On the genera of $X_0(N)$

János A. Csirik

AT&T Shannon Lab, 180 Park Ave, Florham Park, NJ 07932–0971
E-mail: janos@research.att.com

and

Joseph L. Wetherell *

Department of Mathematics, University of Southern California, Los Angeles, CA 90089–1113
E-mail: jlwether@alum.mit.edu

and

Michael E. Zieve *

Center for Communications Research, 29 Thanet Rd., Princeton, NJ 08540–3699
E-mail: zieve@idaccr.org

Proposed running head: Genera of $X_0(N)$

Address for correspondence:
Michael Zieve
Center for Communications Research
29 Thanet Rd.
Princeton, NJ 08540–3699
e-mail: zieve@idaccr.org
phone: 609-924-4600
fax: 609-924-3061

Let $g_0(N)$ be the genus of the modular curve $X_0(N)$. We record several properties of the sequence $\{g_0(N)\}$. Even though the average size of $g_0(N)$ is $(1.25/\pi^2)N$, a random positive integer has probability zero of being a value of $g_0(N)$. We give bounds (in terms of x) on the size of the set of values of $g_0(N)$ below some given x. Finally, we investigate the distribution of $g_0(N)$ as N varies modulo a fixed prime ℓ.

1. INTRODUCTION

For each positive integer N, the modular curve $X_0(N)$ parametrizes elliptic curves together with a cyclic subgroup of order N (for more details, see [10] and [13]). The genus $g_0(N)$ of $X_0(N)$ tends to infinity as the level N increases. We will examine the sequence $\{g_0(N)\}$ more closely. Among other things, we will show that the average size of $g_0(N)$ is $1.25N/\pi^2$; however, the values of $g_0(N)$ form a density-zero subset of the integers. These two properties imply that there is much collapsing under the map $N \mapsto g_0(N)$: for instance, there are integers whose preimage under this map is arbitrarily large.

The results of this note are:

1. Upper and lower bounds on $g_0(N)$, including the asymptotic results $\liminf g_0(N)/N = 1/12$, and $\limsup g_0(N)/(N \log\log N) = e^\gamma/(2\pi^2)$.
2. Average behavior: $\lim_{B\to\infty}(1/B)\sum_{N\le B} g_0(N)/N = 1.25/\pi^2$.
3. Natural density: $\{g_0(N)\}$ is a density zero subset of the integers. More specifically, let

$$S(x) = \{n \in \mathbb{Z}\colon n \le x \text{ and } n = g_0(N) \text{ for some } N\}.$$

We then prove

THEOREM 1.1 (Theorem One). *For $x \ge 3$,*

$$\frac{x}{\log x} e^{a(\log\log\log x)^2} \ll \#S(x) \ll \frac{x}{(\log x)^b (\log\log x)^c}.$$

(For positive $f(x), g(x)$, the notation $f(x) \ll g(x)$ is equivalent to $f(x) \le O(g(x))$.) Here a is any constant less than a_0, where the constants $a_0 = 0.8168146...$ and $b = 0.2587966...$ and $c = 0.2064969...$ are specified precisely in Section 6.

*Supported in part by NSF Mathematical Sciences Postdoctoral Research Fellowships.

4. Non-uniformity of $g_0(N)$ modulo a fixed prime p: for instance, $g_0(N)$ is odd with probability 1, and (for a fixed odd prime p) the probability that $g_0(N) \equiv 1 \pmod{p}$ is much less than $1/p$. For more details, see Theorem Two in Section 7.

This note arose from a question about curves over finite fields. Typically one estimates the number of points on such a curve by means of the Weil (upper) bound. However, in various situations this bound can be improved, which leads to the converse question of producing curves with many points (of a given genus, over a given field) in order to see how far the Weil bound can be improved. It is known that, if the prime p does not divide N, then $X_0(N)$ has many rational points over the finite field $\mathbb{F}_{p^2}$. Covers of these curves have been used to show that there are curves with many points (over $\mathbb{F}_{p^2}$) in every genus [1]. It is natural to ask whether covers are needed to prove the latter result, or whether the genera of $X_0(N)$ already achieve all sufficiently large integer values. The present note grew from our proof that infinitely many positive integers do not occur in the sequence $\{g_0(N)\}$.

After circulating an earlier draft of this paper, the authors found out about [14], where S. Wong independently proved a subset of the results presented here.

2. THE GENUS OF $X_0(N)$

For a positive integer N, let $g_0(N)$ denote the genus of $X_0(N)$. By [13, Prop. 1.43], we have

$$g_0(N) = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

where ν_2 and ν_3 are the numbers of solutions in $\mathbb{Z}/N\mathbb{Z}$ of the equations $x^2 + 1 = 0$ and $x^2 + x + 1 = 0$, respectively; $\nu_\infty = \sum_d \varphi(\gcd(d, N/d))$; and $\mu = N \sum_a 1/a$. Here φ denotes Euler's totient function, d ranges over the positive divisors of N, and a ranges over the squarefree positive divisors of N. Likewise, let p range over the prime divisors of N, and write $N = \prod_p p^{r_p}$. Then $\mu = \prod_p (p+1)p^{r_p - 1}$. Also ν_2 is 0 if $4 \mid N$ or if some $p \equiv 3 \pmod 4$, and otherwise $\nu_2 = 2^s$ where s is the number of $p \equiv 1 \pmod 4$; similarly, ν_3 is 0 if $9 \mid N$ or if some $p \equiv 2 \pmod 3$, and otherwise $\nu_3 = 2^t$ where t is the number of $p \equiv 1 \pmod 3$. Finally, $\nu_\infty = \prod_p \theta(p, r_p)$, where we define $\theta(p, 2R+1) = 2p^R$ and $\theta(p, 2R) = (p+1)p^{R-1}$.

3. BOUNDS ON $g_0(N)$

We now give general upper and lower bounds on $g_0(N)$. For the lower bound we show that

$$g_0(N) \geq (N - 5\sqrt{N} - 8)/12,$$

with equality if and only if $N = p^2$ where p is a prime congruent to 1 (mod 12). For the upper bound we show the asymptotic result

$$\limsup_{N\to\infty} \frac{g_0(N)}{N \log\log N} = \frac{e^\gamma}{2\pi^2}$$

and the explicit bound

$$g_0(N) < N\frac{e^\gamma}{2\pi^2}(\log\log N + 2/\log\log N) \quad \text{for } N > 2,$$

where $\gamma = 0.5772...$ is Euler's constant.

We start by proving the lower bound $g_0(N) \geq (N - 5\sqrt{N} - 8)/12$. If N is a prime power (or $N = 1$), it is easy to prove this bound and to show that equality occurs precisely when N is the square of a prime congruent to 1 (mod 12). It is also easy to check the lower bound for N less than 2000, so we may assume in the sequel that $N \geq 2000$.

Suppose that N has exactly two distinct prime factors p and q. Then $\mu - N > N/p + N/q > 2\sqrt{N}$. Since $\nu_\infty \leq \mu/\sqrt{N}$ and $\nu_2, \nu_3 \leq 4$, we have $g_0(N) \geq 1 + \mu/12 - 4/4 - 4/3 - \mu/(2\sqrt{N})$. Thus,

$$\begin{aligned} 12g_0(N) &\geq \mu(1 - 6/\sqrt{N}) - 16 \\ &> (N + 2\sqrt{N})(1 - 6/\sqrt{N}) - 16 \\ &> N - 5\sqrt{N} - 8. \end{aligned}$$

Finally, consider the case where N has at least 3 distinct prime factors. In this case we observe that $\mu - N > 3N^{2/3}$ and $\nu_2, \nu_3 \leq \nu_\infty$. It follows that $g_0(N) \geq 1 + \mu/12 - (1/4 + 1/3 + 1/2)\nu_\infty$; hence,

$$\begin{aligned} 12g_0(N) &\geq 12 + \mu - 13\mu/\sqrt{N} \\ &> (N - 5\sqrt{N} - 8) + (\mu - N)(1 - 13/\sqrt{N}) - 8\sqrt{N} + 20 \\ &> (N - 5\sqrt{N} - 8) + 3N^{4/6} - 39N^{1/6} - 8N^{3/6} + 20. \end{aligned}$$

The largest real root of $3x^4 - 8x^3 - 39x + 20$ is $3.5495... < 2000^{1/6}$. The lower bound on $g_0(N)$ follows.

We now prove the limsup result. We have already noted that ν_2, ν_3, and ν_∞ are each bounded by $\mu/\sqrt{N}$; thus, it suffices to show that

$$\limsup_{N\to\infty} \frac{\mu}{N \log\log N} = \frac{6}{\pi^2} e^\gamma.$$

For any $x \geq 2$ let $N_x = \prod_{p \leq x} p$. Among all N with $N_x \leq N < N_{x+1}$ (for fixed x), the case $N = N_x$ maximizes μ/N and minimizes $\log\log N$. Thus, we need only consider values $N = N_x$. For these N, Mertens showed in 1874 that μ/N is asymptotic to $(\log x)e^\gamma 6/\pi^2$ [6, p. 429]; the limsup result follows, since $\log\log N_x$ is asymptotic to $\log x$ [6, p. 341].

The upper bound on $g_0(N)$ is easily verified for $N < 210$, so we now assume $N \geq 210$. Note that $g_0(N) \leq \mu/12$, so our upper bound follows from the inequality $\mu/N < (\log\log N + 2/\log\log N)e^\gamma/(2\pi^2)$. As above, it suffices to prove this inequality when $N = N_x$ (since $N \geq 210 = N_7$). But in this case the inequality follows easily from results in [11].

4. DATA FOR SMALL N

We now determine the first few positive integers n which do not occur as $g_0(N)$ for any N. The lower bound of the previous section implies that, if $n = g_0(N)$, then $N < 12n + 18\sqrt{n} + 40$. So, to determine whether n occurs as $g_0(N)$, we just check all levels N up to this bound. Doing this by computer, we find the first few missed values (i.e., positive integers n not of the form $g_0(N)$): 150, 180, 210, 286, 304, 312, ... Note that all of these are even; in fact, the first several thousand missed values are even. It is easy to describe all positive integers N for which $g_0(N)$ is even. They are given in the following list, where p denotes a prime and r denotes a positive integer:

1. $N = 1, 2, 3, 4, 8$ or 16;
2. $N = p^r$ where $p \equiv 5 \pmod 8$;
3. $N = p^r$ where $p \equiv 7 \pmod 8$ and r odd;
4. $N = p^r$ where $p \equiv 3 \pmod 8$ and r even;
5. $N = 2p^r$ where $p \equiv \pm 3 \pmod 8$;
6. $N = 4p^r$ where $p \equiv 3 \pmod 4$ and r odd.

It follows that, if N is a randomly chosen positive integer, then $g_0(N)$ is odd with probability 1. This shows that a randomly chosen even positive integer has probability zero of occurring as a value of $g_0(N)$.

Looking further in the list of integers not of the form $g_0(N)$, we do eventually find some odd values, the first one occuring at the 3885th position. There are four such up to 10^5 (out of 9035 total missed values), namely 49267, 74135, 94091, 96463. In Section 6 we will show that the paucity of odd missed values is not a general phenomenon, but instead an accident caused by the fact that 'small' numbers do not have enough prime factors. In particular, we will see that there are infinitely many positive odd integers not of the form $g_0(N)$, and in fact the set of integers of the form $g_0(N)$ has density zero in the set of all nonnegative integers.

5. AVERAGE SIZE OF $g_0(N)$

We have shown that $g_0(N)$ is sometimes as small as $N/12$, and sometimes as large as $cN \log\log N$. We now determine the average behavior. More precisely, we show that

$$\frac{1}{B}\sum_{N=1}^{B} g_0(N) = \frac{5}{8\pi^2}B + o(B).$$

By Abel's lemma [12, VI. §2.], this result is equivalent to the following (for the forward or backward implication, set (a_n, b_n) to $(g_0(n), 1/n)$ or $(g_0(n)/n, 1)$, respectively):

$$\lim_{B\to\infty} \frac{1}{B}\sum_{N=1}^{B} \frac{g_0(N)}{N} = \frac{5}{4\pi^2} = 0.12665... \tag{1}$$

In Section 3, we showed that $g_0(N)/N = (1/12)\sum_{a|N}(1/a) + o(1)$, and we can ignore the error term since it contributes nothing to the limit. The following computation proves (1) (for notational simplicity, we let the sums involving a run over square-free integers only):

$$\begin{aligned}\lim_{B\to\infty} (1/B)\sum_{N=1}^{B}\sum_{a|N} 1/a &= \lim_{B\to\infty} (1/B)\sum_{a\le B} (B/a)(1/a) \\ &= \sum_{a<\infty} 1/a^2 = \zeta(2)/\zeta(4) = 15/\pi^2.\end{aligned}$$

6. DENSITY OF $\{g_0(N)\}$

In this section we consider the (natural) density of the set $\{g_0(N)\}$ as a subset of the non-negative integers. We have already seen that $g_0(N)$ is almost never even, so this density (if it exists) is at most $1/2$.

Here is a quick proof that $\lim_{x\to\infty}(\#S(x))/x = 0$, (with $S(x)$ as defined in the Introduction). Let N be a positive integer and suppose that N is divisible by at least $s > 2$ distinct odd primes. The formulas in Section 2 imply that 2^{s-1} divides ν_3 and 2^s divides each of μ, ν_2, and ν_∞. It follows that $g_0(N) \equiv 1 \pmod{2^{s-2}}$.

We now show that $\#S(x) \le x/2^d + o_d(x)$ for each positive integer d; this implies that $\#S(x) = o(x)$, as desired. Fix a positive integer d. Clearly the number of $n \in S(x)$ with $n \equiv 1 \pmod{2^d}$ is less than $x/2^d + 1$. It remains to show that the number of $n \in S(x)$ with $n \not\equiv 1 \pmod{2^d}$ is $o(x)$. Each

such n has the form $g_0(N)$ where N has at most $d+1$ distinct odd prime divisors and $N < 12x+18\sqrt{x}+40$. And the number of such N (hence also the number of such n) is well-known to be $o(x)$ [6, p. 356].

Now we can prove:

THEOREM 6.1 (Theorem One). *For $x \geq 3$,*

$$\frac{x}{\log x} e^{a(\log\log\log x)^2} \ll \#S(x) \ll \frac{x}{(\log x)^b (\log\log x)^c}.$$

(For positive $f(x), g(x)$, the notation $f(x) \ll g(x)$ is equivalent to $f(x) \leq O(g(x))$.) Here a is any constant less than a_0, where the constants $a_0 = 0.8168146...$ and $b = 0.2587966...$ and $c = 0.2064969...$ are defined as follows. Let B be the unique root of $1/B + \log B = 1 + \log 2$ in the interval $(0,1)$, let A be the unique root of $\sum_{n=1}^{\infty} A^n((n+1)\log(n+1) - n\log n - 1) = 1$ in the interval $(0,1)$, and put $a_0 = -1/(2\log A)$ and $b = B\log 2$ and $c = (B\log 2)/(2-2B)$.

Proof of Theorem One, lower bound. The lower bound is proved by considering numbers N which are products of a fixed number k of distinct primes, the least of which is 11; for such N we have $g_0(N) = 1 - 2^{k-1} + (1/12)\prod_{p|N}(p+1)$. Each of these $g_0(N)$ are distinct, and thus we obtain the lower bound by pluggin in the results of [7].

Proof of Theorem One, upper bound. The upper bound is proved by optimizing the choice of d in our density-zero proof, after one has modified that proof by replacing the $o(x)$ bound from [6, p. 356] by the more precise bound from [5].

Let $W_j(x)$ denote the number of positive integers less than x which have exactly j distinct prime factors. Lemma B of Hardy–Ramanujan is: there are positive constants G and H such that for all $x > 2$ and all positive j,

$$W_j(x) \leq Gx(H + \log\log x)^{j-1}/[(\log x)(j-1)!]$$

For fixed x and d, the number of elements of $S(x)$ congruent to 1 mod 2^{d-1} is less than $1 + x/2^{d-1}$, and any other element of $S(x)$ must be $g_0(N)$ where $N \leq 12x+18\sqrt{x}+40$ and N has at most $d+1$ distinct prime factors; thus, $\#S(x) \leq x/2^{d-1} + \sum_{j<d+2} W_j(12x + 18\sqrt{x} + 40)$.

Put $y = 12x+18\sqrt{x}+40$. Let $D = B(H+\log\log y)+B/(2-2B)\log\log\log y$, and let d be the least integer $>= D$, where $B = 0.373364...$ satisfies $1/B + \log B = 1 + \log 2$. Throughout this argument, we assume y is larger than any convenient absolute constant – so to start with, y is big enough

so that $\log\log\log y$ is defined and positive. Also $c', c'', \ldots$ denote positive absolute constants.

We give a preliminary upper bound on $\sum_{j<d+2} W_j(y)$: for $1 \le j \le d+2$, we have $j \le (H + \log\log y)/2$ (for large y), so

$$\begin{aligned} Gy(H+\log\log y)^{j-1}/((\log y)(j-1)!) &\le (1/2)Gy(H+\log\log y)^j/((\log y)j!) \\ &\le 1/2^{d+1-j}Gy(H+\log\log y)^d/((\log y)d!) \end{aligned}$$

Applying Hardy–Ramanujan, we get $\sum_{j<d+2} W_j(y) < 2Gy(H+\log\log y)^d/((\log y)d!)$.

Next we bound this last expression:

$$\begin{aligned} \sum_{j<d+2} W_j(y) &< 2G(y/\log y)(H+\log\log y)^d/((d/e)^d\sqrt{2\pi d}) \\ &= c'(y/\log y)(e/d*(H+\log\log y))^d/\sqrt{d} \end{aligned}$$

Note that $(e/d)(H+\log\log y) \le e/B/(1+(\log\log\log y)/(2-2B)/(H+\log\log y))$ is bounded (e.g., by $2e/B$) when y is sufficiently large; thus, replacing the exponent d by D only increases our bound by a constant factor:

$$\begin{aligned} ((e/d)(H &+ \log\log y))^d \le c''(e/d(H+\log\log y))^D \le c''(e/B)^D(1+(\log\log\log y)/(2-2*B)/(H+\log\log y \\ &= c''(e/B)^D \exp(-D*\log(1+(\log\log\log y)/(2-2*B)/(H+\log\log y))) \\ &= c''(e/B)^D \exp(-B/(2-2B)(\log\log\log y)+o(1)) \\ &= c'' \exp((B-B\log B)(H+\log\log y)-(B\log B)/(2-2B)(\log\log\log y)+o(1)) \\ &\le c''' \exp((B-B\log B)(\log\log y)-(B\log B)/(2-2B)(\log\log\log y)) \\ &= c'''(\log y)^{B-B\log B}(\log\log y)^{(-B\log B)/(2-2B)}. \end{aligned}$$

Also we have $1/sqrtd \le 1/sqrtD < (1/sqrtB)(\log\log y)^(- 1/2)$. Putting these bounds together gives

$$\begin{aligned} \sum_{j<d+2} W_j(y) &< c''''y(\log y)^{-1+B-B\log B}(\log\log y)^{-1/2-B(\log B)/(2-2B)} \\ &= c''''y(\log y)^{-B\log 2}(\log\log y)^{(-B\log 2)/(2-2B)}. \end{aligned}$$

Next we bound $x/2^{d-1}$.

$$\begin{aligned} x/2^{d-1} &< c''''' x/2^D \\ &= c''''' x/\exp(D\log 2) \\ &< c''''' x/\exp((B\log 2)(\log\log y) + (B\log 2)/(2-2B)(\log\log\log y)) \\ &= c''''' x(\log y)^{-B\log 2}(\log\log y)^{(-B\log 2)/(2-2B)} \end{aligned}$$

Combining our last two bounds gives $\#S(x) < c''''''' y\log y)^{-B\log 2}(\log\log y)^{(-B\log 2)/(2-2B)}$.

Finally, y/x is bounded, so we can replace y by x in the above (as long as we increase the constant by the appropriate factor). This gives the desired bound.

Remark. Similar bounds have been proved for the number $\#V(x)$ of distinct values of Euler's φ-function not exceeding x. In this setting, our upper bound is essentially an optimization of the paper [9]. In [7], upper and lower bounds are proved for $\#V(x)$, both of which have the same shape as the above lower bound (but the upper bound is for any $b > b_0$). The precise order of magnitude of $\#V(x)$ is determined in the excellent paper [2], which (together with [3]) also contains several other interesting results whose analogues would be interesting to study in our situation. However, the multiplicativity of $\varphi(n)$ plays a crucial role in all proofs giving better upper bounds for $\#V(x)$ than our upper bound for $\#S(x)$ above. Since $g_0(N)$ (and $g_0(N)-1$) is not multiplicative, it seems that these methods do not apply to $\#S(x)$. We do not know which of our upper and lower bounds is closer to the truth.

7. DISTRIBUTION OF $g_0(N)$ MODULO PRIMES

We now study the distribution of $g_0(N)$ modulo a fixed prime ℓ as N varies. We will see that some residue classes occur more often than others. Let ℓ be a fixed prime. We may restrict to levels N having a prime factor p congruent to -1 modulo 12ℓ, since the set of such N's has density 1 in the set of positive integers. Our assumption on N forces $\nu_2 = \nu_3 = 0$ and $12\ell \mid \mu$, so

$$g_0(N) \equiv 1 - \nu_\infty/2 \pmod{\ell}.$$

First consider the case $\ell = 2$: for our restricted class of N's, we have $g_0(N) \equiv 1 \pmod 2$ unless N is either p^{2r} or $4p^{2r}$, so certainly $g_0(N)$ is odd with probability 1 (as was observed in Section 4).

We have seen that the sequence of residues mod 2 of $g_0(N)$ is biased. We now show a similar result modulo other primes ℓ.

THEOREM 7.1. *Theorem 2 Let $\ell > 2$ be a prime. Then the density of N such that $g_0(N) \equiv 1 \pmod \ell$ is*

$$p_\ell = (1 - 1/\ell^3) \prod (1 - 1/(s^2 + s)).$$

Proof.. As above, we may assume N has a prime factor p with $12\ell \mid (p + 1)$; then $\ell \mid (g_0(N) - 1)$ is equivalent to $\ell \mid \nu_\infty$, and this occurs precisely when either $\ell^3 \mid N$ or some prime congruent to -1 mod ℓ divides N with (positive) even multiplicity. By a standard argument (similar to [8, Thm. 2.18]), the probability that N does not satisfy either of these conditions is

$$(1 - 1/\ell^3) \prod_{\substack{s \equiv -1 \pmod \ell \\ s \text{ prime}}} (1 - 1/s^2 + 1/s^3 - 1/s^4 + 1/s^5 - \dots),$$

which equals p_ℓ.

The following table gives upper bounds for the probability $P(\ell)$ that $g_0(N) \equiv 1 \pmod \ell$:

ℓ	3	5	7	11	13	17	19	23
$P(\ell) <$	1/4	1/78	1/105	1/653	1/1542	1/1793	1/978	1/5821

In these first few cases, we see that the probability is much less than $1/\ell$. More generally, it is easy to see that for every ℓ we have $P(\ell) < 3/\ell^2$.

Also note that other cosets mod ℓ will have special behavior as well. If N is squarefree, ν_∞ is a power of 2, so that $g_0(N)$ is congruent modulo ℓ to a number of the form $1 - 2^k$. Recall that N is squarefree with probability $6/\pi^2 = 0.6079...$ [6, p. 269]. Thus, if 2 is not a primitive root mod ℓ, then the residue classes (mod ℓ) of the integers $1 - 2^k$ will occur more frequently than the other residue classes. For example, for $\ell = 7$, the classes $0, 4, 6$ occur much more frequently than the classes $2, 3, 5$.

Using the fact that the number of prime factors of square-free integers are distributed uniformly modulo ℓ, we can go further.

Claim 7.1. Let $\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^\times$. The density of N such that

$$g_0(N) \equiv 1 - \lambda \pmod \ell$$

depenends only on the orbit of λ under the multiplicative action of 2.

As we have seen above, the orbit with 1 in it is always the one corresponding to the highest density.

The above Claim, combined with Theorem Two, immediately yields

COROLLARY 7.1. *Let ℓ be a prime such that 2 is a primitive root modulo ℓ (and thus the action of 2 on $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is transitive). Then for all $1 \neq \mu \in \mathbb{Z}/\ell\mathbb{Z}$, the density of N such that*

$$g_0(N) \equiv \mu \pmod{\ell}$$

is $(1 - p_\ell)/(\ell - 1)$.

The proof of the claim, which will be given elsewhere, proceeds by writing $N = ab$, where a is powerful, b is square-free, and $(a, b) = 1$. Noting that $\nu_\infty(N) = \nu_\infty(a)\nu_\infty(b)$, and fixing a and letting b vary, we obtain the proof.

ACKNOWLEDGMENTS

The first author thanks H. Zhu for bringing this topic to his attention. The third author thanks A. Granville, C. Pomerance, and J. Vanderkam for helpful correspondence. The authors used the computer package `GP/PARI` for various computations related to this note. The authors thank the referee for useful suggestions.

REFERENCES

1. N. Elkies, E. Howe, A. Kresch, B. Poonen, J. Wetherell, and M. Zieve, Curves of every genus with many points: on a question of Serre, preprint, 1999.
2. K. Ford, The distribution of totients, *Ramanujan J.* **2** (1998), 67–151.
3. K. Ford, The number of solutions of $\varphi(x) = m$, *Ann. of Math.* **150** (1999), 283–311.
4. H. Halberstam and H.-E. Richert, "Sieve Methods," Academic Press, New York, 1974.
5. G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, *Quart. J. Math.* **48** (1917), 76–92.
6. G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 5th ed., Oxford University Press, New York, 1979.
7. H. Maier and C. Pomerance, Distinct values of Euler's φ-function, *Acta Arith.* **49** (1988), 263–275.
8. W. Narkiewicz, "Number Theory," World Scientific, Singapore, 1983.
9. S. S. Pillai, On some functions connected with $\varphi(n)$, *Bull. Amer. Math. Soc.* **35** (1929), 832–836.
10. D. E. Rohrlich, Modular curves, Hecke correspondences, and L-functions, *in* "Modular Forms and Fermat's Last Theorem," (G. Cornell et al., eds.), Springer-Verlag, New York, 1997, 41–100.

11. J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

12. J.-P. Serre, "A Course in Arithmetic," Springer-Verlag, New York, 1973.

13. G. Shimura, "Introduction to the Arithmetic Theory of Automorphic Functions," Princeton University Press, Princeton, 1971.

14. S. Wong, Unpublished manuscript, 1995.