EXPOSITIONES
MATHEMATICAE

Expo. Math. 9 (1991), 335–350

On pairs of coprime integers with no large prime factors

Andrew Granville

Abstract. We give an estimate for Gunderson's function, which counts pairs of coprime integers with no large prime factors, and then use this function, in place of the Dickman-De Bruijn function, to get improved results in a number of classical number theory questions (e.g. upper bounds for kth power non-residues, lower bounds on S-unit equations, primality testing, etc.).

1. Introduction

Let P be a given set of prime numbers, and for each $x \geq 2$ define $S(x;P)$ to be the set of positive integers $\leq x$, all of whose prime factors come from the set P. We denote the size of this set by $\psi(x;P)$; when $P = P(z)$ is the set of all prime numbers $\leq z$, then we write $S(x;z)$ for $S(x;P)$ and $\psi(x;z)$ for $\psi(x;P)$ — $\psi(x;z)$ is called the *Dickman-De Bruijn* function. The function $\psi(x;z)$ has been extensively studied and is widely used when dealing with a variety of number theoretic questions (see [20] for a review).

For $x, y \geq 2$, define $S(x,y;P)$ to be the set of pairs of integers (a,b) where $a \in S(x;P)$, $b \in S(y;P)$ and $\gcd(a,b) = 1$; we denote the size of this set by $\psi(x,y;P)$. Again if $P = P(z)$ we write $S(x,y;z)$ and $\psi(x,y;z)$. The function $\psi(x,y;z)$ was first defined by Norman Gunderson [12] in his PhD. thesis, but has recieved little attention since. In this paper we will see how it can be used in place of the Dickman-De Bruijn function in a variety of applications to get slightly superior results.

2. Least kth power non residues (mod n)

Suppose that n and k are positive integers where k divides $\phi(n)$ and ϕ is Euler's totient function. An old problem in analytic number theory is to bound the least positive integer q, prime to n, that is not congruent to the kth power of an integer

0723-0869/91/040335-16$4.70

(mod n). We describe an elementary approach to this question in this section. First we give some facts about kth power residues:

Lemma 1. *Suppose that n and k are positive integers where k divides $\phi(n)$. Then* (i) *The product of a finite set of kth power residues* (mod n), *is itself a kth power residue* (mod n); (ii) *If a and b are both kth power residues* (mod n) *and $(b,n) = 1$ then a/b is also a kth power residue* (mod n); (iii) *The number of distinct kth power residues* (mod n), *that are coprime with n, is precisely $\phi(n)/k$.*

The proof of lemma 1 is straightforward.

Lemma 2. *Suppose that n and k are positive integers, where k divides $\phi(n)$, and that P is a set of primes, each of which are kth power residues* (mod n) *and do not divide n. Then*

$$(i) \qquad \psi(n;P) \le \frac{\phi(n)}{k};$$

and if $xy = n$ with $x, y \ge 1$ then

$$(ii) \qquad \psi(x,y;P) \le \frac{\phi(n)}{k}.$$

Proofs: (i) If $a \in S(x;P)$ then a is a kth power residue (mod n), by Lemma 1(i), as all of the prime factors of a lie in the set P. Therefore $\psi(n;P) \le \phi(n)/k$, by Lemma 1(iii).

(ii) If $(a,b) \in S(x,y;P)$ then a and b are both kth power residues (mod n), by Lemma 1(i), and thus so is a/b, by Lemma 1(ii). We claim that if (a,b) and (c,d) are distinct elements of $S(x,y;P)$ then $a/b \not\equiv c/d$ (mod n). (Otherwise, if $a/b \equiv c/d$ (mod n) then n divides $ad - bc$ and $|ad - bc| \le n - 1$ so that $ad = bc$. But then, as $(a,b) = (c,d) = 1$ we have $a = c$ and $b = d$). Therefore $\psi(x,y;P) \le \phi(n)/k$, by Lemma 1(iii).

Remark: Gunderson [12] actually proved a slightly stronger result than Lemma 2(ii): If $xy = n/2$ and $x, y \ge 1$ then $\psi(x,y;P) \le \phi(n)/2k$. The only difference in the proof is to show that $a/b \not\equiv \pm c/d$ (mod n).

Lemma 2 is a simple but effective tool for putting upper bounds on the least kth power non-residues (mod p), by the following argument:

If the least kth power non-residue is $> m$ then $\psi(n;m) \le \phi(n)/k$, by Lemma 2(i). Therefore we can ensure that there is a kth power non-residue $\le m$, by choosing m so that $\psi(n;m) \ge n/k$.

In 1930 Dickman [4], showed that for any fixed $u \ge 1$,

$$\psi(x;x^{1/u}) \sim x\varrho(u) \qquad \text{as} \quad x \to \infty \tag{1}$$

where $\varrho(u)$, the *Dickman function*, is defined as the continuous solution of the differential difference equation

$$u\varrho'(u) + \varrho(u-1) = 0 \qquad (u > 1) \tag{2a}$$

with the initial condition

$$\varrho(u) = 1 \qquad (0 \le u \le 1) \tag{2b}$$

It is not hard to use (2) to show that

$$\varrho(u) = 1 - \log u \qquad (1 \le u \le 2),$$

and to prove that ϱ is a decreasing function for $u \ge 1$, that tends to 0 as u tends to ∞. Define u_k to be the solution of $\varrho(u) = 1/k$, so that, for any $u < u_k$, we have $\psi(n; n^{1/u}) > n/k$ for all sufficiently large n. (N.B. By [3], $u_2 = e^{1/2}$ and $u_k \sim \log k/(\log\log k - 1)$).

Therefore we have proved

Lemma 3. *Suppose that k is a fixed positive integer, and choose u to be a positive real number $< u_k$ (the solution of $\varrho(u_k) = 1/k$). Then, for all sufficiently large integers n, with k dividing $\phi(n)$, the smallest positive integer q, that is prime to n, and is not a kth power residue* (mod n), *is less than $n^{1/u}$.* In particular, for any $\varepsilon > 0$, if p is a sufficiently large prime then the least positive integer, that is not a quadratic residue (mod p) is less than $n^{\varepsilon + e^{-1/2}}$.

Better estimates than Lemma 3 have been obtained by modifications of this argument; currently the best results are due to Burgess [2] and Norton [20] who showed that one can take $4u_k$ in place of u_k in Lemma 3.

In the above we have taken k to be fixed and have let n get larger. In this paper we will be interested in what happens if k gets larger along with n; specifically when $k = p^s$ and $n = p^r$ are prime powers for some fixed $r > s \ge 1$. As we shall see, such questions have applications to many different problems.

3. Lower bounds for Gunderson's function and the Dickman-De Bruijn function

Before we start investigating applications we should have some elementary lower bounds for our functions.

Theorem 1. *Suppose that $P = \{p_1, \dots, p_n\}$ is a given set of primes, each less than z. For any given positive integers u, v and w,*

$$\psi(z^u; P) \geq \binom{n+u}{u} \tag{i}$$

and

$$\psi(z^v, z^w; P) \geq \binom{n+v}{v}\binom{n+w-v}{w}. \tag{ii}$$

Proofs: (i) if $a_1 + \cdots + a_n \leq u$ where each $a_i \geq 0$ then $p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \leq z^u$ so that $\psi(z^u; P) \geq \sum_{a_1+\cdots+a_n \leq u} 1 = \binom{n+u}{u}$.

(ii) Suppose that $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ with each $a_i \geq 0$. If b is prime to a and contains only prime factors from P, then all of its prime factors actually come from the set $P \setminus \{p_i : a_i \geq 1\}$ ($= P_a$ say), which has cardinality at least $n - \sum_{i=1}^{n} a_i$. Therefore

$$\begin{aligned}\psi(z^v, z^w; P) &\geq \sum_{a_1+\cdots+a_n \leq v} \psi(z^w; P_a) \\ &\geq \sum_{a_1+\cdots+a_n \leq v} \binom{n+w-v}{w} \qquad \text{(by (i))} \\ &= \binom{n+v}{v}\binom{n+w-v}{w}.\end{aligned}$$

Remark: Theorem 1(i) has previously been proved by Lehmer [16], then by De Bruijn [3], and most recently by Lenstra [17]!

Corollary 1. *For any $a > 1/e$ and for any fixed δ, $0 < \delta < 1$, both $\psi(x; (a \log x)^{1/(1-\delta)})$ and $\psi(x, x; (a \log x)^{1/(1-\delta)})^{1/2}$ are greater than x^δ, for all sufficiently large values of x.*

Proof: As $\pi(z) > z/\log z$ for $z \geq 17$ ([22]), we can use Stirling's formula ($\log n! = n(\log n - 1) + O(\log n)$) together with Theorem 1 to get the lower bound $\delta \log x + \frac{\log x}{\log z}\{1 + \log a + O(1)\}$ for both $\log \psi(x; z)$ and $\log(\psi(x, x; z))/2$, where $z = (a \log x)^{1/(1-\delta)}$; the result follows immediately.

In Section 10 we will use Stirling's formula more precisely to prove:

Theorem 2. *For each* $x > 9 \cdot 10^{18}$

$$\psi(x; \log^2 x) \geq x^{1/2}, \tag{i}$$

and for each $x \geq 10$,

$$\psi(x, x; \log^2 x) \geq x. \tag{ii}$$

Theorem 2(i) was proved by Lenstra [17]. We will give a number of other estimates for Gunderson's function in Section 9.

4. The least p^s-th power non-residue (mod p^r)

In this section we will determine an upper bound on the least p^sth power non-residue (mod p^r) for fixed $r > s \geq 1$: If z equals $(ar \log p)^{r/s}$ or $((ar/2) \log p)^{r/s}$ then $\psi(p^r; z)$ or $\psi(p^{r/2}, p^{r/2}; z)$ is greater than p^{r-s}, respectively, by Corollary 1; therefore there is a p^sth power non-residue (mod p^r) which is less than z, by Lemma 2. We get a similar, but more accurate, result by using Theorem 2, rather than Corollary 1, in the case $r = 2$, $s = 1$ and $a = 1$. Note that in each of the cases above, the result by using Gunderson's function is better than that by using the Dickman-De Bruijn function by a factor of $2^{r/s}$. Thus we may state

Theorem 3. *Suppose that* $\varepsilon > 0$ *and* t *is a fixed rational number, with* $t = r/s > 1$ *and* $(r, s) = 1$. *For all sufficiently large prime powers* q, *of the form* p^a *with* a *divisible by* r, *the least* $q^{1/t}$*th power non-residue,* mod q , *is less than* $(1 + \varepsilon)(\log q/2e)^t$.
In particular, for any prime $p \geq 5$, *the least* p*th power non-residue* (mod p^2) *is less than* $\log^2 p$.

The first part of this result is new. A weaker version of the last part was proved by both Fouché [8] and Lenstra [17] — they obtained the bound $4 \log^2 p$ by using the Dickman-De Bruijn function.

Presumably Theorem 3 is far from the best possible result: it is probable true that for each prime $p \geq 5$, either 2 or 3 is not a pth power non-residue (mod p^2), but this seems to be very difficult to prove!!

5. The First Case of Fermat's Last Theorem

The First Case of Fermat's Last Theorem is said to hold for prime p, if there do not exist integers x, y and z for which

$$x^p + y^p + z^p = 0 \quad \text{and} \quad p \text{ does not divide } x, y \text{ or } z. \tag{3}$$

In 1909, Wieferich [24] gave a criterion that is independent of the values of x, y and z: If (3) has solutions then 2 is a pth power residue (mod p^2) — For a lovely proof see Agoh [1]. The following year Mirimanoff [19] showed that if (3) has solutions then 3 is a pth power residue (mod p^2). A succession of authors have extended this and most recently Granville and Monagan [9] have shown that if (3) has solutions then each prime ≤ 89 is a pth power residue (mod p^2). In [10] it was shown that if either one of two conjectures about matrices is true and if (3) has solutions then q is a pth power residue (mod p^2) for all primes $q \leq \max\{97, 3 + 1.643 \log^{1/4} p\}$. We conjecture that it is possible to improve the last part of Theorem 3 as follows:

Conjecture. *For all odd primes p, the least pth power non-residue* (mod p^2) *is less than* $\max\{97, 3 + 1.643 \log^{1/4} p\}$.

If this conjecture holds as well as either Conjecture 11 or 12 in [10], then this would give a proof of the First Case of Fermat's Last Theorem for all prime exponents.

Gunderson himself gave an excellent lower bound for $\psi(x, y; z)$, particularly in the range where $z^2 < \max(\log x, \log y)$, (see (18) in Section 9). This bound, together with Lemma 2(ii), enabled Granville and Monagan to use the residue criteria up to 89, to show that the First Case of Fermat's Last Theorem holds for all prime exponents up to 714,591,416,091,389. From a method suggested in Gunderson's thesis, Tanner and Wagstaff [23] have used a computer to push this lower bound up to 156,442,236,847,241,651; and very recently Coppersmith [25] has introduced some new ideas to obtain 7.568×10^{17}.

Many researchers have investigated the equation

$$x^q + y^q + z^q = 0, \quad q = p^t \quad \text{and prime } p \text{ does not divide } x, y \text{ or } z. \tag{4}$$

Hellegouarch [13] has shown that if (4) does have solutions then p^{2t} divides both $2^p - 2$ and $3^p - 3$. We now prove

Lemma 4. *For any odd prime p and integer $t \geq p^{1/2}/\log p$, 2 and 3 cannot both be p^{2t-1}th power residues* mod p^{2t} *(i.e. p^{2t} cannot divide both $2^p - 2$ and $3^p - 3$).*

Proof: Gunderson [12] gave the (easily proven) lower bound

$$\psi(x, x; 3) \geq 1 + \frac{3 \log^2 x - \log 12 \log x}{\log 2 \log 3}$$

for each $x \geq 1$. Therefore, for $t \geq p^{1/2}/\log p$, we have

$$\psi(p^t, p^t; 3) \geq 1 + \frac{3p - p^{1/2} \log 12}{(\log 2 \log 3)} \geq p$$

and so the result follows from Lemma 2(ii).

Thus, if there are solutions to (4), then p^{2t} divides both $2^p - 2$ and $3^p - 3$ by Hellegouarch's criteria, and so $t \geq p^{1/2}/\log p$ by Lemma 4. Therefore we have

Theorem 4. *For any odd prime p and integer $t \geq p^{1/2}/\log p$, there do not exist integer solutions x, y, z to equation* (4).

6. Polynomial time test of whether a given integer is squarefree

In a number of the algorithms used to test the primality, or to find the factors, of a given integer, it is necessary to determine whether or not the integer is a product of distinct primes. Lenstra [17], whilst investigating Miller's primality test [18], gave a polynomial time algorithm to test whether a given integer is squarefree (m^2 in the number of digits m). We can use our Theorem 4 to get a test 4 times as fast as Lenstra's.

Theorem 5. *Let n be a positive integer, $n > 32$, and assume that $a^{n-1} \equiv 1 \pmod n$ for every prime number $a < \frac{1}{4}\log^2 n$. Then n is a squarefree integer.*

Proof: Suppose that p^2 divides n, for some prime p; then, as $3 < \frac{1}{4}\log^2 n$ we know that $2^{n-1} \equiv 3^{n-1} \equiv 1 \pmod n$ by the hypothesis, and so p is neither 2 nor 3.

For any prime number $a < \log^2 p \left(< \frac{1}{4}\log^2 n \right)$ we have $a^{n-1} \equiv 1 \pmod{p^2}$, by the hypothesis. Therefore the multiplicative order, d, of $a \pmod{p^2}$ is a divisor of $n - 1$ and of $\phi(p^2) = p(p-1)$. But p divides n, so that $(p, n-1) = 1$, implying that d divides $(n-1, p(p-1)) = (n-1, p-1)$, which divides $p - 1$. Therefore $a^{p-1} \equiv 1 \pmod{p^2}$ for all primes $a < \log^2 p$, contradicting Theorem 3.

Remark: Theorem 5 is only of interest in the context of a primality test, as there are obviously many composite integers n with $a^{n-1} \not\equiv 1 \pmod n$ for all $a < \log^2 n$.

7. Bounds on the number of small pth power residues

In Section 10 we shall prove

Theorem 6. *If u is any positive integer and p is any odd prime, $p \geq u^{2u}$, then the number of primes $a \leq p^{1/u}$, such that a is a pth power residue $\pmod{p^2}$ is less than $up^{1/2u}$.*

The case $u = 1$ gives, for any odd prime p,

$$\#\{\text{primes } a : 1 \leq a \leq p \text{ and } p \text{ divides } a^p - a\} \leq p^{1/2},$$

which corresponds in an interesting way to a result of Kruswijk [15] who showed that there exists a constant $k > 0$ such that

$$\#\{\text{integers } a : 1 \leq a \leq p \text{ and } p \text{ divides } a^p - a\} \leq p^{1/2 + k/\log_2 p}.$$

8. S-unit equations with lots of solutions

Let S be a set of s primes. A classical question of transcendental number theory is to ask how many solutions there are to the equations

$$a+b=c \tag{5a}$$

$$\gcd(a,b,c)=1 \tag{5b}$$

$$\text{where all prime factors of } a,\ b \text{ and } c \text{ lie in the set } S. \tag{6}$$

In 1984, Evertse [7] showed that the system of equations (5) and (6) can have no more than 3.7^{2s+3} solutions; in the other direction, Erdös, Stewart and Tijdeman [6] exhibited sets S of s primes where (5) and (6) have at least as many as

$$\exp((4+o(1))(s/\log s)^{1/2}) \tag{7}$$

solutions. Their argument went as follows:

Pick z so that $s=\pi(z)+4\sqrt{z}+O(1)$ and x so that $z=\log^2 x/4$. For each positive integer $b\le x$, let $A_b(x;z)$ be the number of pairs of integers $a,c\in S(x;z)$ for which (5a) holds. Then

$$\max_{1\le b\le x} A_b(x;z) \ge \frac{1}{x}\sum_{b=1}^{x} A_b(x;z) = \frac{1}{x}\binom{\psi(x;z)}{2}$$
$$> \exp\left((4+O(1))\left(\frac{s}{\log s}\right)^{1/2}\right).$$

Now if b is a value for which $A_b(x;z)$ is maximal then, for each pair $(a,c)\in A_b(x;z)$ let $g=\gcd(a,c)$ and so $a'=a/g$, $b'=b/g$, $c'=c/g$ is a solution of (5) and (6). Thus by taking S to be the set of primes $\le z$ together with those dividing b (of which there are less than $(1+o(1))\log x$, by the prime number theorem), we see that the number of solutions of (5) and (6) is least the value in (7).

The last part of the argument, where one divides a,b and c by g, is unpleasant and, as in the paper of Erdös, Stewart and Tijdeman, we shall now pick b so as to maximize $\overline{A}_b(x;z)$ (the number of pairs in $A_b(x;z)$ also satisfying (5b), which is the same as the number of pairs $(a,c)\in S(x,x;z)$ with $c=a-b$). Note that in this case all the solutions of (5) and (6) will have the same value of b. So we have

$$\max_{1\le b\le x} \overline{A}_b(x;z) \ge \frac{1}{x}\sum_{b=1}^{x} \overline{A}_b(x;z) = \frac{1}{2x}(\psi(x,x;z)-1). \tag{8}$$

Erdös, Stewart and Tijdeman did not do their computations in this way and got the lower bound $\exp((2+o(1))(s/\log s)^{1/2})$ for $\overline{A}_b(x;z)$; whereas, by using (8) with z, x

and S as before, we can get the value in (7) as a lower bound for $\overline{A}_b(x;z)$ (N.B. We estimate $\psi(x,x;z)$ by using Theorem 1(ii) together with Stirling's formula). Thus we may state

Theorem 7. *Let $2 = p_1, p_2, \ldots$ be the sequence of prime numbers and fix $\varepsilon > 0$. For any sufficiently large integer s there exists a positive integer b for which there are at least $\exp((4-\varepsilon)(s/\log s)^{1/2})$ solutions to the equation $a+b=c$, where a and c are pairwise coprime integers, all of whose prime factors are $\leq p_t$ (where t equals s minus the number of distinct prime factors of b).*

9. Further estimates for Gunderson's function

In 1951, De Bruijn [3] estimated the order of magnitude of $\psi(x;z)$ in all ranges of x and z:

$$\log\psi(x;z) \sim \frac{\log x}{\log z}\log\left(1+\frac{z}{\log x}\right)+\frac{z}{\log x}\log\left(1+\frac{\log x}{z}\right) \tag{9}$$

as $x \to \infty$. By using the trivial upper bound from

$$\psi(x;z)+\psi(y;z)-1 \leq \psi(x,y;z) \leq \psi(x;z)\psi(y;z) \tag{10}$$

together with (9) and Theorem 1(ii) we can see that

$$\log\psi(x,y;z) \sim \log\psi(x;z)+\log\psi(y;z) \tag{11}$$

in the range

$$x \geq y \geq 2, \quad z \geq 2, \quad \frac{z}{\log x} \to \infty \quad \text{as } x \to \infty. \tag{12}$$

On the other hand

$$\psi(x,y;z) = \sum_{n \in S(xy;z)} \#\{\text{pairs } (a,b): ab=n, \quad (a,b)=1, \quad a \leq x, \quad b \leq y\}$$
$$\leq \psi(xy;z)2^{\pi(z)}.$$

Therefore, by using this together with the trivial lower bound in (10), we can use (9) to get the estimate

$$\log\psi(x,y;z) \sim \log\psi(x;z) \tag{13}$$

in the range

$$x \geq y \geq 2, \quad z \geq 2, \quad \frac{z}{\log x} \to 0 \quad \text{as } x \to \infty. \tag{14}$$

It remains to understand the behaviour of $\psi(x,y;z)$ when z is a fixed power of $\log x$. We shall prove, in Section 10:

Theorem 8. *We have the estimate*

$$\log\psi(x^{1-\delta},x^{\delta};z)\sim\frac{\log x}{\log z}G(\delta,t)\qquad(as\ x\to\infty)$$

in the range $1/2\geq\delta\geq 0,\quad x\geq z\geq 2$, *where*

$$t=\frac{z}{\log x},$$
$$G(\delta,t)=t\log\left(\frac{1+\nabla}{t}\right)+\log(t+\nabla)+(2\delta-1)\log\left(\frac{t+(1-2\delta)\nabla}{t+1-2\delta}\right)$$
$$-\delta\log(4\delta(1-\delta)),$$

and

$$\nabla^2=t^2+4\delta(1-\delta).$$

It is possible to get precise asymptotic estimates for $\psi(x,y;z)$ in certain ranges: By applying some estimates of Ivič and Tenenbaum [14] to the sieve identity

$$\psi(x,y;z)=\sum_{d\geq 1,\,Q(d)\leq z}\mu(d)\psi\left(\frac{x}{d};z\right)\psi\left(\frac{y}{d};z\right)$$

(where $Q(d)$ is the largest prime factor of d), we can show that, for each $\varepsilon>0$, we have the the estimate

$$\psi(x,y;z)=\frac{\psi(x;z)\psi(y;z)}{\zeta(\alpha)}\left\{1+O_\varepsilon\left(\frac{1}{\log y}+\frac{\log\log(z+1)}{\log z}\right)\right\}$$

in the range

$$x\geq y\geq 2,\quad z\geq(\log x\log y)^{1+\varepsilon},\tag{15}$$

where $\alpha=2-\log(\log x\log y)/\log z$, and ζ is the Riemann-zeta function.

In [11] we use combinatorial methods of counting pairs of orthogonal lattice points inside an n-dimensional tetrahedron to prove that

$$\psi(x,y;z)=\frac{1}{n!\prod_{p\leq z}\log p}\sum_{j=0}^{n}\binom{n}{j}^2\log^j x\log^{n-j}y\left\{1+O\left(\frac{z^2}{\log x\log z}\right)\right\}\tag{16}$$

for $x \geq y$ in the range

$$2 \leq z < \log^{1/2} x, \quad \text{where } n = \pi(z). \tag{17}$$

This compares nicely with the estimate

$$\psi(x;z) = \frac{1}{n! \prod_{p \leq z} \log p} \log^n x \left\{ 1 + O\left(\frac{z^2}{\log x \log z} \right) \right\}$$

in the range (17) which was given by Ennola [5]. Note that this implies that, in the range (17),

$$\psi(x,x;z) = \binom{2\pi(z)}{\pi(z)} \psi(x;z) \left\{ 1 + O\left(\frac{z^2}{\log x \log z} \right) \right\}.$$

If we combine the estimates above, we see that we are only lacking asymptotic estimates for $\psi(x,y;z)$ in the range

$$\log^{1/2} x \leq z \leq (\log x \log y)^{1+\varepsilon} \leq \log^{2+2\varepsilon} x.$$

In his thesis Gunderson [12] gave the one sided estimate

$$\psi(x,y;z) \geq \frac{2}{n! \prod_{p \leq z} \log p} \sum_{j=1}^{n-1} \binom{n-2}{j-1} \binom{n}{j} \log^j x \log^{n-j} y, \tag{18}$$

which is weaker than the estimate (16) only by a small factor; it is thus a very good lower bound in the range (17). Actually Gunderson described a method to get a better lower bound than (18), by including terms of lower degree in $\log x$ and $\log y$; this was recently implemented on a computer by Tanner and Wagstaff [23], who also incorporated some ideas of D.H. Lehmer [16].

It is also possible to get a general upper bound by suitably adapting a method of Rankin [21]: For any $\sigma, \tau > 0$, we see that

$$\begin{aligned} \psi(x,y;z) &\leq \sum_{m,n \geq 1,\, Q(mn) \leq z} \left(\frac{x}{m} \right)^{\sigma} \left(\frac{y}{n} \right)^{\tau} \sum_{d \mid (m,n)} \mu(d) \\ &= \sum_{d \geq 1,\, Q(d) \leq z} \mu(d) \frac{x^{\sigma} y^{\tau}}{d^{\sigma+\tau}} \sum_{r,s \geq 1,\, Q(rs) \leq z} \frac{1}{r^{\sigma}} \frac{1}{s^{\tau}} \end{aligned}$$

where $m = dr$ and $n = ds$,

$$= x^{\sigma} y^{\tau} \zeta(\sigma;z) \frac{\zeta(\tau;z)}{\zeta(\sigma+\tau;z)}, \tag{19}$$

where

$$\zeta(s;z) = \prod_{p\le z}(1-p^{-\sigma})^{-1}.$$

By choosing σ and τ so as to minimize the expression in (19) we can get a fairly good upper bound.

10. Proofs of Theorems 2, 6 and 8.

Lemma 5. *Fix λ, $1 \le \lambda < e$. For any real z and integers n and u, with $u \ge u_o(\lambda)$, $z \ge \lambda^2 u^2$ and $n \ge uz^{1/2}/\lambda$, we have $\psi(z^u, z^u; P) > z^u$, where P is any set of n primes, each $\le z$. (N.B. $u_0(1) = 1$, $u_0(2) \le 6$).*

Proof: Stirling's formula, $u! = (u/e)^u(2\pi u)^{1/2}\{1+O(1/u)\}$, implies that if $u \ge u_0(\lambda)$ then $u! \le (u/\lambda)^u$. We also have

$$\frac{(n+u)!}{(n-u)!} = \prod_{j=1}^{u}(n-u+j)(n+u+1-j) = \prod_{j=1}^{u}(n^2+n-(u-j)(u+1-j))$$
$$\ge \prod_{j=1}^{u}(n^2+n-u(u-1)) > n^{2u},$$

as $n \ge uz^{1/2}/\lambda \ge u^2 > u(u-1)$. Therefore, by Theorem 1(ii),

$$\psi(z^u, z^u; P) \ge \binom{n+u}{u}\binom{n}{u} = \frac{(n+u)!}{(n-u)!\,u!^2} > \left(\frac{\lambda n}{u}\right)^{2u} \ge z^u.$$

Proof of Theorem 6: Suppose $P = \{\text{primes } a \le p^{1/u}: a \text{ is a } p\text{th power residue } (\mathrm{mod}\, p)\}$ has $n \ge up^{1/2u}$ elements. Taking $\lambda = 1$ and $z = p^{1/u}$ in Lemma 5, we get $\psi(p,p;P) > z^u = p$; but, by Lemma 2(ii), $\psi(p,p;P) \le p-1$, giving a contradiction.

Lemma 6. *If $x \ge \exp(39)$ then $\psi(x, x; \log^2 x) > x$.*

Proof: Let u be the smallest integer $\ge \log x/2\log_2 x$ and $z = x^{1/u} = \log^2 x/\vartheta^2$, so that $u \ge 6$ and $\vartheta \ge 1$. Therefore $\log\vartheta = (2u\log_2 x - \log x)/2u \le \log_2 x/u \le 2\log_2^2 x/\log x < \log 2$ as $x > \exp(39)$, and so $\log_2 x \ge \log 39 > 2+\log 2 > \vartheta+\log\vartheta$. Thus $x^{1/2} = \log x/\vartheta > \log x/(\log_2 x - \log\vartheta) = 2u$. Therefore, by taking $\lambda = 2$ in Lemma 5 we get $\psi(x, x; \log^2 x) \ge \psi(z^u, z^u; z) > z^u = x$, as $u \ge 6$, $z = x^{1/u} \ge 4u^2 \ge 17$ and $\pi(z) \ge z/\log z$ ([22], Corollary 1) $\ge (\log x/\log z)z^{1/2}/\vartheta \ge uz^{1/2}/2$.

Proof of Theorem 2: By Lemma 6 it suffices to show that the result holds for $10 \le x \le \exp(39)$.

We give below a table of values of x_j such that $\psi(x_j, x_j; \log^2 x_j) \geq x_{j+1}$ for each $j \leq 18$. This is proved by direct computation for $j = 1, 2$ and 3, and by taking $x = x_j$, $u = 1 + [\log x / 2 \log_2 x]$ and $n = \pi(x^{1/u})$ in Theorem 1(ii), so that

$$\psi(x_j, x_j; \log^2 x_j) \geq \psi(x, x; x^{1/u}) \geq \binom{n+u}{u}\binom{n}{u}$$

and

$$\binom{n+u}{u}\binom{n}{u} \geq x_{j+1}$$

(by computation), for each $j \geq 4$.

Therefore if $10 \leq x \leq \exp(39)$ then there exists j, $1 \leq j \leq 18$ such that $x_j \leq x \leq x_{j+1}$ and so

$$\psi(x, x; \log^2 x) \geq \psi(x_j, x_j; \log^2 x_j) \geq x_{j+1} \geq x.$$

$x_1 = 10$	$x_6 = 53130$	$x_{11} = 2.41 \cdot 10^7$	$x_{16} = 5.316 \cdot 10^{13}$
$x_2 = 45$	$x_7 = 10^5$	$x_{12} = 9.011 \cdot 10^8$	$x_{17} = 4.84 \cdot 10^{15}$
$x_3 = 551$	$x_8 = 2.47 \cdot 10^5$	$x_{13} = 1.015 \cdot 10^{10}$	$x_{18} = 6.534 \cdot 10^{16}$
$x_4 = 1980$	$x_9 = 1.085 \cdot 10^6$	$x_{14} = 3.533 \cdot 10^{11}$	$x_{19} > \exp(39)$.
$x_5 = 5500$	$x_{10} = 9.5 \cdot 10^6$	$x_{15} = 3.219 \cdot 10^{12}$	

Proof of Theorem 8: By (11) and (13) we may assume that t is bounded non-trivially both above and below. We may also assume that δ is bounded below by some constant greater than zero: if not then the result follows from the trivial bounds in (10), and the estimate $\psi(x^\delta; z) = \psi(x^{1-\delta}; z)^{O(1)}$ which we can deduce from (9).

We define $M(A, B; n)$ to be the number of pairs of vectors $(\boldsymbol{a}, \boldsymbol{b})$ of non-negative integers, with n components each, such that $\boldsymbol{a}.\mathbf{1} \leq A$, $\boldsymbol{b}.\mathbf{1} \leq B$ and $\boldsymbol{a}.\boldsymbol{b} = \mathbf{0}$.

Let $k = z/\log z$ and $p_1 < p_2 < \cdots < p_n$ be the primes in (k, z). If $(\boldsymbol{a}, \boldsymbol{b})$ is a pair counted in $M((1-\delta)\frac{\log x}{\log z}, \delta\frac{\log x}{\log z}; n)$ (where $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$), then $(a, b) \in S(x^{1-\delta}, x^\delta; z)$ (where $a = p_1^{a_1} \ldots p_n^{a_n}$, $b = p_1^{b_1} \ldots p_n^{b_n}$); therefore

$$M\left((1-\delta)\frac{\log x}{\log z}, \delta\frac{\log x}{\log z}; n\right) \leq \psi(x^{1-\delta}, x^\delta; z). \tag{20}$$

If $(a, b) \in S(x^{1-\delta}, x^\delta; z)$ (where $a = a' p_1^{a_1} \ldots p_n^{a_n}$, $b = b' p_1^{b_1} \ldots p_n^{b_n}$) then $a' \in S(x^{1-\delta}; k)$, $b' \in S(x^\delta; k)$ and the pair $(\boldsymbol{a}, \boldsymbol{b})$ is counted in $M((1-\delta)\frac{\log x}{\log k}, \delta\frac{\log x}{\log k}; n)$ (where $\boldsymbol{a} = (a_1, \ldots, a_n)$, $\boldsymbol{b} = (b_1, \ldots, b_n)$). Therefore

$$\psi(x^{1-\delta}, x^\delta; z) \leq M\left((1-\delta)\frac{\log x}{\log k}, \delta\frac{\log x}{\log k}; n\right)\psi(x^{1-\delta}; k)\psi(x^\delta; k). \tag{21}$$

Now note that $\log k = \log z\{1 + o(1)\}$ and

$$\psi(x^\delta; k) \le \psi(x^{1-\delta}; k) = \psi(x; z)^{o(1)} = \psi(x^{1-\delta}, x^\delta; z)^{o(1)}$$

by (9) and (10), as t and δ are assumed to be bounded non-trivially. Therefore the result follows from substituting the following result into (20) and (21):

Theorem 9. *Fix $c_1 > c_2 > 0$. The estimate*

$$M((1-\delta)x, \delta x; tx) = \exp[xG(\delta, t) + O(\log x)]$$

holds in the range $c_1 \ge t \ge c_2$, $1/2 \ge \delta \ge c_2$.

Proof: Let $n = tx$, $B = (1-\delta)x$ and $A = \delta x$ so that $A \le B$. Then

$$\begin{aligned} M(A, B; n) &= \sum_{\substack{a_1 + \cdots + a_n \le A, \quad b_1 + \cdots + b_n \le B \\ \text{and } a_i \text{ or } b_i = 0 \text{ for each } i.}} 1 \\ &= \sum_{a=0}^{A} \sum_{b=0}^{B} \text{ coefficient of } X^a Y^b \text{ in } (1 + X + Y + X^2 + Y^2 + \cdots)^n \\ &= \text{ coefficient of } X^A Y^B \text{ in} \frac{1}{(1-X)(1-Y)} \left(1 + \frac{X}{1-X} + \frac{Y}{1-Y}\right)^n \\ &= \sum_{i+j+k=n} \binom{n}{i, j, k} \binom{A}{i} \binom{B}{j} \\ &= \sum_{j=0}^{\min(B,n)} \binom{n}{j} \binom{B}{j} \binom{A+n-j}{A}. \end{aligned} \tag{22}$$

Now, by comparing each pair of successive terms of the sum in (22), it is easy to show that the maximum of $\binom{n}{j}\binom{B}{j}\binom{A+n-j}{A}$ occurs when j is an integer within a distance O(1) of one of the solutions of

$$(B + n - A)\left(\frac{j}{n}\right)^2 - (n + 2B)\left(\frac{j}{n}\right) + B = 0.$$

Now as the larger of the two roots of this equation is certainly larger than $\min(B, n)$ we see that

$$\frac{j}{n} = \frac{(n + 2B - \Delta)}{2(B + n - A)} + O(1),$$

where $\Delta^2 = n^2 + 4AB \quad (= \nabla^2 x^2)$. When we substitute this into (22) we see that

$$\begin{aligned} \log M(A, B; n) &= n \log\left(\frac{A + B + \Delta}{n}\right) + A \log\left(\frac{A + n - j}{A}\right) \\ &\quad + B \log\left(\frac{B}{B - j}\right) + O(\log(n + x)) \\ &= xG(\delta, t) + O(\log x), \qquad \text{after some rearrangement.} \end{aligned}$$

Acknowledgements

Parts of this paper were included in the author's doctoral thesis, done at Queen's University in Kingston, Ontario under the supervision of Paulo Ribenboim. I would also like to thank Gerald Tenenbaum for drawing my attention to [14], and Karen Moisiadis for her part in the typing.

References

1. Agoh T., On the criteria of Wieferich and Mirimanoff, C.R. Math. Rep. Acad. Sci. Canada, 8 (1986) 49–52.
2. Burgess D.A., The distribution of quadratic residues and non-residues, Mathematika, 4 (1957) 106–112.
3. de Bruijn N.G., On the number of positive integers $\leq x$ and free of prime factors $> y$, Ned. Akad. Wetensch. Proc., Ser. A, I, 54 (1951) 50–60; II, 69 (1966) 239–247.
4. Dickman K., On the frequency of numbers containing prime factors of a certain relative magnitude, Ark. Mat. Astr. Fys., 22 (1930) 1–14.
5. Ennola V., On numbers with small prime divisors, Ann. Acad. Sci. Fenn. Ser. A I, 440 (1969) 16pp.
6. Erdős P., Stewart C.L. & Tijdeman R., Some Diophantine equations with many solutions, Compositio Math., 66 (1988) 37–56.
7. Evertse J.H., On equations in S-units and the Thue-Mahler equation, Invent. Math., 75 (1984) 561–584.
8. Fouché W.L., On the Kummer-Mirimanoff Congruences, Quart. J. Math. Oxford (2), 37 (1986) 257–261.
9. Granville A. & Monagan M.B., The First Case of Fermat's Last Theorem is true for all prime exponents up to 714, 591, 416, 091, 389, Trans. Amer. Math. Soc., 306 (1988) 329–359.
10. Granville A., Some conjectures related to Fermat's Last Theorem, to appear in Proc. Canadian Number Theory Assoc. (Banff. 1988).
11. Granville A., The lattice points of an n-dimensional tetrahedron, to appear.
12. Gunderson N.G., Derivation of Criteria for the First Case of Fermat's Last Theorem and the Combination of these Criteria to Produce a New Lower Bound for the Exponent, Thesis, Cornell University, (1948).
13. Hellegouarch Y., Courbes Elliptiques et Equation de Fermat, Thesis, Besançon, (1972).
14. Ivič A. & Tenenbaum G., Local densities over integers free of large prime factors, Quart. J. Math. Oxford (2), 37 (1986) 401–417.

15. Kruswijk D., On the congruence $u^{p-1} \equiv 1$ modulo p^2, Math. Centrum Amsterdam Afd. Zuivere Wisk., ZW-003 (1966) 7pp.

16. Lehmer D.H., The lattice points of an n-dimensional tetrahedron, Duke Math. J. 7 (1940) 341–353.

17. Lenstra H.W.Jr., Miller's primality test, Information Processing letters, 8 (1979) 86–88.

18. Miller G.L., Riemann's hypothesis and tests for primality, J. Comp. System Sci 13 (1976) 300–317.

19. Mirimanoff D., Sur le dernier théorème de Fermat. C.R. Acad. Sci. Paris, 150 (1910) 204–206.

20. Norton K.K., Numbers with small prime factors and the least kth power non-residue, Mem. Amer. Math. Soc., 106 (1971) 106pp.

21. Rankin R.A., The difference between consecutive prime numbers, J. London Math. Soc., 13 (1938) 242–247.

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

23. Tanner J.W. & Wagstaff S.S.Jr., New Bound for the first case of Fermat's Last Theorem, (preprint).

24. Wieferich A., Zum letzten Fermat'schen Theorem, J. reine u. angew. Math., 136 (1909) 293–302.

25. Coppersmith D., Fermat's Last Theorem (case 1) and the Wieferich Criterion, (preprint).

Received: 20.11.89
Revised: 03.01.90

Department of Mathematics
University of Toronto, Toronto, Ontario
CANADA M5S 1A1

Current Address:
School of Mathematics
The Institute for Advanced Study
Princeton NJ 08540, USA