

ON THE EQUATION $a^x \equiv x \pmod{b}$

JAM GERMAIN

ABSTRACT. Recently Jimenez and Yebra [3] constructed, for any given a and b , solutions x to the title equation. Moreover they showed how these can be lifted to higher powers of b to obtain a b -adic solution for certain integers b . In this paper we find all solutions x to the title equation, proving that, for given a and b , there are $X/b + O_b(1)$ solutions $x \leq X$. We also show how solutions may be lifted in more generality. Moreover we show that the construction of [3] (and obvious modifications) cannot always find all solutions to $a^x \equiv x \pmod{b}$.

INTRODUCTION

Jimenez and Yebra begin [3] with: “The fact that 7^{343} ends in 343 could just be a curiosity. However, when this can be uniquely extended to

$7^{7659630680637333853643331265511565172343} = \dots 7659630680637333853643331265511565172343,$

and more, it begins to be interesting.” They go on to show that one can construct such an x satisfying $a^x \equiv x \pmod{10^n}$ for any $a \geq 1$ with $(a, 10) = 1$ and any $n \geq 1$.

To find solutions to $a^x \equiv x \pmod{b}$ Jimenez and Yebra proceed as follows: From a solution y to $a^y \equiv y \pmod{\phi(b)}$ one takes $x = a^y$ and then $a^x \equiv x \pmod{b}$ by Euler’s theorem. Since $\phi(b) < b$ for all $b \geq 2$, one can recursively construct solutions, simply and elegantly. The only drawback here is that the method does not obviously give *all* solutions. In this paper we proceed in a more pedestrian manner (via the Chinese Remainder Theorem) to find all solutions, beginning with all solutions modulo a prime power:

For any prime p and each n , $0 \leq n \leq p - 2$ define a sequence $\{x_k(p, n)\}_{k \geq 0}$ of residues $\pmod{p^k(p - 1)}$, by $x_0 = n$ and then

$$(1) \quad x_{k+1} \equiv px_k - (p - 1)a^{x_k} \pmod{p^{k+1}(p - 1)}$$

for each $k \geq 0$ (where $x_k = x_k(p, n)$ for simplicity of notation).

Remark. If $p = 2$ and a is odd then we have the simpler definition $x_0 = 0$ and then $x_{k+1} \equiv a^{x_k} \pmod{2^{k+1}}$ for each $k \geq 0$, as $2(x_k - a^{x_k}) \equiv 0 \pmod{2^{k+1}}$.

Thanks are due to Professor Jorge Jimenez-Urroz for introducing me to this problem, and to Professor Granville for his encouragement and for outlining the proof of (2).

Theorem 1. *Suppose that prime p and integer a are given. If $p|a$ then $a^x \equiv x \pmod{p^k}$ if and only if $x \equiv 0 \pmod{p^k}$. If $(p, a) = 1$ then*

$$a^x \equiv x \pmod{p^k} \text{ if and only if } x \equiv x_k(p, n) \pmod{p^k(p-1)} \text{ for some } 0 \leq n \leq p-2.$$

Actually one can “simplify” this a little bit:

Corollary 1. *Suppose that prime p and integer a are given. If $p|a$ then $a^x \equiv x \pmod{p^k}$ if and only if $x \equiv 0 \pmod{p^k}$. If $(p, a) = 1$ then define, for n , $0 \leq n \leq \text{ord}_p(a) - 1$, a sequence $\{x'_k(p, n)\}_{k \geq 0}$ of residues $\pmod{p^k \text{ord}_p(a)}$ with $x'_0 = n$ and then*

$$x'_{k+1} \equiv px'_k - (p-1)a^{x'_k} \pmod{p^{k+1} \text{ord}_p(a)}$$

for each $k \geq 0$. Then

$$a^x \equiv x \pmod{p^k} \text{ if and only if } x \equiv x'_k(p, n) \pmod{p^k \text{ord}_p(a)} \text{ for some } 0 \leq n \leq \text{ord}_p(a) - 1.$$

To construct p -adic solutions we need the following result:

Lemma 1. *Suppose that prime p and integers n and a are given. Then*

$$x_{k+1}(p, n) \equiv x_k(p, n) \pmod{p^k(p-1)}.$$

for each $k \geq 0$.

Hence,

$$x_\infty(p, n) := \lim_{k \rightarrow \infty} x_k(p, n)$$

exists in $\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ (where $\mathbb{Z}_p := \lim_{k \leftarrow \infty} \mathbb{Z}/p^k\mathbb{Z}$ are the p -adic numbers) and

$$a^{x_\infty} = x_\infty \text{ in } \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Note that there are $p-1$ distinct solutions if $(a, p) = 1$.

Theorem 2. *Given integers a and b , let $L(b, a) := \text{LCM}[b; p-1, p|b, p \nmid a]$. The integers x such that $a^x \equiv x \pmod{b}$ are those integers that belong to exactly $L(b, a)/b$ residue classes mod $L(b, a)$. That is, $1/b$ of the integers satisfy this congruence.*

Note that $L(b, a)$ divides $\text{LCM}[b, \phi(b)]$ for all a .

Example. If $b = 10$ and $5 \nmid a$ then $L(10, a) = [10, 4, 1] = 20$ so exactly 2 out of the 20 residue classes mod 20 satisfy each given congruence. If $b = 10$ and $5|a$ then $L(10, a) = [10, 1] = 10$ so exactly 1 out of the 10 residue classes mod 10 satisfy each given congruence.

a	x
0	10 mod 10
1	1, 11 mod 20
2	14, 16 mod 20
3	7, 13 mod 20
4	6, 16 mod 20
5	5 mod 10
6	6, 16 mod 20
7	3, 17 mod 20
8	14, 16 mod 20
9	9, 19 mod 20

All integers $x \geq 1$ such that $a^x \equiv x \pmod{10}$

Note that, in general $a^{1-p} \equiv 1 - p \pmod{p}$ whenever $p \nmid a$, and so $a^x \equiv x \pmod{p}$ for $x \equiv 1 - p \equiv (p - 1)^2 \pmod{p(p - 1)}$.

Theorem 2 can be improved in the spirit of Corollary 1:

Corollary 2. *Given integers a and b , let $L'(b, a) := \text{LCM}[b; \text{ord}_p(a), p|b, p \nmid a]$. The integers x such that $a^x \equiv x \pmod{b}$ are those integers that belong to exactly $L'(b, a)/b$ residue classes mod $L'(b, a)$. That is, $1/b$ of the integers satisfy this congruence.*

Let $v_p(r)$ denote the largest power of p dividing r . Theorem 2 yields the following result about lifting solutions:

Corollary 3. *Let $b = \prod_p p^{b_p}$ and then m be the smallest integer $\geq v_p(q - 1)/b_p$ for all primes $p, q|b$ with $p, q \nmid a$. The solutions of $a^x \equiv x \pmod{b^m}$ lift, in a unique way, to the solutions of $a^x \equiv x \pmod{b^n}$, for all $n \geq m$.*

Proof. Since $L(b^n, a) := \text{LCM}[b^n; p - 1, p|b, p \nmid a]$ for all $n \geq 1$, we note that $L(b^n, a)/b^n = L(b^m, a)/b^m$ for all $n \geq m$. Hence, by Theorem 2, there are the same number of residue classes of solutions mod b^n as mod b^m so each must lift uniquely.

Using Corollary 2 in place of Theorem 2, one can let m be the smallest integer $\geq v_p(\text{ord}_q(a))/b_p$ for all primes $p, q|b$ with $p, q \nmid a$.

Proposition 3 (in section 5) explicitly gives the lift of Corollary 3, in terms of a recurrence relation based on (1).

It is certainly aesthetically pleasing if, as in the solutions to $7^x \equiv x \pmod{10^n}$ discussed at the start of the introduction, one can lift solutions $x \pmod{b^n}$ (rather than $x \pmod{L(b^n, a)}$ as in Corollary 3) and thus obtain a b -adic limit. From Theorem 2 and Corollary 3 this occurs if $L(b^m, a) = b^m$ (and, from Corollaries 2 and 3, if $L'(b^m, a) = b^m$). Moreover $L'(b^m, a) = b^m$ if and only if all of the prime factors of $\text{ord}_q(a)$ with $q|b, q \nmid a$, divide b . Note that if this happens then there is a unique solution $x \pmod{b^m}$ (by Theorem 2).

This condition becomes most stringent if we select a to be a primitive root modulo each prime dividing b , in which case it holds if and only if prime q divides b whenever q divides $p - 1$ for some p dividing b (or, alternatively, prime q divides b whenever q divides $\phi(b)$). In that case $L(b^m, a) = b^m$ for all integers $a \geq 1$.

Jimenez and Yebra [3] called such an integer b a *valid basis*. Note that b is a valid basis if and only if the squarefree part of b (that is, $\prod_{p|b} p$) is a valid basis. Hence 10 is a valid basis, and 10^n for all $n \geq 1$, as well as 2 and its powers. Also 6, 42 and $2F_n$ for any Fermat prime $F_n = 2^{2^n} + 1$, as well as $\prod_{p \leq y} p, \dots$. We also note that b is a valid basis if and only if every prime p dividing every non-zero iterate of Euler's totient function acting on b (that is, $\phi(\phi(\dots\phi(b)\dots)) \geq 1$) also divides b . We note what we have discussed as the next result:

Proposition 1. *Let b be a squarefree, valid basis, and select m to be the largest power of a prime dividing $\text{LCM}[q-1, q|b]$. If $n \geq m$ then there is a unique solution $x_n \pmod{b^n}$ to $a^{x_n} \equiv x_n \pmod{b^n}$, and these solutions have a b -adic limit, i.e. $x_\infty := \lim_{n \rightarrow \infty} x_n$ which satisfies $a^{x_\infty} = x_\infty$ in \mathbb{Z}_b .*

To be a valid basis seems to be quite a special property, so one might ask how many there are: Let $V(x) = \#\{b \leq x : b \text{ is a valid basis}\}$. In section 6 we obtain the following upper and lower bounds:

Theorem 3. *We have*

$$(2) \quad x^{19/27} \ll V(x) \ll \frac{x}{e^{\{1+o(1)\}} \sqrt{\log x \log \log \log x}}.$$

We certainly believe that $V(x) = x^{1+o(1)}$, and give a heuristic which suggests that

$$V(x) \gg x^{1-\{1+o(1)\} \frac{\log \log \log x}{\log \log x}}.$$

It would be interesting to get a more precise estimate, or even guesstimate, for $V(x)$; for example find $c \in [\frac{1}{2}, 1]$ (if it exists) such that $V(x) = x / \exp((\log x)^{c+o(1)})$.

2. FINDING ALL SOLUTIONS TO $a^x \equiv x \pmod{p^k}$

Proof of Lemma 1. Note that $x_{k+1} = a^{x_k} + p(x_k - a^{x_k}) \equiv a^{x_k} \pmod{p^{k+1}} \equiv x_k \pmod{p^k}$, and $x_{k+1} \equiv x_k \pmod{p-1}$. Hence $x_{k+1} \equiv x_k \pmod{p^k(p-1)}$ by the Chinese Remainder Theorem, as desired.

Proof of Theorem 1. If $p|a$ then $x \equiv a^x \equiv 0 \pmod{p^{\min\{k, x\}}}$. Evidently $k < x$ else $p^x | x$ so $p^x \leq x$ which is impossible. Therefore $x \equiv 0 \pmod{p^k}$. But then $a^x \equiv 0 \equiv x \pmod{p^k}$.

If $p \nmid a$ and $a^x \equiv x \pmod{p^{k+1}}$ then $a^x \equiv x \pmod{p^k}$ and so $x \equiv x_k(n) \pmod{p^k(p-1)}$ for some $0 \leq n \leq p-2$. Hence we can write $x = x_k + lp^k(p-1)$ so that $x \equiv x_k - lp^k \pmod{p^{k+1}}$ and $a^x = a^{x_k} (a^{p^k(p-1)})^l \equiv a^{x_k} 1^l = a^{x_k} \pmod{p^{k+1}}$. Hence, $a^x \equiv x \pmod{p^{k+1}}$ if and only if $l \equiv (x_k - a^{x_k})/p^k \pmod{p}$. Therefore l is unique mod p , and $x \equiv x_k + (p-1)(x_k - a^{x_k}) \equiv x_{k+1}(n) \pmod{p^{k+1}(p-1)}$ as claimed.

Proof of Corollary 1. This comes by taking $x'_k(n, p) \equiv x_k(n, p) \pmod{p^k \text{ord}_p(a)}$, which gives all solutions since $x_k(m, p) \equiv x_k(n, p) \pmod{p^k \text{ord}_p(a)}$ whenever $m \equiv n \pmod{\text{ord}_p(a)}$ (as easily follows by induction).

3. FINDING ALL SOLUTIONS TO $a^x \equiv x \pmod{b}$

We proceed using the Chinese Remainder Theorem to break the modulus b up into prime power factors, and then Theorem 1 for the congruence modulo each such prime power factor. The key issue then is whether the congruences for x from Theorem 1, for each prime power, can occur simultaneously. We use the fact that if primes $p_1 < p_2$ then $x \equiv x_1 \pmod{p_1^{k_1}(p_1 - 1)}$ and $x \equiv x_2 \pmod{p_2^{k_2}(p_2 - 1)}$ if and only if $x_2 \equiv x_1 \pmod{(p_1^{k_1}(p_1 - 1), p_2 - 1)}$ as $(p_2, p_1 - 1) = 1$. The details are complicated at first sight:

Let $b = \prod_p p^{b_p}$, $r = \prod_{p|(a,b)} p^{b_p}$ and $R = b/r = \prod_{i=1}^I p_i^{k_i}$ with $p_1 < p_2 < \dots < p_I$. Define

$$L := \text{LCM}[b; p - 1, p|b, p \nmid a] = \text{LCM}[r, p_j^{k_j}(p_j - 1), 1 \leq j \leq I]$$

We begin by noting that $a^x \equiv x \pmod{b}$ if and only if $a^x \equiv x \pmod{p^{b_p}}$ for all $p|b$, and hence $x \equiv 0 \pmod{r}$. Next we construct the necessary conditions so that the congruences $\text{mod } p_j^{k_j}(p_j - 1)$ can all occur simultaneously:

Step 1. Select any integer n_1 , $0 \leq n_1 \leq p_1 - 2$ with $(r, p_1 - 1)|n_1$. Then determine $x_{k_1}(p_1, n_1) \pmod{p_1^{k_1}(p_1 - 1)}$.

Step 2. Select any integer n_2 , $0 \leq n_2 \leq p_2 - 2$ with $(r, p_2 - 1)|n_2$ and $n_2 \equiv x_{k_1} \pmod{(p_1^{k_1}(p_1 - 1), p_2 - 1)}$. Then determine $x_{k_2}(p_2, n_2) \pmod{p_2^{k_2}(p_2 - 1)}$.

...

Step $m \geq 3$. Select any integer n_m , $0 \leq n_m \leq p_m - 2$ with $(r, p_m - 1)|n_m$ and $n_m \equiv x_{k_j} \pmod{(p_j^{k_j}(p_j - 1), p_m - 1)}$ for each $j < m$. Then determine $x_{k_m}(p_m, n_m) \pmod{p_m^{k_m}(p_m - 1)}$.

Finally we can select $x \pmod{L}$, such that $x \equiv 0 \pmod{r}$ and

$$x \equiv x_{k_j}(p_j, n_j) \pmod{p_j^{k_j}(p_j - 1)}$$

for each j . This works since if $i < j$ then

$$\gcd(p_i^{k_i}(p_i - 1), p_j^{k_j}(p_j - 1)) = \gcd(p_i^{k_i}(p_i - 1), p_j - 1)$$

and we have $x_{k_j}(p_j, n_j) \equiv n_j \equiv x_{k_i}(p_i, n_i) \pmod{(p_i^{k_i}(p_i - 1), p_j - 1)}$, by construction.

From this we can deduce the

Proof of Theorem 2. The number of choices for n_1 above is $\frac{p_1 - 1}{(r, p_1 - 1)} = \frac{[r, p_1 - 1]}{r} = \frac{L_2/p_1^{k_1}}{L_1}$ where $L_m := \text{LCM}[r, p_j^{k_j}(p_j - 1), 1 \leq j < m]$ for each $m \geq 1$. Similarly the number of choices for n_m above is $\frac{p_m - 1}{(L_m, p_m - 1)} = \frac{[L_m, p_m - 1]}{L_m} = \frac{L_{m+1}/p_m^{k_m}}{L_m}$. Hence, in total, the number of choices for the set $\{n_1, n_2, \dots, n_I\}$, using our algorithm above, is

$$\prod_{m=1}^I \frac{L_{m+1}/p_m^{k_m}}{L_m} = \frac{L_{I+1}/R}{L_1} = \frac{L}{rR} = \frac{L}{b},$$

as $L := \text{LCM}[b, p_j - 1, 1 \leq j \leq I]$.

4. THE SPANISH CONSTRUCTION

In the introduction we described how the Spanish mathematicians Jimenez and Yebra [3] constructed solutions to $a^x \equiv x \pmod{b}$: From a solution y to $a^y \equiv y \pmod{\phi(b)}$ one takes $x = a^y$ and then $a^x \equiv x \pmod{b}$ by Euler's theorem. As I have described it, this argument is not quite correct since Euler's theorem is only valid if $(a, b) = 1$. However this can be taken into account:

Lemma 2. *If $a^y \equiv y \pmod{\phi(b)}$ with $y \geq 1$ then $a^x \equiv x \pmod{b}$ where $x = a^y$.*

Proof. Since $a^x \equiv x \pmod{b}$ if and only if $a^x \equiv x \pmod{p^k}$ for every prime power $p^k \parallel b$, we focus on the prime power congruences. Now $\phi(p^k) \mid \phi(b)$ and so $a^y \equiv y \pmod{\phi(p^k)}$. If $p \nmid a$ then we deduce that $a^x \equiv x \pmod{p^k}$ by Euler's theorem. If $p \mid a$ then $p^{k-1} \mid y$ by Theorem 1, since $a^y \equiv y \pmod{p^{k-1}}$. Hence $p^{p^{k-1}} \mid a^y = x$ and a^x , so that $a^x \equiv 0 \equiv x \pmod{p^k}$ as $p^{k-1} \geq k$.

Let $\lambda(b) := \text{LCM}[\phi(p^k) : p^k \mid b]$. One can improve Lemma 2 to "If $a^y \equiv y \pmod{\lambda(b)}$ with $y \geq 1$ then $a^x \equiv x \pmod{b}$ where $x = a^y$," by much the same proof. Let

$$\mathcal{O}(b, a) := \text{LCM}[p^{k-1} \text{ord}_p(a), p^k \mid b, p \nmid a]$$

and

$$k(b, a) := \max\{k : \text{There exists prime } p \text{ such that } p^k \mid b, p \nmid a\}.$$

Lemma 2'. *If $a^y \equiv y \pmod{\mathcal{O}(b, a)}$ with $y \geq k(b, a)$ then $a^x \equiv x \pmod{b}$ where $x = a^y$.*

Does the Spanish construction give *all* solutions to $a^x \equiv x \pmod{b}$? An example shows not: For $b = 11$ and $a = 23$ we begin with the solutions to $23^y \equiv y \pmod{10}$: Then $y \equiv \pm 7 \pmod{20}$ (as we saw in the table in the introduction), leading to the solutions $x \equiv 23$ or $67 \pmod{110}$. However $23^x \equiv x \pmod{11}$ holds if and only if $x \equiv 1 \pmod{11}$; so there are many other solutions x .

There is a variation on the Spanish construction: If $(a + kb)^y \equiv y \pmod{\phi(b)}$ for some given integer k , then

$$a^{(a+kb)^y} \equiv (a + kb)^{(a+kb)^y} \equiv (a + kb)^y \pmod{b}$$

so we can take $x \equiv (a + kb)^y \pmod{L}$. For $b = 11$ and $a = 23$ we look for solutions to $(23 + 11k)^y \equiv y \pmod{10}$ and then take $x = (23 + 11k)^y \pmod{110}$. Using the table in the introduction we obtain the solutions 23, 67; 56; 45; 56; 23, 67; 34, 56; 89; 1; 100; 34, 56 $\pmod{110}$ for $k = 0, 1, \dots, 9$, respectively, missing 12 and 78 $\pmod{110}$.

Another variation on the Spanish construction is to use Lemma 2' in place of Lemma 2, and with this we could have trivially found all solutions to $23^x \equiv x \pmod{11}$. If we now take the example $b = 11$ and $a = 6$ then $\mathcal{O}(11, 6) = 10 = \phi(11)$ so Lemma 2' and Lemma 2 are identical. In this case we proceed as above, using the table in the introduction we obtain the solutions 16; 73, 107; 16, 64; 79; 100; 61; 16, 64; 73, 107; 16; 65 $\pmod{110}$ missing 48 and 102 $\pmod{110}$.

Note that 12 and 78, and 48 and 102 are all even and quadratic non-residues mod 5. It can be proved that this is true in general (though we suppress the proof):

Proposition 2. *Suppose that $b = p = 1 + 2q$ where p and q are odd primes, and that a is a primitive root mod p . The Spanish construction and our variations fail to find the solution $x \equiv n \pmod{p-1}$ to $a^x \equiv x \pmod{p}$ if and only if n is even and $(n/q) = -1$.*

5. b -ADIC SOLUTIONS, b SQUAREFREE

Let $\lambda := \text{LCM}[p-1 : p|b, p \nmid a]$ and $\lambda' = \prod_{q^e \parallel \lambda, q \nmid b} q^e$ so that $L(b^k) = \text{LCM}[b^k, \lambda]$. This equals $\lambda' b^k$ for $k \geq m$. Let $X_k = \{x \pmod{L(b^k)} : a^x \equiv x \pmod{b^k}\}$.

Proposition 3. *Let $\nu \equiv 1/b \pmod{\lambda'}$ (and $\nu = 1$ if $\lambda' = 1$). If $k \geq m$ then X_{k+1} is the set of values $\pmod{L(b^{k+1})}$ given by*

$$(3) \quad x_{k+1} \equiv a^{x_k} + b\nu(x_k - a^{x_k}) \pmod{L(b^{k+1})},$$

for each $x_k \in X_k$.

Proof. We will lift a solution $\pmod{b^k}$ to a solution $\pmod{b^{k+1}}$ by doing so for each prime p dividing m (and combining the results using the Chinese Remainder Theorem). The recurrence relation (1) gives

$$x_{k+1} \equiv p(x_k - a^{x_k}) + a^{x_k} \equiv a^{x_k} \pmod{p^{k+1}}$$

(and this is also true if $p|a$ since then both sides are $\equiv 0$) for each $p|b$, and so combining them, by the Chinese Remainder Theorem, gives

$$x_{k+1} \equiv a^{x_k} \pmod{b^{k+1}}.$$

The recurrence relation (1) also gives $x_{k+1} \equiv x_k \pmod{p-1}$ if $p|b, p \nmid a$, and so $x_{k+1} \equiv x_k \pmod{\lambda}$. Therefore, if $k \geq m$ then $x_{k+1} \equiv a^{x_k} \pmod{b^{k+1}}$ and $x_{k+1} \equiv x_k \pmod{\lambda'}$. One can verify that combining these two by the Chinese Remainder Theorem gives (3) since $L(b^{k+1}) = \lambda' b^{k+1}$.

6. COUNTING VALIDITY

In this section we use estimates on

$$\Pi(x, y) := \#\{\text{primes } q \leq x : p|q-1 \implies p \leq y\}$$

and

$$\Phi_1(x, y) := \#\{n \leq x : p|\phi(n) \implies p \leq y\}.$$

These have been long investigated, and it is believed that for $x = y^u$ with u fixed, we have

$$(4) \quad \Pi(x, y) = \pi(x)/u^{\{1+o(1)\}u}$$

and

$$\Phi_1(x, y) = x/(\log u)^{\{1+o(1)\}u}.$$

These are proved under reasonable assumptions by Lamzouri [4, Theorems 1.3 and 1.4].

6.1. Upper bound on $V(x)$. Banks, Friedlander, Pomerance and Shparlinski [2] showed that

$$\Phi_1(x, y) \leq x/(\log u)^{\{1+o(1)\}u}$$

provided $x \geq y \geq (\log \log x)^{1+o(1)}$ and $u \rightarrow \infty$.

Now suppose that $n \in V(x)$ and there exists prime $p > y$ which divides $\phi(n)$. Then either p^2 divides n , or there exists $q \equiv 1 \pmod{p}$ such that pq divides n . Hence

$$\begin{aligned} V(x) &\leq \Phi_1(x, y) + \sum_{p>y} \frac{x}{p^2} + \sum_{p>y} \sum_{\substack{q \equiv 1 \pmod{p} \\ pq \leq x}} \frac{x}{pq} \\ &\leq \frac{x}{(\log u)^{\{1+o(1)\}u}} + \sum_{p>y} \frac{x}{p^2} \left(1 + \sum_{1 \leq m \leq x/p^2} \frac{1}{m} \right) \ll \frac{x}{y^{1+o(1)}} \end{aligned}$$

when $y = \exp(\sqrt{\log x \log \log \log x})$, writing $q = 1 + mp$ and using the prime number theorem. This implies the upper bound in (2).

6.2. Lower bound on $V(x)$. Fix $\epsilon > 0$. Let $z = (\log x)^{1-\epsilon}$ and $m = \prod_{p \leq z} p$. Select some $T, z \leq T \leq x/m$ and take $u = \lceil \log(x/m)/\log T \rceil$. Any integer which is m times the product of u primes counted by $\Pi(T, z)$ belongs to $V(x)$, so that

$$(5) \quad V(x) \geq \binom{\Pi(T, z) + u - 1}{u} \geq \frac{\Pi(T, z)^u}{u!} \gg \left(\frac{e\Pi(T, z)}{u} \right)^u.$$

Now suppose that $\Pi(T, z) \geq T^{1-o(1)}$ for $T = z^B$. Then $u \sim \log x / \log T = T^{1/B+O(\epsilon)}$ so (5) becomes $V(x) \geq x^{1-1/B+O(\epsilon)-o(1)}$. Letting $\epsilon \rightarrow 0$, we obtain $V(x) \geq x^{1-1/B-o(1)}$. Baker and Harman [1] show that one can take $B = 3.3772$ implying the lower bound in (2). It is believed that one can take B arbitrarily large in which case one would have $V(x) \geq x^{1-o(1)}$, and hence $V(x) = x^{1-o(1)}$ (using the lower bound from the previous subsection).

Suppose that (4) holds for $y = \exp(\sqrt{\log x})$ for all sufficiently large x . Let $T = z^{\log z}$ so that $\Pi(T, z) = T/(\log z)^{\{1+o(1)\}\log z}$ by (4), and thus $e\Pi(T, z)/u = T/(\log z)^{\{1+o(1)\}\log z}$. Hence (5) implies that

$$V(x) \geq \frac{x}{(\log z)^{\{1+o(1)\}\frac{\log x}{\log z}}} = x^{1-\{1+o(1)\}\frac{\log \log z}{\log z}} = x^{1-\{1+o(1)\}\frac{\log \log \log x}{\log \log x}}$$

letting $\epsilon \rightarrow 0$, as claimed at the end of the introduction.

REFERENCES

1. R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith **83** (1998), 331–361.
2. William D. Banks, John B. Friedlander, Carl Pomerance and Igor Shparlinski, *Multiplicative structure of values of the Euler function*, “High primes and misdemeanours”, Fields Inst. Comm **41** (2004), 29–47.

3. Jorge Jimenez-Urroz and J. Luis A. Yebra, *On the equation $a^x \equiv x \pmod{b^n}$* (to appear).
4. Youness Lamzouri, *Smooth values of the iterates of the Euler phi-function*, *Canad. J. Math* **59** (2007), 127–147.
5. Carl Pomerance and Igor Shparlinski, *Smooth orders and cryptographic applications*, “Algorithmic number theory”, *Lecture Notes in Comp. Sci* **2369** (2002), 338–348.