1

On the equation $a^x \equiv x \pmod{b^n}$

J. Jiménez Urroz and J. Luis A. Yebra

September 17, 2008

Abstract

This paper deals with the solutions of the equation $a^x \equiv x \pmod{b^n}$. It turns out that for several values of b the solutions have a particularly rich structure. Already for $b = 10$ we find that for every a which is not a multiple of 10 and for every $n \geq 2$ the equation has just one solution $x_n(a)$. Moreover, the solutions for different values of n come from a precise sequence $x(a) = \{x_n\}_{n\geq 0}$, in the form $x_n(a) = \sum_{i=0}^{n-1} x_i 10^i$. For instance, for $a = 8$ we obtain

$$8^{56} \equiv 56 \pmod{10^2}, \quad 8^{856} \equiv 856 \pmod{10^3}, \quad 8^{5856} \equiv 5856 \pmod{10^4}, \quad \ldots$$

In the paper we prove these results and characterize the bases b with this property.

1 Introduction

The fact that 7^{343} ends in 343 could just be a curiosity. However, when this can be uniquely extended to

$$7^{765963068063733385364333126551156517234 3} = \ldots 765963068063733385364333126551156517234 3,$$

and more, it begins to be interesting. Moreover, instead of 7 any other positive integer a (as far as it is not a multiple of 10) will do. For instance, for $a = 12$

$$12^{791752396359135848584931714421454012416} = \ldots 791752396359135848584931714421454012416.$$

More precisely, we prove below that for any positive integer a, not a multiple of 10, there exists just one infinite sequence of digits,

$$x(a) = \{x_i\}_{i\geq 0} = \ldots\, x_i \ldots x_2\, x_1\, x_0$$

such that for every $n \geq 2$ the number

$$x_n(a) = \sum_{i=0}^{n-1} x_i 10^i = x_{n-1} \ldots x_2 x_1 x_0$$

is the only such number which satisfies

$$a^{x_n(a)} \equiv x_n(a) \pmod{10^n}. \tag{1}$$

Moreover, this fact does not restrict to the decimal basis $b = 10$. When b is square free and such that for every prime $p|b$ and every prime $q|p-1$ we have $q|b$, and for some value of n_b which is characterized below, an analogous results holds: For any positive integer a, not a multiple of b, there exists one infinite sequence of b-digits,

$$x(a, b) = \{x_i\}_{i\geq 0} = (\ldots\, x_i \ldots x_2\, x_1\, x_0)_b$$

*The first author was partially supported by Secretaría de Estado de Universidades e Investigación del Ministerio de Educación y Ciencia of Spain, DGICYT Grants MTM2006-15038-C02-02 and TSI2006-02731.

such that for every $n \geq n_b$ the number

$$x_n(a,b) = \sum_{i=0}^{n-1} x_i b^i = (x_{n-1} \dots x_2\, x_1\, x_0)_b$$

is the only such number which satisfies

$$a^{x_n(a,b)} \equiv x_n(a,b) \,(\text{mod } b^n)\,. \tag{2}$$

For instance, for $b = 6$ and $a = 4$:

$$x(4,6) = \dots 3211201450455542325540435055354110453104_6,$$

so that when, say, $n = 11$, we have

$$x_{11}(4,6) = 54110453104_6 = 344639488 \qquad \text{and} \qquad 4^{344639488} \equiv 344639488 \left(\text{mod } 6^{11}\right).$$

When the basis b is not squarefree, an analogous result holds. In this case, however, instead of multiples of b, we have to remove any multiple of $s(b)$, the squarefree part of b, for obvious reasons.

Finally, the conditions described above are suffcient to guarantee the existence of such a sequence $x(a,b)$, but they are not necessary. It might be the case that for some basis b and some value of a there exists a sequence $x(a,b)$ as above. As an example we have for $b = 9$ and $a = 4$ the sequence $x(4,9) = ...4444444_9$.

2 Main results.

We will write the prime factorization of an integer b as $b = \prod_p p^{v_p(b)}$, and denote $e(b) = \max_{p|b}\{v_p(b)\}$, the highest power of a prime dividing b. We will also denote $s(b) = \prod_{p|b} p$ the squarefree part of b.

Theorem 1 *For every pair of integers a, b there exists an integer $x \geq e(b)+1$ such that*

$$a^x \equiv x \,(mod\ b)\,.$$

For the proof we will need the following observation.

Lemma 2 *Let a, b integers and $x \geq e(b)$ a solution to the equation*

$$a^x \equiv x \,(mod\ \varphi(b))\,.$$

Then

$$a^{a^x} \equiv a^x \,(mod\ b)\,.$$

Proof: Let $b = b_1 b_2$ where $(b_1, a) = 1$ and if $p|b_2$ then $p|a$. Then $\varphi(b_1)|\varphi(b)$ and, hence, $a^x \equiv x \,(\text{mod } \varphi(b_1))$. It is now a simple consequence of Euler´s theorem to get

$$a^{a^x} \equiv a^x \,(\text{mod } b_1)\,.$$

On the other hand we have trivially

$$a^{a^x} \equiv a^x \equiv 0 \,(\text{mod } b_2)\,.$$

The result is now an application of the Chinese Remainder Theorem.

Proof of Theorem 1: We proceed by induction on b, noting that the result is trivial for $b = 1, 2$. Let us suppose we have already proven the theorem for every integer less than b and we want to prove the result for the integer b. We will also suppose $a > 1$. Now, noting that $\varphi(b) < b$ we can apply induction to obtain a solution $x \geq e(\varphi(b)) + 1$ to the equation

$$a^x \equiv x \,(\mathrm{mod}\ \varphi(b))\,.$$

In this case, since $e(\varphi(b)) \geq e(b) - 1$ by definition, we can apply Lemma 2 to get

$$a^{a^x} \equiv a^x \,(\mathrm{mod}\ b)\,.$$

Now, noting that $a^x = (1 + (a-1))^x = \sum_{j=0}^{x} \binom{x}{j}(a-1)^j \geq 1 + x$ for any integers $a > 1$, x, we get $a^x \geq x + 1 \geq e(b) + 1$, as wanted.

Definition 3 *We say that an integer b is a valid basis if for every prime $p|b$ and every prime $q|p-1$ we have $q|b$. We will let $n(b)$ be the minimum integer such that $(p-1)|b^{n(b)}$ for every $p|b$.*

Remark: The existence of such an integer $n(b)$ is clear by the definition of valid basis. Observe that, for example for b squarefree, $n(b) = \max_{p|b}\{\max_{q|b}\{v_q(p-1)\}\}$. Thus, when $b = 10$ we have $n(b) = 2$, while for $b = 34$, we get $n(b) = 4$. However, for $b = 100$, we get $n(100) = 1$. It is straitforward to see that a valid base b must be even and that $b = 2, 4, 6, 8, 10, 12, 16, 18, 20, 24, 30$ are the first valid basis.

Apart from the basis given in the previous Remark, one can ask whether there exist any other valid basis and how to find them. The following give different ways of constructing new valid basis. In particular we see the existence of infinitely many valid basis.

- The product of valid basis is a valid basis.
- If b is a valid basis and p is a prime such that $p - 1|b^r$, for some r, then pb is also a valid basis.
- $b = n!$ is a valid basis for every n.
- For every integer r, $b = \prod_{p \leq r} p$ is a valid basis.

The first two are direct consequences of the definition. For the last ones, we just have to note that if $p|b$ and $q|p-1$, then $q \leq n$ in the first case, while $q \leq r$ in the second.

Theorem 4 *Let b be a valid basis, and $s(b)$ its squarefree part. Then, for every integer a not a multiple of $s(b)$ there exist a unique sequence $\{c_n\}_{n \geq n_b}$ of digits $0 \leq c_n < b$ such that the integers $x_{n+1} = x_n + c_n b^n$, verify*

$$a^{x_n} \equiv x_n \,(mod\ b^n)\,,$$

for every $n \geq n(b)$.

Proof: To clarify the argument, we first present the case where b is a squarefree integer. In any of the cases below, we will proceed by induction in n.

Case I b is squarefree and $(a, b) = 1$. Suppose

$$a^{x_n} \equiv x_n \,(\mathrm{mod}\ b^n)\,,$$

for some $n \geq n(b)$. (Observe that we know this is true for $n = n(b)$ by Theorem 1 with $b = b^{n(b)}$). Then,

$$a^{x_n} \equiv x_n + c_n b^n \left(\mathrm{mod}\ b^{n+1}\right),$$

for some $0 \leq c_n < b$. Now, it is immediate to observe that for a valid basis it is always true that $\varphi(p^{n+1})|b^n$ for every integer $n \geq n(b)$ and every prime $p|b$. Hence, since $a^{\varphi(p^{n+1})} \equiv 1 \left(\mathrm{mod}\ p^{n+1}\right)$, we have, for every integer m

$$a^{mb^n} \equiv 1 \left(\mathrm{mod}\ b^{n+1}\right),$$

by the chinese remainder theorem. In particular

$$a^{x_n + c_n b^n} \equiv a^{x_n} \left(\mathrm{mod}\ b^{n+1}\right) \equiv x_n + c_n b^n \left(\mathrm{mod}\ b^{n+1}\right),$$

that is

$$a^{x_{n+1}} \equiv x_{n+1} \left(\mathrm{mod}\ b^{n+1}\right),$$

and the selection of c_n is unique.

Case II b is squarefree and $(a, b) > 1$. Let $b = b_1 b_2$ such that $(b_1, a) = 1$, and $b_2|a$. Again the proof proceed by induction, and we suppose

$$a^{x_n} \equiv x_n \left(\mathrm{mod}\ b^n\right) \equiv x_n + c_n b^n \left(\mathrm{mod}\ b^{n+1}\right), \tag{3}$$

for $n \geq n(b)$. In this case, and in the same way as before, we have for every integer m

$$a^{mb^n} \equiv 1 \left(\mathrm{mod}\ b_1^{n+1}\right),$$

since $(a, b_1) = 1$. In particular

$$a^{x_n + c_n b^n} \equiv a^{x_n} \left(\mathrm{mod}\ b_1^{n+1}\right) \equiv x_n + c_n b^n \left(\mathrm{mod}\ b_1^{n+1}\right).$$

On the other hand it is easy to see that $b_2^{n+1} | (a^{x_n + c_n b^n}, x_n + c_n b^n)$. Indeed, if $x_n \geq n + 1$, then trivially $b_2^{n+1} | a^{x_n + c_n b^n}$ and $b_2^{n+1} | (a^{x_n}, b^{n+1})$ and, hence, it divides $x_n + c_n b^n$ by (3). Furthermore, $x_n > 0$ and so, again by (3), we can see that $b_2^n | x_n$ and, in particular, $x_n \geq n + 1$. Hence,

$$a^{x_n + c_n b^n} \equiv x_n + c_n b^n \left(\mathrm{mod}\ b_2^{n+1}\right),$$

and the result follows by the chinese remainder theorem.

Case III b is not squarefree and $(a, b) = 1$. Let $b = \prod p^{v_p(b)} = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ where $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ and P_i are squarefree for $i = 1, \ldots, r$. We will also denote $B_j = \prod_{i=1}^{j-1} P_i^{\alpha_i}$, and $B_1 = 1$. Suppose again

$$a^{x_n} \equiv x_n \left(\mathrm{mod}\ b^n\right)$$

for some $n \geq n(b)$. Then

$$a^{x_n} \equiv x_n + c_{1,1,n} b^n \left(\mathrm{mod}\ P_1 b^n\right),$$

and $0 \leq c_{1,1,n} < P_1$. Again as before $\varphi(p^{n v_p(b)+1}) | b^n$ for any $n \geq n(b)$ and $p|P_1$ so, arguing as before, we get that for any integer m

$$a^{mb^n} \equiv 1 \left(\mathrm{mod}\ P_1 b^n\right).$$

In particular

$$a^{x_n + c_{1,1,n} b^n} \equiv a^{x_n} \left(\mathrm{mod}\ P_1 b^n\right) \equiv x_n + c_{1,1,n} b^n \left(\mathrm{mod}\ P_1 b^n\right).$$

Repeating this process, and noting that $\varphi(p^{nv_p(b)+i})|P_1^{i-1}b^n$ we get

$$a^{x_{n,1}} \equiv x_{n,1} \pmod{P_1^{\alpha_1} b^n}, \tag{4}$$

for a unique

$$x_{n,1} = x_n + \left(\sum_{i=0}^{\alpha_1 - 1} c_{i,1,n} P_1^i \right) b^n,$$

where $0 \leq c_{i,1,n} < P_1$. Now we just have to note that for any $1 \leq l \leq r$ and any $j_l < \alpha_l$ we have $\varphi(p^{nv_p(b)+j_l})|P_l^{j_l-1}B_l b^n$, to build, by iterating the previous process, a unique

$$x_{n+1} = x_n + \left(\sum_{j=1}^{r} \sum_{i=0}^{\alpha_j - 1} c_{i,j,n} P_j^i B_j \right) b^n,$$

where $c_{i,j,n} \leq P_j - 1$, such that

$$a^{x_{n+1}} \equiv x_{n+1} \left(\mathrm{mod}\ b^{n+1} \right).$$

Hence, since

$$\sum_{j=1}^{r} \sum_{i=0}^{\alpha_j - 1} c_{i,j,n} P_j^i B_j \leq \sum_{j=1}^{r} (P_j - 1) \sum_{i=0}^{\alpha_j - 1} P_j^i B_j = \sum_{j=1}^{r} (P_j^{\alpha_j} - 1) B_j = \sum_{j=1}^{r} (B_{j+1} - B_j) = b - 1,$$

the result follows.

Case IV b is not squarefree and $(a, b) > 1$. The proof is now the same as in Case II and we omit it.

Remark: It is very important to note that, whenever $n \geq n(b)$, even if the solution guaranteed by Theorem 1 is $x \geq b^n$, we can find another one $y < b^n$. Hence, for any integer $n \geq n(b)$ the integer x_n indeed gives the n first digits in base b of the integer x_m for every $m \geq n$. To see this, observe that if

$$a^x \equiv x \pmod{b^n},$$

and $x > b^n$, then $x = \sum_{i=0}^{n-1} c_i b^i + \sum_{i=n}^{k} c_i b^i = y + b^n Y$ for some $y \neq 0$, since otherwise a is a multiple of $s(b)$. But then,

$$y \equiv 0 \pmod{b_2^n},$$

since $a^x \equiv 0 \pmod{b_2^n}$ and $a^x \equiv y \pmod{b_2^n}$. But, then, $y \geq b_2^n \geq e(b_2)n$, and we also have

$$a^y \equiv 0 \equiv y \pmod{b_2^n}.$$

Finally, since $n \geq n(b)$, $a^{b^n} \equiv 1 \pmod{b_1^n}$, and so

$$a^y \equiv y \pmod{b_1^n}.$$

The chinese remainder theorem ends the result.

Corollary 5 *If b is a valid basis, for every integer a, not a multiple of $s(b)$, there exist one sequence $\{x_n\}_{n \geq 0}$ of digits $0 \leq x_n < b$ such that the integers*

$$x_n(a, b) = \sum_{i=0}^{n-1} x_i b^i = (x_{n-1} \ldots x_2\, x_1\, x_0)_b$$

verify

$$a^{x_n(a,b)} \equiv x_n(a,b) \,(mod\ b^n)\,,$$

for every $n \geq n(b)$. *When* b *is square free,* $s(b) = b$ *and this holds for every integer* a, *not a multiple of* b.

3 Other basis

As we mentioned in the introduction, Corollary 5 gives suffcient conditions for the basis b to ensure the existence of the sequence $x(a,b)$ for any nontrivial integer a. When b is not a valid basis, still this sequence $x(a,b)$ can appear for some integers a. Indeed, as we can see in the proof of Theorem 4, the only condition needed is that in fact, $a^{c_n b^n} \equiv 1 \,(\text{mod } b)^{n+1}$. This is true for any valid basis, but we can build many other examples for non valid basis. For example, consider an integer b and let $m|b-1$ such that $m^b \equiv -1 \,(\text{mod } b)$, and let $a = m^m$. Then it is easy to see by induction that $m^{b^r} \equiv -1 \,(\text{mod } b^r)$ for any r, and so

$$m a^{\frac{b-1}{m}\sum_{i=0}^{n-1} b^i} = m^{b^n} \equiv -1 \,(\text{mod } b^n)\,.$$

On the other hand

$$m\left(\frac{b-1}{m}\right)\sum_{i=0}^{n-1} b^i = b^n - 1 \equiv -1 \,(\text{mod } b^n)\,,$$

and so $x(a,b) = \overline{\left(\frac{b-1}{m}\right)}_b$ is the desired sequence to the equation $a^{x_n} \equiv x_n \,(\text{mod } b^n)$. The example at the end of the introduction, $x(4,9) = \bar{4}_9$, is a particular case of this example with $m = 2$, $b = 9$. Also this framework allow us to prove the following simple example as a corollary.

Theorem 6 *Let* $b > 1$ *an odd integer and* $a = (b-1)^{b-1}$. *Then*

$$a^{x_n} \equiv x_n \,(mod\ b^n)\,,$$

for any n *and* $x_n = \sum_{i=0}^{n-1} b^i$. *In other words,* $x(a,b) = \bar{1}_b$.

Acknowledgment. This work was done while the first author was visiting CRM at Montreal, and he wishes to thank this institute for its hospitality. Also he wants to thank M. C. Muñoz Lecanda.