Czechoslovak Mathematical Journal

Stuart Clary; Jacek Fabrykowski

Arithmetic progressions, prime numbers, and squarefree integers

Czechoslovak Mathematical Journal, Vol. 54 (2004), No. 4, 915–927

Persistent URL: http://dml.cz/dmlcz/127940

Czechoslovak Mathematical Journal, 54 (129) (2004), 915–927

ARITHMETIC PROGRESSIONS, PRIME NUMBERS, AND SQUAREFREE INTEGERS

Stuart Clary, Akron, and Jacek Fabrykowski, Youngstown

(Received January 2, 2002)

Abstract. In this paper we establish the distribution of prime numbers in a given arithmetic progression $p \equiv l \pmod{k}$ for which $ap + b$ is squarefree.

Keywords: primes in arithmetic progressions, squarefree integers, Artin's constant

MSC 2000: 11B25, 11N13, 11N69, 11B05, 11K65, 11N25, 11N37

1. Introduction

This note is our answer to a question of N. S. Mendelsohn [6]: *Are there infinitely many prime numbers* $p \equiv 5 \pmod{6}$ *such that* $p+1$ *is squarefree*? We prove that the answer is "yes" by generalizing a theorem of Mirsky [7] that shows that the relative density of the primes p for which $p + 1$ is squarefree is equal to Artin's constant [9]

$$A = \prod_{q \in \mathbb{P}} \left(1 - \frac{1}{q(q-1)}\right) \approx 0.37395\,58136\,19202\,28805\,47280\,54346, \tag{1}$$

where $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ is the set of prime numbers. Mirsky also determined the relative density of the primes p for which $p + b$ is squarefree, where b is any fixed integer, positive, negative, or zero. If $b \neq 0$, then that density is always a nonzero rational multiple of A, the rational multiplier being constructed from the prime divisors of b, in effect removing a finite number of factors from the product in (1). If $b = 0$, then the relative density is 1, since every prime number is squarefree.

In the theorem in Section 4 below we generalize Mirsky's theorem to the case in which the primes p are constrained to lie in a residue class $p \equiv l \pmod{k}$ relative

to some modulus $k > 0$. We insist that the constants k and l be relatively prime; Dirichlet's theorem on primes in arithmetic progressions then guarantees that we start with an infinite set of primes. At the same time we generalize somewhat further by asking for squarefree integers having the form $ap + b$, $a > 0$, instead of only the simpler form $p + b$. In every case, the relative density is either a rational number or a rational multiple of Artin's constant.

Mirsky's proof requires more knowledge of the distribution of primes than is provided by the standard prime number theorem, since it is necessary to keep track of residue classes. For this the proof uses the prime number theorem for arithmetic progressions, and it uses it with an error term with uniformity in the O-constants. The same theorem suffices for our more general result.

Setting $(k, l, a, b) = (6, 5, 1, 1)$ in our theorem answers Mendelsohn's question. Not only are there infinitely many primes $p \equiv 5 \pmod 6$ such that $p + 1$ is squarefree, but the density of such primes in the set of all primes of the form $6j + 5$ is $4A/5 \approx 0.29916465$.

Except for 2 and 3, all primes are congruent to either 1 or 5 modulo 6, so it is natural to ask the corresponding question for primes of the form $6j + 1$. We shall see that there are infinitely many primes $p \equiv 1 \pmod 6$ such that $p + 1$ is squarefree, and that this time the density of such primes in the set of all primes of the form $6j + 1$ is $6A/5 \approx 0.44874698$. This follows from our theorem upon setting $(k, l, a, b) = (6, 1, 1, 1)$.

As a further illustration of the results contained in our theorem, consider primes in the four residue classes $p = 10j + 1$, $p = 10j + 3$, $p = 10j + 7$, and $p = 10j + 9$. The theorem implies that the following approximate percentages of all primes in those residue classes yield squarefree values for $ap + b$ when $a = 3$, for the first seven positive values of b.

Class	$3p+1$	$3p+2$	$3p+3$	$3p+4$	$3p+5$	$3p+6$	$3p+7$
$p = 10j + 1$	47.24%	75.58%	23.62%	94.47%	47.24%	47.24%	38.71%
$p = 10j + 3$	37.79%	94.47%	23.62%	94.47%	47.24%	37.79%	48.39%
$p = 10j + 7$	47.24%	94.47%	23.62%	75.58%	47.24%	47.24%	48.39%
$p = 10j + 9$	47.24%	94.47%	18.89%	94.47%	47.24%	47.24%	48.39%

Thus, for example, approximately 38.71% of all primes of the form $p = 10j + 1$ yield squarefree values for $3p + 7$. In terms of Artin's constant A, the exact value in that case is $4032A/3895$.

The subject matter of this paper can be regarded as combining two lines of investigation. One line is that premier problem in analytic number theory, the distribution of primes in arithmetic progressions, a subject in which the first successes were achieved by Dirichlet. The other line is the problem of the distribution of squarefree

numbers in arithmetic progressions, a subject that goes back to Landau [5, §174], and to which Prachar [8] and others have made significant contributions.

2. Heuristics

From a heuristic point of view it is not surprising that the "probability" that $p+1$ is squarefree for primes of the form $p = 6j+5$ is $2/3$ times the corresponding probability for primes of the form $p = 6j+1$. For a large prime $p = 6j+1$, $p+1$ is not divisible by 3, so there is no chance that the prime 3 can prevent $p+1$ from being squarefree. On the other hand, for a large prime $p = 6j+5$, $p+1$ is sure to be divisible by 3, and it has a $1/3$ chance of being divisible by a second 3 and thus not being squarefree, but there is a $2/3$ chance that that second 3 does not hit. Since the other primes affect primes p of the forms $6j+5$ and $6j+1$ equally, the probability that $p+1$ is squarefree is $2/3$ as great for primes of the form $6j+5$ as for primes of the form $6j+1$.

Similar non-rigorous reasoning explains why the $p+1$ case of Mirsky's theorem should involve Artin's constant. We want to determine the probability that $p+1$ is squarefree, given that p is prime. Let p be a large prime, and let q be any prime that is much smaller than $\sqrt{p}$. Under that assumption, it is reasonable to assume that p is uniformly randomly distributed among the residue classes modulo q^2, except that, being itself a prime, p cannot be in any of the q residue classes modulo q^2 that contain numbers divisible by q. Thus there are $q^2-q = q(q-1)$ residue classes modulo q^2 that could contain p. For only one of these is $p+1$ divisible by q^2. Thus the probability that $p+1$ is not divisible by q^2 is $1-1/(q(q-1))$, and the probability that $p+1$ is squarefree is the product of that quantity over all primes q under consideration. As $p \to \infty$, that becomes the product of $1-1/(q(q-1))$ over all primes, which is Artin's constant as given in (1). Mirsky's theorem shows that this heuristic conclusion is actually correct.

The same kind of heuristic reasoning, though with many cases to be considered, is what led us to the formula given in our theorem in Section 4. Since it is long and based on the same ideas as those above, we omit that reasoning here.

3. Notation conventions

Except for x and y, which always denote positive real numbers, the lower case Latin letters always denote integers. If a letter is restricted to representing positive integers (as is usual for d, for instance), that will always be indicated in the notation or mentioned in the course of a computation. The letters p and q will always denote primes, but that too will be made explicit.

We write $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ for the set of prime numbers, $\log x$ for the natural logarithm, $\log^B x$ for $(\log x)^B$, and $\mathrm{li}(x)$ for the logarithmic integral. For our purposes it does not matter what lower limit of integration is used in the definition of $\mathrm{li}(x)$, and we choose

$$\mathrm{li}(x) = \int_2^x \frac{\mathrm{d}\xi}{\log \xi}.$$

For integers k and l with $k > 0$, we write $\pi(x; k, l)$ for the number of primes p less than or equal to x that satisfy the congruence $p \equiv l \pmod{k}$.

Also, $\varphi(n)$ is the Euler totient function, $\mu(n)$ is the Möbius function, (u, v) is the greatest common divisor function, and $[u, v]$ is the least common multiple function. We usually write $u \perp v$ rather than $(u, v) = 1$ to indicate that u and v are relatively prime [3, p. 115], putting the emphasis on the relation rather than on the function.

Even when b is negative, the quantity $ap + b$ that appears in our theorem can be negative only a finite number of times. The asymptotic estimate of how many times $ap + b$ is squarefree is not affected by those finitely many negative values, so it does not matter whether we restrict the term "squarefree" to apply only to positive numbers. We follow Landau [5, p. 567] in this matter, defining a squarefree number as a *positive* integer not divisible by the square of any prime.

Both the statement and the proof of our theorem benefit from the use of an abbreviation for what is, in effect, the world's most general characteristic function. We adopt the "bracket" version of Iverson's notation [3, pp. 24–25] for this, writing $[\mathcal{B}]$, where $\mathcal{B}$ is any Boolean-valued expression in any set of variables, to mean 1 if $\mathcal{B}$ is true and 0 if $\mathcal{B}$ is false.

4. The Theorem

In the proof of our theorem below we use the prime number theorem for arithmetic progressions in the form [2, Theorem 8.8] that states that for any constant $H > 1$ we have

$$\pi(x; k, l) = \frac{1}{\varphi(k)} \mathrm{li}(x) + O\left(\frac{x}{\log^H x}\right) \quad \text{as } x \to \infty \tag{2}$$

whenever $l \perp k$. This estimate is uniform for $0 < k < \log^H x$, which is sufficient for our needs since we hold k, l, a, and b constant.

In order not to clutter the proof of our theorem inordinately, we find it convenient to preface the theorem with the following lemma, which may be of some small interest in its own right.

Lemma. *Let k, c and a be positive integers and let l and b be integers. Then the system*

$$\begin{aligned} u &\equiv l \pmod{k}, \\ au + b &\equiv 0 \pmod{c} \end{aligned} \tag{3}$$

of congruences in the unknown u has a solution if and only if

$$(ak, c) \mid al + b. \tag{4}$$

If (4) *is satisfied, then the set of all integers u satisfying the system* (3) *coincides with one of the residue classes modulo $h = kc/(ak, c) = [k, c/(a, c)]$. Furthermore, if* (4) *is satisfied and $l \perp k$, then the members of that residue class are relatively prime to the modulus h if and only if*

$$(a, c) = (b, c). \tag{5}$$

P r o o f. The calculation

$$\begin{aligned} [k, c/(a, c)] &= \frac{k \cdot c/(a, c)}{(k, c/(a, c))} \\ &= kc/(k(a, c), c) \\ &= kc/((ka, kc), c) \\ &= kc/(ka, (kc, c)) \\ &= kc/(ak, c) \end{aligned}$$

shows that the two expressions for the modulus h are equal.

Now assume that the system has a solution, and call one solution $u = kv + l$. It then follows that $a(kv+l)+b \equiv 0 \pmod{c}$, so $al+b \equiv -(ak)v \pmod{c}$, that is, $al+b$ is an integer linear combination of ak and c. But being such a linear combination is equivalent to being a multiple of (ak, c).

Reversing the reasoning proves the converse. Assume that $al + b$ is a multiple of (ak, c). It is therefore an integer linear combination of ak and c, say $al + b = -v(ak) + wc$, from which $a(kv + l) + b \equiv 0 \pmod{c}$ follows. Letting $u = kv + l$, we have both $u \equiv l \pmod{k}$ and $au + b \equiv 0 \pmod{c}$, as required.

Next, assume that $(ak, c)|al + b$. We need to show that the set of solutions of the system is one of the residue classes modulo h.

Let u_1 and u_2 be two solutions of the system, say $u_1 = kv_1+l$ and $u_2 = kv_2+l$. We have $a(kv_1+l)+b \equiv 0 \pmod{c}$ and $a(kv_2+l)+b \equiv 0 \pmod{c}$, so $a(kv_1+l) \equiv a(kv_2+l)$

(mod c), that is, $ak(v_1 - v_2) \equiv 0 \pmod{c}$. Dividing through by (ak, c), we obtain $ak(ak, c)^{-1}(v_1 - v_2) \equiv 0 \pmod{c/(ak, c)}$. The factor $ak/(ak, c)$ can now be cancelled because it is relatively prime to the modulus $c/(ak, c)$, and we conclude that v_1 and v_2 are congruent modulo $c/(ak, c)$, from which it follows that u_1 and u_2 are congruent modulo $kc/(ak, c)$. Thus all solutions to the system of congruences are in the same residue class modulo $kc/(ak, c)$, which is h. It is even easier to see that if u_1 is a solution of the system and u_2 is in the same residue class modulo h, then u_2 is also a solution of the system. Thus the set of all solutions coincides with one of the residue classes modulo h, as claimed.

All that remains is to prove the condition for relative primality. Assuming that an integer u satisfying the system (3) exists and that $l \perp k$, we must show that $u \perp h$ if and only if $(a, c) = (b, c)$. We will prove a stronger statement, namely, that $(u, h) = (b, c)/(a, c)$.

Since $l \perp k$ and $u \equiv l \pmod{k}$, we have $u \perp k$. Next, writing the congruence $au + b \equiv 0 \pmod{c}$ in the form $a(a, c)^{-1}u + b(a, c)^{-1} \equiv 0 \pmod{c/(a, c)}$ makes the coefficient $a/(a, c)$ relatively prime to the modulus $c/(a, c)$, so there exists an integer z that is also relatively prime to $c/(a, c)$ and that is a multiplicative inverse of $a/(a, c)$ modulo $c/(a, c)$. Multiplying by z shows that $u \equiv -bz/(a, c) \pmod{c/(a, c)}$. With those remarks in hand, we are now ready for the calculation

$$\begin{aligned}(u, h) &= (u, [k, c/(a, c)]) \\ &= [(u, k), (u, c/(a, c))] \\ &= [1, (u, c/(a, c))] \\ &= (u, c/(a, c)) \\ &= (bz/(a, c), c/(a, c)) \\ &= (b/(a, c), c/(a, c)) \\ &= (b, c)/(a, c),\end{aligned}$$

where in the second step we have used the theorem that greatest common divisor and least common multiple are distributive with respect to each other.

That completes the proof of the lemma. □

Theorem. *Let k, l, a and b be integers with $l \perp k$, $k > 0$, and $a > 0$. Let $\mathcal{S} = \mathcal{S}_{k,l,a,b} = \{p \in \mathbb{P}\colon\ p \equiv l \pmod{k}$ and $ap + b$ is positive and squarefree$\}$, and let $S(x) = S_{k,l,a,b}(x)$ be the number of elements of $\mathcal{S}$ that are less than or equal to x. Then for any constant $B > 1$ we have*

$$S(x) = K \operatorname{li}(x) + O(x/\log^B x) \quad \text{as } x \to \infty, \tag{6}$$

where the constant K is

$$K = K_{k,l,a,b} = \frac{1}{\varphi(k)} \prod_{q \in \mathbb{P}} \left(1 - \frac{\kappa_q}{q(q-1)}\right), \tag{7}$$

where $\kappa_q = \kappa_q(k,l,a,b)$ is defined for prime q by

$$\kappa_q = \begin{cases} [q \nmid b] & \text{if } q \nmid ka, \\ (q-1)[q \mid al+b] & \text{if } q \parallel k \text{ and } q \nmid a, \\ q[q \parallel b] & \text{if } q \nmid k \text{ and } q \parallel a, \\ q(q-1)[q^2 \mid al+b] & \text{if } q^2 \mid ka. \end{cases} \tag{8}$$

Remark. The infinite product for K is convergent, so K is finite in all cases, and is zero if and only if there is a zero factor in the infinite product. If $K \neq 0$, then $\mathcal{S}$ is an infinite set. If $K = 0$, then $\mathcal{S}$ has at most one element. There are two ways that $K = 0$ can happen, either by having $(ka, al+b)$ not squarefree, in which case $\mathcal{S} = \emptyset$, or by having k odd and $a \equiv b \equiv 2 \pmod 4$, in which case either $\mathcal{S} = \emptyset$ or $\mathcal{S} = \{2\}$.

P r o o f. Throughout this proof it is to be understood that the letters p and q denote primes, that d denotes a positive integer, and that x and y are large real numbers.

The proof proceeds in five steps.

We begin by letting γ denote the characteristic function of the (positive) squarefree integers,

$$\gamma(n) = \begin{cases} 1 & \text{if } n \text{ is squarefree,} \\ 0 & \text{otherwise,} \end{cases}$$

where all integers n are considered, not only the positive integers. For positive values of n, $\gamma(n)$ can be expressed in terms of the Möbius function μ by the formula

$$\gamma(n) = \sum_{d^2 \mid n} \mu(d),$$

and we have $\gamma(n) = 0$ when $n \leqslant 0$. Putting these together, we have

$$\gamma(n) = \sum_{d} \mu(d)[d^2 \mid n > 0], \tag{9}$$

where $d^2 \mid n > 0$ means that we have both the relations $d^2 \mid n$ and $n > 0$. We now use (9) and an interchange of order of summation to calculate

$$\begin{aligned} S(x) &= \sum_{p \leqslant x} [p \in \mathcal{S}] \\ &= \sum_{p \leqslant x} [p \equiv l \pmod{k}] \gamma(ap+b) \\ &= \sum_{p \leqslant x} [p \equiv l \pmod{k}] \sum_d \mu(d) [d^2 \mid ap+b > 0] \\ &= \sum_d \mu(d) \sum_{p \leqslant x} [p \equiv l \pmod{k}] [d^2 \mid ap+b > 0] \\ &= \sum_d \mu(d) \sum_{p \leqslant x} [p \equiv l \pmod{k}] [d^2 \mid ap+b] [ap+b > 0]. \end{aligned}$$

Therefore

$$S(x) = \sum_d \mu(d) P(x,d), \tag{10}$$

where $P(x,d) = P_{k,l,a,b}(x,d)$ counts the number of primes $p \leqslant x$ that satisfy the two congruences $p \equiv l \pmod{k}$ and $ap+b \equiv 0 \pmod{d^2}$ and also the condition $ap+b > 0$.

Motivated by the lemma (with d^2 in place of c), we begin the second step of the proof by defining three functions $M(d) = M_{k,l,a,b}(d)$, $D(d) = D_{k,l,a,b}(d)$, and $E(d) = E_{k,l,a,b}(d)$ as follows:

$$M(d) = kd^2/(ak, d^2), \tag{11}$$

$$D(d) = \varphi(kd^2/(ak, d^2)), \tag{12}$$

$$E(d) = [(ak, d^2) | al+b][(a, d^2) = (b, d^2)]. \tag{13}$$

(The *modulus* is $M(d)$, $\mathrm{li}(x)$ gets *divided* by $D(d)$, and $E(d)$ checks for *existence*.) According to the lemma, if $E(d) = 1$, then the system of congruences $p \equiv l \pmod{k}$ and $ap+b \equiv 0 \pmod{d^2}$ involved in the definition of $P(x,d)$ has solutions, and the set of all of those solutions coincides with one of the $D(d)$ residue classes modulo $M(d)$ that are relatively prime to $M(d)$. Therefore the prime number theorem for arithmetic progressions, equation (2), implies that

$$P(x,d) = \frac{1}{D(d)} \mathrm{li}(x) + O(x/\log^H x),$$

uniformly in d, where H is any constant greater than 1. (We will eventually choose $H = 2B$.) On the other hand, if $E(d) = 0$, then that system of congruences either

has no solutions or has all of its solutions in a residue class that is not relatively prime to $M(d)$, and therefore

$$0 \leqslant P(x,d) \leqslant 1.$$

In either case we have

$$P(x,d) = \frac{E(d)}{D(d)}\operatorname{li}(x) + O(x/\log^H x) \quad \text{as } x \to \infty, \tag{14}$$

and the constants implicit in the O-symbol are independent of d.

For the third step of the proof, we split $S(x)$ into two parts and estimate each part separately. We write $S(x) = s_1(x,y) + s_2(x,y)$ where

$$s_1(x,y) = \sum_{d \leqslant y} \mu(d) P(x,d)$$

and

$$s_2(x,y) = \sum_{d > y} \mu(d) P(x,d).$$

(We will later choose $y = \log^B x$.)

It is easy to show that $s_2(x,y) = O(x/y)$. Clearly $P(x,d) \leqslant \max((ax+b)/d^2, 0)$, so $P(x,d) = O(x/d^2)$ where the constants implicit in the O-symbol hold uniformly in x and d. Therefore

$$|s_2(x,y)| \leqslant \sum_{d>y} P(x,d) = O\Big(\sum_{d>y} \frac{x}{d^2}\Big) = O(x/y). \tag{15}$$

We next use (14) to approximate $s_1(x,y)$, obtaining

$$\begin{aligned} s_1(x,y) &= \sum_{d \leqslant y} \mu(d) \Big\{ \frac{E(d)}{D(d)}\operatorname{li}(x) + O(x/\log^H x) \Big\} \\ &= \sum_{d \leqslant y} \frac{\mu(d)E(d)}{D(d)}\operatorname{li}(x) + O\Big(\sum_{d \leqslant y} \frac{x}{\log^H x}\Big) \\ &= \sum_{d=1}^{\infty} \frac{\mu(d)E(d)}{D(d)}\operatorname{li}(x) - \sum_{d>y} \frac{\mu(d)E(d)}{D(d)}\operatorname{li}(x) + O(xy/\log^H x) \\ &= K\operatorname{li}(x) + O\Big(\sum_{d>y} \frac{\log\log d}{d^2}\Big)\operatorname{li}(x) + O(xy/\log^H x), \end{aligned} \tag{16}$$

where we have written

$$K = \sum_{d=1}^{\infty} \frac{\mu(d)E(d)}{D(d)} \tag{17}$$

for short, and where we have used the theorem [4, Theorem 328] that $\varphi(d)$ is greater than some positive constant multiple of $d/\log\log d$ to deduce that $D(d)$ is greater than some positive constant multiple of $d^2/\log\log d$. We now use the asymptotic formulas

$$\sum_{d>y} \frac{\log\log d}{d^2} \sim \int_y^{\infty} \frac{\log\log \xi}{\xi^2}\,\mathrm{d}\xi \sim \frac{\log\log y}{y} \quad \text{as } y \to \infty$$

to conclude that

$$\begin{aligned} s_1(x,y) &= K\,\mathrm{li}(x) + O\biggl(\frac{\log\log y}{y}\biggr)\,\mathrm{li}(x) + O(xy/\log^H x) \\ &= K\,\mathrm{li}(x) + O\biggl(\frac{\log\log y}{y}\cdot\frac{x}{\log x}\biggr) + O(xy/\log^H x) \\ &= K\,\mathrm{li}(x) + O(x/y) + O(xy/\log^H x), \end{aligned} \tag{18}$$

as long as $\log\log y = O(\log x)$ as $x \to \infty$.

Combining (15) and (18), we obtain

$$S(x) = K\,\mathrm{li}(x) + O(xy/\log^H x) + O(x/y),$$

assuming that $\log\log y = O(\log x)$. When $y = \log^B x$ and $H = 2B$, this becomes

$$S(x) = K\,\mathrm{li}(x) + O(x/\log^B x) \quad \text{as } x \to \infty. \tag{19}$$

That is the conclusion of our theorem, except that the constant K still needs to be expressed as the infinite product described in the theorem.

For the fourth step of the proof, we show that K can be rewritten in the form

$$K = \frac{1}{\varphi(k)} \prod_q \biggl(1 - \frac{\varphi(k)E(q)}{D(q)}\biggr). \tag{20}$$

We do this by showing that multiplying $\varphi(k)$ times the individual terms of the infinite series for K yields a quantity, namely $\varphi(k)\mu(d)E(d)/D(d)$, that is a multiplicative function of d. To see that this function is multiplicative, consider the three factors $\mu(d)$, $E(d)$, and $D(d)/\varphi(k)$ separately. That $\mu(d)$ is multiplicative is a standard theorem of elementary number theory, and the multiplicativity of $E(d)$ follows easily upon considering each of the factors on the right hand side of (13).

To see that $D(d)/\varphi(k)$ is a multiplicative function of d, we begin with the calculation

$$\begin{aligned} D(d) &= \varphi([k, d^2/(a, d^2)]) \\ &= \varphi(kd^2/(ka, d^2)) \\ &= \varphi(k)\varphi(d^2/(ka, d^2))\frac{(k, d^2/(a, d^2))}{\varphi((k, d^2/(ka, d^2)))}, \end{aligned}$$

where the last step follows from the formula $\varphi(mn) = \varphi(m)\varphi(n)(m, n)/\varphi((m, n))$ (see [1, page 28, Theorem 2.5 (b)]). Therefore we have

$$\frac{D(d)}{\varphi(k)} = \frac{(k, d^2/(a, d^2)) \cdot \varphi(d^2/(ka, d^2))}{\varphi((k, d^2/(ka, d^2)))}.$$

From this representation it is fairly easy to verify that $D(d)/\varphi(k)$ is multiplicative. We begin by noting that, for any fixed integer $t > 0$, the greatest common divisor function $G_t(d) = (t, d)$ is multiplicative in d. It is then a routine calculation to show first that the functions $(k, d^2/(a, d^2))$ and $(k, d^2/(ka, d^2))$ are multiplicative, and then that $\varphi((k, d^2/(a, d^2)))$ and $\varphi((k, d^2/(ka, d^2)))$ are also multiplicative.

Since products and quotients of multiplicative functions are multiplicative, it then follows that the infinite series

$$\varphi(k)K = \sum_{d=1}^{\infty} \frac{\varphi(k)\mu(d)E(d)}{D(d)}$$

has the Euler product representation

$$\begin{aligned} \varphi(k)K &= \prod_q \left(1 + \frac{\varphi(k)\mu(q)E(q)}{D(q)} + \frac{\varphi(k)\mu(q^2)E(q^2)}{D(q^2)} + \dots\right) \\ &= \prod_q \left(1 - \frac{\varphi(k)E(q)}{D(q)}\right). \end{aligned}$$

and that proves (20).

For the fifth and final step of the proof, it remains only to verify the formulas given in the theorem for κ_q when q is prime. We need to show that the quantity

$$q(q-1)\frac{\varphi(k)E(q)}{D(q)} = \frac{\varphi(k)\varphi(q^2)E(q)}{D(q)}$$

is equal to the values claimed for κ_q in all four cases.

In Case I we have $q \nmid ka$, and therefore

$$\begin{aligned}\frac{\varphi(k)\varphi(q^2)E(q)}{D(q)} &= \frac{\varphi(k)\varphi(q^2)[(ak,q^2)|al+b][(a,q^2)=(b,q^2)]}{\varphi(kq^2/(ak,q^2))}\\ &= \frac{\varphi(k)\varphi(q^2)[1 \mid al+b][1=(b,q^2)]}{\varphi(kq^2)}\\ &= \frac{\varphi(k)\varphi(q^2)[q \nmid b]}{\varphi(k)\varphi(q^2)}\\ &= [q \nmid b],\end{aligned}$$

as required.

In Case II we have $q \parallel k$ and $q \nmid a$, and therefore

$$\begin{aligned}\frac{\varphi(k)\varphi(q^2)E(q)}{D(q)} &= \frac{\varphi(k)\varphi(q^2)[(ak,q^2)|al+b][(a,q^2)=(b,q^2)]}{\varphi(kq^2/(ak,q^2))}\\ &= \frac{\varphi(k)\varphi(q^2)[q|al+b][1=(b,q^2)]}{\varphi(kq^2/q)}\\ &= \frac{\varphi((k/q)q)\varphi(q^2)[q|al+b][q \nmid b]}{\varphi((k/q)q^2)}\\ &= \frac{\varphi(k/q)\varphi(q)\varphi(q^2)[q|al+b]}{\varphi(k/q)\varphi(q^2)}\\ &= (q-1)[q|al+b],\end{aligned}$$

as required. We were able to drop the factor $[q \nmid b]$ because $q \nmid b$ is a consequence of $q \mid al+b$. Reason: If we had both $q \mid al+b$ and $q \mid b$, then it would follow that $q \mid al$ and then that $q \mid l$, contradicting the assumption that $l \perp k$.

In Case III we have $q \nmid k$ and $q \parallel a$, and therefore

$$\begin{aligned}\frac{\varphi(k)\varphi(q^2)E(q)}{D(q)} &= \frac{\varphi(k)\varphi(q^2)[(ak,q^2)|al+b][(a,q^2)=(b,q^2)]}{\varphi(kq^2/(ak,q^2))}\\ &= \frac{\varphi(k)\varphi(q^2)[q \mid al+b][q=(b,q^2)]}{\varphi(kq^2/q)}\\ &= \frac{\varphi(k)\varphi(q^2)[q|al+b][q\|b]}{\varphi(kq)}\\ &= \frac{\varphi(k)\varphi(q^2)[q\|b]}{\varphi(k)\varphi(q)}\\ &= q[q\|b],\end{aligned}$$

as required. We were able to drop the factor $[q \mid al+b]$ because $q \mid al+b$ is a consequence of $q \parallel b$.

In Case IV we have $q^2 \mid ka$, and therefore

$$\begin{aligned}\frac{\varphi(k)\varphi(q^2)E(q)}{D(q)} &= \frac{\varphi(k)\varphi(q^2)[(ak,q^2)|al+b][(a,q^2)=(b,q^2)]}{\varphi(kq^2/(ak,q^2))}\\ &= \frac{\varphi(k)\varphi(q^2)[q^2|al+b][(a,q^2)=(b,q^2)]}{\varphi(kq^2/q^2)}\\ &= \frac{\varphi(k)\varphi(q^2)[q^2|al+b]}{\varphi(k)}\\ &= q(q-1)[q^2|al+b],\end{aligned}$$

as required. We were able to drop the factor $[(a,q^2)=(b,q^2)]$ because $(a,q^2)=(b,q^2)$ is a consequence of $q^2 \mid al+b$. Reason: There are only three possible values for (a,q^2), namely, 1, q, and q^2, as covered in the following three cases. In each case we use the hypothesis that $al \equiv -b \pmod{q^2}$.

(a) If $(a,q^2)=1$, then $q \nmid a$, so $q \mid k$, so $q \nmid l$ (since $l \perp k$), so $q \nmid al$, so $q \nmid b$, and therefore $(b,q^2)=1$.

(b) If $(a,q^2)=q$, then $q \parallel a$, so $q \mid k$, so $q \nmid l$ (since $l \perp k$), so $q \parallel al$, so $q \parallel b$, and therefore $(b,q^2)=q$.

(c) If $(a,q^2)=q^2$, then $q^2 \mid a$, so $q^2 \mid b$, and therefore $(b,q^2)=q^2$.

That completes the proof of the theorem. □

References

[1] *Tom M. Apostol*: Introduction to Analytic Number Theory. Springer-Verlag, 1976.

[2] *William Ellison and Fern Ellison*: Prime Numbers. John Wiley & Sons, 1985.

[3] *Ronald L. Graham, Donald E. Knuth and Oren Patashnik*: Concrete Mathematics: A Foundation for Computer Science. Addison-Wesley, second edition, 1994.

[4] *G. H. Hardy and E. M. Wright*: An Introduction to the Theory of Numbers. Oxford at the Clarendon Press, fourth edition, 1960.

[5] *Edmund Landau and Paul T. Bateman*: Handbuch der Lehre von der Verteilung der Primzahlen. Chelsea, New York, second edition, 1974; Two volumes combined as one.

[6] *N. S. Mendelsohn*: Private communication to Jacek Fabrykowski. 1989.

[7] *L. Mirsky*: The number of representations of an integer as the sum of a prime and a k-free integer. Amer. Math. Monthly *56* (1949), 17–19.

[8] *Karl Prachar*: Über die kleinste quadratfrei Zahl einer arithmetischen Reihe. Monatsh. Math. *3* (1958), 173–176.

[9] *John W. Wrench, Jr.*: Evaluation of Artin's constant and the twin-prime constant. Math. Comp. *15* (1961), 396–398.

Authors' addresses: S. Clary, The University of Akron, Akron, Ohio, U.S.A., e-mail: clary@uakron.edu; J. Fabrykowski, Youngstown State University, Youngstown, Ohio, U.S.A., e-mail: jfabryk@math.ysu.edu.