Rapport BIPM-95/6

On the divisibility of powers of integers

by Jörg W. Müller

Bureau International des Poids et Mesures, F-92312 Sèvres Cedex

Abstract

We examine the residues obtained when powers of integers are divided by the square of the exponent. For a given value n of the exponent, the residues exhibit a striking pattern which is discussed for $n \leq 16$.

1. Introduction

The surprising observation that the fourth power of any integer N is either an exact multiple of 16 or exceeds such a value by one unit, i.e. that (for k = 0, 1, 2, ...)

$$N^4 = 16 \cdot k + 0 \text{ or } 1 ,$$

naturally leads to the question of whether there exist similar simple relationships for powers in general.

Problems of divisibility are a basic topic in number theory and they have produced a rich literature. It may nevertheless happen that some of the relationships concerning residue classes of powers of natural numbers considered in what follows are new.

Let us have a look at the residues (mod n^2) of expressions of the type N^n, where both N and n are natural numbers. To illustrate our approach, we first consider the two special cases where the exponents are n = 2 and n = 3, before discussing the problem in general.

2. Two special cases

For the case n = 2 we choose for N the decomposition

$$N = 2k + r ,$$

where r = 0 or 1.

Since

$$N^2 = 4k^2 + 4k\, r + r^2 ,$$

we have

$$N^2 = r^2 = 0 \text{ or } 1 \pmod 4 . \qquad (1)$$

It follows from (1) that for any square N^2 we have the relation

$$N^2 = 0 \text{ or } 1 \pmod 4 .$$

In the same way, for n = 3 we write

$$N = 3k + r ,$$

with $r = 0, \pm 1$.

It is then clear that

$$N^3 = (3k + r)^3 = 27\, k^3 + 27\, k^2\, r + 9\, k\, r^2 + r^3 ,$$

thus

$$N^3 = r^3 = 0, 1 \text{ or } -1 \pmod 9 . \qquad (2)$$

Negative residuals are used for convenience and, in particular, to avoid large numbers. Thus

$$N = -\alpha \pmod m$$

is always equivalent to

$$N = m - \alpha \pmod m .$$

3. The general case

For the general case, it may be useful to discuss separately the cases of an even or odd power n.

a) For n odd, say $n = 2s + 1$, with $s = 0, 1, \ldots$, we write the integers N in the form

$$N = nk + r ,$$

with $r = 0, \pm 1, \pm 2, \ldots, \pm s$.

Then

$$N^n = (nk + r)^n$$

$$= (nk)^n + n\, (nk)^{n-1}\, r + \ldots + n\, (nk)^1\, r^{n-1} + r^n .$$

By taking this modulo n^2 we find

$$N^n = 0 + r^n \pmod{n^2}$$

$$= (0, \pm 1, \pm 2^n, \ldots, \pm s^n) \pmod{n^2}. \qquad (3)$$

The possible residues resulting from (3) are listed in Table 1.

Table 1 - The residues occurring in (3), for n odd.

n	r^n						$R = r^n \pmod{n^2}$					
1	0						0					
3	0,	± 1					0,	± 1				
5	0,	± 1,	$\pm 2^n$				0,	± 1,	± 7			
7	0,	± 1,	$\pm 2^n$,	$\pm 3^n$			0,	± 1,	± 18,	± 19		
9	0,	± 1,	$\pm 2^n$,	$\pm 3^n$,	$\pm 4^n$		0,	± 1,	± 26,	± 28		
11	0,	± 1,	$\pm 2^n$,	$\pm 3^n$,	$\pm 4^n$,	$\pm 5^n$	0,	± 1,	± 3,	± 9,	± 27,	± 40

b) For <u>n even</u>, say $n = 2s$, the integers N are again written as

$$N = nk + r,$$

with $r = 0, \pm 1, \pm 2, \ldots, \pm(s-1), +s$.

This yields for the power n as before

$$N^n = (nk + r)^n = (nk)^n + \ldots + r^n,$$

thus modulo n^2 becomes

$$N^n = r^n \pmod{n^2}$$

$$= (0, 1, 2^n, \ldots, s^n) \pmod{n^2}. \qquad (4)$$

For even powers n we are led to the residues given in Table 2.

Table 2 - The residues occurring in (4), for n even.

n	r^n							$R = r^n \pmod{n^2}$				
2	0,	1						0,	1			
4	0,	1,	2^n					0,	1			
6	0,	1,	2^n,	3^n				0,	1,	-8,	9	
8	0,	1,	2^n,	3^n,	4^n			0,	1,	33		
10	0,	1,	2^n,	3^n,	4^n,	5^n		0,	1,	25,	± 24,	49
12	0,	1,	2^n,	3^n,	4^n,	5^n,	6^n	0,	1,	-63,	64	

From the above it follows that, for n even or n odd, we have the general relation

$$N^n = R \pmod{n^2}, \tag{5}$$

with the values of R given (for $n \leq 12$) in Tables 1 and 2.

4. Some complements

For a more detailed insight, the residues R do not only have to be known globally for a given exponent n, as presented in Tables 1 and 2, but their association with the specific values of N must also be given. Since the residues R have a particular structure with period n, it is sufficient to list them for the n possible values of m = N (mod n). This has been done in Table 3 (for $n \leq 16$).

Table 3 - List of the residues R = R(n,m) for the powers N^n, with N = m (mod n). Values not listed for m are zero.

	m=1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n=2	1														
3	1	-1													
4	1	0	1												
5	1	7	-7	-1											
6	1	-8	9	-8	1										
7	1	-19	-18	18	19	-1									
8	1	0	33	0	33	0	1								
9	1	26	0	28	-28	0	-26	-1							
10	1	24	49	-24	25	-24	49	24	1						
11	1	-9	3	-40	27	-27	40	-3	9	-1					
12	1	64	-63	64	1	0	1	64	-63	64	1				
13	1	80	-23	-22	70	19	-19	-70	22	23	-80	-1			
14	1	-80	-19	-68	-31	-48	49	-48	-31	-68	-19	-80	1		
15	1	-82	-18	-26	-100	-99	-107	107	99	100	26	18	82	-1	
16	1	0	65	0	-63	0	129	0	129	0	-63	0	65	0	1

A closer look at this tabulation reveals some interesting symmetries. Thus, it is readily seen that

$$\begin{aligned} R(n,m) &= R(n,n-m), \quad \text{for n even, and} \\ R(n,m) &= -R(n,n-m), \quad \text{for n odd,} \end{aligned} \tag{6}$$

with $m \leq n/2$.

Exact divisibility ($R = 0$) occurs only for exponents n which are of the form

$$n = c\,h^2 , \tag{7}$$

where $c \geq 1$ and $h \geq 2$.

Then $R(n,m_0) = 0$ if m_0 is a multiple of c h (below n).

This may be illustrated by the following examples:

If $n = 8 = 1\cdot 2^3$, then $m_0 = 2,\ 2\cdot 2$ or $3\cdot 2$;
if $n = 9 = 1\cdot 3^2$, then $m_0 = 3$ or $2\cdot 3$;
if $n = 12 = 3\cdot 2^2$, then $m_0 = 3\cdot 2$.

However, many other features of Table 3 remain mysterious, such as the occurrence of the sequences -8, 9, -8 (for n = 6), -24, 25, -24 (for n = 10) or 64, -63, 64 (for n = 12).

In addition, many of the equivalences given above can apparently be simplified. Thus, for n = 2, 3 and 4 we have, for example, the relations

$$\begin{aligned} N^2 \ (\mathrm{mod}\ 4) &= N^2 \ (\mathrm{mod}\ 2) = N \ (\mathrm{mod}\ 2) , \\ N^3 \ (\mathrm{mod}\ 9) &= N^3 \ (\mathrm{mod}\ 3) = N \ (\mathrm{mod}\ 3) , \\ N^4 \ (\mathrm{mod}\ 16) &= N^4 \ (\mathrm{mod}\ 4) = N \ (\mathrm{mod}\ 2) , \end{aligned} \tag{8}$$

if we agree systematically to use negative residues when $r > n/2$.

The general rules applicable to decompositions similar to (8), however, are not known to the author.

(July 1995)