ON m-TIC RESIDUES MODULO n

JOHN H. E. COHN
London, N. W., England

1. INTRODUCTION

The object of this paper is to investigate the values of the residues modulo n of x^m, where $0 \le x \le (n-1)$, and in particular for the case $n = m$. We shall define

$$\Sigma(n;m) = \{x^m \pmod{n} \mid 0 \le x \le (n-1)\}$$

and

$$\Phi(n;m) = \{x^m \pmod{n} \mid 1 \le x \le (n-1),\ (n,x) = 1\}$$

Clearly $\Phi(n;m)$ is a subset of $\Sigma(n;m)$. We shall use the symbol $\phi(n;m)$ to denote the number of distinct elements of $\Phi(n;m)$. Also whenever there is no risk of confusion we shall omit the symbol (mod n). We shall prove certain theorems which will enable the work of computing $\Sigma(n;m)$ to be reduced considerably, and conclude with a table of $\Sigma(n;n)$.

2. PROPERTIES OF $\Phi(n;m)$

Theorem 1. $\Sigma(n;m) = \{xy^m \mid x \in \Phi(n;m),\ y|n\}$

Proof. Suppose $z \in \Sigma(n;m)$. Then $z \equiv d^m \pmod{n}$. Now let $y = (n,d)$. Then $d = cy$, $(n,c) = 1$, $y\ n$. Hence $s = xy^m$, where $x = c^m \in \Phi(n;m)$. This concludes the proof of the theorem. In view of it, and the fact that for several reasons $\Phi(n;m)$ is rather easier to deal with, we shall first consider the properties of $\Phi(n;m)$.

In the first place, we shall define the integer $1(n)$ for $n \ge 2$, as follows

(i) if $n = p^r$, where p is an odd prime and $r > 1$, then $1(n) = p^{r-1}(p-1)$

(ii) if $n = 2^r$, then $1(n) = 2^{r-1}$ if $r = 1, 2$ and $1(n) = 2^{r-2}$ if $r \ge 3$.

(iii) if

(Received Jan., 1965)

$$n = \prod_{i=1}^{N} p_i^{r_i} ,$$

then

$$1(n) = \text{l. c. m.} \{1(p_i^{r_i})\}, \quad t = 1, 2, \cdots, N .$$

Then we have

<u>Theorem 2.</u> If

$$k = (m, 1(n)),$$

then if $k \neq 1(n)$,

$$\Phi(n;m) = \Phi(n;k) ,$$

whereas if $k = 1(n)$, then $\Phi(n;m) = \{1\}$.

<u>Proof.</u>

$$\Phi(n;1) = \{x | (n,x) = 1\}$$

is a multiplicative Abelian Group whose structure is known

$$\Phi(n;1) = \begin{matrix} C_{1(p_1^{r_1})} \times C_{1(p_2^{r_2})} \times \cdots \times C_{1(p_n^{r_n})} & \text{if } 8 \nmid n \\ C_{1(p_1^{r_1})} \times C_{1(p_2^{r_2})} \times \cdots \times C_{1(p_n^{r_n})} \quad C_2 & \text{if } 8 | n \end{matrix}$$

Now

$$1(n) = \text{l. c. m.} \{1 (p_1^{r_1})\}$$

and so

$$\Phi(n;1(n)) = \{1\} ,$$

and clearly $1(n)$ is the least integer for which this is true. Thus we have

$$x^{1(n)} \equiv 1 \pmod n$$

if

$$(n, x) = 1 .$$

Now if

$$k = 1(n) = (m, 1(n)),$$

then

$$1(n) | m ,$$

and so whenever $(n,x) = 1$, $x^m \equiv 1 \pmod{n}$, i.e., $\Phi(n;m) = \{1\}$.

Secondly, if $(m, (n)) = k$ where $0 \le k \le l(n)$, then there exist integers a, b, c such that

$$m = ak \quad \text{and} \quad k = bm - cl(n) .$$

Hence if $(n,x) = 1$ we have

$$x^m = x^{ak} \equiv (x^a)^k \pmod{n}$$

and so

$$\Phi(n;m) \subset \Phi(n;k)$$

Also,

$$x^k = x^{bm-cl(n)} \equiv x^{bm} \pmod{n}$$
$$\equiv (x^b)^m, \pmod{n}$$

Thus

$$\Phi(n;k) \subset \Phi(n;m) ,$$

and so by our previous result

$$\Phi(n;k) = \Phi(n;m) .$$

Hence in considering $\Phi(n;m)$ we need only consider values of m which are divisors of $l(n)$.

3. PROPERTIES OF $\Sigma(n;m)$

<u>Theorem 3.</u> if

$$x \equiv y \pmod{n}$$

and $a \mid n$, then

$$x^a \equiv y^a \pmod{an} .$$

<u>Proof.</u> Let

$$x = y + cn .$$

Then

$$x^a = (y + cn)^a$$
$$= y^a + acny^{a-1} + \cdots +$$
$$+ a(cn)^{a-1}y + (cn)^a$$
$$\equiv y^a \pmod{an} \text{ since } a \mid n .$$

This concludes the proof. A simple induction argument now shows that for any r, if $x \equiv y \pmod n$ and $a|n$ then

$$x^{a^r} \equiv y^{a^r} \pmod{a^r n}$$

and this gives immediately

Theorem 4.

$$\Sigma(a^r n;\ a^r m) = \{ x^{a^r} \pmod{a^r n} \mid x \in \Sigma(n;m)\}$$

where a is any factor of n.

Theorem 5. If n is square-free, and if $\Phi(n;m) = \Phi(n;1)$, then $\Sigma(n;m) = \Sigma(n;1)$, for by Theorem 1,

$$\begin{aligned}\Sigma(n;m) &= \{xy^m \mid x \in \Phi(n;m),\ \ y|n\} \\ &= \{xy^m \mid (n,x) = 1,\ \ y|n\}\end{aligned}$$

Now consider any prime factor p of n. Since n is square free $(p^m, n) = p$ and so there exist integers a, b such that

$$\begin{aligned} p &= ap^m + bn \\ &\equiv ap^m \pmod n \ \text{ and so } (n,a) = 1 \text{ or } p\end{aligned}$$

Now if $(n,a) = p$ then let $a' = a + n/p$. Then $(n,a') = 1$ and $p \equiv a'p^m$ (mod n). Hence $p \in \Sigma(n;m)$, and so every prime factor belongs to $\Sigma(n;m)$. Hence if m is any number between 1 and $(n - 1)$

$$z = c\prod_1^N p_i^{s_i}$$

where $(c,n) = 1$ and the p_i are prime factors of n. Hence $z \equiv a^m \pmod n$. This concludes the proof, since clearly $0 \in \Sigma(n;m)$.

Theorem 6. If $k = (m, l(n))$ then if

$$n = \prod_{i=1}^N p_i^{r_i}$$

$$\phi(n;m) = \begin{cases} \prod_{i=1}^{N} \dfrac{l(p_i^{r_i})}{(k, l(p_i^{r_i}))} & \text{unless } 8 \mid n \text{ and } m \text{ is odd} \\ 2\prod_{i=1}^{N} \dfrac{l(p_i^{r_i})}{(k, l(p_i^{r_i}))} & \text{if } 8 \mid n \text{ and } m \text{ is odd .} \end{cases}$$

For, $(n;m) = \phi(n;k)$ and the result follows from the structure of $\Phi(n;1)$, since when s n, k is odd if and only if m is odd.

4. PROPERTIES OF $\Sigma(n;n)$

Theorem 7. $\Sigma(n;n) = \{0, 1, 2, \cdots, (n-1)\}$ if and only if $(n, l(n)) = 1$.

Proof. (i) If $\Sigma(n;n) = \{0, 1, 2, \cdots, (n-1)\}$ then $\Phi(n;n) = \Phi(n;1)$ and so by Theorem 6 $(n, l(n)) = 1$.

(ii) If $(n, l(n)) = 1$ then by Theorem 2 $\Phi(n;n) = \Phi(n;1)$ and so by Theorem 5, $\Sigma(n;n) = \Sigma(n;1)$ since n must be square-free to make $(n, l(n)) = 1$.

Theorem 8. If $l(n) \mid n$, then $\Sigma(n;n) = \{x^n \mid x \mid n\}$. This follows immediately from Theorems 1 and 2.

Theorem 9. (i) if $n = 2^r$, then $\Sigma(n;n) = \{0, 1\}$

(ii) if $n = 3^r$, then $\Sigma(n;n) = \{0, 1, n-1\}$

(iii) if $n = p^r$, where p is an odd prime then $\Sigma(n;n)$ consists of the p different elements $0, \pm 1, \pm 2^t, \cdots, \pm\{\frac{1}{2}(p-1)\}^t$ where $t = p^{r-1}$.

Proof. (i) if $n = 2^r$, then since $\Sigma(2;2) = \{0, 1\}$, the result follows by Theorem 4.

(ii) if $n = 3^r$, then since $\Sigma(3;3) = \{0, 1, 2\}$ or equivalently $\{0, 1, -1\}$ it follows by Theorem 4 that $\Sigma(n;n) = \{0, 1, n-1\}$.

(iii) if $n = p^r$, then since $l(p) = p - 1$, $(p, l(p)) = 1$ and so by Theorem 7, $\Sigma(p;p) = \{0, 1, 2, \cdots, (p-1)\}$ or equivalently, $\{0, \pm 1, \pm 2, \cdots, \pm\frac{1}{2}(p-1)\}$. Hence by Theorem 4,

$$\Sigma(n;n) = \{0, \pm 1, \pm 2^t, \cdots, \pm\{\tfrac{1}{2}(p-1)\}^t\} \qquad t = p^{r-1}$$

It merely remains to show that all these p elements are distinct. Now $n = p^r$, $l(n) = p^{r-1}(p-1)$, $k = (n, l(n)) = p^{r-1}$. Hence by Theorem 6, $\phi(n;n) = p - 1$.

Hence the elements $\pm 1, \pm 2^t, \cdots, \pm \frac{1}{2}(p-1)^t$ are all distinct, and clearly they are all distinct from 0. This concludes the proof.

Theorem 10. If $n = 2p$, p an odd prime, then

$$\Sigma(n;n) = \{0, p, q, q + p \mid (q|p) = +1\}$$

Proof. $l(n) = p - 1$, and so $k = (n, l(n)) = 2$. Hence

$$\Phi(n;n) = \Phi(n;2) = \{x^2 \mid (z,x) = 1\} ,$$

by Theorem 2. Hence by Theorem 1,

$$\Sigma(n;n) = \{ay^n \mid s \in \Phi(n;2), \quad y = 0, 1, 2, p\}$$

Now $y = 0$ gives only the element 0, and since must always be odd, $y = p$ gives only the element p. Also,

$$2^p \equiv 2 \pmod 2$$

and

$$2^p \equiv 2 \pmod p$$

hence

$$2^p \equiv 2 \pmod n$$

hence

$$2^n \equiv 4 \pmod n$$

Thus

$$\Sigma(n;n) = \{0, p, z, 4z \mid z \in \Phi(n;2)\}$$

Now

$$z = x^2$$

where

$$(n, x) = (p, x) = 1$$

and

$$4z = (2x)^2 = y^2 \pmod{n}$$

where

$$(y, n) = (2x, 2p) = 2 .$$

Hence

$$\Sigma(n;n) = \{0, p, x^2 \mid (x, p) = 1\}$$

For each element of the form x^2 there are now two possibilities.

(i) $0 < x^2 \pmod{n} < p$. Then $x^2 \equiv q$ where $0 < q < p$, $(q|p) = +1$

(ii) $p < x^2 \pmod{n} < 2p$.

Then

$$\begin{aligned}(x + p)^2 &= x^2 + 2px + p^2 \\ &\equiv x^2 - p \pmod{n}\end{aligned}$$

Hence

$$x^2 \equiv p + q \pmod{n}$$

where

$$0 < q < p \text{ and } (q|p) = +1$$

This concludes the proof.

<u>Theorem 11.</u> If $n = 2p^r$ where p is an odd prime, then

$$\Sigma(n;n) = \{0, p^r, q^t, p^r + q^t \mid t = p^{r-1}, 0 < q < p, (q|p) = +1\}$$

<u>Proof.</u> For each p, we shall prove the result by induction on r. By the previous theorem, the result is true for $r = 1$. Now suppose that it is true for $r = R$. Thus

$$\Sigma(2p^R;2p^R) = \{0, p^R, q^t, q^t + p^R\} \text{ where } t = p^R$$

Hence by Theorem 4,

$$\Sigma(2p^{R+1};2p^{R+1}) = \{x^p \mid x \in \Sigma(2p^R; 2p^R)\}$$

Now $x = 0$ gives $x^p = 0$ and $x = p^R$ gives

$$\begin{aligned} x^p &= p^{pR} \\ &= p^{R+1}(p^{pR-R-1} - 1) + p^{R+1} \\ &\equiv p^{R+1} \quad (\text{mod } n) \end{aligned}$$

$x = q^t$ gives

$$x^p = q^{tp} = q^T \quad \text{where } R = pt = p^{R+1}$$

$x = q^t + p^R$ gives

$$\begin{aligned} x^p &= (q^t + p^R)^p \\ &= q^T + q^{t(p-1)}p^{R+1} + q^{t(p-2)}p^{2R+1}\binom{p-1}{2} \\ &\quad + \cdots + q^t p^{R(p-1)+1} + p^{Rp} \\ &\equiv q^T \quad (\text{mod } p^{R+1}) \\ &\equiv q^T + p^{R+1} \quad (\text{mod } p^{R+1}) \end{aligned}$$

Also $$x^p \equiv q^T + p^{R+1} \quad (\text{mod } 2)$$

for if x is even, q is odd and vice-versa.

Hence

$$x^p \equiv q^T + p^{R+1} \quad (\text{mod } n)\ .$$

This concludes the proof, and gives, for example,

$$\Sigma(2 \cdot 3^r; 2 \cdot 3^r) = \{0, 1, 3^r, 3^r + 1\}$$

$$\Sigma(2 \cdot 5^r; 2 \cdot 5^r) = \{0, 1, 5^r - 1, 5^r, 5^r + 1, 2 \cdot 5^r - 1\}$$

<u>Theorem 12.</u> If $n = 4p$, where p is an odd prime, then

(i) if $p \equiv 3 \pmod 4$, $\Sigma(n;n) = \{x^2 \mid x = 0, 1, 2, \cdots, p\}$

(ii) if $p \equiv 1 \pmod 4$,

$$\Sigma(n;n) = \{x^2 \mid x = 0,\ p,\ q \text{ where } 0 < q < p,\ (q|p) = +1\}$$

Proof. By Theorem 4,

$$\Sigma(n;n) = \{x^2 \mid x \in \Sigma(2p;2p)\},$$

and so by Theorem 10,

$$\Sigma(n;n) = \{x^2 \mid x = 0,\ p,\ q,\ q + p\ ,$$

where $$0 \le q \le p \text{ and } (q|p) = +1\}$$

(i) if $p \equiv 3 \pmod 4$ then $(-1|p) = -1$ and so q takes exactly half of the values $1, 2, \cdots, (p - 1)$ and the other half are of the form $p - q$. Now

$$(q + p)^2 - (p - q)^2 = 4pq \equiv 0 \pmod n$$

Hence in this case

$$\Sigma(n;n) = \{x^2 \mid x = 0, 1, 2, \cdots, p\}$$

(ii) if $p \equiv 1 \pmod 4$ then $(-1|p) = +1$ and so q takes half the values $1, 2, \cdots, (p - 1)$, these same values being of the form $(p - q)$ and again

$$(q + p)^2 \equiv (p - q)^2 \pmod n$$

Hence

$$\Sigma(n;n) = \{x^2 \mid x = 0, p, q, \text{ where } 0 \le q \le p \text{ and } (q|p) = +1\}$$

This concludes the proof.

Theorem 13. If $1(n)|n$ and if $n = rs$ where $(r, s) = 1$ and if $R \equiv r^n \pmod n$ and $S \equiv s^n \pmod n$ are elements of $\Sigma(n;n)$ then $R + S \equiv 1 \pmod n$.

Proof. Since $1(n)|n$, it follows from Theorem 2 that $\Phi(n;n) = \{1\}$.

Since $n = rs$ and $(r, s) = 1$, $(n, r + s) = 1$ and so

$$(r + s)^n \equiv 1 \pmod{n} .$$

Now each of r and s is a factor of $(r + s)^n - r^n - s^n$ and so since r and s have no factor in common and $n = rs$,

$$(r + s)^n \equiv r^n + s^n \pmod{n}$$
$$\equiv R + s \pmod{n}$$

Hence by the above remark,

$$R + S \equiv 1 \pmod{n} .$$

5. TABLES OF $\Sigma(n;n)$

Our theorems enable us to compute tables of $\Sigma(n;n)$ fairly easily, at least in the cases that n can be factorized into fairly small factors. By Theorem 7, $\Sigma(n;n)$ consists of all the residues when n is a prime, and so there is no need to calculate the residues in this case. Also it is clear that the elements 0 and 1 always belong to $\Sigma(n;n)$. We give a table; giving $\Sigma(n;n)$ for all values other than primes up to $n = 100$ and also for a few easily calculable values between 100 and 1000.

n	$\Sigma(n;n)$ contains 0, 1, and
4	no others
6	3, 4
8	no others
9	8
10	4, 5, 6, 9
12	4, 9
14	2, 4, 7, 8, 9, 11
15	all residues
16	no others

18	9, 10
20	5, 16
21	6, 7, 8, 13, 14, 15, 20
22	3, 4, 5, 9, 11, 12, 14, 15, 16, 20
24	9, 16
25	7, 18, 24
26	3, 4, 9, 10, 12, 13, 14, 16, 17, 22, 23, 25
27	26
28	4, 8, 9, 16, 21, 25
30	4, 6, 9, 10, 15, 16, 19, 21, 24, 25
32	no others
33	all residues
34	2, 4, 8, 9, 13, 15, 16, 17, 18, 19, 21, 25, 26, 30, 32, 33
35	all residues
36	9, 28
38	4, 5, 6, 7, 9, 11, 16, 17, 19, 20, 23, 24, 25, 26, 28, 30, 35, 36
39	5, 8, 12, 13, 14, 18, 21, 25, 26, 27, 31, 34, 38
40	16, 25
42	7, 15, 21, 22, 28, 36
44	4, 5, 9, 12, 16, 25, 33, 36, 37
45	8, 9, 10, 17, 18, 19, 26, 27, 28, 35, 37, 37, 44
46	2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 23, 24, 25, 26, 27, 29, 31, 32, 35, 36, 39, 41
48	16, 33
49	18, 19, 30, 31, 48
50	24, 25, 26, 49
51	all residues
52	9, 13, 16, 29, 40, 48
54	27, 28
55	10, 11, 12, 21, 22, 23, 32, 33, 34, 43, 44, 45, 54
56	8, 9, 16, 25, 32, 49
57	7, 8, 11, 12, 18, 19, 20, 26, 27, 30, 31, 37, 38, 39, 45, 46, 49, 50, 56
58	4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28, 29, 30, 33, 34, 35, 36, 38, 42, 45, 49, 51, 52, 53, 54, 57
60	16, 21, 25, 36, 40, 45

62	2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28, 31, 32, 33, 35, 36, 38, 39, 40, 41, 45, 47, 49, 50, 51, 56, 59
63	8, 27, 28, 35, 36, 55, 62
64	no others
65	all residues
66	3, 4, 9, 12, 15, 16, 22, 25, 27, 31, 33, 34, 36, 37, 42, 45, 48, 49, 55, 58, 60, 64
68	4, 13, 16, 17, 21, 33, 52, 64
69	all residues
70	4, 9, 11, 14, 15, 16, 21, 25, 29, 30, 35, 36, 39, 44, 46, 49, 50, 51, 56, 60, 64, 65
72	9, 64
74	3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36, 37, 38, 40, 41, 44, 46 47, 48, 49, 53, 58, 62, 63, 64, 65, 67, 70, 71, 73
75	7, 18, 24, 25, 26, 32, 43, 49, 50, 51, 68, 74
76	4, 5, 9, 16, 17, 20, 24, 25, 28, 36, 44, 45, 49, 57, 61, 64, 68, 73
77	all residues
78	12, 13, 25, 27, 39, 40, 51, 52, 64, 66
80	16, 65
81	80
82	2, 4, 5, 8, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40, 41, 42, 43, 45, 46, 49, 50, 51, 57, 59, 61, 62, 64, 66, 72, 73, 74, 77, 78, 80, 81
84	21, 28, 36, 49, 57, 64
85	all residues
86	4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41, 43, 44, 47, 49, 52, 53, 54, 56, 57, 58, 59, 60, 64, 66, 67, 68, 74, 78, 79, 81, 83, 84
87	all residues
88	9, 16, 25, 33, 48, 49, 56, 64, 80, 81
90	9, 10, 19, 36, 45, 46, 54, 55, 64, 81
91	all residues
92	4, 8, 9, 12, 13, 16, 24, 25, 29, 32, 36, 41, 48, 49, 52, 64, 69, 72, 73, 77, 81, 85
93	2, 4, 8, 15, 16, 23, 27, 29, 30, 31, 32, 33, 35, 39, 46, 47, 54, 58, 60, 61, 62, 63, 64 66, 70, 77, 78, 85, 89, 91, 92
94	2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42, 48, 49, 50, 51, 53, 54, 55, 56, 59, 61, 63, 64, 65, 68, 71, 72, 74, 75, 79, 81, 83, 84, 89
95	all residues
96	33, 64
98	32, 44, 49, 67, 79, 86

99	8, 9, 10, 17, 18, 19, 26, 27, 28, 35, 36, 37, 44, 45, 53, 54, 55, 62, 63, 64, 71, 72, 73, 80, 81, 82, 89, 90, 91, 98
100	25, 76
108	28, 81
120	16, 25, 40, 81, 96, 105
125	57, 68, 124
128	no others
136	16, 17, 33, 120
144	64, 81
150	24, 25, 49, 51, 75, 76, 99, 100, 124, 126
160	65, 96
162	81, 82
192	64, 129
200	25, 176
216	81, 136
240	16, 81, 96, 145, 160, 225
243	242
250	124, 125, 126, 249
256	no others
272	17, 256
288	64, 225
300	25, 76, 100, 201, 225, 276
320	65, 256
324	81, 244
360	81, 136, 145, 216, 225, 280
384	129, 256
400	176, 225
432	81, 352
480	96, 160, 225, 256, 321, 385
486	243, 244
500	125, 376

512	no others
544	256, 289
576	64, 513
600	25, 201, 225, 376, 400, 576
625	182, 443, 624
640	256, 385
648	81, 568
720	81, 145, 225, 496, 576, 640
729	728
768	256, 513
800	225, 576
864	352, 513
900	100, 225, 325, 576, 676, 801
960	256, 321, 385, 576, 640, 705
972	244, 729
1000	376, 625

The author wishes to thank the referee most sincerely for some valuable suggestions.

* * * * *

The Fibonacci Association invites Educational Institutions to apply for Academic Membership in the Association. The minimum subscription fee is $25 annually. (Academic Members will receive two copies of each issue and will have their names listed in the Journal.)

* * * * *

The Fibonacci Bibliographical Research Center desires that any reader finding a Fibonacci reference send a card giving the reference and a brief description of the contents. Please forward all such information to:

Fibonacci Bibliographical Research Center,
Mathematics Department,
San Jose State College,
San Jose, California.

* * * * *