Journal of Integer Sequences, Vol. 12 (2009),
Article 09.8.8

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

J. Jiménez Urroz and J. Luis A. Yebra
Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Campus Nord, Edifici C3
C. Jordi Girona, 1-3
08034 Barcelona
Spain
jjimenez@ma4.upc.edu
yebra@ma4.upc.edu

Abstract

We study the solutions of the equation $a^x \equiv x \pmod{b^n}$. For some values of b, the solutions have a particularly rich structure. For example, for $b = 10$ we find that for every a that 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 arise from a sequence $x(a) = \{x_i\}_{i\geq 0}$, in the form $x_n(a) = \sum_{i=0}^{n-1} x_i 10^i$. For instance, for $a = 8$ we obtain

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

In this paper we prove these results and provide sufficient conditions for the base b to have analogous properties.

1 Introduction

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

$$7^{6306806373338536433312655115651723 43} = \cdots 630680637333853643331265511565172343,$$

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

$$12^{523963591358485849317144214540124 16} = \cdots 523963591358485849317144214540124 16.$$

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

$$x(a) = \cdots\, x_i \cdots x_2\, x_1\, x_0$$

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

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

is the only such number that satisfies

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

Moreover, this result holds not just for base $b = 10$; an analogous result holds when b is squarefree and such that for every prime $p|b$ and every prime $q|p-1$ we have $q|b$.

For any positive integer a, not a multiple of b, there exists an infinite sequence of b-digits,

$$x(a,b) = (\cdots\, x_i \cdots x_2\, x_1\, x_0)_b$$

such that for every $n \geq n(b)$, which is characterized below, the number

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

satisfies

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

For instance, for $b = 6$ and $a = 4$ we have

$$x(4,6) = \cdots 32112014504555423255404350553541104531046_6,$$

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

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

When the base b is not squarefree, instead of multiples of b, we must 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 at least one such sequence $x(a,b)$, but they are not necessary. It might be the case that for some other base b and some value of a there exist a sequence $x(a,b)$ as above. As an example we have for $b = 9$ and $a = 4$ the sequence $x(4,9) = \cdots 4444444_9$.

2 Main results

We only use elementary number theory and refer to Hardy and Wright [1] or Riesel [2] for any concept not defined here. We will write the prime factorization of an integer b as $b = \prod_p p^{v_p(b)}$, and denote by $e(b) = \max_{p|b}\{v_p(b)\}$, 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*

$$a^x \equiv x \pmod{b}.$$

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*

$$a^x \equiv x \pmod{\varphi(b)}.$$

Then

$$a^{a^x} \equiv a^x \pmod{b}.$$

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

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

On the other hand, we trivially have

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

The result now follows from 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 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 $a > 1$ and $x \geq 0$, we get $a^x \geq x + 1 \geq e(b) + 1$, as desired.

Definition: We say that an integer b is a *valid base* 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 $p|b$.

Remarks: The existence of such an integer $n(b)$ is clear from the definition of valid base. It is straightforward to see that a valid base b must be even. It is also easy to see that $b = 2, 4, 6, 8, 10, 12, 16, 18, 20, 24$, and 30 are the first valid bases while $b = 2, 6, 10, 30, 34, 42, 78, 102$ and 110 are the first valid squarefree bases. Observe also that when b is squarefree, $n(b) = \max_{p|b}\{\max_{q|b}\{v_q(p-1)\}\}$. Thus, we have $n(10) = 2$ and $n(34) = 4$, while $n(100) = 1$.

Apart from the bases given in this Remark, one can ask whether there exist other valid bases and how to find them. The following list provides different ways of constructing new valid bases. In particular we note the existence of infinitely many valid bases.

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

The first two statements are direct consequences of the definition. For the third and fourth we just have to note that if $p|b$ and $q|p-1$, then $q \le m$ in the third statement, while $q \le r$ in the last one.

The main result, where we denote the number $x_n(a, b)$ by x_n for short, follows.

Theorem 3. *Let b be a valid base, and $s(b)$ its squarefree part. Then, for every integer a not a multiple of $s(b)$ there exist a unique sequence $\{c_n\}_{n \ge n_b}$ of digits, $0 \le c_n < b$, such that the integers $x_{n+1} = x_n + c_n b^n$ verify*

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

for every $n > n(b)$.

Proof: To clarify the argument, we first present the case when b is a squarefree integer. In all the cases below, we will proceed by induction on n.

Case I: b is squarefree and $\gcd(a, b) = 1$.

Suppose that for some $n \ge n(b)$

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

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

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

for some $0 \le c_n < b$. Now, it is immediate to observe that for a valid base it is always true that $\varphi(p^{n+1})|b^n$ for every integer $n \ge n(b)$ 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

$$a^{x_n+c_nb^n} \equiv a^{x_n} \left(\bmod\ b^{n+1}\right) \equiv x_n + c_nb^n \left(\bmod\ b^{n+1}\right),$$

that is

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

and the selection of c_n is unique.

Case II: b is squarefree and $\gcd(a,b) > 1$.

Let $b = b_1b_2$ be such that $\gcd(b_1, a) = 1$, and $b_2|a$. Again the proof proceeds by induction, and we suppose

$$a^{x_n} \equiv x_n \,(\bmod\ b^n) \equiv x_n + c_nb^n \left(\bmod\ b^{n+1}\right), \tag{3}$$

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

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

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

$$a^{x_n+c_nb^n} \equiv a^{x_n} \left(\bmod\ b_1^{n+1}\right) \equiv x_n + c_nb^n \left(\bmod\ b_1^{n+1}\right).$$

On the other hand, it is easy to see that $b_2^{n+1} | \gcd(a^{x_n+c_nb^n}, x_n + c_nb^n)$. Indeed, if $x_n \geq n+1$ then trivially $b_2^{n+1}|a^{x_n+c_nb^n}$ and $b_2^{n+1}| \gcd(a^{x_n}, b^{n+1})$. Hence, b_2^{n+1} divides $x_n + c_nb^n$ 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,

$$a^{x_n+c_nb^n} \equiv x_n + c_nb^n \left(\bmod\ b_2^{n+1}\right),$$

and the result follows from the Chinese Remainder Theorem.

Case III: b is not squarefree and $\gcd(a,b) = 1$.

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

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

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

$$a^{x_n} \equiv x_n + c_{1,1,n}b^n \,(\bmod\ P_1b^n),$$

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

$$a^{mb^n} \equiv 1 \,(\bmod\ P_1b^n).$$

In particular,

$$a^{x_n+c_{1,1,n}b^n} \equiv a^{x_n} \,(\bmod\ P_1b^n) \equiv x_n + c_{1,1,n}b^n \,(\bmod\ P_1b^n).$$

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

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

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 $\varphi(p^{nv_p(b)+j_l}) | P_l^{j_l - 1} B_l b^n$. By iterating the previous process, we can then build 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

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

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 $\gcd(a, b) > 1$.
The proof is now the same as in Case II and we omit it.

Remark: It is very important to notice 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

$$a^x \equiv x \left(\text{mod } b^n \right),$$

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,

$$y \equiv 0 \left(\text{mod } b_2^n \right),$$

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

$$a^y \equiv 0 \equiv y \left(\text{mod } b_2^n \right).$$

Finally, since $n \geq n(b)$, $a^{b^n} \equiv 1 \left(\text{mod } b_1^n \right)$, and so

$$a^y \equiv y \left(\text{mod } b_1^n \right).$$

The result is now a consequence of the Chinese Remainder Theorem.

Besides, it is easily verified that when $b = 10$ there is just one solution $y < 10^{n(10)} = 100$ for every a (not a multiple of 10), since it suffices to check values of a mod 100. Thus there is a unique sequence $x(a)$ for every a. Although this seems to be the case for all valid bases b, it does not follow from Theorem 1.

Corollary 4. *If b is a valid base, for every integer a, not a multiple of $s(b)$, there exist a sequence $\{x_n\}_{n\geq 0}$ of digits $0 \leq x_n < b$ such that the integers*

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

verify

$$a^{x_n(a,b)} \equiv x_n(a,b) \pmod{b^n}, \tag{2}$$

for every $n \geq n(b)$. When b is squarefree, $s(b) = b$ and this holds for every integer a, not a multiple of b. For $b = 10$ there exists just one such sequence $x(a)$.

3 Other bases

As we mentioned in the introduction, Corollary 4 uses sufficient conditions for the base b to ensure the existence of a sequence $x(a,b)$ for any nontrivial integer a. When b is not a valid base, however, a sequence $x(a,b)$ can still appear for some integers a. Indeed, as we can see in the proof of Theorem 3, the only condition needed is that $a^{c_n b^n} \equiv 1 \,(\mathrm{mod}\ b^{n+1})$ holds. This is true for any valid base, but we can build many other examples for invalid bases. For example, consider an integer b and let $m|b-1$ such that $m^b \equiv -1 \,(\mathrm{mod}\ b)$, and let $a = m^m$. Then it is easy to see by induction that $m^{b^r} \equiv -1 \,(\mathrm{mod}\ b^r)$ for any r, and so

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

On the other hand

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

and so $x(a,b) = \overline{\left(\frac{b-1}{m}\right)}_b$ is the desired sequence which provides a solution to the equation $a^{x_n} \equiv x_n \,(\mathrm{mod}\ b^n)$ for every 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 allows us to prove the following simple example

Corollary 5. *Let $b > 1$ an odd integer and $a = (b-1)^{b-1}$. Then*

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

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

4 Acknowledgments

This work was partially supported by Secretaría de Estado de Universidades e Investigación del Ministerio de Educación y Ciencia of Spain, DGICYT through grants MTM2006-15038-C02-02, TSI2006-02731 and MTM2009-11068 for the first author and TEC2005-03575 for the second author. It was done while the first author was visiting CRM at Montreal, and he wishes to thank this institute for its hospitality. Finally, the authors want to thank M. C. Muñoz Lecanda.

References

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 2008.

[2] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhauser, 1994.

2000 *Mathematics Subject Classification*: Primary 11A07.
Keywords: exponential, congruences, integer sequences.

(Concerned with sequences A133612, A133613, A133614, A133615, A133616, A133617, A133618, A133619, A144539, A144540, A144541, A144542, A144543, A144544, A151999, and A152000.)

Received June 10 2009; revised version received November 18 2009. Published in *Journal of Integer Sequences*, November 25 2009.

Return to Journal of Integer Sequences home page.