



Euler's Function in Residue Classes

THOMAS DENCE

tdence@ashland.edu

Department of Mathematics, Ashland University, Ashland, OH 44805

CARL POMERANCE,

carl@ada.math.uga.edu

Department of Mathematics, University of Georgia, Athens, GA 30602

Dedicated to the memory of Paul Erdős

Received June 28, 1996; Accepted October 16, 1996

Abstract. We discuss the distribution of integers n with $\varphi(n)$ in a particular residue class, showing that if a residue class contains a multiple of 4, then it must contain infinitely many numbers $\varphi(n)$. We get asymptotic formulae for the distribution of $\varphi(n)$ in the various residue classes modulo 12.

Key words:

1991 Mathematics Subject Classification:

1. Introduction

Let φ denote Euler's arithmetic function, which counts the number of positive integers up to n that are coprime to n . Given a residue class $r \pmod{m}$ must there be infinitely values of $\varphi(n)$ in this residue class? Let $N(x, m, r)$ denote the number of integers $n \leq x$ with $\varphi(n) \equiv r \pmod{m}$. If there are infinitely many Euler values in the residue class $r \pmod{m}$, can we find an asymptotic formula for $N(x, m, r)$ as $x \rightarrow \infty$? It is to these questions that we address this paper.

Since $\varphi(n)$ is even for each integer $n > 2$, we immediately see that if the residue class $r \pmod{m}$ does not contain any even numbers, then it cannot contain infinitely many values of $\varphi(n)$. Is this the only situation where we cannot find infinitely many Euler values? We conjecture that this is the case.

Conjecture. *If the residue class $r \pmod{m}$ contains an even number then it contains infinitely many numbers $\varphi(n)$.*

This conjecture is a consequence of Dirichlet's theorem on primes in arithmetic progressions and the following elementary assertion: *If the residue class $r \pmod{m}$ contains an even number, then there are integers a, k with $k \geq 0$ and $(a, m) = 1$ such that $a^k(a-1) \equiv r \pmod{m}$.* We have not been able to prove or disprove this assertion, though we conjecture it is true.

We can prove the following result.

Theorem 1.1. *If the residue class $r \pmod m$ contains a multiple of 4 then it contains infinitely many numbers $\varphi(n)$.*

The proof is an elementary application of Dirichlet's theorem on primes in an arithmetic progression, and is inspired by an argument in a paper of Narkiewicz [6].

One relevant result from [6] is that if m is coprime to 6 and r is coprime to m , then there are infinitely many Euler values in the residue class $r \pmod m$. In particular, it is shown that asymptotically $1/\varphi(m)$ of the integers n with $\varphi(n)$ coprime to m have $\varphi(n) \equiv r \pmod m$. From this it is a short step to get an asymptotic formula for $N(x, m, r)$ for such pairs m, r .

In fact, for any specific pair m, r it seems possible to decide if $N(x, m, r)$ is unbounded and to obtain an asymptotic formula in case it is. We shall illustrate the kinds of methods one might use for such a project in the specific case $m = 12$.

We only have to consider the even residue classes mod 12. By Dirichlet's theorem we immediately see that the residue classes 0, 4, 6, 10 mod 12 each contain infinitely many φ -values, since there are infinitely many primes in each of the residue classes 1, 5, 7, 11 mod 12. This leaves $r = 2$ and 8. If p is an odd prime $\equiv 2 \pmod 3$, then $\varphi(4p) \equiv 8 \pmod{12}$, so 8 mod 12 contains infinitely many φ -values. As noticed in [3], the residue class 2 mod 12 is tougher for φ to occupy. But if $p \equiv 11 \pmod{12}$ and p is prime, then $\varphi(p^2) \equiv 2 \pmod{12}$, so occupied it is.

Now we turn to estimating $N(x, 12, r)$ for r even. We begin with examining the numerical data in Table 1. Perhaps the most striking feature of Table 1 is the paucity of integers n with $\varphi(n) \equiv 2 \pmod{12}$. This behavior was already noticed in [3], and it was shown there that the set of such integers has asymptotic density 0. Another observation that one might make is that the numbers for the 0 residue class keep growing as a percentage of the whole, from 30% at 100 to over 73% at 10^7 . Though their contribution decreases as a percentage of the whole, the columns for 4 and 8 grow briskly, and seem to keep in approximately the same ratio. And the columns for 6 and 10 seem to be about equal. Can anything be proved concerning these observations? We prove the following theorem.

Theorem 1.2. *We have, as $x \rightarrow \infty$,*

$$N(x, 12, 0) \sim x, \tag{1.1}$$

Table 1. The number of $n \leq x$ with $\varphi(n)$ in a particular residue class modulo 12.

x	0	2	4	6	8	10
10^2	30	3	21	17	18	9
10^3	511	6	185	84	145	67
10^4	6114	13	1651	511	1233	476
10^5	66646	32	15125	3761	10743	3691
10^6	703339	81	140155	30190	96165	30068
10^7	7300815	208	1313834	253628	878141	253372

$$N(x, 12, 2) \sim \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \frac{\sqrt{x}}{\log x}, \quad (1.2)$$

$$N(x, 12, 4) \sim c_1 \frac{x}{\sqrt{\log x}}, \quad (1.3)$$

$$N(x, 12, 6) \sim \frac{3}{8} \frac{x}{\log x}, \quad (1.4)$$

$$N(x, 12, 8) \sim c_2 \frac{x}{\sqrt{\log x}}, \quad (1.5)$$

$$N(x, 12, 10) \sim \frac{3}{8} \frac{x}{\log x}, \quad (1.6)$$

where $c_1 \doteq .6109136202$ is given by

$$c_1 = \frac{\sqrt{2\sqrt{3}}}{3\pi} c_3^{-1/2} (2c_3 + c_4), \quad (1.7)$$

with

$$c_3 = \prod_{\substack{p \text{ prime} \\ p \equiv 2(3)}} \left(1 + \frac{1}{p^2 - 1}\right), \quad c_4 = \prod_{\substack{p \text{ prime} \\ p \equiv 2(3)}} \left(1 - \frac{1}{(p + 1)^2}\right), \quad (1.8)$$

and $c_2 \doteq .3284176245$ is given by the same expression as for c_1 , except that $2c_3 + c_4$ is replaced by $2c_3 - c_4$.

The case of $0 \pmod{12}$ follows from a more general result of Erdős.

Theorem (Erdős). *For any positive integer m , $N(x, m, 0) \sim x$ as $x \rightarrow \infty$.*

We have not been able to find the first place this result appears but the proof follows from the fact that the sum of the reciprocals of the primes $p \equiv 1 \pmod{m}$ is infinite, so that almost all integers n are divisible by such a prime. But if such a prime p divides n , then $\varphi(n) \equiv 0 \pmod{m}$.

There is a fairly wide literature on the distribution in residue classes of values of multiplicative functions, in fact there is a monograph on the subject by Narkiewicz [7]. However, but for Narkiewicz's result above, and a result of Delange [2] (which can be used to give an asymptotic formula for the number of n up to x for which $\varphi(n)$ is not divisible by a fixed integer m), the problems considered here appear to be new.

We begin now with the proof of Theorem 1.2, giving the proof of Theorem 1.1 at the end of the paper. In the sequel, the letter p shall always denote a prime.

2. The residue classes 2, 6 and 10 mod 12

Let $\mathcal{S}_{m,r}$ denote the set of integers n with $\varphi(n) \equiv r \pmod{m}$. So $N(x, m, r)$ counts how many members $\mathcal{S}_{m,r}$ has up to x .

We begin by explicitly describing $\mathcal{S}_{12,r}$ for $r = 2, 6$ and 10 . This is easy since these residue classes are contained in the class $2 \pmod{4}$, so that $\mathcal{S}_{12,r} \subset \mathcal{S}_{4,2}$ for $r = 2, 6, 10$. The set $\mathcal{S}_{4,2}$ is particularly simple, consisting of numbers p^k , where p is a prime that is $3 \pmod{4}$, the doubles of these numbers, and the number 4 .

We have,

$$\begin{aligned}\mathcal{S}_{12,2} &= \{3, 4, 6\} \cup \{n : n \text{ or } n/2 = p^{2k} \text{ where } p \equiv 11 \pmod{12}\}, \\ \mathcal{S}_{12,6} &= \{n : n \text{ or } n/2 = p^k \text{ where } p \equiv 7 \pmod{12}, \text{ or } n \text{ or } n/2 = 3^k \text{ where } k \geq 2\}, \\ \mathcal{S}_{12,10} &= \{n : n \text{ or } n/2 = p^{2k+1} \text{ where } p \equiv 11 \pmod{12}\}.\end{aligned}$$

We thus get (1.2), (1.4) and (1.6) of Theorem 1.2 using the prime number theorem for arithmetic progressions. For a reference on this theorem, see [1], Ch. 20.

3. Reduction to the modulus 3

Note that $n > 2$ and $\varphi(n) \equiv 1 \pmod{3}$ if and only if $\varphi(n) \equiv 4$ or $10 \pmod{12}$. Further, $\varphi(n) \equiv 2 \pmod{3}$ if and only if $\varphi(n) \equiv 2$ or $8 \pmod{12}$. In light of (1.2) and (1.6) of Theorem 1.2, it will suffice for (1.3) and (1.5) to show the following theorem.

Theorem 3.1. *As $x \rightarrow \infty$, we have*

$$N(x, 3, 1) \sim c_1 \frac{x}{\sqrt{\log x}}, \quad (3.1)$$

$$N(x, 3, 2) \sim c_2 \frac{x}{\sqrt{\log x}} \quad (3.2)$$

where c_1 and c_2 are given in Theorem 1.2.

Also note that $\varphi(n) \not\equiv 0 \pmod{3}$ if and only if 9 does not divide n and n is not divisible by any prime $p \equiv 1 \pmod{3}$. We begin our proof of Theorem 3.1 by first considering numbers n not divisible by 3 . It is an easy leap from these numbers to the general case.

Let \mathcal{S}_i be the set of integers n not divisible by 3 for which $\varphi(n) \equiv i \pmod{3}$, for $i = 1, 2$. Further, let $N_i(x)$ be the number of members of \mathcal{S}_i up to x , for $i = 1, 2$. Then the following result is immediate.

Lemma 3.2. *For $i = 1, 2$ and $x > 0$ we have*

$$\begin{aligned}N(x, 3, 1) &= N_1(x) + N_2(x/3), \\ N(x, 3, 2) &= N_2(x) + N_1(x/3).\end{aligned}$$

Indeed, using the notation of Section 2, we have $n \in \mathcal{S}_{3,1}$ and $n \leq x$ if and only if $n \in \mathcal{S}_1$, $n \leq x$ or $n = 3m$ where $m \in \mathcal{S}_2$, $m \leq x/3$. We have a similar characterization of the members of $\mathcal{S}_{3,2}$ up to x .

Every natural number n has a unique decomposition as qf where $q = q(n)$ is the largest squarefull divisor of n and $f = f(n) = n/q$ is squarefree. (We say an integer is

squarefull if it is divisible by p^2 whenever it is divisible by p .) For example, for the integer $n = 2200 = 2^3 \cdot 5^2 \cdot 11$, we have $q = q(2200) = 2^3 \cdot 5^2 = 200$ and $f = f(2200) = 11$.

Suppose n is only divisible by primes $\equiv 2 \pmod 3$ and write $n = qf$ as above. Then $\varphi(n) = \varphi(q)\varphi(f)$ and $\varphi(f) \equiv 1 \pmod 3$, so that

$$\varphi(n) \equiv \varphi(q) \pmod 3. \quad (3.3)$$

Let \mathcal{F} denote the set of squarefree integers each of whose prime factors is $2 \pmod 3$. Then $\mathcal{F} \subset \mathcal{S}_1$. Let \mathcal{Q} denote the set of squarefull integers each of whose prime factors is $2 \pmod 3$. From (3.3) we have the following lemma.

Lemma 3.3. *The set \mathcal{S}_1 is the disjoint union of the sets $q\mathcal{F}$ where $q \in \mathcal{S}_1 \cap \mathcal{Q}$. The set \mathcal{S}_2 is the disjoint union of the sets $q\mathcal{F}$ where $q \in \mathcal{S}_2 \cap \mathcal{Q}$.*

Of course, by $q\mathcal{F}$ we mean the set of integers qf where $f \in \mathcal{F}$.

4. A theorem of Landau and some consequences

In [5], Landau gives a more general theorem of which the following is a special case.

Theorem (Landau). *There is a positive constant c such that the number of integers $n \leq x$ divisible only by primes $\equiv 2 \pmod 3$ is $\sim cx/\sqrt{\log x}$ as $x \rightarrow \infty$.*

We shall identify the constant c in Landau's theorem in Section 6.

We now deduce the following consequence of Landau's theorem. Let \mathcal{N} denote the set of integers divisible only by primes $\equiv 2 \pmod 3$. Recall that \mathcal{Q} is the set of squarefull numbers in \mathcal{N} .

Proposition 4.1. *For any subset \mathcal{Q}_0 of \mathcal{Q} , we have*

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ q(n) \in \mathcal{Q}_0}} 1 \sim cc_3^{-1} \frac{x}{\sqrt{\log x}} \sum_{q \in \mathcal{Q}_0} \frac{1}{q} \prod_{p|q} \frac{p}{p+1}$$

as $x \rightarrow \infty$, where c is the constant in Landau's theorem and c_3 is given in (1.8).

Note that in the special case $\mathcal{Q}_0 = \{1\}$, Proposition 4.1 asserts that the number of members of \mathcal{F} up to x is $\sim cc_3^{-1}x/\sqrt{\log x}$ as $x \rightarrow \infty$.

Proof of Proposition 4.1: From Landau's theorem there is a constant c_5 such that for all $x > 1$,

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N}}} 1 \leq c_5 \frac{x}{\sqrt{\log x}}. \quad (4.1)$$

Also, since the number of squarefull numbers $\leq x$ is $O(\sqrt{x})$, it follows that there is a constant c_6 such that for all $x > 1$,

$$\sum_{\substack{q > x \\ q \in \mathcal{Q}}} \frac{1}{q} \leq \frac{c_6}{\sqrt{x}}. \quad (4.2)$$

From (4.1) and (4.2) we deduce the following: For each $\epsilon > 0$, there are numbers N, x_0 such that if $x \geq x_0$, then

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ q(n) > N}} 1 \leq \epsilon \frac{x}{\sqrt{\log x}}. \quad (4.3)$$

Indeed, the sum in (4.3) is

$$\begin{aligned} \sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ N < q(n) \leq \sqrt{x}}} 1 + \sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ q(n) > \sqrt{x}}} 1 &\leq c_5 \sum_{\substack{N < q \leq \sqrt{x} \\ q \in \mathcal{Q}}} \frac{x/q}{\sqrt{\log(x/q)}} + \sum_{\substack{q > \sqrt{x} \\ q \in \mathcal{Q}}} \frac{x}{q} \\ &\leq 2c_5 \sum_{\substack{q > N \\ q \in \mathcal{Q}}} \frac{x/q}{\sqrt{\log x}} + c_6 x^{3/4} \\ &\leq 2c_5 c_6 \frac{x}{\sqrt{N} \sqrt{\log x}} + c_6 x^{3/4}. \end{aligned}$$

Therefore, (4.3) follows by taking N and x sufficiently large.

Next note that for a fixed $d \in \mathcal{N}$, it follows from Landau's theorem that

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ d|n}} 1 \sim c \frac{x/d}{\sqrt{\log(x/d)}} \sim \frac{c}{d} \cdot \frac{x}{\sqrt{\log x}} \quad (4.4)$$

as $x \rightarrow \infty$. Let $P(m)$ denote the largest prime factor of m when $m > 1$ and let $P(1) = 1$. Thus for any positive integer N ,

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ (q(n), N!) = 1}} 1 = \sum_{\substack{m \in \mathcal{N} \\ P(m) \leq N}} \mu(m) \sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ m^2 | n}} 1, \quad (4.5)$$

where μ is the Möbius function. Indeed, $m^2 | n$ if and only if $m^2 | q(n)$, so that $\sum \mu(m)$ for $m^2 | q(n)$, $P(m) \leq N$, is 0 whenever $(q(n), N!) > 1$ and 1 otherwise. Putting (4.4) and (4.5) together, we get that

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ (q(n), N!) = 1}} 1 \sim \frac{cx}{\sqrt{\log x}} \sum_{\substack{m \in \mathcal{N} \\ P(m) \leq N}} \frac{\mu(m)}{m^2} = \frac{cx}{\sqrt{\log x}} \prod_{\substack{p \equiv 2(3) \\ p \leq N}} \left(1 - \frac{1}{p^2}\right) \quad (4.6)$$

as $x \rightarrow \infty$.

We now use (4.3), (4.6) and the convergence of the infinite product $\prod_{p \equiv 2(3)} (1 - 1/p^2)$ (to the limit c_3^{-1}) to see that the proposition holds in the case $\mathcal{Q}_0 = \{1\}$. By a similar argument we can get an asymptotic formula for the number of $n \leq x$ with $n \in \mathcal{N}$, n squarefree and $(n, m) = 1$, where $m \in \mathcal{N}$ is fixed. This involves removing the factors $(1 - 1/p^2)$ from the infinite product corresponding to the primes $p \mid m$ and replacing them with $(1 - 1/p)$. That is, we should introduce the factor $p/(p + 1)$. We have for fixed $m \in \mathcal{N}$,

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ q(n)=1 \\ (n,m)=1}} 1 \sim cc_3^{-1} \frac{x}{\sqrt{\log x}} \prod_{p \mid m} \frac{p}{p+1} \quad (4.7)$$

as $x \rightarrow \infty$.

We are now ready to establish the general case of the proposition. To say that $n \in \mathcal{N}$ and $q(n) = q$ is to say that $n = n_1 q$ where $n_1 \in \mathcal{N}$, n_1 is squarefree and $(n_1, q) = 1$. Thus, from (4.7) we have for a fixed $q \in \mathcal{Q}_0$ that

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ q(n)=q}} 1 \sim cc_3^{-1} \frac{x}{\sqrt{\log x}} \frac{1}{q} \prod_{p \mid q} \frac{p}{p+1}$$

as $x \rightarrow \infty$. Now using (4.3) and the convergence of the sum $\sum_{q \in \mathcal{Q}_0} 1/q$, we get that

$$\sum_{\substack{n \leq x \\ n \in \mathcal{N} \\ q(n) \in \mathcal{Q}_0}} 1 \sim cc_3^{-1} \frac{x}{\sqrt{\log x}} \sum_{q \in \mathcal{Q}_0} \frac{1}{q} \prod_{p \mid q} \frac{p}{p+1}$$

as $x \rightarrow \infty$, which is what we wished to prove. \square

5. The sums S_1 and S_2

We can now get asymptotic estimates for the quantities $N_i(x)$, $i = 1, 2$, that count the number of members of \mathcal{S}_i up to x . Recall that \mathcal{S}_i is the set of integers n not divisible by 3 for which $\varphi(n) \equiv i \pmod{3}$. From Lemma 3.3 and Proposition 4.1 we immediately get that

$$N_i(x) \sim cc_3^{-1} \frac{x}{\sqrt{\log x}} \sum_{q \in \mathcal{S}_i \cap \mathcal{Q}} \frac{1}{q} \prod_{p \mid q} \frac{p}{p+1} \quad (5.1)$$

as $x \rightarrow \infty$ for $i = 1, 2$.

Let

$$S_i = \sum_{q \in \mathcal{S}_i \cap \mathcal{Q}} \frac{1}{q} \prod_{p \mid q} \frac{p}{p+1} \quad (5.2)$$

for $i = 1, 2$. Thus from (1.8), Lemma 3.2, (5.1) and (5.2) we get that as $x \rightarrow \infty$,

$$\begin{aligned} N(x, 3, 1) &\sim cc_3^{-1} \left(S_1 + \frac{1}{3} S_2 \right) \frac{x}{\sqrt{\log x}}, \\ N(x, 3, 2) &\sim cc_3^{-1} \left(S_2 + \frac{1}{3} S_1 \right) \frac{x}{\sqrt{\log x}}. \end{aligned} \quad (5.3)$$

We shall show the following result.

Proposition 5.1. *With c_3, c_4 defined in (1.8), we have*

$$S_1 + \frac{1}{3} S_2 = \frac{2}{3} c_3 + \frac{1}{3} c_4, \quad S_2 + \frac{1}{3} S_1 = \frac{2}{3} c_3 - \frac{1}{3} c_4.$$

Proposition 5.1 serves a numerical purpose, since it is easier to estimate the infinite products c_3, c_4 than the sums S_1, S_2 .

Proof of Proposition 5.1: One can get a simple expression for $S_1 + S_2$. Since $q^{-1} \prod_{p|q} p/(p+1)$ is a multiplicative function of q , we have

$$\begin{aligned} S_1 + S_2 &= \sum_{q \in \mathcal{Q}} \frac{1}{q} \prod_{p|q} \frac{p}{p+1} \\ &= \prod_{p \equiv 2(3)} \left(1 + \frac{p}{p+1} \sum_{a=2}^{\infty} \frac{1}{p^a} \right) \\ &= \prod_{p \equiv 2(3)} \left(1 + \frac{1}{p^2 - 1} \right) = c_3. \end{aligned} \quad (5.4)$$

Let $\omega(m)$ denote the number of distinct prime factors of m and let $\Omega(m)$ denote the number of prime factors of m counted with multiplicity. Then for $q \in \mathcal{Q}$ we have

$$\varphi(q) = q \prod_{p|q} \left(1 - \frac{1}{p} \right) \equiv (-1)^{\Omega(q)} (-1)^{\omega(q)} \pmod{3}.$$

Thus,

$$\begin{aligned} S_1 - S_2 &= \sum_{q \in \mathcal{Q}} (-1)^{\Omega(q) + \omega(q)} \frac{1}{q} \prod_{p|q} \frac{p}{p+1} \\ &= \prod_{p \equiv 2(3)} \left(1 - \frac{p}{p+1} \sum_{a=2}^{\infty} \frac{(-1)^a}{p^a} \right) \\ &= \prod_{p \equiv 2(3)} \left(1 - \frac{1}{(p+1)^2} \right) = c_4. \end{aligned} \quad (5.5)$$

Proposition 5.1 follows immediately from (5.4) and (5.5). \square

We now say a few words on the numerical estimation of the products c_3 and c_4 in (5.4) and (5.5). Both products converge quadratically, in fact, better than quadratically, since they are over primes. However, we can hasten the convergence, making them even easier to calculate. Let

$$\bar{c}_3 = \prod_{p \neq 2(3)} \left(1 + \frac{1}{p^2 - 1} \right),$$

so that

$$c_3 \bar{c}_3 = \prod_p \left(1 + \frac{1}{p^2 - 1} \right) = \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \dots \right) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Then

$$c_3 = \sqrt{\frac{c_3 \bar{c}_3}{\bar{c}_3 / c_3}} = \frac{\pi}{\sqrt{6}} \sqrt{\frac{c_3}{\bar{c}_3}}. \quad (5.6)$$

Let $\chi_1(n)$ be ± 1 when $n \equiv \pm 1 \pmod{3}$, respectively, and note that

$$\frac{c_3}{\bar{c}_3} = \frac{9}{8} \prod_{p \neq 3} \left(1 + \frac{1}{p^2 - 1} \right)^{\chi_1(p)}.$$

This last product converges considerably faster than do the separate products c_3 and \bar{c}_3 , and it is via this product and (5.6) that we get the estimate $c_3 \doteq 1.4140643909$. It is now a simple matter to estimate c_4 since we have that $c_4 = (c_4 c_3) / c_3$, where

$$c_4 c_3 = \prod_{p \equiv 2(3)} \left(1 + \frac{2p + 1}{(p^2 - 1)(p + 1)^2} \right)$$

converges cubically. By means of our estimation for c_3 and an estimation for $c_4 c_3$, we get that $c_4 \doteq .8505360177$.

From (1.2), (1.6), (5.3), (5.4) and (5.5) we have

$$\frac{N(x, 12, 4)}{N(x, 12, 8)} \sim \frac{N(x, 3, 1)}{N(x, 3, 2)} \sim \frac{3S_1 + S_2}{S_1 + 3S_2} = \frac{2c_3 + c_4}{2c_3 - c_4},$$

as $x \rightarrow \infty$. The ratio of the modulo 3 counts converges to this limit more rapidly than the ratio of the modulo 12 counts, as can be seen numerically in Table 1. This is due to the modulo 12 ratio leaving out the residue class $10 \pmod{12}$, which is negligible asymptotically, but not so at small levels.

6. The calculation of Landau's constant c

In this section we shall show the following.

Proposition 6.1. *The number c in Landau's theorem is $\sqrt{2c_3\sqrt{3}}/\pi$, where c_3 is given in (1.8).*

Note that Theorem 3.1 (and so (1.3) and (1.5) of Theorem 1.2) follows immediately from (5.3), Propositions 5.1 and 6.1.

Proof of Proposition 6.1: Using a theorem of Wirsing [8], we have that

$$c = \frac{\frac{1}{2}Ke^{-\gamma/2}}{\Gamma(\frac{3}{2})} = \frac{Ke^{-\gamma/2}}{\sqrt{\pi}}, \quad (6.1)$$

where γ is Euler's constant and K is the number that satisfies

$$\prod_{\substack{p \leq x \\ p \equiv 2(3)}} \left(1 + \frac{1}{p-1}\right) \sim K(\log x)^{1/2} \quad (6.2)$$

as $x \rightarrow \infty$. Thus, in light of (6.1), to prove Proposition 6.1 it will suffice to show that

$$K = e^{\gamma/2} \sqrt{\frac{2c_3\sqrt{3}}{\pi}}. \quad (6.3)$$

We take the logarithm of (6.2) getting that

$$\begin{aligned} \log K + \frac{1}{2} \log \log x &= \sum_{\substack{p \leq x \\ p \equiv 2(3)}} \log \left(1 + \frac{1}{p-1}\right) + o(1) \\ &= \sum_{\substack{p \leq x \\ p \equiv 2(3)}} \frac{1}{p} + \sum_{p \equiv 2(3)} \left(\log \left(1 + \frac{1}{p-1}\right) - \frac{1}{p} \right) + o(1), \end{aligned} \quad (6.4)$$

as $x \rightarrow \infty$.

Let B be the number such that

$$\sum_{\substack{p \leq x \\ p \equiv 2(3)}} \frac{1}{p} = \frac{1}{2} \log \log x + B + o(1) \quad (6.5)$$

as $x \rightarrow \infty$. So from (6.4) and (6.5) we get

$$\log K = B + \sum_{p \equiv 2(3)} \left(\log \left(1 + \frac{1}{p-1}\right) - \frac{1}{p} \right) \quad (6.6)$$

We now compute the number B in (6.5). Mertens showed how to do this over 100 years ago; we follow his method. Let χ_0, χ_1 be the Dirichlet characters mod 3, where

$$\chi_0(n) = \begin{cases} 1, & \text{if 3 does not divide } n \\ 0, & \text{otherwise,} \end{cases}$$

and

$$\chi_1(n) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod{3} \\ -1, & \text{if } n \equiv -1 \pmod{3} \\ 0, & \text{if } n \equiv 0 \pmod{3}. \end{cases}$$

Then $(\chi_0(n) - \chi_1(n))/2$ is the characteristic function of the integers $n \equiv 2 \pmod{3}$. We thus have

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv 2(3)}} \frac{1}{p} &= \frac{1}{2} \sum_{p \leq x} \frac{\chi_0(p) - \chi_1(p)}{p} \\ &= -\frac{1}{6} + \frac{1}{2} \sum_{p \leq x} \frac{1}{p} - \frac{1}{2} \sum_{p \leq x} \frac{\chi_1(p)}{p}. \end{aligned} \quad (6.7)$$

From Theorem 428 in Hardy and Wright [4] we have

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + \gamma + \sum_p \left(\log \left(1 - \frac{1}{p} \right) + \frac{1}{p} \right) + o(1) \quad (6.8)$$

as $x \rightarrow \infty$. Since the series $\sum_p \chi_1(p)/p$ converges (as we shall soon see), it follows from (6.5), (6.7) and (6.8) that

$$B = -\frac{1}{6} + \frac{1}{2}\gamma + \frac{1}{2} \sum_p \left(\log \left(1 - \frac{1}{p} \right) + \frac{1}{p} \right) - \frac{1}{2} \sum_p \frac{\chi_1(p)}{p}. \quad (6.9)$$

To evaluate the last series, consider the L -function

$$L(s, \chi_1) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^s}$$

for $s > 0$. (It follows from the Abel summation formula that the series converges for $s > 0$.) Since $\chi_1(n)n^{-s}$ is a multiplicative function of n , we have

$$L(s, \chi_1) = \prod_p \left(1 + \frac{\chi_1(p)}{p^s} + \frac{\chi_1(p)^2}{p^{2s}} + \cdots \right) = \prod_p \left(1 - \frac{\chi_1(p)}{p^s} \right)^{-1}.$$

Letting $s = 1$ and taking the logarithm we get

$$\begin{aligned}\log L(1, \chi_1) &= - \sum_p \log \left(1 - \frac{\chi_1(p)}{p} \right) \\ &= \sum_p \frac{\chi_1(p)}{p} - \sum_p \left(\log \left(1 - \frac{\chi_1(p)}{p} \right) + \frac{\chi_1(p)}{p} \right).\end{aligned}\quad (6.10)$$

It follows from Dirichlet's class number formula (see [1], Ch. 6) that $L(1, \chi_1) = \pi/3^{3/2}$, so that from (6.1) we have

$$\sum_p \frac{\chi_1(p)}{p} = \log \left(\frac{\pi}{3^{3/2}} \right) + \sum_p \left(\log \left(1 - \frac{\chi_1(p)}{p} \right) + \frac{\chi_1(p)}{p} \right).$$

Putting this identity in (6.9), we get

$$\begin{aligned}B &= -\frac{1}{6} + \frac{1}{2}\gamma - \frac{1}{2} \log \left(\frac{\pi}{3^{3/2}} \right) + \frac{1}{2} \sum_p \left(\log \left(\frac{1 - 1/p}{1 - \chi_1(p)/p} \right) + \frac{1 - \chi_1(p)}{p} \right) \\ &= -\frac{1}{6} + \frac{1}{2}\gamma - \frac{1}{2} \log \left(\frac{\pi}{3^{3/2}} \right) + \frac{1}{2} \left(\log \left(\frac{2}{3} \right) + \frac{1}{3} \right) + \frac{1}{2} \sum_{p \equiv 2(3)} \left(\log \left(\frac{1 - 1/p}{1 + 1/p} \right) + \frac{2}{p} \right).\end{aligned}\quad (6.11)$$

Thus, from (6.6) and (6.11), we have

$$\begin{aligned}\log K &= \frac{1}{2}\gamma - \frac{1}{2} \log \left(\frac{\pi}{2 \cdot 3^{1/2}} \right) + \frac{1}{2} \sum_{p \equiv 2(3)} \left(2 \log \left(1 + \frac{1}{p-1} \right) + \log \left(\frac{1 - 1/p}{1 + 1/p} \right) \right) \\ &= \frac{1}{2}\gamma - \frac{1}{2} \log \left(\frac{\pi}{2 \cdot 3^{1/2}} \right) + \frac{1}{2} \sum_{p \equiv 2(3)} \log \left(\frac{p^2}{p^2 - 1} \right).\end{aligned}$$

This gives (6.3), and so we have the proposition. \square

7. The proof of Theorem 1.1

Given a residue class $r \pmod m$ that contains a multiple of 4, we shall show that there are integers s, t with $(s+1)(t+1)$ coprime to m and either $st \equiv r \pmod m$ or $st(t+1) \equiv r \pmod m$. By Dirichlet's theorem, the former condition assures that there are infinitely many pairs of different primes p, q with $p \equiv s+1 \pmod m$ and $q \equiv t+1 \pmod m$. If $st \equiv r \pmod m$, then $\varphi(pq) = (p-1)(q-1) \equiv r \pmod m$, while if $st(t+1) \equiv r \pmod m$, then $\varphi(pq^2) = (p-1)(q-1)q \equiv r \pmod m$. In either case, there are infinitely many integers n with $\varphi(n) \equiv r \pmod m$.

Say the prime factorization of m is $p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. We first consider the case when $r \not\equiv 2 \pmod{3}$. Let s, t be integers such that for each odd p_i we have

$$s \equiv \begin{cases} r \pmod{p_i^{a_i}}, & \text{when } r \not\equiv -1 \pmod{p_i} \\ 2^{-1}r \pmod{p_i^{a_i}}, & \text{when } r \equiv -1 \pmod{p_i}, \end{cases}$$

$$t \equiv \begin{cases} 1 \pmod{p_i^{a_i}}, & \text{when } r \not\equiv -1 \pmod{p_i} \\ 2 \pmod{p_i^{a_i}}, & \text{when } r \equiv -1 \pmod{p_i}. \end{cases}$$

These congruences define s and t modulo the odd part of m . Suppose m is even and $2^a \parallel m$. If $a = 1$, then we choose s and t so that they are even, and so we have defined them modulo m . If $a \geq 2$, then by our hypothesis, $4 \mid r$. Take

$$s \equiv \frac{r}{2} \pmod{2^a}, \quad t \equiv 2 \pmod{2^a}.$$

In all cases we have that $st \equiv r \pmod{m}$ and $(s+1)(t+1)$ is coprime to m . These facts may be verified by looking at the situation modulo each $p_i^{a_i}$. For example, suppose p_i is odd and $r \equiv -1 \pmod{p_i}$. By our hypothesis, p_i is not 3. Then $s+1 \equiv 2^{-1}r+1 \equiv 2^{-1}(r+2) \equiv 2^{-1} \not\equiv 0 \pmod{p_i}$ and $t+1 \equiv 3 \not\equiv 0 \pmod{p_i}$. The other conditions follow similarly.

Now consider the case when $r \equiv 2 \pmod{3}$. Let s, t be integers such that for each odd p_i we have

$$s \equiv \begin{cases} 2^{-1}r \pmod{p_i^{a_i}}, & \text{when } r \not\equiv -2 \pmod{p_i} \\ 6^{-1}r \pmod{p_i^{a_i}}, & \text{when } r \equiv -2 \pmod{p_i}, \end{cases}$$

$$t \equiv \begin{cases} 1 \pmod{p_i^{a_i}}, & \text{when } r \not\equiv -2 \pmod{p_i} \\ 2 \pmod{p_i^{a_i}}, & \text{when } r \equiv -2 \pmod{p_i}, \end{cases}$$

(Note that if $p_i = 3$ then $r \not\equiv -2 \pmod{p_i}$, so we do not need the multiplicative inverse of 6.) Again suppose $2^a \parallel m$. If $a = 1$ then take s and t to be even. If $a \geq 2$, then by hypothesis, $4 \mid r$. Take

$$s \equiv 3^{-1} \frac{r}{2} \pmod{2^a}, \quad t \equiv 2 \pmod{2^a}.$$

This time note that $st(t+1) \equiv r \pmod{m}$ and that $(s+1)(t+1)$ is coprime to m . This completes the proof of the theorem.

Added in proof: The conjecture in the Introduction is false; for example, consider the residue classes 302 and 790 (mod 1092). Examples such as this are discussed in "Residue classes free of values of Euler's function," by K. Ford, S. Konyagin and C. Pomerance, to appear in the Proceedings of the Number Theory Conference, Zakopane, Poland, 1997. It is shown there that asymptotically almost all numbers that are $2 \pmod{4}$ are in a residue class free of values of Euler's function.

Acknowledgments

We thank Joseph B. Dence for his assistance in calculating $L(1, \chi_1)$ by an alternate method. We also thank the referee for informing us of [7] which led us to the papers [6] and [2], and ultimately led us to the proof of Theorem 1.1. The calculation of Table 1 and of the numbers c_1, c_2, c_3, c_4 was done with the aid of Mathematica. This paper was written while the first author was visiting The University of Georgia. The second author is supported in part by a National Science Foundation grant.

References

1. H. Davenport, *Multiplicative Number Theory*, 2nd edition, Springer-Verlag, New York, 1980.
2. H. Delange, "Sur les fonctions multiplicatives à valeurs entiers," *C. R. Acad. Sci. Paris, Série A* **283** (1976), 1065–1067.
3. J.B. Dence and T. Dence, "A surprise regarding the equation $\phi(x) = 2(6n + 1)$," *The College Math. J.* **26** (1995), 297–301.
4. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford University Press, p. 351, 1979.
5. E. Landau, *Handbuch der Lehre von der verteilung der Primzahlen*, 3rd edition, Chelsea Publ. Co., pp. 668–669, 1974.
6. W. Narkiewicz, "On distribution of values of multiplicative functions in residue classes," *Acta Arith.* **12** (1966/67), 269–279.
7. W. Narkiewicz, "Uniform distribution of sequences of integers in residue classes," vol. 1087 in *Lecture Notes in Math.*, Springer-Verlag, Berlin, 1984.
8. E. Wirsing, "Über die Zahlen, deren Primteiler einer gegebenen Menge angehören," *Arch. der Math.* **7** (1956), 263–272.