Indian J. pure appl. Math., 12(1) : 22–30, January 1981

EULER'S TOTIENT FUNCTION AND ITS INVERSE

HANSRAJ GUPTA*, F.N.A.

Panjab University, Chandigarh 160014

(*Received* 31 *October* 1980)

Euler's totient function $\phi(n)$ can be defined for all positive integral values of n by the relations:

(1) $\phi(1) = 1$:

and for any prime p and $u \geq 1$

(2) $\phi(pu) = p\phi(u)$ or $(p-1)\,\phi(u)$

according as p does or does not divide u.

The simple reduction formula (2) which is so suitable for computing the values of $\phi(n)$, does not appear to have been stated before.

A method of finding all the elements of the set

$$\phi^{-1}(m) = \{n : \phi(n) = m\}$$

is described, and the conjecture that the inequality

$$\phi(x) < m$$

has about twice as many even solutions than it has odd ones is shown to be true. It is also shown that sets $\phi^{-1}(m)$ with all elements even exist.

1. INTRODUCTION

In what follows, small letters denote positive integers; p's denote primes: E denotes an empty set; and if A is any set, then

$$tA = \{ta : a \in A\}. \qquad \ldots(1.1)$$

For any given positive integer n, Euler's totient function $\phi(n)$ denotes the number of positive integers which are prime to n and do not exceed n.

The following properties of $\phi(n)$ are well-known and are stated here for ready reference:

(i) $\phi(1) = 1 = \phi(2)$. $\qquad \ldots(1.2)$

(ii) $\phi(n)$ is multiplicative, i.e. for $(n_1, n_2) = 1$,

$$\phi(n_1 n_2) = \phi(n_1)\,\phi(n_2). \qquad \ldots(1.3)$$

(iii) For any prime p,

$$\phi(p^c) = p^{c-1}(p-1). \qquad \ldots(1.4)$$

*402 Mumfordganj, Allahabad 211002.

From (1.3) and (1.4), it follows that

$$\phi(n) = n \prod_{p \mid n} (1 - p^{-1}). \qquad \ldots(1.5)$$

(iv) $\phi(n)$ is even for each $n \geqslant 3$. $\qquad \ldots(1.6)$

This means that there is no x for which

$$\phi(x) = 2t + 1, t \geqslant 1.$$

On the other hand,

$$\phi(x) = 2t, t \geqslant 1$$

may or may not have any solution for a given t and if it has a solution, it may not be unique.

Thus $\phi(x) = 6$ has exactly four solutions viz. $x = 7, 9, 14, 18$; while there is no x for which $\phi(x) = 14$.

(v) If for some n, $\phi(n) = m$, then

$\phi(2n) = m$ if and only if n is odd. $\qquad \ldots(1.7)$

2. A Reduction Formula for $\phi(n)$

We have $\phi(1) = 1$:

for $n \geqslant 2$, we can write

$$n = pu$$

where p is a prime divisor of n and u is some integer $\geqslant 1$. Then it is easy to see that

$$\phi(n) = p\phi(u) \text{ or } (p - 1)\,\phi(u) \qquad \ldots(2.1)$$

according as p does or does not divide u.

(In practice it is best to take p as the smallest prime divisor of n.)

With $\phi(1) = 1$, (2.1) completely defines $\phi(n)$ for all positive integral values of n. Actually, (2.1) provides a simple reduction formula for $\phi(n)$. This formula does not appear to have been given before.

After the author had computed values of $\phi(n)$ for $n \leqslant 7500$ manually, Ajeet Singh of the Moti Lal Engineering College, Allahabad and Nirmal Roberts of the Computer Centre at the I.I.T., Kanpur, were able to write independently programmes for the computation of $\phi(n)$. These were based directly on (2.1). Finally, Nirmal produced a table of values of $\phi(n)$ for $n \leqslant 25000$ which is a considerable extension of available tables.

3. The Set $\phi^{-1}(m)$

For any given m, we define $\phi^{-1}(m)$ by the relation:

$$\phi^{-1}(m) = \{n : \phi(n) = m\}. \qquad \ldots(3.1)$$

This set is empty for all odd values of $m > 1$ and for many even values of m also. Our interest will be mainly in those values of m for which the set is non-empty.

Theorem 1 — Any non-empty set $\phi^{-1}(m)$ is bounded both above and below.

PROOF : Let n be any element of $\phi^{-1}(m)$.

Evidently, then $m \leqslant n$.

The set is therefore, bounded below.

Again, from (1.5), we have

$$n/\phi(n) = \prod_{p \mid n} p/(p-1) \qquad \ldots(3.2)$$

$$\leqslant \prod_{(p-1) \mid m} p/(p-1). \qquad \ldots(3.3)$$

This follows from the fact that if $p \mid n$, then $(p-1) \mid m$; but if $(p-1) \mid m$, then p may or may not divide n.

Hence, no n for which $\phi(n) = m$, can exceed $U(m)$ where

$$U(m) = m. \prod_{(p-1) \mid m} p/(p-1). \qquad \ldots(3.4)$$

This completes the proof of the theorem.

Corollary — If q is the largest odd element of $\phi^{-1}(m)$, then

$$q \leqslant U(m)/2. \qquad \ldots(3.5)$$

(This follows from the fact that $2q$ is also an element of $\phi^{-1}(m)$.)

We can find another upper bound for $n/\phi(n)$ as follows. Let P_k denote the product of the first k primes

$$p_1^*, p_2^*, p_3^*, \ldots, p_k^*$$

with $p_1^* = 2, p_2^* = 3, p_3^* = 5$, and so on.

Then for any n for which $P_k \leqslant n < P_{k+1}$, we have

$$n/\phi(n) \leqslant P_k/(p_1^* - 1)(p_2^* - 1) \ldots (p_k^* - 1). \qquad \ldots(3.6)$$

This follows from the fact that no n in the said interval can have more than k distinct prime divisors.

The sign of equality actually holds in (3.6) for $n = P_k$ and may be for several other numbers too.

Results (3.4) and (3.6) can often be used together with advantage. Take $m = 192$ for example. Then using (3.4), we find that no element of $\phi^{-1}(m)$ can exceed

$$192.(2/1)\ (3/2)\ (5/4)\ (7/6)\ (13/12)\ (17/16)\ (97/96)\ (193/192)$$

which is just less than 983.

Since 983 lies between P_4 and P_5 and for any n in this interval

$$n/\phi(n) \leqslant (2/1)\ (3/2)\ (5/4)\ (7/6),$$

no element of $\phi^{-1}(192)$ can exceed 840.

Our tables show that 840 is actually the largest element of $\phi^{-1}(192)$ (this is, however, purely a matter of chance and we cannot assert that this will always be so). For $m = 400$, (3.4) gives 1820 as an upper bound for the set $\phi^{-1}(400)$. Use of (3.6) improves it to 1750 while the largest element of $\phi^{-1}(400)$ is 1650.

4. Determination of $\phi^{-1}(m)$

Let n be an element of $\phi^{-1}(m)$ for a given m. Assume that p is the least prime divisor of n. Let

$$n = p^d u, \text{ where } (u, p) = 1.$$

This clearly implies that u has no prime divisor $\leqslant p$.

Evidently, we have

$$m = \phi(n) = \phi(p^d)\,\phi(u). \qquad \ldots(4.1)$$

For (4.1) to hold, it is necessary that our p be such that

$$(p - 1) \mid m \qquad \ldots(4.2)$$

and u belong to that subset of $\phi^{-1}(m/\phi(p^d))$ which consists of those of its elements which have no prime divisor $\leqslant p$. Such a subset can conveniently be denoted by $\phi_p^{-1}(m/\phi(p^d))$. It will be clear that every element of

$$p^d\phi^{-1}(m/\phi(p^d)) \qquad \ldots(4.3)$$

gives a solution of the equation

$$\phi(x) = m. \qquad \ldots(4.4)$$

In fact, (4.3) provides all those solutions of (4.4) which have p as their least prime divisor and p^d as the highest power of p which divides them.

Letting p run through all those primes which satisfy condition (4.2) and d through all those values for which $\phi(p^d)$ divides m, all the solutions of (4.4) can be

obtained. These determine $\phi^{-1}(m)$. For any prime p satisfying (4.2), we can ignore all those values of d for which $m/\phi(p^d)$ is an odd number > 1.

For reasons which will be clear a little later, it will be best to consider values of p in descending order of magnitude and those of d in an ascending order.

The following example will clarify the procedure.

Example — Take $m = 576$.

To get the primes p for which $(p-1) \mid m$, we write out all the divisors of m; add 1 to each one of them and retain the primes alone. Now, $576 = 2^6.3^2$, the divisors of 576, therefore are:

1, 2, 4, 8, 16, 32, 64; 3, 6, 12, 24, 48, 96, 192; 9, 18, 36, 72, 144, 288, 576.

Adding 1 to each of these, we get

2, 3, 5, 9, 17, 33, 65; 4, 7, 13, 25, 49, 97, 193; 10, 19, 37, 73, 145, 289, 577.

The primes in this list arranged in descending order are:

577, 193, 97, 73, 37, 19, 17, 13, 7, 5, 3, 2.

We assume that sets $\phi^{-1}(x)$ are available for all $x < 576$. Those that we shall need are:

x	$\phi^{-1}(x)$
1	{1, 2}
6	{7, 9, 14, 18}
8	{15, 16, 20, 24, 30}
16	{17, 32, 34, 40, 48, 60}
18	{19, 27, 38, 54}
32	{51, 64, 68, 80, 96, 102, 120}
36	{37, 57, 63, 74, 76, 108, 114, 126}
48	{65, 104, 105, 112, 130, 140, 144, 156, 168, 180, 210}
72	{73, 91, 95, 111, 117, 135, 146, 148, 152, 182, 190, 216, 222, 228, 234, 252, 270}
96	{97, 119, 153, 194, 195, 208, 224, 238, 260, 280, 288, 306, 312, 336, 360, 390, 420}
144	{185, 219, 273, 285, 292, 296, 304, 315, 364, 370, 380, 432, 438, 444, 456, 468, 504, 540, 546, 570, 630}
288	{323, 365, 455, 459, 555, 584, 585, 592, 608, 646, 728, 730, 740, 760, 864, 876, 888, 910, 912, 918, 936, 1008, 1080, 1092, 1110, 1140, 1170, 1260}

Our calculations can now be presented in the following tabular form:

p	d	$m/\phi(p^d)$	$p^d\phi_p^{-1}(m/\phi(p^d))$
577	1	1	577 {1} = {577}
193	1	3	Discarded
97	1	6	97. E
73	1	8	73. E
37	1	16	37. E
19	1	32	19. E
17	1	36	17 {37} = {629}
13	1	48	13. E
7	1	96	7 {97} = {679}
5	1	144	5. E
3	1	288	3 {323, 365, 455} = {969, 1095, 1365}
3	2	96	9 {97, 119} = {873, 1071}
3	3	32	27. E

At the next step, we need all the odd elements of $\phi^{-1}(576)$ and these have already become available. This explains why we decided to consider the primes in descending order.

2	1	576	2 {577, 629, 679, 969, 1095, 1365, 873, 1071}
			= {1154, 1258, 1358, 1938, 2190, 2730, 1746, 2142}
2	2	288	4 {323, 365, 455, 459, 555, 585}
			= {1292, 1460, 1820, 1836, 2220, 2340}
2	3	144	8 {185, 219, 273, 285, 315}
			= {1480, 1752, 2184, 2280, 2520}
2	4	72	16 {73, 91, 95, 111, 117, 135}
			= {1168, 1456, 1520, 1776, 1872, 2160}
2	5	36	32 {37, 57, 63}
			= {1184, 1824, 2016}
2	6	18	64 {19, 27}
			= {1216, 1728}

We have thus obtained all the elements of $\phi^{-1}(576)$. Arranging these in order, we can record them in our table.

It is noteworthy that in our calculations, the even elements of sets recorded earlier, play no role.

Note: Let $C_o(x)$ denote the set of odd and $C_e(x)$ that of even elements of $\phi^{-1}(x)$, then we leave it to the reader to show that

$C_e(2m) = 2\{C_o(2m) \cup C_e(m)\}$.

The importance of this observation will be realized in the next section.

5. The Number of Solutions of the Equation $\phi(x) = m$

For any given m, let $v_o(m)$ and $v_e(m)$ denote respectively the number of the odd and the even solutions of the equation

$$\phi(x) = m. \qquad \ldots(5.1)$$

Then from the example in the preceding section, it will be clear that for $m = 2^k m_o$, where m_o is an odd number $\geqslant 1$, we have

$$\begin{aligned} v_e(2^k m_o) &= v_o(2^k m_o) + v_o(2^{k-1} m_o) + \ldots + v_o(2m_o) + v_o(m_o) \\ &= v_o(2^k m_o) + v_e(2^{k-1} m_o),\ k \geqslant 1. \end{aligned} \qquad \ldots(5.2)$$

For $k = 0$, we have

$$v_e(m_o) = 0 = v_o(m_o),\ m_o \geqslant 3;$$

$$v_e(1) = 1 = v_o(1).$$

Here, we must state that there is no method of finding $v_o(m)$ except by actual computation, as explained in the preceding section. For $m = 2^k$, we have, however, the following:

Theorem 2 — $v_o(2^k) = 1$, if $0 \leqslant k \leqslant 31$;

$= 0$, otherwise.

The proof depends on a well-known property of Fermat's numbers.

Proof : The divisors of 2^k are

$$1, 2, 4, \ldots, 2^k.$$

The only values of j for which $2^j + 1$ is a prime are

$$j = 0, 1, 2, 4, 8, 16.$$

Since 2^k has no prime divisor other than 2, any odd number n for which

$$\phi(n) = 2^k$$

must be a product of distinct odd primes of the form $2^j + 1$. The theorem is true for $k = 0$, and every integer from 1 to 31 has a unique partition into the elements 1, 2, 4, 8, 16. Hence the first part of the theorem follows. The second part also follows if we accept that the Fermat numbers $2^{2^n} + 1$ are all composite for $n \geqslant 5$. In case this conjecture is untrue, the theorem will have to be stated in the form

$$v_o(2^k) = 1 \text{ or } 0$$

for all values of k including 0. In particular it is zero for $k = 32$ and 1 for each $k \leqslant 31$.

Example — The only odd solution of the equation

$$\phi(x) = 2^{29}$$

is $x = (2^{16} + 1)(2^8 + 1)(2^4 + 1)(2 + 1)$.

6. The Inequality $\phi(x) \leqslant m$

In this section we assume that m is not too small.

Let $V_o(m)$ and $V_e(m)$ denote respectively the numbers of odd and even solutions of the inequality

$$\phi(x) \leqslant (m).$$

Then from (5.2), we immediately have

$$V_e(m) + V_o(2m) = V_e(2m). \qquad \ldots(6.1)$$

From our tables it appears that real numbers α and β exist such that

$$V_o(x) \doteq \alpha x \text{ and } V_e(x) \doteq \beta x$$

($\doteq$ means approximately equal to).

Assuming this to be true, (6.1) will give

$$\beta x + 2\alpha x \doteq 2\beta x.$$

Hence $$\beta \doteq 2\alpha.$$

This means that the number of even solutions of $\phi(x) \leqslant m$ is about twice the number of its odd solutions.

Tables show that

$$\alpha \doteq 0.648; \text{ and } \beta \doteq 1.295$$

Acknowledgement

The author must thank Messrs Ajeet Singh and Nirmal Roberts for their kind help. Also J. C. Parnami, using a well-know Lemma, was able to show that α, β do exist and

$$\alpha = \frac{1}{3} \prod_p \left(1 + \frac{1}{p(p-1)}\right)$$

where p runs over all primes.

A specimen page from the Table of values of V_o, V_e

m	V_o	V_e	m	V_o	V_e	m	V_o	V_e
1408	913	1828	1600	1037	2085	1804	1174	2348
1416	914	1830	1606	1038	2086	1806	1175	2349
1422	915	1831	1608	1041	2089	1808	1176	2353
1424	916	1835	1612	1042	2090	1810	1177	2354
1426	917	1836	1616	1043	2092	1812	1178	2356
1428	920	1839	1618	1044	2093	1820	1179	2358
1432	922	1843	1620	1051	2101	1822	1180	2359
1436	923	1845	1624	1053	2104	1824	1182	2366
1438	924	1846	1626	1054	2105	1830	1183	2367
1440	944	1898	1632	1060	2119	1836	1188	2373
1446	945	1899	1636	1061	2120	1840	1192	2382
1450	946	1900	1640	1065	2126	1846	1193	2383
1452	949	1904	1644	1066	2128	1848	1197	2391
1456	950	1905	1652	1067	2130	1856	1200	2403
1458	952	1907	1656	1076	2144	1860	1204	2408
1464	954	1912	1660	1077	2145	1864	1205	2411
1470	955	1913	1662	1078	2146	1866	1206	2412
1472	956	1919	1664	1079	2152	1870	1207	2413
1476	959	1923	1666	1080	2153	1872	1220	2437
1480	961	1925	1668	1081	2154	1876	1221	2438
1482	962	1926	1672	1082	2157	1878	1222	2439
1484	963	1928	1676	1083	2159	1880	1223	2441
1486	964	1929	1680	1100	2192	1888	1224	2442
1488	966	1933	1692	1103	2195	1892	1225	2444
1492	967	1934	1696	1105	2201	1896	1227	2446
1498	968	1935	1698	1106	2202	1900	1229	2448
1500	972	1940	1704	1107	2204	1904	1231	2454
1510	973	1941	1708	1108	2205	1906	1232	2455
1512	983	1960	1712	1109	2207	1908	1234	2457
1520	985	1966	1716	1111	2210	1912	1236	2461
1522	986	1967	1720	1114	2215	1920	1248	2512
1528	987	1970	1722	1115	2216	1930	1249	2513
1530	988	1971	1724	1116	2218	1932	1253	2518
1536	994	2004	1728	1130	2266	1936	1254	2519
1540	995	2005	1732	1131	2267	1940	1255	2521
1542	996	2006	1740	1133	2269	1944	1264	2537
1544	997	2008	1746	1134	2270	1948	1265	2538
1548	998	2009	1752	1139	2278	1950	1266	2539
1552	1000	2013	1758	1140	2279	1952	1267	2541
1558	1001	2014	1760	1146	2297	1960	1270	2546
1560	1008	2024	1764	1149	2301	1964	1271	2548
1566	1009	2025	1768	1150	2304	1968	1274	2555
1568	1010	2029	1772	1151	2306	1972	1275	2556
1570	1011	2030	1776	1155	2315	1978	1276	2557
1572	1014	2034	1780	1156	2316	1980	1283	2565
1578	1015	2035	1782	1157	2317	1986	1284	2566
1582	1016	2036	1786	1158	2318	1992	1289	2576
1584	1029	2063	1788	1159	2319	1996	1290	2577
1592	1030	2065	1792	1162	2334	1998	1291	2578
1596	1031	2066	1800	1173	2347	2000	1295	2589