2.14 is $\tilde{O}(D^{9/11})$, by the inequalities in (2.16). This proves 4.4. $\qed$

5. Algebraic properties of pseudofields

In Section 2 we defined pseudofields, and the present section is devoted to their basic algebraic properties.

For a ring A, an element $\alpha \in A$, and a ring automorphism σ of A, we will have occasion to refer to the condition

(5.1) $\sigma\alpha$ belongs to the subring of A generated by α.

This condition is implied by condition (2.3), if n is a positive integer.

Proposition 5.2. *Let A be a ring, let $\alpha \in A$, let $d \in \mathbb{Z}_{>0}$, and let σ be a ring automorphism of A such that (2.4), (2.5), and (5.1) are satisfied. Then for any $i, j \in \mathbb{Z}$ with $i \not\equiv j \bmod d$ one has $\sigma^i \alpha - \sigma^j \alpha \in A^*$.*

Proof. Let $h \in \mathbb{Z}$, $h \notin d\mathbb{Z}$, and let $I = (\sigma^h\alpha - \alpha)$ be the A-ideal generated by $\sigma^h\alpha - \alpha$. The set $\{\beta \in A : \sigma^h\beta \equiv \beta \bmod I\}$ is a subring of A that contains α, so by (5.1) it contains $\sigma\alpha$; that is, $\sigma^{h+1}\alpha \equiv \sigma\alpha \bmod I$, so $\sigma(\sigma^h\alpha - \alpha)$ belongs to I, and therefore $\sigma I \subset I$. Since σ^d maps $\sigma^h\alpha - \alpha$ to itself, we actually have $\sigma I = I$, so for all $m \in \mathbb{Z}$ one has $\sigma^m I = I$. It follows that the set $H = \{m \in \mathbb{Z} : \sigma^m\alpha \equiv \alpha \bmod I\}$ is a subgroup of $\mathbb{Z}$. It contains d and h, where $h \notin d\mathbb{Z}$, so $H = d'\mathbb{Z}$ where d' is a divisor of d with $1 \le d' < d$. Choose a prime number l that divides d/d'. Then $d/l \in d'\mathbb{Z} = H$, so $\sigma^{d/l}\alpha - \alpha \in I$. Thus, by (2.5) the ideal I contains a unit, and therefore $I = A$. This implies $\sigma^h\alpha - \alpha \in A^*$. Now let $i, j \in \mathbb{Z}$ with $i \not\equiv j \bmod d$. Then the integer $i - j$ does not belong to $d\mathbb{Z}$, so by the result just proved we have $\sigma^{i-j}\alpha - \alpha \in A^*$. Applying σ^j we find $\sigma^i\alpha - \sigma^j\alpha \in A^*$, as required. This proves 5.2.

Lemma 5.3. *Let A be a ring, let $k \in \mathbb{Z}_{\ge 0}$, and let $\alpha_1, \ldots, \alpha_k \in A$ be such that $\alpha_i - \alpha_j \in A^*$ whenever $1 \le i < j \le k$. Then for each $g \in A[X]$ which vanishes at $\alpha_1, \ldots, \alpha_k$, one has $g \in A[X] \cdot \prod_{i=1}^k (X - \alpha_k)$.*

Proof. Let $I_i = A[X] \cdot (X - \alpha_i)$ for $1 \le i \le k$. For $i \ne j$, the unit $\alpha_i - \alpha_j$ can be written as $-(X - \alpha_i) + (X - \alpha_j)$, so $I_i + I_j = A[X]$. This implies $\prod_{i=1}^k I_i = \bigcap_{i=1}^k I_i$, by [3, Proposition 1.10(i)]. From $X \equiv \alpha_i \bmod I_i$ one obtains $g \equiv g(\alpha_i) \bmod I_i$ for each $g \in A[X]$, so if each $g(\alpha_i)$ vanishes then $g \in \bigcap_{i=1}^k I_i = \prod_{i=1}^k I_i = A[X] \cdot \prod_{i=1}^k (X - \alpha_k)$, as required. This proves 5.3.

The following result summarizes the technical information on pseudofields that we shall need.

Proposition 5.4. *Let A be a ring, let $\alpha \in A$, and let the integers $n, d \in \mathbb{Z}_{>0}$ and the ring automorphism σ of A satisfy (2.1), (2.2), (2.4), (2.5), and (5.1). Then:*

(a) *for each $\beta \in A$ there are unique $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}/n\mathbb{Z}$ with $\beta = \sum_{i=0}^{d-1} a_i\alpha^i$;*
(b) *$\#A = n^d$, and σ^d equals the identity;*
(c) *the polynomial $f = \prod_{i=0}^{d-1}(X - \sigma^i\alpha)$ belongs to the subring $(\mathbb{Z}/n\mathbb{Z})[X]$ of $A[X]$;*
(d) *the ring homomorphism $(\mathbb{Z}/n\mathbb{Z})[X] \to A$ sending X to α is surjective, and its kernel is generated by the polynomial f from* (c)*;*
(e) *if $I \subset A$ is an ideal, then one has $\sigma I \subset I$ if and only if there exists a divisor m of n such that $I = mA$;*
(f) *for each prime factor p of n there exists a unique residue class $(i \bmod d)$ such that for all $\beta \in A$ one has $\beta^p \equiv \sigma^i\beta \bmod pA$.*

Proof. It is clear that there is a unique ring homomorphism $\psi\colon (\mathbb{Z}/n\mathbb{Z})[X] \to A$ as in (d), and that it maps each $g \in (\mathbb{Z}/n\mathbb{Z})[X]$ to $g(\alpha)$. If $g \in \ker\psi$, then for each $i \in \mathbb{Z}$ one has $g(\sigma^i\alpha) = \sigma^i(g(\alpha)) = \sigma^i(\psi(g)) = 0$, so by 5.2 and 5.3 one has $g \in A[X]f$, where f is as in (c). Since each non-zero $g \in A[X]f$ has degree at least d, this implies

$$\ker\psi \cap \big((\mathbb{Z}/n\mathbb{Z}) + (\mathbb{Z}/n\mathbb{Z})X + \cdots + (\mathbb{Z}/n\mathbb{Z})X^{d-1}\big) = \{0\},$$

so that the restriction of ψ to $(\mathbb{Z}/n\mathbb{Z}) + (\mathbb{Z}/n\mathbb{Z})X + \cdots + (\mathbb{Z}/n\mathbb{Z})X^{d-1}$ is injective. From (2.2) one now sees that it is surjective as well, which proves (a), the first statement of (b),

and the surjectivity in (d). Since each element of A can be expressed in α, the second statement of (b) follows from (2.4). Applying (a) to $\beta = \alpha^d$, one finds $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}/n\mathbb{Z}$ for which the polynomial $g = X^d - \sum_{i=0}^{d-1} a_i X^i$ belongs to $\ker \psi$; hence $g \in A[X]f$, and comparing degrees and leading coefficients one finds $g = f$. This implies (c). We have $\ker \psi = A[X]f \cap (\mathbb{Z}/n\mathbb{Z})[X] = (\mathbb{Z}/n\mathbb{Z})[X]f$, the latter equality because f is a monic polynomial in $(\mathbb{Z}/n\mathbb{Z})[X]$. This proves the remaining assertion of (d).

The "if" part of (e) is clear. For the "only if" part, let I be an ideal of A with $\sigma I \subset I$, and let $\bar{A}$ be the ring A/I. From $\sigma I \subset I$ it follows that σ induces a ring homomorphism $\bar{\sigma}: \bar{A} \to \bar{A}$. From (b) one sees that $\bar{\sigma}^d$ is the identity on $\bar{A}$, so $\bar{\sigma}$ is an automorphism of $\bar{A}$. Put $m = \operatorname{char} \bar{A}$. Then m divides n, and we have $mA \subset I$, so from (a) we see $\#\bar{A} \leq \#A/mA = m^d$, with equality if and only if $mA = I$. We claim that (2.1), (2.2), (2.4), (2.5), and (5.1), with $\bar{A}, m, d, \bar{\sigma},$ and $\bar{\alpha} = (\alpha \bmod I)$ in the roles of $A, n, d, \sigma,$ and α, are satisfied. For (2.2) we have just proved this, (2.1) is true by definition, and (2.4), (2.5), and (5.1) follow from the corresponding properties of $A, n, d, \sigma,$ and α. Hence, applying (b) to this new situation, we find $\#\bar{A} = m^d$, so that $mA = I$. This proves (e).

To prove (f), we replace, for notational convenience, n and A by p and A/pA, so that we may assume $n = p$. Let $\phi: A \to A$ be the ring homomorphism that maps each $\beta \in A$ to β^p, and let $g \in (\mathbb{Z}/n\mathbb{Z})[X]$ be such that $\sigma\alpha = g(\alpha)$. If $\rho: A \to A$ is any ring homomorphism with $\sigma\rho = \rho\sigma$, then $\sigma(\rho\alpha) = \rho(\sigma\alpha) = \rho(g(\alpha)) = g(\rho\alpha)$. Applying this to $\rho = \phi$ and to $\rho = \sigma^i$, where $i \in \mathbb{Z}$, we obtain $\sigma(\phi\alpha) = g(\phi\alpha)$ and $\sigma(\sigma^i\alpha) = g(\sigma^i\alpha)$ and therefore $\sigma(\phi\alpha) \equiv \sigma(\sigma^i\alpha) \bmod (\phi\alpha - \sigma^i\alpha)A$. Hence, for any $i \in \mathbb{Z}$, the ideal $I = (\phi\alpha - \sigma^i\alpha)A$ satisfies $\sigma I \subset I$, so by (e) and the fact that n is prime one has $I = A$ or $I = nA = 0$, so that $\phi\alpha - \sigma^i\alpha$ is either a unit or 0. From $\prod_{i=0}^{d-1}(\phi\alpha - \sigma^i\alpha) = f(\phi\alpha) = \phi(f(\alpha)) = 0^p = 0$ we see that not all $\phi\alpha - \sigma^i\alpha$ can be units, so at least one of them is 0. Then $\phi\alpha = \sigma^i\alpha$, so $\phi = \sigma^i$ by (a). The uniqueness of $(i \bmod d)$ follows from 5.2. This proves 5.4.

We can now prove two propositions stated in Section 2.

Proof of Proposition 2.6. Let the notation and hypotheses be as in 2.6. Since (2.3) implies (5.1), Proposition 5.4 applies. The existence of f as in 2.6 follows from 5.4(d). No two distinct monic polynomials in $(\mathbb{Z}/n\mathbb{Z})[X]$ generate the same ideal, so f is unique. From 5.4(c) one sees $\deg f = d$. This proves 2.6.

Proof of Proposition 2.7. Let p, A, and α be as in 2.7. For the "if" part, assume that A is a finite field with $A = \mathbb{F}_p(\alpha)$. Write $d = [A : \mathbb{F}_p]$ and define $\sigma: A \to A$ by putting $\sigma\beta = \beta^p$ for every $\beta \in A$. It is a standard property of finite fields that σ is a field automorphism of A of order d. Now (2.1)–(2.4) are obvious. If l is a prime number dividing d, then $\sigma^{d/l}$ is not the identity, so from $A = \mathbb{F}_p(\alpha)$ we have $\sigma^{d/l}\alpha \neq \alpha$; since A is a field, this implies (2.5).

To prove the "only if" part and the last statement of 2.7, assume that (A, α) is a pseudofield. Write d for the degree and σ for the Frobenius automorphism. Since p is prime, the map $A \to A$ sending each β to β^p is a ring homomorphism. It agrees with σ on α, so by 5.4(a) on all of A, which is the last statement of 2.7. To prove that A is a field, we let $\beta \in A$, and we prove that β equals 0 or is a unit. Put $I = A\beta$. From $\sigma\beta = \beta^p$ one

sees $\sigma I \subset I$, so by 5.4(e) and the fact that p is prime we have $I = A$ or $I = pA = 0$. In the first case, β is a unit, in the second case it equals 0. Thus, A is a field. By 5.4(a), it is finite, and one has $A = \mathbb{F}_p(\alpha)$. This completes the proof of 2.7.

6. Primality testing with pseudofields

In this section we prove 2.8. We begin with an elegant lemma.

Lemma 6.1. *Let R be a ring, and let G be a finite subgroup of R^* such that for each $\beta \in G$, $\beta \neq 1$, one has $\beta - 1 \in R^*$. Then G is cyclic.*

Proof. We may clearly assume $R \neq \{0\}$, so that we can choose a maximal ideal M of R. For each $\beta \in G$, $\beta \neq 1$, the unit $\beta - 1$ does not belong to M, so that β is not in the kernel of the natural group homomorphism $R^* \to (R/M)^*$. Hence the restriction of the latter map to G is injective, and G is isomorphic to its image in $(R/M)^*$. Since any finite subgroup of the multiplicative group of a field is cyclic, this implies 6.1.

The reader may enjoy proving 6.1 without using maximal ideals, for example by applying 5.3.

Let (A, α) be a pseudofield, and denote by n, d, and σ its characteristic, its degree, and its Frobenius automorphism, respectively. We let p be a prime divisor of n, and put $R = A/pA$. We shall simply write α for the image of α in R, and σ for the automorphism of R induced by σ. Note that the conditions of Proposition 5.4, with R, α, p, d, σ in the roles of A, α, n, d, σ, are satisfied. As in the proof of 2.7, we have

$$(6.2) \qquad \text{if } \beta \in R \text{ satisfies } \sigma\beta \in R\beta, \text{ then } \beta = 0 \text{ or } \beta \in R^*,$$

by 5.4(e) applied to $I = R\beta$. We put

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

For any $\beta \in G$, one has $\sigma\beta = \beta^n \in R\beta$, so $\beta \in R^*$ by (6.2). Since G is finite and closed under multiplication, and contains 1, it is a subgroup of R^*. Also, for any $\beta \in G$, $\beta \neq 1$, one has $\sigma\beta = \beta^n \equiv 1 \bmod R \cdot (\beta - 1)$, so $\sigma(\beta - 1) \in R \cdot (\beta - 1)$ and $\beta - 1 \in R^*$, again by (6.2). Thus, Lemma 6.1 implies

$$(6.3) \qquad\qquad G \text{ is a cyclic subgroup of } R^*.$$

Lemma 6.4. *If $\#G > n^{\sqrt{d/3}} - 1$, then n is a power of p.*

Proof. If $n = p$ the lemma is true, so assume $n > p$. We let ϕ be the ring homomorphism $R \to R$ that sends each $\beta \in R$ to β^p. By 5.4(f), this map is a power of σ; in particular, it is an *automorphism* of R. The definitions of ϕ and G then imply that for all $\beta \in G$ one has $(\sigma\phi^{-1})\beta = \beta^{n/p}$.

Let L be the kernel of the group homomorphism $\mathbb{Z}^2 \to \langle\sigma\rangle$ that maps (i, j) to $(\sigma\phi^{-1})^i \phi^j$. Since the image $\langle\sigma\rangle$ of the group homomorphism has order d, the group L

is a lattice of determinant d (see [14, Chapter I]). Consider the closed convex symmetric subset

$$K = \left\{ (x, y) \in \mathbb{R}^2 : \max\{|x \log(n/p)|, |y \log p|, |x \log(n/p) + y \log p|\} \leq t \right\}$$

of $\mathbb{R}^2$, where $t \in \mathbb{R}_{>0}$ is chosen such that the area $3 \cdot t^2/(\log(n/p) \cdot \log p)$ of K equals $4d$. (Note that K is the hexagonal region with vertices at $\pm(t/\log(n/p), 0)$, $\pm(0, t/\log p)$, and $\pm(t/\log(n/p), -t/\log p)$.) By the inequality of the means we have

$$t = 2\sqrt{d/3} \cdot \left(\log(n/p) \cdot \log p\right)^{1/2} \leq \sqrt{d/3} \cdot \log n.$$

According to Minkowski's lattice point theorem (see [14, Chapter III, Theorem II]), the set K contains a non-zero element (i, j) of L. Multiplying (i, j) by ± 1, we may assume that $i \geq 0$. Note that $(i, j) \in K$ implies that $(n/p)^i p^j \leq n^{\sqrt{d/3}}$ if $j \geq 0$, and

$$|(n/p)^i - p^{-j}| \leq \max\{(n/p)^i, p^{-j}\} - 1 \leq n^{\sqrt{d/3}} - 1$$

if $j < 0$. From $(\sigma \phi^{-1})^i \phi^j = \mathrm{id}_R$ we see that for all $\beta \in G$ one has $\beta^{(n/p)^i p^j} = \beta$. By (6.3), we can choose β to be a generator of G. Thus $(n/p)^i p^j \equiv 1 \bmod \#G$ if $j \geq 0$, and $(n/p)^i \equiv p^{-j} \bmod \#G$ if $j < 0$. But, by hypothesis, $\#G > n^{\sqrt{d/3}} - 1$, so in either case we have $(n/p)^i p^j = 1$. By unique factorization in $\mathbb{Z}$ and $(i, j) \neq (0, 0)$, this equation forces n to be a power of p. This concludes the proof of 6.4.

Proof of Proposition 2.8. We let the notation and the assumptions be as in Proposition 2.8, and in addition we write $B = \lfloor (d/3)^{1/2}(\log n)/\log 2 \rfloor$. Note that the condition $d > (\log n)^2/(3 \cdot (\log 2)^2)$ implies $d > B$.

We apply the theory just developed to a prime factor p of n that satisfies $p > B$. As $\sigma \alpha = \alpha^n$, we see that the element α of $R = A/pA$ belongs to the subgroup G of R^*. From $\sigma(\alpha + a) = \sigma \alpha + a = \alpha^n + a = (\alpha + a)^n$ for $a = 1, \ldots, B$ and from 5.4(a), which implies each $\alpha + a \neq 0$, we see that $\alpha + 1, \ldots, \alpha + B$ also belong to G. For each proper subset S of $\{0, 1, \ldots, B\}$, the element $\prod_{a \in S}(\alpha + a)$ also belongs to G. There are $2^{B+1} - 1$ such sets S, and we claim that they give rise to $2^{B+1} - 1$ different elements of G. To see this, note that since $p > B$, the polynomials $X + a$, $a = 0, 1, \ldots, B$, are distinct in $\mathbb{F}_p[X]$, and by unique factorization in $\mathbb{F}_p[X]$ the polynomials $\prod_{a \in S}(X + a)$, with S as above, are pairwise distinct. As $d > B$, all these polynomials have degrees smaller than d, so by 5.4(a) (applied to R) they give rise to $2^{B+1} - 1$ different elements $\prod_{a \in S}(\alpha + a)$ of G, as asserted.

It follows that

$$\#G \geq 2^{B+1} - 1 > 2^{(d/3)^{1/2}(\log n)/\log 2} - 1 = n^{\sqrt{d/3}} - 1.$$

Applying 6.4 we conclude that n is a power of p. This proves 2.8.

7. Tensor products

Tensor products (see [3, Chapter 2], [24, Chapter XVI]) can be used to construct "large" pseudofields out of "small" ones, in the following manner.

Proposition 7.1. *Let (A_1, α_1) and (A_2, α_2) be pseudofields with* char $A_1 =$ char $A_2 = n$, *and suppose that the degrees d_1, d_2 of these pseudofields satisfy $d_1 > 1$, $d_2 > 1$, and* $\gcd(d_1, d_2) = 1$. *Then the tensor product $(A_1 \otimes_{\mathbb{Z}/n\mathbb{Z}} A_2, \alpha_1 \otimes \alpha_2)$ is a pseudofield of characteristic n and degree $d_1 d_2$.*

Proof. We check that $A = A_1 \otimes_{\mathbb{Z}/n\mathbb{Z}} A_2$, $\alpha = \alpha_1 \otimes \alpha_2$, n, $d = d_1 d_2$, and $\sigma = \sigma_1 \otimes \sigma_2$ satisfy (2.1)–(2.5). By 5.4(a), each A_i is a free $\mathbb{Z}/n\mathbb{Z}$-module with basis $1, \alpha_i, \ldots, \alpha_i^{d_i - 1}$, so from [24, Chapter XVI, Corollary 2.4] one sees that A is a free $\mathbb{Z}/n\mathbb{Z}$-module with basis $(\alpha_1^i \otimes \alpha_2^j)_{0 \le i < d_1, 0 \le j < d_2}$. This implies both (2.1) and (2.2). One has $\sigma(\alpha) = \sigma_1(\alpha_1) \otimes \sigma_2(\alpha_2) = \alpha_1^n \otimes \alpha_2^n = \alpha^n$, which is (2.3). Each $\sigma_i^{d_i}$ is the identity on A_i, so σ^d is the identity on A, which implies (2.4). Finally, to prove (2.5), let l be a prime number dividing d. Then l divides exactly one of d_1 and d_2; by symmetry we may assume it divides d_2. Let k be a prime number dividing d_1. As $\sigma_1 \alpha_1 = \alpha_1^n$, the A_1-ideal $A_1 \alpha_1$ is mapped to itself by σ_1 and therefore contains $\sigma_1^{d_1/k} \alpha_1 - \alpha_1$; the latter element is a unit of A_1, so α_1 is a unit of A_1 as well. Since d/l is divisible by d_1, we have $\sigma_1^{d/l} \alpha_1 = \alpha_1 \in A_1^*$. Since d/l is not divisible by d_2, Proposition 5.1 implies $\sigma_2^{d/l} \alpha_2 - \alpha_2 \in A_2^*$. It follows that the element $\sigma^{d/l} \alpha - \alpha = (\sigma_1^{d/l} \alpha_1) \otimes (\sigma_2^{d/l} \alpha_2) - \alpha_1 \otimes \alpha_2 = \alpha_1 \otimes (\sigma_2^{d/l} \alpha_2 - \alpha_2)$ is a product of two units, and therefore belongs to A^*. This proves 7.1.

We next address the problem of designing an algorithm that, given two pseudofields (A_i, α_i) as in 7.1, computes their tensor product. Here it is assumed, as in Section 2, that a pseudofield is specified by its characteristic and its characteristic polynomial. For the general context of our algorithm one may consult [11].

Let R be a commutative ring, let $m \in \mathbb{Z}_{\ge 0}$, and write S for the ring $R[t]/(t^{m+1})$, where t denotes a polynomial variable. The elements $1, t, \ldots, t^m$ form a basis for S over R, in the sense that every element of S has a unique representation of the form $\sum_{i=0}^m a_i t^i$ with each $a_i \in R$. The elements $\sum_{i=0}^m a_i t^i$ with $a_0 = 0$ form the ideal tS of S, and the elements with $a_0 = 1$ form a subgroup of the group S^* of units of S; we write $1 + tS$ for this subgroup. We define the maps $D \colon S \to tS$ and $L \colon 1 + tS \to tS$ by

$$D\left(\sum_{i=0}^m a_i t^i\right) = \sum_{i=0}^m i a_i t^i \quad (a_i \in R),$$

$$L(u) = D(u) \cdot u^{-1} \quad (u \in 1 + tS).$$

(The notation reflects that, up to a factor t, the maps D and L are differentiation and logarithmic differentiation, respectively.) One readily verifies that for $u, v \in S$ one has $D(uv) = uD(v) + vD(u)$, and consequently L is a group homomorphism from the multiplicative group $1 + tS$ to the additive group tS. For a monic polynomial $g = X^k + \sum_{i=1}^k b_i X^{k-i} \in R[X]$, we write $g^\flat$ for the image of $1 + \sum_{i=1}^k b_i t^i$ in S, which belongs to $1 + tS$. Evidently, we have $(gh)^\flat = g^\flat \cdot h^\flat$ for any two monic polynomials $g, h \in R[X]$. The *Hadamard product* $*$ is the operation defined on S by

$$\left(\sum_{i=0}^m a_i t^i\right) * \left(\sum_{i=0}^m b_i t^i\right) = \sum_{i=0}^m a_i b_i t^i,$$

for $a_i, b_i \in R$.

For any ring homomorphism $\psi \colon R_1 \to R_2$, the composition of the induced ring homomorphism $S_1 = R_1[t]/(t^{m+1}) \to S_2 = R_2[t]/(t^{m+1})$ with $D \colon S_2 \to t S_2$ equals the composition of $D \colon S_1 \to t S_1$ with the induced map $t S_1 \to t S_2$. Similar remarks apply to L, $\flat$, and $*$.

In the following result we use the definitions just given for the ring $R = \mathbb{Z}/n\mathbb{Z}$.

Proposition 7.2. *Let the hypotheses and notation be as in 7.1. Moreover, write f_1, f_2, f for the characteristic polynomials of the pseudofields (A_1, α_1), (A_2, α_2), and $(A_1 \otimes_{\mathbb{Z}/n\mathbb{Z}} A_2, \alpha_1 \otimes \alpha_2)$, respectively. Then for any non-negative integer m we have the identity*

$$L(f^{\flat}) = -L(f_1^{\flat}) * L(f_2^{\flat})$$

in $t(\mathbb{Z}/n\mathbb{Z})[t]/(t^{m+1})$.

Proof. Let the notation A, α, d, σ_1, σ_2, σ be as in the proof of 7.1. We view A_1 and A_2 as subrings of A, identifying α_1 with $\alpha_1 \otimes 1$ and α_2 with $1 \otimes \alpha_2$, so that $\alpha = \alpha_1 \alpha_2$. It suffices to prove the identity in $t A[t]/(t^{m+1})$. From $f = \prod_{i=0}^{d-1}(X - \sigma^i \alpha)$ we obtain $f^{\flat} = \prod_{i=0}^{d-1}(1 - (\sigma^i \alpha)t)$. From $L(1 - (\sigma^i \alpha)t) = -(\sigma^i \alpha)t/(1 - (\sigma^i \alpha)t) = -\sum_{j=1}^{m}(\sigma^i \alpha)^j t^j$ we thus obtain

$$L(f^{\flat}) = \sum_{i=0}^{d-1} L(1 - (\sigma^i \alpha)t) = -\sum_{j=1}^{m}\Big(\sum_{i=0}^{d-1}(\sigma^i \alpha)^j\Big)t^j.$$

Likewise,

$$L(f_1^{\flat}) = -\sum_{j=1}^{m}\Big(\sum_{i=0}^{d_1-1}(\sigma_1^i \alpha_1)^j\Big)t^j, \qquad L(f_2^{\flat}) = -\sum_{j=1}^{m}\Big(\sum_{i=0}^{d_2-1}(\sigma_2^i \alpha_2)^j\Big)t^j.$$

Since $\sigma^i \alpha = (\sigma_1^i \alpha_1) \cdot (\sigma_2^i \alpha_2)$ and the orders d_1 and d_2 of σ_1 and σ_2 are coprime, we have

$$\sum_{i=0}^{d-1}(\sigma^i \alpha)^j = \Big(\sum_{i=0}^{d_1-1}(\sigma_1^i \alpha_1)^j\Big) \cdot \Big(\sum_{i=0}^{d_2-1}(\sigma_2^i \alpha_2)^j\Big)$$

for all $j \geq 1$. The identity to be proved now follows from the definition of the Hadamard product. This proves 7.2.

Proposition 7.3. *For positive integers n, m, let $S_{n,m}$ denote the ring $(\mathbb{Z}/n\mathbb{Z})[t]/(t^{m+1})$.*

(a) *Let n and m be positive integers such that each prime factor of n exceeds m. Then the map $L \colon 1 + t S_{n,m} \to t S_{n,m}$ is a group isomorphism.*

(b) *There is an algorithm that, given positive integers n and m, and an element $u \in 1 + t S_{n,m}$, computes the element $L(u)$ of $t S_{n,m}$ in time $\tilde{O}(m \log n)$.*

(c) *There is an algorithm that, given integers $n > 1$, $m > 0$, and an element $s \in t S_{n,m}$, either computes a prime factor of n that is at most m or correctly decides that no such prime factor exists, and in the latter case computes the element $L^{-1}(s)$ of $1 + t S_{n,m}$, all in time $\tilde{O}(m \log n)$.*

Proof. (a) Since each prime factor of n exceeds m, we have $i \in (\mathbb{Z}/n\mathbb{Z})^*$ for $i = 1, \ldots, m$, so D restricts to a group automorphism of $t S_{n,m}$. For the same reason, there

are well-defined maps $\log\colon 1 + tS_{n,m} \to tS_{n,m}$ and $\exp\colon tS_{n,m} \to 1 + tS_{n,m}$ with

$$\log(1 - x) = -\sum_{i=1}^{m} x^i/i, \quad \exp(x) = \sum_{i=0}^{m} x^i/i!$$

for $x \in tS_{n,m}$. It is well known that log and exp are inverse group isomorphisms. An easy computation shows $L = D \circ \log$. It follows that L is an isomorphism, with inverse $\exp \circ D^{-1}$.

(b) In [7, Section 8] one finds an algorithm that computes $L(u)$ by means of $\tilde{O}(m)$ ring operations in $\mathbb{Z}/n\mathbb{Z}$; this particular algorithm does not depend on the condition, in [7, Section 8], that the field $\mathbb{Q}$ of rational numbers be contained in the coefficient ring. By [21, Sections 8.3 and 9.1], each ring operation in $\mathbb{Z}/n\mathbb{Z}$ can be done in time $\tilde{O}(\log n)$.

(c) We describe an algorithm with the stated properties. Using the extended Euclidean algorithm (see [21, Corollary 11.10]), one attempts to compute $i^{-1} \in \mathbb{Z}/n\mathbb{Z}$ for $i = 1, \ldots, m$; this can only fail if among those i a prime factor of n is found, in which case the algorithm halts. Suppose it does not fail. Then one computes $D^{-1}(s)$ directly from the definition of D by means of m multiplications in $\mathbb{Z}/n\mathbb{Z}$, and next one uses the algorithm from [7, Section 9] to compute $L^{-1}(s) = \exp(D^{-1}(s))$ using $\tilde{O}(m)$ ring operations in $\mathbb{Z}/n\mathbb{Z}$; inspection of this algorithm shows that the condition from [7, Section 9] that $\mathbb{Q}$ be contained in the coefficient ring may be replaced by the weaker condition that multiplicative inverses of each of $i = 1, \ldots, m$ be available; this condition is satisfied in the present case.

This proves 7.3.

Proposition 7.4. *There is an algorithm with the following property. Given an integer n and two pseudofields of characteristic n and of coprime degrees d_1, d_2 greater than 1, it either finds a prime factor of n that is at most $d_1 d_2$ or it constructs the tensor product of the two given pseudofields, and it does so in time $\tilde{O}(d_1 d_2 \log n)$.*

Proof. The following algorithm has the stated properties. Let f_1, f_2 be the characteristic polynomials of the two given pseudofields. Put $m = d_1 d_2$ and $S = (\mathbb{Z}/n\mathbb{Z})[t]/(t^{m+1})$, and compute $f_1^\flat$, $f_2^\flat \in 1 + tS$ from the definition of $\flat$. Next compute $L(f_1^\flat)$ and $L(f_2^\flat)$ by means of the algorithm of 7.3(b), and compute $L(f_1^\flat) * L(f_2^\flat)$ by $d_1 d_2$ multiplications in $\mathbb{Z}/n\mathbb{Z}$. Finally, apply the algorithm of 7.3(c) to $s = -L(f_1^\flat) * L(f_2^\flat)$; this either yields a prime factor of n that is at most $m = d_1 d_2$, or it finds $L^{-1}(s) \in 1 + tS$; in the latter case, the characteristic polynomial of the tensor product is the unique monic polynomial $f \in (\mathbb{Z}/n\mathbb{Z})[X]$ of degree $d_1 d_2$ that satisfies $f^\flat = L^{-1}(s)$. This completes the description of the algorithm. It is correct by 7.2, and 7.3 readily implies that it runs in time $\tilde{O}(d_1 d_2 \log n)$. This proves 7.4.

8. Gaussian periods

In this section we let n be an integer with $n > 1$, we let r be a prime number not dividing n, and we define $\Phi_r = \sum_{i=0}^{r-1} X^i \in (\mathbb{Z}/n\mathbb{Z})[X]$. The element $(X \bmod \Phi_r)$ of the ring $(\mathbb{Z}/n\mathbb{Z})[X]/(\Phi_r)$ is denoted by ζ_r, and that ring itself by $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. We have $\zeta_r^r =$

$1 \neq \zeta_r$, so ζ_r is an element of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^*$ of order r. From $\deg \Phi_r = r - 1$ and $1 + \zeta_r + \cdots + \zeta_r^{r-1} = 0$ one sees that the elements ζ_r^i, $1 \leq i \leq r - 1$, form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ over $\mathbb{Z}/n\mathbb{Z}$.

For each $a \in \mathbb{Z} \setminus r\mathbb{Z}$, the ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ has a unique automorphism mapping ζ_r to ζ_r^a; we write σ_a for this automorphism. The set Δ of all automorphisms of the form σ_a is a group under composition, and the map $\sigma_a \mapsto (a \bmod r)$ is a group isomorphism $\Delta \cong \mathbb{F}_r^*$. One concludes that Δ is cyclic of order $r - 1$, and that the elements $\tau\zeta_r$, $\tau \in \Delta$, form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ over $\mathbb{Z}/n\mathbb{Z}$.

Next let q be a positive integer dividing $r - 1$. Then $\Delta^q = \{\tau^q : \tau \in \Delta\}$ is a subgroup of index q of Δ. The subset $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q} = \{\beta \in (\mathbb{Z}/n\mathbb{Z})[\zeta_r] : \rho\beta = \beta$ for all $\rho \in \Delta^q\}$ is a subring of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. An element $\sum_{\tau \in \Delta} a_\tau \cdot \tau\zeta_r$ with each a_τ in $\mathbb{Z}/n\mathbb{Z}$ belongs to this subring if and only if $a_\tau = a_{\tau\rho}$ for all $\tau \in \Delta$ and $\rho \in \Delta^q$. Hence, if we put $\eta_{r,q} = \sum_{\rho \in \Delta^q} \rho\zeta_r$, then the elements $\tau\eta_{r,q}$ with τ ranging over a set of coset representatives for Δ modulo Δ^q form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q}$ over $\mathbb{Z}/n\mathbb{Z}$; in particular, one has $\#(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q} = n^q$. The elements $\tau\eta_{r,q}$ are called *Gaussian periods* of degree q and conductor r. For example, $\eta_{r,r-1} = \zeta_r$ and $\eta_{r,1} = -1$. We write

$$f_{r,q} = \prod_{\tau\Delta^q \in \Delta/\Delta^q} (Y - \tau\eta_{r,q}).$$

This is a monic polynomial in Y of degree q with $f_{r,q}(\eta_{r,q}) = 0$. Its coefficients, which belong to $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$, are readily checked to be invariant under all $\rho \in \Delta$, so they belong to $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^1} = (\mathbb{Z}/n\mathbb{Z}) \cdot \eta_{r,1} = \mathbb{Z}/n\mathbb{Z}$. Thus, $f_{r,q} \in (\mathbb{Z}/n\mathbb{Z})[Y]$.

Proposition 8.1. *Let $n \in \mathbb{Z}_{>1}$, let r be a prime number not dividing n, and let q be a divisor of $r - 1$ with the property that the element $(n^{(r-1)/q} \bmod r)$ of $\mathbb{F}_r^*$ has order q. Let the notation ζ_r, σ_a, Δ, $\eta_{r,q}$, $f_{r,q}$ be as just defined. Then:*

(a) *if n is prime, then in the ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ one has $\eta_{r,q}^n = \sigma_n \eta_{r,q}$;*

(b) *if in the ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ one has $\eta_{r,q}^n = \sigma_n \eta_{r,q}$, then $((\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q}, \eta_{r,q})$ is a pseudofield of characteristic n and degree q, with characteristic polynomial $f_{r,q}$.*

Proof. To prove (a), suppose that n is prime. Then the map from $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ to itself sending each β to β^n is a ring homomorphism, and since it agrees with σ_n on ζ_r it coincides with σ_n on all of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. This implies (a).

To prove (b), we first observe that the kernel of the group homomorphism $\mathbb{F}_r^* \to \mathbb{F}_r^*$ sending each x to $x^{(r-1)/q}$ equals the subgroup $\mathbb{F}_r^{*q}$ of index q of $\mathbb{F}_r^*$. Hence the condition that $(n^{(r-1)/q} \bmod r)$ have order q implies that the coset $(n \bmod r)\mathbb{F}_r^{*q}$ generates the group $\mathbb{F}_r^*/\mathbb{F}_r^{*q}$, and consequently the coset $\sigma_n\Delta^q$ generates Δ/Δ^q.

For brevity, write $A = (\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q}$. Define the ring homomorphism $\phi : (\mathbb{Z}/n\mathbb{Z})[Y] \to A$ by $\phi(g) = g(\eta_{r,q})$. Its image is the subring of A generated by $\eta_{r,q}$. From $\sigma_n\eta_{r,q} = \eta_{r,q}^n$ it follows that that subring is mapped to itself by σ_n. Since all elements of Δ^q act as the identity on A, and $\sigma_n\Delta^q$ generates Δ/Δ^q, the subring is mapped to itself by *all* $\tau \in \Delta$. Hence, in addition to $\eta_{r,q}$ it contains all $\tau\eta_{r,q}$, so that it is equal to all of A; in other words, ϕ is surjective. The kernel of ϕ contains the $(\mathbb{Z}/n\mathbb{Z})[Y]$-ideal

generated by $f_{r,q}$, and since both of these ideals have index n^q in $(\mathbb{Z}/n\mathbb{Z})[Y]$, we must have equality. Thus, ϕ induces a ring isomorphism $(\mathbb{Z}/n\mathbb{Z})[Y]/(f_{r,q}) \cong A$.

We prove that A, $\alpha = \eta_{r,q}$, n, $d = q$, and σ equal to the restriction of σ_n to A satisfy (2.1)–(2.5). Conditions (2.1)–(2.3) are clearly satisfied, and (2.4) follows from $\sigma_n^q \in \Delta^q$. We prove (2.5). Since $\sigma_n \Delta^q$ generates the group Δ/Δ^q of order q, we may rewrite the definition of $f_{r,q}$ as

$$f_{r,q} = \prod_{i=0}^{q-1} (Y - \sigma^i \eta_{r,q}).$$

It follows that the derivative $f'_{r,q} = \mathrm{d}f_{r,q}/\mathrm{d}Y$ satisfies $f'_{r,q}(\eta_{r,q}) = \prod_{i=1}^{q-1}(\eta_{r,q} - \sigma^i \eta_{r,q})$, so that to prove (2.5) it will suffice to prove $f'_{r,q}(\eta_{r,q}) \in A^*$.

Let p be a prime number dividing n. Taking the isomorphism $(\mathbb{Z}/n\mathbb{Z})[Y]/(f_{r,q}) \cong A$ modulo p, we see that the ring $\mathbb{F}_p[Y]/(f)$, where $f = (f_{r,q} \bmod p) \in \mathbb{F}_p[Y]$, is isomorphic to a subring of $\mathbb{F}_p[X]/(g)$, where $g = \sum_{i=0}^{r-1} X^i$. Since g divides $X^r - 1$ where r is a prime number different from p, one has $\gcd(g, \mathrm{d}g/\mathrm{d}X) = 1$ in the ring $\mathbb{F}_p[X]$. From Lemma 8.2, stated and proved below, it follows that $\gcd(f, \mathrm{d}f/\mathrm{d}Y) = 1$ in the ring $\mathbb{F}_p[Y]$. Thus, there are $u, v \in \mathbb{F}_p[Y]$ with $uf + v\,\mathrm{d}f/\mathrm{d}Y = 1$. Lifting u, v to $(\mathbb{Z}/n\mathbb{Z})[Y]$, one obtains $u_p, v_p, w_p \in (\mathbb{Z}/n\mathbb{Z})[Y]$ such that $u_p f_{r,q} + v_p f'_{r,q} = 1 + pw_p$. Applying ϕ one gets, for each prime number p dividing n, an identity in A of the form $v_p(\eta_{r,q}) \cdot f'_{r,q}(\eta_{r,q}) - p \cdot w_p(\eta_{r,q}) = 1$. Take the product over p, repeating the pth identity just as many times as p occurs in n. On the right, we get 1. On the left, the only term that does not have a factor $f'_{r,q}(\eta_{r,q})$ is divisible by n and is therefore 0. Hence, 1 is divisible by $f'_{r,q}(\eta_{r,q})$ in A, so that the latter element is a unit, as required. The formula we gave for $f_{r,q}$ shows that it is indeed the characteristic polynomial for the pseudofield.

Lemma 8.2. *Let p be a prime number, and let $f, g \in \mathbb{F}_p[X]$ be non-zero polynomials for which the ring $\mathbb{F}_p[X]/(f)$ is isomorphic to a subring of $\mathbb{F}_p[X]/(g)$. Suppose also $\gcd(g, \mathrm{d}g/\mathrm{d}X) = 1$. Then $\gcd(f, \mathrm{d}f/\mathrm{d}X) = 1$.*

Proof. A non-zero polynomial $h \in \mathbb{F}_p[X]$ satisfies $\gcd(h, \mathrm{d}h/\mathrm{d}X) = 1$ if and only if h is squarefree in the ring $\mathbb{F}_p[X]$, and if and only if there is no non-zero nilpotent element in the ring $\mathbb{F}_p[X]/(h)$. Thus, the lemma follows from the trivial observation that if a ring has no non-zero nilpotent element, then the same is true for a subring. This proves 8.2 and completes the proof of 8.1.

We next describe an algorithm that will prove Propositions 2.13 and 2.14.

Algorithm 8.3. Given an integer $n > 1$, which may or may not be known to be prime, and a period system $\mathcal{P}$ for n satisfying $n > \deg \mathcal{P}$, this algorithm attempts to construct a pseudofield of characteristic n and degree $\deg \mathcal{P}$.

Step 1. For all $(r, q) \in \mathcal{P}$ in succession, do the following. Compute $\eta_{r,q} \in (\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ as well as all of its conjugates $\tau \eta_{r,q}$, and form the product of the q polynomials $Y - \tau \eta_{r,q}$ in $(\mathbb{Z}/n\mathbb{Z})[\zeta_r][Y]$; the result is $f_{r,q}$, which has coefficients in the subring $\mathbb{Z}/n\mathbb{Z}$ of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. If n is not known to be prime, compute by an nth powering

in the ring $(\mathbb{Z}/n\mathbb{Z})[Y]/(f_{r,q})$ the unique polynomial $g_{r,q} \in (\mathbb{Z}/n\mathbb{Z})[Y]$ satisfying $Y^n \equiv g_{r,q} \bmod f_{r,q}$ and $\deg g_{r,q} < q$, and test whether in $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ one has $g_{r,q}(\eta_{r,q}) = \sigma_n \eta_{r,q}$; if this test fails, declare n composite and halt.

Step 2. [If the algorithm arrives at this point then, as we shall prove below, for each $(r, q) \in \mathcal{P}$ the pair $(n, f_{r,q})$ specifies a pseudofield.] Applying the algorithm of 7.4 at most $\#\mathcal{P} - 1$ times, either find a prime factor of n that is at most $\deg \mathcal{P}$, or construct the repeated tensor product of the $\#\mathcal{P}$ pseudofields specified by the pairs $(n, f_{r,q})$ for $(r, q) \in \mathcal{P}$. In the former case, declare n composite and halt, and in the latter case return the tensor product computed by the algorithm and halt.

This completes the description of Algorithm 8.3.

Proposition 8.4. *Algorithm* 8.3, *when given n, $\mathcal{P}$ satisfying $n > \deg \mathcal{P}$, runs in time*

$$\tilde{O}\Big(\Big(\deg \mathcal{P} + \sum_{(r,q)\in\mathcal{P}} qr\Big) \log n\Big) \quad or \quad \tilde{O}\Big(\Big(\deg \mathcal{P} + \sum_{(r,q)\in\mathcal{P}} q(r + \log n)\Big) \log n\Big)$$

according as n is or is not known to be prime, and either correctly declares n composite or constructs a pseudofield of characteristic n and degree $\deg \mathcal{P}$.

Proof. We first prove the correctness of the algorithm. Since $f_{r,q}(\eta_{r,q}) = 0$, the congruence $Y^n \equiv g_{r,q} \bmod f_{r,q}$ in Step 1 implies $g_{r,q}(\eta_{r,q}) = \eta_{r,q}^n$. Thus, by 8.1(a), the condition $g_{r,q}(\eta_{r,q}) = \sigma_n \eta_{r,q}$ is necessary for n to be prime, and the algorithm is correct if it halts in Step 1. If it passes Step 1, then by 8.1(b) there is for each $(r, q) \in \mathcal{P}$ a pseudofield of characteristic n with characteristic polynomial $f_{r,q}$. Hence by 7.4 the algorithm either constructs the desired tensor product, or finds a prime factor of n that is at most $\deg \mathcal{P}$; in the latter case, n is composite because $n > \deg \mathcal{P}$. This proves the correctness of the algorithm.

The run time of Step 1 is dominated by the computation of the polynomials $f_{r,q}$ and, if n is not known to be prime, the polynomials $g_{r,q}$ and their values at $\eta_{r,q}$. The computation of $f_{r,q}$, if done by means of Algorithm 10.3 from [21], runs in time $\tilde{O}(qr \log n)$. The computation of $g_{r,q}$ involves $O(\log n)$ multiplications in the ring $(\mathbb{Z}/n\mathbb{Z})[Y]/(f_{r,q})$ and can therefore be performed in time $\tilde{O}(q \cdot (\log n)^2)$. The computation of $g_{r,q}(\eta_{r,q})$ runs in time $\tilde{O}(qr \log n)$. By 7.4, Step 2 runs in time $\tilde{O}(\log n \cdot \deg \mathcal{P})$.

This proves 8.4. $\square$

Proposition 2.13 is an immediate corollary of 8.4. In addition, if n is prime, then it is not declared composite, so that the algorithm returns a pseudofield; whence by 2.7, this pseudofield is a finite field. Thus, by 2.6, its characteristic polynomial is irreducible in $\mathbb{F}_n[X]$. So Proposition 2.14 follows from 8.4 as well.

9. The continuous Frobenius problem

In this section we prove Theorem 3 from the Introduction. As mentioned there, our proof is adapted from Bleichenbacher [10].

For any open subset S of the positive reals, let

$$M(S) = \int_S \frac{\mathrm{d}x}{x},$$

and let S^* denote the additive semigroup generated by S. We first prove the theorem in the case that S is a finite union of n open intervals, after which the general case will be seen to follow easily.

To prove the theorem for the union of n open intervals, we proceed by induction. In particular, the theorem is true vacuously for $n = 0$. Henceforth we shall assume that

(9.1) $n \geq 1$ and the theorem holds for the union of n' open intervals for all $0 \leq n' < n$.

Definition 9.2. Let n be a positive integer, let $t \in (0, 1]$, and let $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$ with

(9.3) $$t \geq b_1 \geq a_1 \geq \cdots \geq b_n \geq a_n \geq 0, \quad b_1 > \cdots > b_n > 0.$$

Let

(9.4) $$S(\mathbf{a}, \mathbf{b}) = \bigcup_{i=1}^{n} (a_i, b_i).$$

As a union of open intervals, $S(\mathbf{a}, \mathbf{b})$ is an open subset of $\mathbb{R}_{>0}$. Let $\mathcal{S}_{t,n}$ denote the set of such sets $S(\mathbf{a}, \mathbf{b}) \subset (0, t)$ such that for each $\mathbf{h} \in (\mathbb{Z}_{\geq 0})^n$ with $h_i = 0$ whenever $a_i = b_i$,

(9.5) $$\text{either } \mathbf{h} \cdot \mathbf{b} \leq 1 \text{ or } 1 \leq \mathbf{h} \cdot \mathbf{a}.$$

Lemma 9.6. *If $S \in \mathcal{S}_{t,n}$, then $1 \notin S^*$. Conversely, if S is the union of at most n open intervals in $(0, t)$ with $1 \notin S^*$, then $S \in \mathcal{S}_{t,n}$.*

Proof. Suppose $S = S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}$. If $1 \in S^*$ there are elements $s_1, \ldots, s_N \in S$ with sum 1. For $1 \leq i \leq n$, let h_i be the number of these elements s_j with $s_j \in (a_i, b_i)$. With $\mathbf{h} = (h_1, \ldots, h_n)$ we thus have $\mathbf{h} \in (\mathbb{Z}_{\geq 0})^n$, $h_i = 0$ whenever $a_i = b_i$, and

$$\mathbf{h} \cdot \mathbf{a} < s_1 + \cdots + s_N = 1 < \mathbf{h} \cdot \mathbf{b},$$

in violation of (9.5). Thus, $1 \notin S^*$. Conversely, suppose that S is the union of at most n open intervals in $(0, t)$. We may write any such S as in (9.3) and (9.4). Assume that there is some $\mathbf{h} \in (\mathbb{Z}_{\geq 0})^n$ for which $h_i = 0$ whenever $a_i = b_i$ and (9.5) fails; that is, $\mathbf{h} \cdot \mathbf{a} < 1 < \mathbf{h} \cdot \mathbf{b}$. Let $A = \mathbf{h} \cdot \mathbf{a}$, $B = \mathbf{h} \cdot \mathbf{b}$, $\alpha = (B - 1)/(B - A)$, $\beta = (1 - A)/(B - A)$. Then α, β are positive with $\alpha + \beta = 1$. For $1 \leq i \leq n$, let $c_i = \alpha a_i + \beta b_i$. Then, if $h_i \neq 0$, we have $c_i \in (a_i, b_i)$, so that $\mathbf{h} \cdot \mathbf{c} \in S^*$. But, by construction,

$$\mathbf{h} \cdot \mathbf{c} = \alpha \mathbf{h} \cdot \mathbf{a} + \beta \mathbf{h} \cdot \mathbf{b} = \alpha A + \beta B = 1,$$

so that $1 \in S^*$. This completes the proof of the lemma.

Lemma 9.7. *Fix an arbitrary vector $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{R}^n$ for which $t \geq b_1 > \cdots > b_n > 0$. Then $M(S(\mathbf{a}, \mathbf{b}))$ achieves a maximum value $M_\mathbf{b}$ over all $\mathbf{a} \in \mathbb{R}^n$ for which $S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}$. Furthermore, $M_\mathbf{b} > 0$.*

Proof. Note that by (9.3) and (9.5), the set of vectors $\mathbf{a}$ with $S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}$ is a compact subset of $\mathbb{R}^n$. Moreover, if $\mathbf{a}$ is in this set, we have $a_n \neq 0$ since otherwise $1 \in S(\mathbf{a}, \mathbf{b})^*$, so that Lemma 9.6 implies that $S(\mathbf{a}, \mathbf{b}) \notin \mathcal{S}_{t,n}$. Thus, $M(S(\mathbf{a}, \mathbf{b}))$ is continuously defined over this set. There are vectors $\mathbf{a}$ with $S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}$, indeed $\mathbf{a} = \mathbf{b}$ is permitted. It follows that $M(S(\mathbf{a}, \mathbf{b}))$ attains a maximum $M_{\mathbf{b}}$ as claimed. To see that $M_{\mathbf{b}} > 0$, let m be the least integer with $m > 1/b_1$, and then choose $a_1 = 1/m$ and $a_i = b_i$ for $2 \leq i \leq n$. The vector $\mathbf{a}$ satisfies (9.3) and since $1 \notin S(\mathbf{a}, \mathbf{b})^*$, Lemma 9.6 implies that $S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}$. But $M(S(\mathbf{a}, \mathbf{b})) = \log(mb_1)$ and this expression is positive since $mb_1 > 1$. This completes the proof of the lemma.

Definition 9.8. Let $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$ as in (9.3). We say $S(\mathbf{a}, \mathbf{b})$ is *degenerate* if either $a_i = b_i$ for some i with $1 \leq i \leq n$ or $a_{i-1} = b_i$ for some i with $2 \leq i \leq n$.

Lemma 9.9. *Suppose* $\mathbf{b}$ *satisfies the hypothesis of Lemma* 9.7. *If* $S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}$ *is such that* $M(S(\mathbf{a}, \mathbf{b})) = M_{\mathbf{b}}$, *then either* $M_{\mathbf{b}} < t$ *or* $S(\mathbf{a}, \mathbf{b})$ *is non-degenerate.*

Proof. Suppose $S = S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}$ has $M(S(\mathbf{a}, \mathbf{b})) = M_{\mathbf{b}}$. First, we delete each empty interval, that is, each interval with $a_i = b_i$. This preserves the property $1 \notin S^*$ and does not change $M(S)$. However, it does allow us to reduce to some $n' < n$, and by (9.1), $M(S) < t$. Next, suppose that $a_{i-1} = b_i$ for some i with $2 \leq i \leq n$. 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}) keeping the property that $1 \notin S^*$ and not changing the value of $M(S)$. Indeed the latter claim is clear, and if 1 is now representable by a sum of members of $S \cup \{b_i\}$, then b_i must be involved in the sum, say with positive integral coefficient d. If $d = 1$, then replace b_i in the sum with $b_i + \epsilon$ for a suitably small $\epsilon > 0$, and then replace another member $x \in S$ 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, and we have represented 1 as a sum of members of S, contradicting $S \in \mathcal{S}_{t,n}$ (see Lemma 9.6). If $d \geq 2$, then since $b_i + \epsilon/(d-1)$ and $b_i - \epsilon$ are both in S for ϵ small enough, we can replace the d copies of b_i in the sum with $d - 1$ copies of $b_i + \epsilon/(d-1)$ and one copy of $b_i - \epsilon$, and so represent 1 as a sum of members of S. 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. Again, by (9.1), we have $M(S) < t$. We conclude that either $M(S) < t$ or S is non-degenerate, proving the lemma.

We now assume that the vectors $\mathbf{a}, \mathbf{b}$ satisfy

$$(9.10) \qquad\qquad S(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_{t,n}, \quad M(S(\mathbf{a}, \mathbf{b})) = M_{\mathbf{b}},$$

and

$$(9.11) \qquad\qquad t \geq b_1 > a_1 > \cdots > b_n > a_n > 0.$$

We partition the vectors $\mathbf{h} \in (\mathbb{Z}_{\geq 0})^n$ into three disjoint sets. Let

$$H_0 = \{\mathbf{h} \in (\mathbb{Z}_{\geq 0})^n \ : \ \mathbf{h} \cdot \mathbf{a} < 1\},$$
$$H_1 = \{\mathbf{h} \in (\mathbb{Z}_{\geq 0})^n \ : \ \mathbf{h} \cdot \mathbf{a} = 1\},$$
$$H_2 = \{\mathbf{h} \in (\mathbb{Z}_{\geq 0})^n \ : \ \mathbf{h} \cdot \mathbf{a} > 1\}.$$

Since $a_i > 0$ for each i, it follows that H_0, H_1 are finite sets.

Lemma 9.12. *Let* $\mathbf{a}$, $\mathbf{b}$ *be as in* (9.10), (9.11) *and for notational convenience, let* $a_{n+1} = b_{n+1} = 0$. *If* $\mathbf{h} \in H_1$, *then*

$$h_k \mathbf{h} \cdot (\mathbf{b} - \mathbf{a}) \le h_k(b_k - b_{k+1}) \quad \text{for } 1 \le k \le n.$$

Proof. Let $\mathbf{e}_k$ be the kth standard basis vector in $\mathbb{R}^n$. For $k = 1, \ldots, n$, 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 $\mathbf{h}' = \mathbf{h} - \mathbf{e}_k + \mathbf{e}_{k+1}$ if $k < n$, and $\mathbf{h}' = \mathbf{h} - \mathbf{e}_k$ if $k = n$. Then $\mathbf{h}' \in H_0$. Hence, since (9.5) holds for $\mathbf{h}'$, we have $\mathbf{h}' \cdot \mathbf{b} \le 1$. That is,

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

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

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

Thus,

$$h_k \mathbf{h} \cdot (\mathbf{b} - \mathbf{a}) \le h_k(b_k - b_{k+1}),$$

an inequality that continues to hold if $h_k = 0$. This completes the proof.

Let $\mathbf{v}$ be an arbitrary vector in $\mathbb{R}^n$ and for real numbers x, let

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

Note that

(9.13) $$f_{\mathbf{v}}'(0) = -\mathbf{v} \cdot m(\mathbf{a}),$$

where $m(\mathbf{a}) := (1/a_1, \ldots, 1/a_n)$.

Lemma 9.14. *Let* $\mathbf{v} \in \mathbb{R}^n$ *be such that* $\mathbf{h} \cdot \mathbf{v} \ge 0$ *for all* $\mathbf{h} \in H_1$. *Let* $\epsilon_{\mathbf{v}} > 0$ *be a real number such that* $a_i + \epsilon_{\mathbf{v}} < b_i$ *for* $i = 1, \ldots, n$. *Then for each real* $x \in [0, \epsilon_{\mathbf{v}}]$, *the vector* $\mathbf{a} + x\mathbf{v}$ *satisfies* (9.11) *in place of* $\mathbf{a}$. *Further, by possibly reducing* $\epsilon_{\mathbf{v}} > 0$, *one has* $S(\mathbf{a} + x\mathbf{v}, \mathbf{b}) \in \mathcal{S}_{t,n}$ *for every* $x \in [0, \epsilon_{\mathbf{v}}]$. *In addition,* $\mathbf{v} \cdot m(\mathbf{a}) \ge 0$.

Proof. Assume that $\mathbf{v} \in \mathbb{R}^n$ has $\mathbf{h} \cdot \mathbf{v} > 0$ for all $\mathbf{h} \in H_1$ and that $\epsilon_{\mathbf{v}}$ has been chosen as described. It is clear that $\mathbf{a} + x\mathbf{v}$ satisfies (9.11) for each $x \in [0, \epsilon_{\mathbf{v}}]$. Suppose that $\mathbf{h} \in (\mathbb{Z}_{\ge 0})^n$, so that $\mathbf{h} \in H_0, H_1$, or H_2. If $\mathbf{h} \in H_0$, since (9.5) holds for $\mathbf{a}$, we have $\mathbf{h} \cdot \mathbf{b} \le 1$. Thus, (9.5) holds for all of the vectors $\mathbf{a} + x\mathbf{v}$ and all $\mathbf{h} \in H_0$. Now suppose $\mathbf{h} \in H_1$. By hypothesis, $\mathbf{h} \cdot (\mathbf{a} + x\mathbf{v}) = 1 + x\mathbf{h} \cdot \mathbf{v} \ge 1$ for all $x \in \mathbb{R}_{\ge 0}$, so that (9.5) holds for each $\mathbf{a} + x\mathbf{v}$ and all $\mathbf{h} \in H_1$. Finally, we consider H_2. Since $\mathbf{a} \in \mathbb{R}_{>0}^n$, there is a finite "minimal" set $H_2^* \subset H_2$ such that $\mathbf{h} \in H_2$ if and only if there is some $\mathbf{h}^* \in H_2^*$ with $\mathbf{h} - \mathbf{h}^* \in \mathbb{Z}_{\ge 0}^n$. Let

$$W = \{\mathbf{w} \in \mathbb{R}_{>0}^n : \mathbf{w} \cdot \mathbf{h}^* > 1 \text{ for all } \mathbf{h}^* \in H_2^*\}.$$

Then W is an open set that contains $\mathbf{a}$. Thus, given $\mathbf{v}$, by possibly reducing $\epsilon_{\mathbf{v}} > 0$, for all $0 \leq x \leq \epsilon_{\mathbf{v}}$ we have $\mathbf{a} + x\mathbf{v} \in W$. It follows that $\mathbf{h} \cdot (\mathbf{a} + x\mathbf{v}) > 1$ for $0 \leq x \leq \epsilon_{\mathbf{v}}$ and all $\mathbf{h} \in H_2$. That is, (9.5) holds for the vectors $\mathbf{a} + x\mathbf{v}$ and all $\mathbf{h} \in H_2$. Thus, $S(\mathbf{a} + x\mathbf{v}, \mathbf{b}) \in \mathcal{S}_{t,n}$ as asserted. By the maximality of $\mathbf{a}$, we have $f'_{\mathbf{v}}(0) \leq 0$, which implies the last assertion by (9.13). This completes the proof.

It is now clear that H_1 is non-empty, since if $H_1 = \emptyset$, we would have $\mathbf{v} \cdot m(\mathbf{a}) \geq 0$ for all vectors $\mathbf{v} \in \mathbb{R}^n$, which is patently false. Let $r = \#H_1$.

We cite a result of Farkas [20].

Lemma 9.15 (J. Farkas). *Suppose A is an $r \times n$ real matrix and $\mathbf{m} \in \mathbb{R}^n$. Suppose that for all $\mathbf{v} \in \mathbb{R}^n$ with $A\mathbf{v} \in (\mathbb{R}_{\geq 0})^r$ we have $\mathbf{m} \cdot \mathbf{v} \geq 0$. Then there is a vector $\mathbf{p} \in (\mathbb{R}_{\geq 0})^r$ with $\mathbf{p}^T A = \mathbf{m}$.*

(Note that the converse trivially holds: If $A\mathbf{v}, \mathbf{p} \in (\mathbb{R}_{\geq 0})^r$ and $\mathbf{p}^T A = \mathbf{m}$, then $\mathbf{m} \cdot \mathbf{v} = \mathbf{p}^T A \cdot \mathbf{v} = \mathbf{p}^T \cdot A\mathbf{v} \geq 0$.)

Proof of Theorem 3. We apply Lemma 9.15 to the matrix A whose rows are the r vectors in H_1 and to the vector $\mathbf{m} = m(\mathbf{a})$. We have shown in Lemma 9.14 that $A\mathbf{v} \in (\mathbb{R}_{\geq 0})^r$ implies that $\mathbf{m} \cdot \mathbf{v} \geq 0$. Thus, Lemma 9.15 implies there is a vector $\mathbf{p} \in (\mathbb{R}_{\geq 0})^r$ with $\mathbf{p}^T A = \mathbf{m}$. Say $\mathbf{p} = (p_1, \ldots, p_r)$, $H_1 = \{\mathbf{h}_1, \ldots, \mathbf{h}_r\}$, and let each $\mathbf{h}_j$ be $(h_{j1}, \ldots, h_{jn})$. We have

$$\sum_{j=1}^{r} p_j h_{jk} = 1/a_k \quad \text{for } 1 \leq k \leq n.$$

Take the inequality in Lemma 9.12 applied to $\mathbf{h}_j$, multiply it by p_j, and sum over j. For $k = 1, \ldots, n$, we have

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

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

(9.16) $$\sum_{k=1}^{n} a_k \sum_{j=1}^{r} p_j h_{jk} \sum_{i=1}^{n} h_{ji}(b_i - a_i) \leq \sum_{k=1}^{n}(b_k - b_{k+1}) = b_1.$$

The left side of (9.16) equals

$$\sum_{j=1}^{r} p_j \sum_{k=1}^{n} a_k h_{jk} \sum_{i=1}^{n} h_{ji}(b_i - a_i) = \sum_{j=1}^{r} p_j(\mathbf{h}_j \cdot \mathbf{a})(\mathbf{h}_j \cdot (\mathbf{b} - \mathbf{a})) = \sum_{j=1}^{r} p_j \mathbf{h}_j \cdot (\mathbf{b} - \mathbf{a})$$

$$= m(\mathbf{a}) \cdot (\mathbf{b} - \mathbf{a}) = \sum_{i=1}^{n}(b_i - a_i)/a_i.$$

Thus, (9.16) implies that

(9.17) $$\sum_{i=1}^{n}(b_i/a_i - 1) = \sum_{i=1}^{n}(b_i - a_i)/a_i \leq b_1.$$

However, $M((a_i, b_i)) = \log(b_i/a_i) < b_i/a_i - 1$. Hence, by (9.17),

$$M_{\mathbf{b}} = \sum_{i=1}^{n} \log(b_i/a_i) < b_1 \le t.$$

We have $M_{\mathbf{b}} < t$ for each choice of $\mathbf{b}$ satisfying (9.11), and so Theorem 3 holds for any S which is the union of finitely many intervals. If $S \subset (0, t)$ is the union of infinitely many disjoint open intervals and has $1 \notin S^*$, let $S(n)$ be the union of n of these intervals with $S(n) \subset S(n + 1)$ and $\bigcup S(n) = S$. We have $M(S(n)) < t$ for each n, and so $M(S) = \lim_{n \to \infty} M(S(n)) \le t$. This concludes the proof of the theorem.

Remarks. We have seen that the inequality $M(S) < t$ holds when $S \subset (0, t)$ is a finite union of open intervals with 1 not in the additive semigroup generated by S. This inequality for a finite union of intervals is best possible. Indeed, suppose S_n is the intersection of $(0, t)$ and the additive semigroup generated by $(1/(n + 1), 1/n)$, where n is a positive integer. Note that 1 is not in this semigroup. Further, we have

$$M(S_n) \ge \sum_{j=1}^{\lfloor tn \rfloor} M\left(\left(\frac{j}{n+1}, \frac{j}{n}\right)\right) = \sum_{j=1}^{\lfloor tn \rfloor} \log(1 + 1/n) > \lfloor tn \rfloor \left(\frac{1}{n} - \frac{1}{n^2}\right) > t - \frac{1+t}{n}.$$

Thus, as n grows, we have $M(S_n)$ as close as we please to t.

It is possibly true that $M(S) < t$ continues to hold when S is an infinite union of disjoint intervals; that is, the theorem holds with a strict inequality. We leave this as an open question.

10. A number-theoretic application

In this section we give a number-theoretic application to the continuous Frobenius problem, proving a result which contains Theorem 4. The recent paper [22] contains a similar result.

Proposition 10.1. *Let α, ϵ be real numbers with*

$$0 < \epsilon \le \alpha/2 \le 1/4.$$

There is a positive integer $x_0 = x_0(\alpha, \epsilon)$, effectively computable if α, ϵ are rational, with the following property. If x, u, D are real numbers with

$$x > x_0, \quad 2 < u < (\log x)^{1/10}, \quad \text{and} \quad x^{1/(2(\alpha-\epsilon))} \le D \le x^{1/\alpha},$$

then for any set $\mathcal{Q}$ of primes contained in $(x^{1/u}, x^{1/2}]$ with

$$\sum_{q \in \mathcal{Q}} \frac{1}{q} \ge \alpha,$$

there is a squarefree integer d composed of primes from $\mathcal{Q}$ with $D \le d < D + D^{1-\alpha/(4u)}$. Moreover, the number of squarefree integers $d \in [D, 2D)$ composed of primes from $\mathcal{Q}$ exceeds $D/(\log D)^{5u}$.

Before commencing the proof we identify some auxiliary variables and prove some lemmas. Let D be as in 10.1 and write

$$D = x^{1/(2(\alpha-\delta))}, \qquad \alpha/2 \geq \delta \geq \epsilon.$$

Let N be an integer for which

(10.2) $$6u \log x \leq N \leq x^{1/(3u)}.$$

For N satisfying (10.2) and for $i = 1, \ldots, N$, let

$$I_i = [x^{(i-1)/N}, x^{i/N}), \qquad M_i = x^{i/N}/i^2.$$

Further, for $\mathcal{Q}$ as in 10.1, let

(10.3) $$\mathcal{Q}_i = \begin{cases} I_i \cap \mathcal{Q} & \text{if } \#(I_i \cap \mathcal{Q}) > M_i, \\ \emptyset & \text{otherwise.} \end{cases}$$

We remark that $\mathcal{Q}_i = \emptyset$ for $i \leq N/u$.

Lemma 10.4. *If x is sufficiently large, then for $\mathcal{Q}$ as in* 10.1, *N satisfying* (10.2), *and sets $\mathcal{Q}_i$ defined in* (10.3),

$$\sum_{i=1}^{N} \sum_{q \in \mathcal{Q}_i} \frac{1}{q} > \alpha - \delta/2.$$

Proof. The double sum here is smaller than the sum $\sum_{q \in \mathcal{Q}} \frac{1}{q}$ in 10.1, the difference between them coming from intervals I_i with $\#(I_i \cap \mathcal{Q}) \leq M_i$. Since $I_i \cap \mathcal{Q} = \emptyset$ for $i \leq N/u$, the sum of $1/q$ for primes q in intervals I_i with $\#(I_i \cap \mathcal{Q}) \leq M_i$ is at most

$$\sum_{N \geq i > N/u} \frac{M_i}{x^{(i-1)/N}} = \sum_{N \geq i > N/u} \frac{x^{1/N}}{i^2} < \frac{2u}{N} x^{1/N} \leq \frac{1}{3 \log x} e^{1/(6u)} < \frac{1}{\log x},$$

by the first inequality in (10.2). Thus, these primes give a negligible contribution as $x \to \infty$, and we have 10.4.

For N as in (10.2) and for $i = 1, \ldots, N$, write $x^{i/N} = x^{(i-1)/N} + L_i$. Then by the upper bound in (10.2), for all $i > N/u$,

(10.5) $$L_i = x^{(i-1)/N}(x^{1/N} - 1) > x^{(i-1)/N} \frac{\log x}{N} > (x^{(i-1)/N})^{3/5}$$

for all sufficiently large x.

Lemma 10.6. *Suppose that N satisfies* (10.2) *and sets $\mathcal{Q}_i$ are as in* (10.3). *For each i with $\mathcal{Q}_i \neq \emptyset$, let $S(i)$ be the image of I_i under the natural logarithm map, and if $\mathcal{Q}_i = \emptyset$, let $S(i) = \emptyset$. If x is sufficiently large, then*

$$\sum_{i=1}^{N} \int_{S(i)} \frac{dt}{t} > \alpha - \delta.$$

Proof. If $Q_i \neq \emptyset$, we have $i > N/u$, and so we may assume that (10.5) holds. The interval I_i is thus of the shape $[z, z+L)$ where $L > z^{3/5}$. So, by a theorem of Huxley [23], the number of primes in I_i is $(1 + o(1))L_i/\log(x^{(i-1)/N}) = (1 + o(1))x^{(i-1)/N}/i$ as $x \to \infty$, uniformly in i for $N/u < i \leq N$. Let $\eta = (\delta/2)/(\alpha - \delta)$. It follows that for all x larger than some effectively computable bound depending on η and for each i with $Q_i \neq \emptyset$, the number of primes in I_i is smaller than $(1 + \eta)x^{(i-1)/N}/i$ and so

$$(10.7) \qquad \sum_{q \in Q_i} \frac{1}{q} < \frac{1+\eta}{i} < (1 + \eta) \log \frac{i}{i-1} = (1 + \eta) \int_{S(i)} \frac{dt}{t}.$$

Hence, for sufficiently large x, 10.4 and (10.7) imply that

$$\sum_{i=1}^{N} \int_{S(i)} \frac{dt}{t} > (1+\eta)^{-1} \sum_{i=1}^{N} \sum_{q \in Q_i} \frac{1}{q} > \frac{\alpha - \delta/2}{1+\eta} = \alpha - \delta.$$

This proves 10.6.

Proof of Proposition 10.1. We choose as a target for our squarefree number d a number D' slightly above D, since we may miss the target on the low side, and we wish to have $d \geq D$. To be specific, let $D' = D \exp(2u(\log x)/(\alpha N))$ and let S be the additive semigroup generated by

$$\bigcup_{i=1}^{N} \frac{1}{\log D'} S(i),$$

where $S(i)$ is as in 10.6. Note that if $S(i) \neq \emptyset$ we have $x^{(i-1)/N} \leq x^{1/2}$, so that since $D = x^{1/(2(\alpha-\delta))}$,

$$\frac{\log(x^{i/N})}{\log D'} \leq \left(\frac{1}{2} + \frac{1}{N}\right) \frac{\log x}{\log D'} = \left(\frac{1}{2} + \frac{1}{N}\right) \frac{\alpha - \delta}{\frac{1}{2} + \frac{2u}{\alpha N}(\alpha - \delta)} < \alpha - \delta,$$

where in the last step we have used $\alpha - \delta > \alpha/2$ and $u > 2$. Thus, $S(i)/\log D' \subset (0, \alpha - \delta)$. It now follows from 10.6 and the fact that the intervals $S(i)$ are disjoint that

$$\int_{S \cap (0, \alpha - \delta)} \frac{dt}{t} \geq \sum_{i=1}^{N} \int_{S(i)/\log D'} \frac{dt}{t} = \sum_{i} \int_{S(i)} \frac{dt}{t} > \alpha - \delta.$$

From Theorem 3 we know that $1 \in S$. Hence, there are a finite subset F of $\bigcup_i S(i)$ and positive integers $\kappa(f)$ for each $f \in F$ such that

$$\sum_{f \in F} \kappa(f)f = \log D'.$$

Let $F_i = F \cap S(i)$ for $i = 1, \ldots, N$, and let

$$\kappa_i = \sum_{f \in F_i} \kappa(f).$$

Then, using $S(i) = \emptyset$ for $i \le N/u$ from 10.3, we see that

$$
(10.8) \qquad \sum_{i=1}^{N} \kappa_i = \sum_i \sum_{f \in F_i} \kappa(f) \le \sum_i \frac{1}{\log(x^{(i-1)/N})} \sum_{f \in F_i} \kappa(f) f
$$

$$
< \frac{1}{\log(x^{1/u-1/N})} \sum_{f \in F} \kappa(f) f = \frac{\log D'}{(1/u - 1/N) \log x} < 2u/\alpha,
$$

the last inequality holding when x is sufficiently large. If $S(i) \neq \emptyset$, then (10.2) and (10.3) imply that $\#\mathcal{Q}_i > M_i > x^{1/u}/N^2 > 2u/\alpha > \kappa_i$, again since x is large. Thus, for each i with $\kappa_i > 0$ there are at least κ_i distinct primes in the set $\mathcal{Q}_i$. Label a choice for such primes $q_{1,i}, q_{2,i}, \ldots, q_{\kappa_i,i}$ and let

$$
d = \prod_{i=1}^{N} \prod_{j=1}^{\kappa_i} q_{j,i}.
$$

We have

$$
(10.9) \quad |\log D' - \log d|
$$

$$
= \left| \sum_{f \in F} \kappa(f) f - \sum_{i=1}^{N} \sum_{j=1}^{\kappa_i} \log q_{j,i} \right| = \left| \sum_{i=1}^{N} \left(\sum_{f \in F_i} \kappa(f) f - \sum_{j=1}^{\kappa_i} \log q_{j,i} \right) \right|
$$

$$
< \sum_i \kappa_i \left(\log(x^{i/N}) - \log(x^{(i-1)/N}) \right) = \frac{\log x}{N} \sum_i \kappa_i < \frac{2u \log x}{\alpha N},
$$

using (10.8). Thus,

$$
D = D' \exp(-2u(\log x)/(\alpha N)) < d < D' \exp(2u(\log x)/(\alpha N))
$$

$$
< D(1 + 6u(\log x)/(\alpha N)).
$$

By choosing N near the upper end of the interval in (10.2), we have the first assertion in 10.1.

Now we show that there are many squarefree integers in $[D, 2D)$ that are composed of primes from $\mathcal{Q}$. We choose $N = \lceil 6u \log x \rceil$ in (10.2) and we let $D' = \sqrt{2}D$. For each i with $\kappa_i > 0$ choose κ_i primes from $\mathcal{Q}_i$ and let d denote the product of all of these primes over all choices for i. Then, as in (10.9) and by our choice of N,

$$
|\log D' - \log d| < \frac{2u \log x}{N} < \frac{1}{2} \log 2
$$

for x large, so that $D < d < 2D$. It remains to count the number of choices for d in the argument. Since $\#\mathcal{Q}_i > M_i$ when $\kappa_i > 0$, the number of choices for d is at least

$$
\prod_{i:\kappa_i>0} \binom{\lceil M_i \rceil}{\kappa_i} \ge \prod_{i:\kappa_i>0} \left(\frac{M_i}{\kappa_i} \right)^{\kappa_i} = \prod_i \left(\frac{x^{i/N}}{i^2 \kappa_i} \right)^{\kappa_i} > \frac{D}{\prod_i (i^2 \kappa_i)^{\kappa_i}}.
$$

Now, by (10.8),

$$
\prod_{i:\kappa_i>0} i^{2\kappa_i} < N^{2 \sum_i \kappa_i} < N^{4u}
$$

and

$$\prod_{i:\kappa_i>0} \kappa_i^{\kappa_i} < \left(\sum_i \kappa_i\right)^{\sum_i \kappa_i} < (2u)^{2u}.$$

Thus, the number of choices for d exceeds $D/(2uN^2)^{2u}$ and it remains to note that

$$(2uN^2)^{2u} < (\log x)^{5u} \le (\log D)^{5u}$$

for x large. This completes the proof of 10.1.

11. The distribution of primes in residue classes

For a positive integer 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 Λ is von Mangoldt's function.

For fixed q and a coprime to q, we have the asymptotic relations

$$\pi(x, q, a) \sim \frac{\mathrm{li}(x)}{\varphi(q)}, \quad \psi(x, q, a) \sim \frac{x}{\varphi(q)}$$

as $x \to \infty$, where error estimates may be explicitly calculated. In fact the same remains true if q is allowed to tend to infinity slowly with x, say $q < (\log x)^{2-\epsilon}$ for fixed $\epsilon > 0$. For $q > (\log x)^2$ we have either inequalities or ineffective asymptotic estimates. In this section we record some effective inequalities for $\pi(x, q, a)$ that are valid in large ranges for q.

Lemma 11.1 (Brun–Titchmarsh inequality). *If $x > q$, then*

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

The lemma in this form is due to Montgomery and Vaughan [27]. 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, but with a somewhat weaker error estimate, can be found in Timofeev [30, Theorem 2].

Lemma 11.2 (effective Bombieri–Vinogradov inequality). *There are absolute, effectively computable positive numbers c_6, c_7 such that for all real $x \ge 3$, there is an integer $s(x) \in [(\log x)^{1/2}, \exp((\log x)^{1/2})]$ such that for each real $Q \in [x^{1/3} \log x, x^{1/2}]$,*

$$\sum_{\substack{q \le Q \\ s(x) \nmid q}} \max_{2 \le y \le x} \max_{\gcd(a,q)=1} \left| \psi(y, q, a) - \frac{y}{\varphi(q)} \right| \le c_6 x^{1/2} Q(\log x)^5 + c_6 x \exp(-c_7(\log x)^{1/2}).$$

Proof. We follow Vaughan's proof of Bombieri's theorem (see Davenport [15, Chapter 28]). There is an effectively computable positive number c_8 such that for any number $X > 2$, there is at most one integer $s_1 \leq X$ for which there is a primitive (real) character χ_1 with modulus s_1, and for which the L-function $L(z, \chi_1)$ has a real zero $\beta_1 > 1 - c_8/\log X$. Further, if s_1 exists, it is at least $\log X$. If s_1 exists for $X = \exp((\log x)^{1/2})$, we let $s(x) = s_1$ and if s_1 does not exist, we let $s(x) = \lfloor \exp((\log x)^{1/2}) \rfloor$. Thus, $s(x)$ is an integer in the interval $((\log x)^{1/2}, \exp((\log x)^{1/2})]$.

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 $q \leq \exp((\log x)^{1/2})$, q not divisible by $s(x)$, and $2 \leq y \leq x$. Any real zero of the L-function $L(z, \chi)$ must be at most $1 - c_8/(\log x)^{1/2}$. We have

$$|\psi(y, \chi) - \delta(\chi)y| = O\big(y^{1-c_8/(\log x)^{1/2}} + y^{1-c_9/(\log y)^{1/2}}\big),$$

where c_9 is positive and effectively computable. Indeed, this follows from the prime number theorem if χ is principal, and otherwise it is [15, Chapter 20, (8)]. Thus, uniformly for $q \leq \exp((\log x)^{1/2})$ with q not divisible by $s(x)$, if χ has modulus q, then

(11.3) $$\max_{2 \leq y \leq x} |\psi(y, \chi) - \delta(\chi)y| = O\big(x \exp(-c_{10}(\log x)^{1/2})\big),$$

where $c_{10} = \min\{c_8, c_9\}$.

Consider the elementary identity

$$\psi(y, q, a) - \frac{y}{\varphi(q)} = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \bar{\chi}(a)(\psi(y, \chi) - \delta(\chi)y),$$

so that

$$E(x, q) := \max_{2 \leq y \leq x} \max_{\gcd(a,q)=1} \left| \psi(y, q, a) - \frac{y}{\varphi(q)} \right|$$
$$\leq \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \max_{2 \leq y \leq x} |\psi(y, \chi) - \delta(\chi)y|.$$

Let χ_1 be the primitive character that induces $\chi \bmod q$. Then for $q \leq x$,

$$|\psi(y, \chi) - \psi(y, \chi_1)| \leq \sum_{\substack{m \leq y \\ \gcd(m,q)>1}} \Lambda(m) \leq (\log y) \sum_{\substack{p|q \\ p \text{ prime}}} 1 = O((\log x)^2).$$

Thus,

$$E(x, q) = O\left((\log x)^2 + \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \max_{2 \leq y \leq x} |\psi(y, \chi_1) - \delta(\chi_1)y|\right).$$

With $*$ indicating a sum over primitive characters, we have for any real number Q with $2 \leq Q \leq x$,

$$\sum_{q \leq Q} \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \max_{2 \leq y \leq x} |\psi(y, \chi_1) - \delta(\chi_1)y|$$

$$= \sum_{q_1 \leq Q} \sum_{\chi_1 \bmod q_1}^* \max_{2 \leq y \leq x} |\psi(y, \chi_1) - \delta(\chi_1)y| \sum_{k \leq Q/q_1} \frac{1}{\varphi(kq_1)}$$

$$= O\left((\log Q) \sum_{q_1 \leq Q} \frac{1}{\varphi(q_1)} \sum_{\chi_1 \bmod q_1}^* \max_{2 \leq y \leq x} |\psi(y, \chi_1) - \delta(\chi_1)y| \right).$$

For the last step, we have used $\varphi(kq_1) \geq \varphi(k)\varphi(q_1)$ and the estimate

$$(11.4) \qquad \sum_{k \leq Q} \frac{1}{\varphi(k)} = \sum_{k \leq Q} \frac{1}{k} \sum_{\substack{u|k \\ u \text{ squarefree}}} \frac{1}{\varphi(u)} = \sum_{\substack{u \leq Q \\ u \text{ squarefree}}} \frac{1}{\varphi(u)} \sum_{ul \leq Q} \frac{1}{ul}$$

$$= O\left(\sum_{l \leq Q} \frac{1}{l} \right) = O(\log Q).$$

Dropping the subscripts on χ and q, we thus have uniformly and effectively for real numbers Q with $2 \leq Q \leq x$,

$$(11.5) \quad \sum_{q \leq Q} E(x, q)$$

$$= O\left(Q(\log x)^2 + (\log x) \sum_{q \leq Q} \frac{1}{\varphi(q)} \sum_{\chi \bmod q}^* \max_{2 \leq y \leq x} |\psi(y, \chi) - \delta(\chi)y| \right).$$

Let $c_{11} = \min\{1, c_{10}/2\}$ and let $Q_1 = \exp(c_{11}(\log x)^{1/2})$. We use (11.3) to estimate the double sum in (11.5) where we restrict to those q not divisible by $s(x)$, getting

$$(11.6) \quad \sum_{\substack{q \leq Q_1 \\ s(x) \nmid q}} \frac{1}{\varphi(q)} \sum_{\chi \bmod q}^* \max_{2 \leq y \leq x} |\psi(y, \chi) - \delta(\chi)y| = O\left(x Q_1 \exp(-c_{10}(\log x)^{1/2}) \right)$$

$$= O(x/Q_1).$$

We now state a consequence of Vaughan's inequality (see [15, Chapter 28, (2)]): for $1 \leq Q \leq x$,

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

We apply this for real numbers U with $1 \leq U \leq x/2$, getting

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

By breaking $(Q_1, Q]$ into dyadic intervals $(U, 2U]$ and using the inequality for each one, we obtain

$$\sum_{Q_1 < q \leq Q} \frac{1}{\varphi(q)} \sum_{\chi \bmod q}^{*} \max_{2 \leq y \leq x} |\psi(y, \chi)| = O\left(\left(\frac{x}{Q_1} + x^{5/6} \log x + x^{1/2} Q\right)(\log x)^4\right),$$

where there is no restriction on the divisibility of q by $s(x)$. Note that since $q > 1$ in the sum, any primitive χ modulo q is nonprincipal, so that $\delta(\chi) = 0$. Putting this estimate together with (11.5) and (11.6), we have

$$\sum_{\substack{q \leq Q \\ s(x) \nmid q}} E(x, q) = O\left(x^{1/2} Q(\log x)^5 + x \exp(-c_7 (\log x)^{1/2})\right)$$

for any choice of c_7 with $c_7 < c_{11}$. This completes the proof of 11.2.

Lemma 11.7. *With the same notation and hypotheses as in* 11.2*, we have*

$$\sum_{\substack{q \leq Q \\ s(x) \nmid q}} \max_{\gcd(a,q)=1} \left| \pi(x, q, a) - \frac{\mathrm{li}(x)}{\varphi(q)} \right| \leq c_{12} x^{1/2} Q(\log x)^5 + c_{12} x \exp\left(-c_7 (\log x)^{1/2}\right),$$

where c_7 is as in 11.2*, and c_{12} is an absolute, effectively computable number.*

Proof. First note that one may replace the expressions $\psi(y, q, a)$ in 11.2 with $\theta(y, q, a)$, since

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

Thus, the result follows directly from 11.2 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 11.8 (Deshouillers–Iwaniec). *There are effectively computable positive numbers c_{13}, c_{14} such that for each integer m with $m \geq 3$ there is an effectively computable integer x_m with the following property. For arbitrary real numbers x, Q with $x \geq x_m$ and $x^{1/2} \leq Q \leq x^{1-1/m}$, and for an arbitrary integer a with $0 < |a| < x^{1/m}$, we have*

$$\pi(x, q, a) \leq \frac{(4/3 + c_{13}/m)x}{\varphi(q) \log(x/q)}$$

for almost all integers $q \in [Q, 2Q]$ with $\gcd(q, a) = 1$, the number of exceptions being less than $Q x^{-c_{14}/m}$.

This result was announced in [16], and a sketch of the proof was presented in [17]. No claim of effectivity for c_{13}, c_{14}, x_m was made by the authors, but their methods are effective.

12. Sieved primes

The goal of this section is to prove Theorem 5 from the Introduction. We begin with an elementary lemma, which puts more precision into (11.4).

Lemma 12.1. *Let* $\xi = \zeta(2)\zeta(3)/\zeta(6)$, *where* ζ *is the Riemann zeta-function, and let* $\nu = \sum_u (\gamma - \log u)/(u\varphi(u))$, *where* γ *is the Euler–Mascheroni constant and u runs over squarefree numbers. Then for any real number* $t > 1$,

$$\sum_{d<t} \frac{1}{\varphi(d)} = \xi \log t + \nu + O\left(\frac{\log(2t)}{t}\right).$$

Proof. As in (11.4) and with u running over squarefree numbers,

$$\sum_{d<t} \frac{1}{\varphi(d)} = \sum_{u<t} \frac{1}{u\varphi(u)} \sum_{d<t/u} \frac{1}{d} = \sum_{u<t} \frac{1}{u\varphi(u)} \left(\log\left(\frac{t}{u}\right) + \gamma + O\left(\frac{u}{t}\right)\right)$$

$$= (\log t) \sum_{u<t} \frac{1}{u\varphi(u)} + \sum_{u<t} \frac{\gamma - \log u}{u\varphi(u)} + O\left(\frac{1}{t} \sum_{u<t} \frac{1}{\varphi(u)}\right)$$

$$= (\log t) \prod_{p\ \text{prime}} \left(1 + \frac{1}{p(p-1)}\right) + \sum_{u=1}^{\infty} \frac{\gamma - \log u}{u\varphi(u)} + O\left(\frac{\log(2t)}{t}\right)$$

$$= \xi \log t + \nu + O\left(\frac{\log(2t)}{t}\right).$$

Proof of Theorem 5. We shall prove the contrapositive of Theorem 5. Let x be a positive real number, and suppose we have a set of primes $\mathcal{Q} \subset (1, x^{1/2}]$ with $\sum_{q\in\mathcal{Q}} 1/(q-1) \leq 0.2727$. Let $m > 10^4$ be an integer and let $\beta = 1/m$. Let

$$\mathcal{L} = (x^{1/2-2\beta}, x^{1/2-\beta}) \cap \mathbb{Z}, \quad \mathcal{H} = (x^{1/2+\beta}, x^{1/2+2\beta}) \cap \mathbb{Z}.$$

For a prime $r \leq x$, let $g(r)$ denote the number of factorizations of $r - 1$ as lh, where

- $l \in \mathcal{L}, h \in \mathcal{H}$,
- lh is not divisible by any member of $\mathcal{Q}$,
- l is not divisible by $s(x)$,
- h is not divisible by any prime larger than $x^{1/2}$,

where $s(x)$ is as in 11.2. It is possible that $g(r) = 0$; let N denote the number of primes $r \leq x$ with $g(r) > 0$. Then, in the notation of Theorem 5, we have $R(x, \mathcal{Q}) \geq N$. Our goal is to get a good lower bound for $R(x, \mathcal{Q})$ and so it suffices to do so for N.

From Cauchy's inequality, we obtain

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

Our first task is to get an upper bound for $\sum_{r \leq x} g(r)^2$, and to do this we shall ignore the non-divisibility requirements in the definition of $g(r)$ and use only the relatively simple 11.1. We have, with $[a, b]$ denoting the least common multiple of a, b,

$$\sum_{\text{prime } r \leq x} g(r)^2 \leq \sum_{\text{prime } r \leq x} \sum_{\substack{l_1, l_2 | r-1 \\ l_1, l_2 \in \mathcal{L}}} 1 = \sum_{l_1, l_2 \in \mathcal{L}} \pi(x, [l_1, l_2], 1).$$

By 11.1, we thus have

$$\sum_{\text{prime } r \leq x} g(r)^2 \leq 2x \sum_{l_1, l_2 \in \mathcal{L}} \frac{1}{\varphi([l_1, l_2]) \log(x/[l_1, l_2])}$$

$$\leq \frac{x}{\beta \log x} \sum_{l_1, l_2 \in \mathcal{L}} \frac{1}{\varphi([l_1, l_2])}.$$

We have

$$\sum_{l_1, l_2 \in \mathcal{L}} \frac{1}{\varphi([l_1, l_2])} = \sum_{d < x^{1/2-\beta}} \sum_{\substack{\gcd(l_1, l_2) = d \\ l_1, l_2 \in \mathcal{L}}} \frac{1}{\varphi(l_1 l_2 / d)} \leq \sum_{d < x^{1/2-\beta}} \sum_{a, b < x^{1/2-\beta}/d} \frac{1}{\varphi(abd)}$$

$$\leq \left(\sum_{d < x^{1/2}} \frac{1}{\varphi(d)} \right)^3 \leq (\log x)^3,$$

the last inequality following from 12.1 for all x beyond an absolute bound. We conclude that

$$\sum_{\text{prime } r \leq x} g(r)^2 \leq \beta^{-1} x (\log x)^2.$$

We now turn our attention to the heart of the proof, which is to obtain a reasonable lower bound for $\sum_{r \leq x} g(r)$, and for this we shall use 11.7 and 11.8. Let $\mathcal{L}_1$ denote the set of integers $l \in \mathcal{L}$ not divisible by $s(x)$. To begin, we have

$$\sum_{\text{prime } r \leq x} g(r) \geq \sum_{l \in \mathcal{L}_1} \pi(x, l, 1) - \sum_{l \in \mathcal{L}_1} \pi(x^{1/2+\beta} l + 1, l, 1) - \sum_{\substack{l \in \mathcal{L}_1 \\ q | l \text{ for some } q \in \mathcal{Q}}} \pi(x, l, 1)$$

$$- \sum_{\substack{h \in \mathcal{H} \\ q | h \text{ for some } q \in \mathcal{Q}}} \pi(x, h, 1) - \sum_{\substack{h \in \mathcal{H} \\ q | h \text{ for some prime } q > x^{1/2}}} \pi(x, h, 1)$$

$$= S_1 - S_2 - S_3 - S_4 - S_5, \quad \text{say.}$$

Indeed, S_1 counts the number of pairs l, h where $lh + 1$ is a prime $r \leq x$ and $l \in \mathcal{L}_1$, while S_2 removes from this count those pairs where $h \notin \mathcal{H}$, S_3 removes those pairs where l is divisible by some prime in $\mathcal{Q}$, etc.

For S_1 we use 11.7 and get, for x exceeding some bound depending on m,

$$S_1 = \operatorname{li}(x) \sum_{l \in \mathcal{L}_1} \frac{1}{\varphi(l)} + O\left(\frac{x}{(\log x)^2} \right).$$

By 12.1 and using $s(x) \geq (\log x)^{1/2}$ we have, for x above some bound depending on m,

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

By 11.1,

$$S_2 = O\left(\frac{x^{1/2+\beta}}{\log x} \sum_{l \in \mathcal{L}_1} \frac{l}{\varphi(l)}\right).$$

From an argument like (11.4), one has $\sum_{l \in \mathcal{L}_1} l/\varphi(l) = O(x^{1/2-\beta})$, so $S_2 = O(x/\log x)$.

For S_3 we use 11.7 and get, for x exceeding a bound depending on m,

$$S_3 \leq \mathrm{li}(x) \sum_{q \in \mathcal{Q}} \sum_{l \in \mathcal{L}_1,\, q|l} \frac{1}{\varphi(l)} + O\left(\frac{x}{(\log x)^2}\right)$$

$$\leq \mathrm{li}(x) \sum_{q \in \mathcal{Q}} \frac{1}{q-1} \sum_{qk \in \mathcal{L}} \frac{1}{\varphi(k)} + O\left(\frac{x}{(\log x)^2}\right).$$

By 12.1 we have, for $q \in \mathcal{Q}$,

$$\sum_{qk \in \mathcal{L}} \frac{1}{\varphi(k)} \begin{cases} = \xi\beta \log x + O(q \log(2x) x^{2\beta-1/2}) & \text{for } q < x^{1/2-2\beta}, \\ \leq \xi\beta \log x + \nu + O(q \log(2x) x^{\beta-1/2}) & \text{for } x^{1/2-2\beta} \leq q \leq x^{1/2-\beta}, \\ = 0 & \text{for } q > x^{1/2-\beta}. \end{cases}$$

Thus,

$$S_3 \leq \xi\beta x \sum_{q \in \mathcal{Q}} \frac{1}{q-1} + O\left(\frac{x}{\log x}\right).$$

We estimate S_4 by using 11.8 with "m" chosen as our current m 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 11.8, we use the trivial estimate $\pi(x, h, 1) \leq x/h$. Thus, for x exceeding some bound depending on m,

$$S_4 = \sum_{\substack{h \in \mathcal{H} \\ q|h \text{ for some } q \in \mathcal{Q}}} \pi(x, h, 1)$$

$$\leq (4/3 + O(\beta))x \sum_{\substack{h \in \mathcal{H} \\ q|h \text{ for some } q \in \mathcal{Q}}} \frac{1}{\varphi(h) \log(x/h)} + O\left(\frac{x}{\log x}\right)$$

$$\leq (8/3 + O(\beta))\frac{x}{\log x} \sum_{\substack{h \in \mathcal{H} \\ q|h \text{ for some } q \in \mathcal{Q}}} \frac{1}{\varphi(h)} + O\left(\frac{x}{\log x}\right)$$

$$\leq (8/3 + O(\beta))\frac{x}{\log x} \sum_{q \in \mathcal{Q}} \frac{1}{q-1} \sum_{qm \in \mathcal{H}} \frac{1}{\varphi(m)} + O\left(\frac{x}{\log x}\right)$$

$$= (8/3 + O(\beta))\xi\beta x \sum_{q \in \mathcal{Q}} \frac{1}{q-1} + O\left(\frac{x}{\log x}\right).$$

For S_5 it is sufficient to use 11.1. Note that

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

By Mertens' theorem, the first sum on the right is $O(\beta)$, and by 12.1, the second sum is $O(\beta \log x)$. Thus, the sum $\sum 1/\varphi(h)$ is $O(\beta^2 \log x)$, so that

$$S_5 \le 2x \sum_{\substack{h \in \mathcal{H} \\ q \mid h \text{ for some prime } q > x^{1/2}}} \frac{1}{\varphi(h) \log(x/h)}$$

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

Putting together our estimates for S_1, S_2, S_3, S_4, S_5 we find that for x exceeding some bound depending on m,

$$\sum_{\text{prime } r \le x} g(r) \ge S_1 - S_2 - S_3 - S_4 - S_5$$

$$\ge \xi \beta x \left(1 - (11/3 + O(\beta)) \sum_{q \in \mathcal{Q}} \frac{1}{q-1} \right) + O(\beta^2 x) + O(x/(\log x)^{1/4})$$

$$\ge \xi \beta x \left(1 - (11/3 + O(\beta)) 0.2727 \right) + O(x/(\log x)^{1/4})$$

$$= \xi \beta x (10^{-4} + O(\beta)) + O(x/(\log x)^{1/4}).$$

Thus, there is some absolute, computable, positive integer c_{15} such that if $m = c_{15}$ and $\beta = 1/m$, then

$$\sum_{\text{prime } r \le x} g(r) \ge \xi x/m^2 = \xi x/c_{15}^2$$

for $x \ge X_0$, where X_0 is a computable constant. Using this with our upper bound for $\sum_{r \le x} g(r)^2$ and choosing $\delta = \xi^2/c_{15}^5$, we get $N \ge \delta x/(\log x)^2$. This completes the proof of Theorem 5.

Remarks. By using results of Bombieri–Friedlander–Iwaniec instead of 11.8 and the method of Friedlander [20] instead of Balog, one may not only replace "0.2727" with "1/2" in Theorem 5, but the number of primes r satisfying the condition is of order of magnitude $\pi(x)$. However, these tools involve constants that are not effectively computable. If one is not concerned with effective constants, this stronger form of Theorem 5 would support the conclusion of 2.15 with "46/25" replaced with any fixed number $c > 1$ (and with "c_4" depending on c). It is likely that the work of Baker–Harman would lead to a further (ineffective) improvement. See also [22].

13. The existence of period systems

In this section we prove 2.15. We first show that there are many period pairs for n.

Proposition 13.1. *Let $n > 1$ be an integer, and let w, y be real numbers. Each prime number r satisfies at least one of the following conditions:*

  (i) *the element $(n \bmod r)$ of $\mathbb{F}_r$ is either zero or has multiplicative order at most w;*
 (ii) *the number $r - 1$ has a divisor $m > w$ composed of primes at most y;*
(iii) *there is an integer q with $q > y$ and $q^2 \mid r - 1$;*
(iv) *there is a prime q such that $q > y$ and (r, q) is a period pair for n.*

Proof. If $(n \bmod r)$ does not belong to $\mathbb{F}_r^*$ then (i) holds. Suppose $(n \bmod r) \in \mathbb{F}_r^*$, and let m be the order of $(n \bmod r)$ in $\mathbb{F}_r^*$. Then m divides $r - 1$. If $m \leq w$, then (i) holds, so suppose $m > w$. If m has no prime factor exceeding y, then (ii) holds. Suppose therefore that q is a prime factor of m with $q > y$; then q equals the order of $(n^{m/q} \bmod r)$. If q divides $(r - 1)/m$, then (iii) holds. If q does not divide $(r - 1)/m$, then the element $(n^{(r-1)/q} \bmod r) = (n^{m/q} \bmod r)^{(r-1)/m}$ has order q, and (iv) holds. This proves 13.1.

Let $\rho : \mathbb{R}_{\geq 0} \to \mathbb{R}_{>0}$ denote the Dickman–de Bruijn function. That is, ρ is the continuous solution to the equation $\rho'(u) = -u\rho(u-1)$ for $u > 1$, with the initial condition $\rho(u) = 1$ on $[0, 1]$. From [13] we have

$$(13.2) \qquad \log \rho(u) = -u \cdot \log(u \log u) + O(u) \quad \text{for } u \geq 2.$$

Lemma 13.3. *Let x, u, v be real numbers with $x \geq 20$, $1 \leq v \leq u \leq \sqrt{(\log x) \log \log x}$, and put $y = x^{1/u}$, $w = y^v$. The number of prime numbers $r \leq x$ satisfying* 13.1(ii) *is at most*

$$O\left(u\pi(x)\left(\frac{\rho(v)}{\log(2v)} + \rho(u) \right) \right).$$

Proof. This is Theorem 2 from [28].

Proposition 13.4. *For all sufficiently large integers n, if x is a real number such that $x \geq (\log n)^{1.001}$, then the number of prime numbers $r \leq x$ for which there does not exist a period pair (r, q) for n satisfying*

$$q \text{ is prime}, \quad q > x^{1/(\log \log x)^2}$$

is at most $x/(\log x)^3$.

Proof. By 13.1, it suffices to show that when n is a sufficiently large integer and x is a real number with $x \geq (\log n)^{1.001}$, the number of primes $r \leq x$ satisfying one of 13.1(i)–(iii), with $w = x^{1/\log \log x}$ and $y = x^{1/(\log \log x)^2}$, is at most $x/(\log x)^3$. We prove this by showing that the number of such primes r is $o(x/(\log x)^3)$ as $n \to \infty$.

If the prime r satisfies 13.1(i), then either $r \mid n$ or $r \mid n^m - 1$ for some integer m in $[1, w]$. Since the number of distinct prime divisors of a positive integer k is at most $(\log k)/\log 2$, the number of primes r satisfying 13.1(i) is at most

$$\frac{\log n}{\log 2} + \sum_{m \leq w} m \cdot \frac{\log n}{\log 2} \leq w^2 \cdot \frac{\log n}{\log 2} \leq 2x^{1000/1001 + 2/\log \log x} = o(x/(\log x)^3)$$

as $n \to \infty$.

To estimate the number of primes $r \leq x$ satisfying 13.1(ii) we apply 13.3 with $v = \log \log x$ and $u = v^2$; one finds via (13.2) that as $n \to \infty$, this number is at most

$$x/(\log x)^{(1+o(1)) \log \log \log x} = o(x/(\log x)^3).$$

The number of integers r with $1 < r \leq x$ satisfying 13.1(iii) is clearly at most $\sum_{q>y} x/q^2 < x/(y-1) = o(x/(\log x)^3)$ as $n \to \infty$. This proves 13.4.

Let n be an integer at least 20 and choose real numbers x, u with

$$(13.5) \qquad x \geq (\log n)^{1.001}, \quad u = (\log \log x)^2.$$

For a prime r, let $Q(r) = Q(r, n, x, u)$ denote the set of prime divisors q of $r - 1$ with

$$x^{1/u} < q \leq x^{1/2} \quad \text{and} \quad (r, q) \text{ is a period pair for } n.$$

Further, let $\mathcal{Q} = \mathcal{Q}(n, x, u)$ denote the union of the sets $Q(r)$ over all primes $r \leq x$. Note that each subset $\mathcal{S}$ of $\mathcal{Q}$ corresponds to at least one period system for n with degree $\prod_{q \in \mathcal{S}} q$ and where each pair (r, q) used satisfies $r \leq x, q \leq x^{1/2}$, and q prime.

Proposition 13.6. *For all sufficiently large integers n, and with x, u as in (13.5), we have*

$$\sum_{q \in \mathcal{Q}} \frac{1}{q - 1} > 0.2727.$$

Proof. Let

$\mathcal{A} = \{\text{prime } r \leq x : \text{prime } q \mid r - 1 \text{ implies } q \leq x^{1/2} \text{ and } q \notin \mathcal{Q}\}$,

$\mathcal{B} = \{\text{prime } r \leq x : \text{prime } q \mid r - 1 \text{ implies } q \leq x^{1/u} \text{ or } (r, q) \text{ is not a period pair for } n\}$.

Clearly $\mathcal{A} \subset \mathcal{B}$. We use Theorem 5. Suppose n is so large that Theorem 5 and Proposition 13.4 hold for all $x \geq (\log n)^{1.001}$. Since 13.4 implies that $\#\mathcal{B} \leq x/(\log x)^3$, we have $\#\mathcal{A} \leq x/(\log x)^3$. If we use Theorem 5, the conclusion of 13.6 now follows for sufficiently large x.

Proof of Proposition 2.15. Let n, D be integers with $n \geq 20$ and $D > (\log n)^{46/25}$. Further, let $\alpha = 0.2726$, let $x = D^{(25/46)1.001}$ (so that $(\log n)^{1.001} < x < D^{6/11}$), and let $u = (\log \log x)^2$. Then (13.5) holds. Let $\epsilon = 10^{-4}$ and let $c_4 \geq 20$ be so large that $n \geq c_4$ implies that 13.6 holds,

$$x^{-1/u} < \epsilon, \quad 2 < u < (\log x)^{1/10}, \quad \frac{\alpha}{4u} > \frac{1}{15(\log \log D)^2},$$

and $x \geq x_0(\alpha, \epsilon)$ in 10.1. With $\mathcal{Q}$ as above, we have $\sum_{q \in \mathcal{Q}} 1/q > \sum_{q \in \mathcal{Q}} 1/(q-1) - x^{-1/u} > 0.2727 - \epsilon = \alpha$. We apply 10.1 with the current choices for $\alpha, \epsilon, x, u, \mathcal{Q}$, noting that $1/(2(\alpha - \epsilon)) < 46/25$. Since $(\log D)^{5u} < \exp(5(\log \log D)^3)$, we thus have 2.15 with $c_5 = 15$.

References

[1] Adleman, L. M., Lenstra, H. W., Jr.: Finding irreducible polynomials over finite fields. In: Proc. 18th Annual ACM Symp. on Theory of Computing (STOC) (Berkeley, 1986), ACM, 350–355 (1986)

[2] Agrawal, M., Kayal, N., Saxena, N.: PRIMES is in P. Ann. of Math. **160**, 781–793 (2004) Zbl 1071.11070 MR 2123939

[3] Atiyah, M. F., Macdonald, I. G.: Introduction to Commutative Algebra. Addison-Wesley, Reading, MA (1969) Zbl 0175.03601 MR 0242802

[4] Avanzi, R. M., Mihăilescu, P.: Efficient "quasi"-deterministic primality test improving AKS. http://www.uni-math.gwdg.de/preda/mihailescu-papers/ouraks3.pdf

[5] Balog, A.: $p + a$ without large prime factors. In: Seminar on Number Theory, 1983–1984 (Talence, 1983/1984), exp. 31, Univ. Bordeaux I, Talence, 5 pp. (1984) Zbl 0588.10052 MR 0784077

[6] Bernstein, D. J.: Proving primality in essentially quartic random time. Math. Comp. **76**, 389–403 (2007) Zbl 1144.11085 MR 2261028

[7] Bernstein, D. J.: Fast multiplication and its applications. In: J. P. Buhler and P. Stevenhagen (eds.), Algorithmic Number Theory, MSRI Publ. 44, Cambridge Univ. Press, New York, 325–384 (2008) Zbl 1208.68239 MR 2467550

[8] Bernstein, D. J., Lenstra, H. W., Jr., Pila, J.: Detecting perfect powers by factoring into coprimes. Math. Comp. **76**, 385–388 (2007) Zbl 1110.11038 MR 2261027

[9] Berrizbeitia, P.: Sharpening "PRIMES is in P" for a large family of numbers. Math. Comp. **74**, 2043–2059 (2005) Zbl 1071.11071 MR 2164112

[10] Bleichenbacher, D.: The continuous postage problem. Unpublished manuscript (2003)

[11] Bostan, A., Flajolet, P., Salvy, B., Schost, É.: Fast computation of special resultants. J. Symbolic Comput. **41**, 1–29 (2006) Zbl 1121.13037 MR 2194883

[12] Brent, R. P.: Fast multiple-precision evaluation of elementary functions. J. Assoc. Comput. Mach. **23**, 242–251 (1976) Zbl 0324.65018 MR 0395314

[13] de Bruijn, N. G.: The asymptotic behaviour of a function occurring in the theory of primes. J. Indian Math. Soc. (N.S.) **15**, 25–32 (1951) MR 0043838

[14] Cassels, J. W. S.: An Introduction to the Geometry of Numbers. 2nd ed., Springer, Berlin (1971) Zbl 0209.34401 MR 0306130

[15] Davenport, H.: Multiplicative Number Theory. 2nd ed., Grad. Texts in Math. 74, Springer, New York (1980) Zbl 0453.10002 MR 0606931

[16] Deshouillers, J.-M., Iwaniec, H.: Kloosterman sums and Fourier coefficients of cusp forms. Invent. Math. **70**, 219–288 (1982/83) Zbl 0502.10021 MR 0684172

[17] Deshouillers, J.-M., Iwaniec, H.: On the Brun–Titchmarsh theorem on average. In: Topics in Classical Number Theory (Budapest, 1981), G. Halász (ed.), Vol. I, Colloq. Math. Soc. János Bolyai 34, North-Holland, Amsterdam, 319–333 (1984) Zbl 0548.10026 MR 0781145

[18] Erdős, P.: On the normal number of prime factors of $p - 1$ and some related problems concerning Euler's φ-function. Quart. J. Math. (Oxford Ser.) **6**, 205–213 (1935) Zbl 0012.14905

[19] Farkas, J.: Theorie der einfachen Ungleichungen. J. Reine Angew. Math. **124**, 1–27 (1902) JFM 32.0169.02 MR 1580578

[20] Friedlander, J. B.: Shifted primes without large prime factors. In: Number Theory and Applications, R. A. Mollin (ed.), Kluwer, Dordrecht, 393–401 (1989) Zbl 0686.10030 MR 1123085

[21] von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge Univ. Press, Cambridge (1999) Zbl 0936.11069 MR 1689167

[22] Granville, A., Koukoulopoulis, D., Matomäki, K.: When the sieve works. Duke Math. J. **164**, 1935–1969 (2015) Zbl 1326.11055 MR 3369306

[23] Huxley, M. N.: On the difference between consecutive primes. Invent. Math. **15**, 164–170 (1972) Zbl 0241.10026 MR 0292774

[24] Lang, S.: Algebra. 3rd ed., Springer, New York (2002) Zbl 0984.00001 MR 1878556

[25] Lev, V. F.: The continuous postage stamp problem. J. London Math. Soc. **73**, 625–638 (2006) Zbl 1174.11012 MR 2241970

[26] Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley, Reading, MA (1983) Zbl 0554.12010 MR 0746963

[27] Montgomery, H. L., Vaughan, R. C.: The large sieve. Mathematika **20**, 119–134 (1973) Zbl 0296.10023 MR 0374060

[28] Pomerance, C., Shparlinski, I. E.: Smooth orders and cryptographic applications. In: Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Computer Sci. 2369, Springer, Berlin, 338–348 (2002) Zbl 1058.11059 MR 2041095

[29] Shoup, V.: Fast construction of irreducible polynomials over finite fields. J. Symbolic Comput. **17**, 371–391 (1994) Zbl 0815.11059 MR 1289997

[30] Timofeev, N. M.: The Vinogradov–Bombieri theorem. Mat. Zametki **38**, 801–809, 956 (1985) (in Russian) Zbl 0588.10043 MR 0823418