Recreaciones en teoría de números

Phi-Fo-Fu

La función phi de Euler y sus propiedades

Lorenzo Antonio Alvarado Cabrera

18/octubre/2021

Def. – Si $n \geq 1$ entero, entonces $\varphi(n)$ es el numero de enteros positivos menores o iguales a n coprimos con n.

O mas formalmente:

$$\varphi(n) = \left|\{m \in \mathbb{N} : m \leq n \text{ y } (m,n) = 1\}\right|$$

Unos ejemplos son: $\varphi(1) = 1,\ \varphi(4) = 2,\ \varphi(7) = 6$

¿Cual es el valor de $\varphi(n)$ para toda $n \in \mathbb{Z}^+$?

Propiedad 1

Si $n = p$ primo, entonces $\varphi(p) = p - 1$

Demostración. – Como p es primo, entonces $(k,p) = 1 \ \ \forall k < p \ \ \Rightarrow \ \ \varphi(p) = 1$ ■

Propiedad 2

Si $n = p^a$ p – primo y $a \in \mathbb{N}$, entonces $\varphi(p^a) = p^{a-1}(p-1)$

Demostración. –

Propiedad 3

Si $n = p \cdot q$ p, q – primos distintos, entonces $\varphi(pq) = (p-1)(q-1) = \varphi(p)\varphi(q)$

Demostración. –

¿Sera que siempre $\varphi(nm) = \varphi(n)\varphi(m)$?

Propiedad 4 (phi es multiplicativa)

Dados $(m, n) = 1$ se tiene que $\varphi(nm) = \varphi(n)\varphi(m)$

Demostración. – Sea usan sistemas reducidos de residuos... ■

Una vez dados todas estas propiedades podemos dar el valor de $\varphi(n)$ en general.

Teorema

Sea $n \geq 1$, con $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ entonces $\varphi(n) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\cdots p_k^{a_k-1}(p_k-1)$

Demostración. –

Notemos que $(p_i^{a_i}, p_j^{a_j}) = 1 \ \forall i \neq j \ \Rightarrow \ \varphi(n) = \varphi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) \overset{(3)}{=} \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_k^{a_k})$

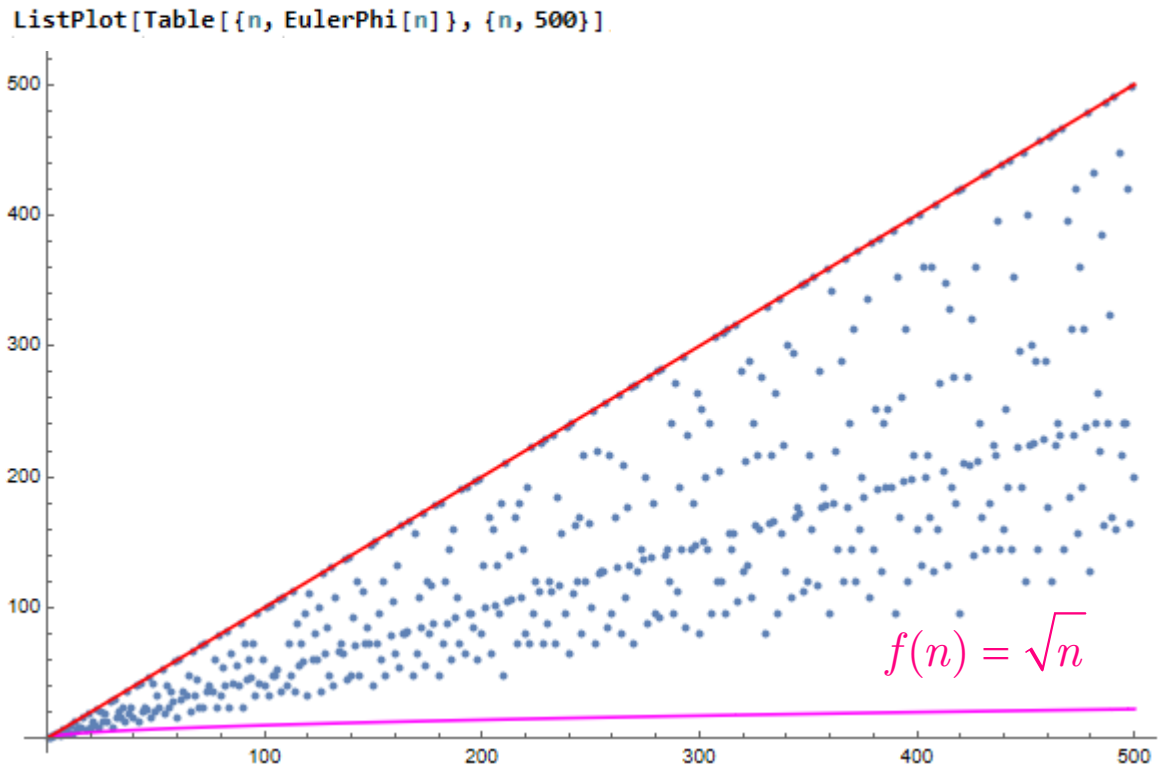
$\overset{(2)}{=} p_1^{a_1}(p_1-1)p_2^{a_2}(p_2-1)\cdots p_k^{a_k}(p_k-1)$. ■

Esto nos ayuda a encontrar mas facilmente los valores de $\varphi(n)$

Por ejemplo, $\varphi(882) = \varphi(2\cdot 49\cdot 9) = \varphi(2\cdot 7^2\cdot 3^2) = \varphi(2)\varphi(7^2)\varphi(3^2) = 2^0(2-1)7^{2-1}(7-1)3^{2-1}(3-1) = (1)(7\cdot 6)(3\cdot 2) = 252$

Sin embargo, para numeros verdaderamente grandes, esto se complicara, pues tenemos que enontrar la factorizacion en primos de cada n.

Asi que es convieniente tratar de estudiar el valor de $\varphi(n)$ para valores grandes de n, aqui convendra tratar de dar una cota.



Aqui tenemos la grafica de la funcion $\varphi(n)$, para $1 \leq n \leq 500$

Y podemos ver claramente una cota superior, muy uniforme, la cual demostraremos que es $f(n) = n$.

Igualmente podemos ver un limite inferior, el cual tiene un comportamiento logaritmico o exponencial.

Una cota inferior eficiente es muy dificil de demostrar pero demostraremos una mas sencilla que es $\sqrt{n}$.

Proposición

Si $n \neq 2$ y $n \neq 6$, entonces $\sqrt{n} \leq \varphi(n) \leq n$

Demostración. –

La desigualdad de la derecha es sencilla, tenemos que $\varphi(n) = \sum_{\substack{(k,n)=1 \\ k \leq n}} 1 \leq \sum_{k=1}^{n} 1 = n \ \therefore \ \varphi(n) \leq n$

continuación... Ahora, veremos la desigualdad de la izquierda.

Queremos probar que $\sqrt{n} \leq \varphi(n) \Leftrightarrow \sqrt{p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}} \leq \varphi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})$

$$\Leftrightarrow \sqrt{p_1^{a_1}} \cdots \sqrt{p_k^{a_k}} \leq \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$$

Entonces si probamos que $\sqrt{p^m} \leq \varphi(p^m) \quad \forall m \geq 1$ y $p-$primo quedaria demostrado.

Tenenmos que $\sqrt{p^m} \leq \varphi(p^m) \Leftrightarrow p^{m/2} \leq p^m - p^{m-1} \Leftrightarrow p^{m/2-1} \leq p^{m-m} - p^{m-1-m} = 1 - p^{-1}$

$$\Leftrightarrow \frac{1}{p^{m/2}} \leq 1 - \frac{1}{p} \Leftrightarrow \frac{1}{p^{m/2}} + \frac{1}{p} \leq 1$$

Pero como $p \geq 2 \Rightarrow \frac{1}{p} \leq \frac{1}{2}$, entonces necesitamos que $\frac{1}{p^{m/2}} \leq \frac{1}{2} \Leftrightarrow 2 \leq p^{m/2} \Leftrightarrow 4^{1/m} \leq p$

$\Leftrightarrow p \geq 4,\ 2,\ 4^{1/3},\ 4^{1/4}, \ldots \therefore p \neq 2,\ 3$ cumple que $\sqrt{p^m} \leq \varphi(p^m) \quad \forall m \geq 1$

- ¿ $p = 2$?

$\Rightarrow \sqrt{2^m} \leq \varphi(2^m) \Leftrightarrow 2 \leq 2^{m/2} \Leftrightarrow m \neq 1$

- ¿ $p = 3$?

$\Rightarrow \sqrt{3^m} \leq \varphi(3^m) \Leftrightarrow 3 \leq 3^{m/2} \Leftrightarrow m \neq 1$

continuación...

Con todo esto sea $n \geq 1$, tenemos que $\varphi(n) = \varphi(\prod_i p_i^{a_i}) = \prod_i \varphi(p_i^{a_i}) = \varphi(2^a)\varphi(3^b) \prod_{p\neq 2,3} \varphi(p_i^{a_i}) \geq \varphi(2^a)\varphi(3^b) \prod_{p\neq 2,3} \sqrt{p_i^{a_i}}$

$$\underset{a,b\neq 1}{\geq} \overset{(*)}{\sqrt{2^a}\sqrt{3^b}} \prod_{p\neq 2,3} \sqrt{p_i^{a_i}} = \prod_i \sqrt{p_i^{a_i}} = \sqrt{n}$$

(*) Esta parte se cumple siempre que $a, b \neq 1$ y no sean los unicos primos pues si hay otros primos,

entonces $\varphi(2^a p) \geq \sqrt{2^a p}$ y $\varphi(3^a p) \geq \sqrt{3^a p}$ pero como $n \neq 2, 6$, esto nunca pasa.

$\therefore$ $\sqrt{n} \leq \varphi(n)$ para toda $n \neq 2, 6$ ■

Asi por ejemplo, sabremos que $\varphi(1607824)$ esta en el intervalo [1268,160784]

Esta cota nos servira mas adelante...

A partir de aqui estudiarremos algunas soluciones de ecuaciones que involucran a $\varphi(n)$

Problema 1

¿$\varphi(n)$ siempre es par para $n > 2$?

Demostración. –

n	$\varphi(n)$	Paridad
1	1	Impar
2	1	Impar
3	2	Par
4	2	Par
5	4	Par
1236	408	Par
8542	4270	Par
36549	23400	Par

Caso 1:

Si n tiene un factor primo impar, es decir, si $n = p^k \cdot m \quad \Rightarrow \quad \varphi(n) = \varphi(p^k \cdot m)$

$= \varphi(p^k)\varphi(m) = p^{k-1}(p-1)\varphi(m)$, y como p es impar $\Rightarrow$ $p-1$ es par $\therefore$ $\varphi(n)$ es par.

Caso 2:

Si n no tiene ningun factor primo impar, es decir, si $n = 2^k \quad \Rightarrow \quad \varphi(n) = \varphi(2^k)$

$= 2^{k-1}(2-1) = 2^{k-1}$ es par, excepto cuando $k = 1$ $\therefore$ $\varphi(n)$ es par con $k > 1$

$\therefore$ $\varphi(n)$ siempre es par para $n > 2$. ■

Problema 2

¿Para cuales n, $\varphi(n) = 12$?

Solución. –

Sabemos que para cada n sabemos que $\varphi(n) = p_1^{a_1}(p_1-1)p_2^{a_2}(p_2-1)\cdots p_k^{a_k}(p_k-1)$. Entonces, nos bastara representar a 12 de esta manera para encontrar soluciones.

Tenemos que $12 = 2\cdot 6,\ 4\cdot 3$

Entonces:

1) $12 = \varphi(13) \Rightarrow n = 13$

2) $12 = 1\cdot 12 = \varphi(2)\varphi(13) \Rightarrow n = 2\cdot 13 = 26$

3) $2\cdot 6 = \varphi(3)\varphi(7) \Rightarrow n = 3\cdot 7 = 21$

4) $2\cdot 6 = \varphi(2^2)\varphi(7) \Rightarrow n = 2^2\cdot 7 = 28$

5) $2\cdot 6 = \varphi(3)\varphi(7) = \varphi(2)\varphi(3)\varphi(7) \Rightarrow n = 2\cdot 3\cdot 7 = 42$

6) $4\cdot 3 = 2^2(2-1)3 = 2^2(2-1)\varphi(?)$

$\Rightarrow 4\cdot 3 = 2(2-1)3(2) = 2^{2-1}(2-1)3^{2-1}(3-1)$

$= \varphi(2^2)\varphi(3^2) \Rightarrow n = 2^2\cdot 3^2 = 36$

$\therefore$ $n = 13, 21, 26, 28, 36, 42$ son las soluciones

■

Problema 3

Encuentra los $n \in \mathbb{N}$ tales que $\varphi(n) = \dfrac{n}{2}$

Solución. –

Caso 1: Si n es impar, entonces no hay solucion, pues $\frac{n}{2}$ no es entero.

Caso 2: Si n es par, entonces, $\underbrace{n = 2^k \cdot m}_{(2^k, m)=1} \Rightarrow \varphi(n) = \frac{n}{2} \Leftrightarrow \varphi(2^k m) = \frac{2^k m}{2} \Leftrightarrow \varphi(2^k)\varphi(m) = 2^{k-1} m$

$\Leftrightarrow 2^{k-1}\varphi(m) = 2^{k-1} m \Leftrightarrow \varphi(m) = m.$ Pero como $(2^k, m) = 1 \Rightarrow m$ impar $\Rightarrow \varphi(m)$ impar $\Leftrightarrow m = 1, 2$

$\therefore \; n = 2^k \;\; \forall k \in \mathbb{Z}^+$ son las soluciones. ■

Este problema fue mas que interesante. Ahora podriamos preguntarnos ¿Cuales $n \in \mathbb{N}$ cumplen que $\varphi(n) = \dfrac{n}{3}$?

O en general ¿Cuales $n \in \mathbb{N}$ cumplen que $\varphi(n) = \dfrac{n}{k}$?

Pero antes de hacer nada, podemos darle otro enfoque. Si nos damos cuenta lo que queremos es resolver la ecuacion

$$k\varphi(n) = n \quad \text{y esto se cumple} \Leftrightarrow \varphi(n) \mid n$$

Problema

¿Para cuales $n \in \mathbb{N}$, $\varphi(n) \mid n$?

```
Position[Table[If[Divisible[n, EulerPhi[n]], 1, 0],
posición      tabla   si  divisible      phi de Euler
  {n, 1, 100000}], 1]
```

```
{{1}, {2}, {4}, {6}, {8}, {12}, {16}, {18}, {24}, {32},
 {36}, {48}, {54}, {64}, {72}, {96}, {108}, {128},
 {144}, {162}, {192}, {216}, {256}, {288}, {324},
 {384}, {432}, {486}, {512}, {576}, {648}, {768},
 {864}, {972}, {1024}, {1152}, {1296}, {1458}, {1536},
 {1728}, {1944}, {2048}, {2304}, {2592}, {2916},
 {3072}, {3456}, {3888}, {4096}, {4374}, {4608},
 {5184}, {5832}, {6144}, {6912}, {7776}, {8192},
 {8748}, {9216}, {10368}, {11664}, {12288}, {13122},
 {13824}, {15552}, {16384}, {17496}, {18432}, {20736},
 {23328}, {24576}, {26244}, {27648}, {31104}, {32768},
 {34992}, {36864}, {39366}, {41472}, {46656}, {49152},
 {52488}, {55296}, {62208}, {65536}, {69984},
 {73728}, {78732}, {82944}, {93312}, {98304}}
```

Solución. –

Descartando los casos $n = 1, 2$ sabemos que $\varphi(n)$ es par y por tanto $\varphi(n) \mid n$ $\Leftrightarrow$ n es par.

Asi sea $n = 2^k m$ con $k \geq 1$ y m impar entonces $\varphi(n) \mid n \Leftrightarrow \varphi(2^k m) \mid 2^k m$ $\Leftrightarrow$ $2^{k-1}\varphi(m) \mid 2^k m \Leftrightarrow \varphi(m) \mid 2m$

Esto me dice que $\varphi(m)$ tiene que tener solo al 2 como factor pues si $\varphi(m) = 2^k r$ con $k > 1 \Rightarrow \varphi(m) \nmid 2m \therefore m = p^a$ con $a > 0$ y $p - primo$

Pues de no serlo, digamos $m = p^a q^b$ tendriamos que $\varphi(m) = \varphi(p^a q^b)$ $= p^{a-1}(p-1)q^b(q-1) = 2^2 \cdot r$ p.a $r > 1$ y tendria un factor par mayor que 2

Por todo lo anterior tenemos que $\varphi(n) \mid n \Leftrightarrow n = 2^k p^a$ para algun p pirmo impar.

Pero $\varphi(2^k p^a) \mid 2^k p^a \Leftrightarrow 2^{k-1} p^{a-1}(p-1) \mid 2^k p^a \Leftrightarrow p - 1 \mid 2p$ y como $p-1$ es par entonces $p - 1 \mid 2$ (pues $p > 2$)

$\Leftrightarrow$ $p = 3$ $\therefore$ los $n \in \mathbb{N}$ tales que $\varphi(n) \mid n$ son $n = 2^a 3^b$ con $a, b \in \mathbb{Z}^+$ ■

Ejemplo : $93,312 = 2^7 \cdot 3^6$

Sin duda es un resultado interesante, ya que como podemos observar, hay infinitos n tales que $\varphi(n) \mid n$
Este tipo de relaciones no son nuevas, y ya han sido estudiadas por los matematicos desde hace mucho tiempo.

DH. Lehmer fue uno de ellos, mas en concreto estudio para cuales n se tiene que $\varphi(n) \mid n-1$ algo que hoy en dia se le conoce como "El Problema de Lehmer"

Problema

Encontrar los $n \in \mathbb{N}$, tales que $\varphi(n) \mid n-1$

Podemos dar varias observaciones sencillas.

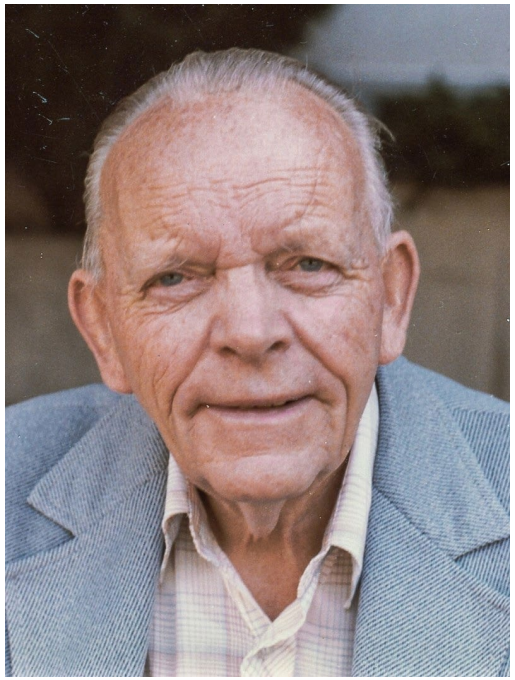
Obs 1.– Si n es primo, se cumple ya que $\varphi(n) = n-1 \mid n-1$
Asi que el problema solamente es encontrar los n compuestos que lo cumplan

Obs 2.– Tenemos que $n = 1,\ 2$ lo cumplen, asi si $n > 2$ es par, entonces $\varphi(n)$ es par y $n-1$ es impar $\therefore\ \varphi(n) \nmid n-1$

$\therefore$ si $\varphi(n) \mid n-1$ entonces n un numero impar compuesto.

Problema de Lehmer

¿Existe un $n \in \mathbb{N}$ impar compuesto tal que $\varphi(n) \mid n-1$?



Derrick Henry "Dick" Lehmer

1905-1991

Fue un matemático estadounidense importante para el desarrollo de la teoría numérica computacional

¿Existiran soluciones?

- Lehmer mostro que si n es solucion, entonces n es impar y libre de cuadrados.

Demostracion. – Si $p^2 \mid n \;\Rightarrow\; n = p^2 \cdot m \;\Rightarrow\; \varphi(n) = \varphi(p^2)\varphi(m) = p(p-1)\varphi(m) \;\Rightarrow\; p \mid \varphi(n)$

Ahora, como n es solucion entonces $\varphi(n) \mid n-1 \;\Rightarrow\; p \mid n-1$. Con lo anterior tenemos que $p \mid n$ y $p \mid n-1$

$\therefore\; p \mid (n)-(n-1) \;\Rightarrow\; p \mid 1 \;\therefore\; p = 1$ y asi n es libre de cuadrados. ■

Esto me dice que n seria de la forma $n = p_1 p_2 \cdots p_k$

- En 1980 Cohen y Hagis demostraron que, para cualquier solucion del problema, $n > 10^{20}$ y el producto de mas de 14 primos distintos. Actualmente se sabe que $n > 10^{22}$ esto es mayor al ultimo primo de mersenne conocido.

- En 1980 Hagis demostro que si 3 divide a cualquier solucion n entonces $n > 10^{1{,}937{,}042}$ y el producto de mas de 298,848 primos distintos. Actualmente se sabe que en este caso $n > 10^{360{,}000{,}000}$ y ser el producto de mas de 40,000,000 de primos distintos. (por el trabajo computacional de P. Burcsi, S. Czirbusz y G. Farkas (2011))

Asi que el problema de Lehmer sigue estando abierto

Podemos hacer una pequeña modificacion del problema de Lehmer y preguntarnos por los n tales que $\varphi(n) \mid n+1$

```
Position[Table[If[Divisible[n + 1, EulerPhi[n]], 1, 0],
posición  tabla  si  divisible  phi de Euler
  {n, 1, 10000000}], 1]
{{1}, {2}, {3}, {15}, {255}, {65535}}
```

Esto es quivalente a preguntarnos la solucion de la ecuacion $k\varphi(n) = n+1$

- Si $k = 1 \Rightarrow \varphi(n) = n+1$ no tiene solucion pues como demostramos $\varphi(n) \leq n$

- Si $k = 2 \Rightarrow 2\varphi(n) = n+1$ tiene como solucion a $n = 3$ y otras mas que se mostraran en la tabla de abajo

- Si $k = 3 \Rightarrow 3\varphi(n) = n+1$ tiene como solucion a $n = 2$, pero si hay otra solución n debe ser el producto de al menos 32 factores primos distintos.

SOLUCIONES DE $k \cdot \Phi(x) = x+1$

k	x	$x+1$	$\Phi(x)$
1	No hay soluciones	---	---
2	3	2^2	2^1
2	$3 \cdot 5$	2^4	2^3
2	$3 \cdot 5 \cdot 17$	2^8	2^7
2	$3 \cdot 5 \cdot 17 \cdot 257$	2^{16}	2^{15}
2	$3 \cdot 5 \cdot 17 \cdot 353 \cdot 929$	$2^{16} \cdot 11 \cdot 29$	$2^{17} \cdot 11 \cdot 29$
2	$3 \cdot 5 \cdot 17 \cdot 257 \cdot 929 \cdot 65537$	2^{32}	2^{31}
2	$3 \cdot 5 \cdot 17 \cdot 353 \cdot 929 \cdot 83623937$	$2^{36} \cdot 11^2 \cdot 29^2$	$2^{35} \cdot 11^2 \cdot 29^2$
2	Producto de al menos 7 primos distintos	---	---
3	2	3	1
3	Producto de al menos 32 primos distintos	---	---

Actualmente seguimos igual : (

Recordando el problema 2 que vimos fue, ¿Para cuales n, $\varphi(n) = 12$? donde encontramos dichas soluciones.
Este problema se puede generalizar, y preguntarnos por los $n´s$ tales que $\varphi(n) = b$. Con ello nos hariamos las dos preguntas mas claras:

1) ¿Dado $b \in \mathbb{Z}^+$, siempre hay soluciones?

2) Dado b ¿Cuantas soluciones hay?

1) ¿Dado $b \in \mathbb{Z}^+$, siempre hay soluciones? *NO*

Recordemos que probamos que para $n > 2$, $\varphi(n)$ es par $\Rightarrow$ si b es impar, entonces la ecuacion $\varphi(n) = b$ es cierta solo si $b = 1$ y $n = 1, 2$ Esto descarta todos los numeros primos tambien.

¿Y entonces para b par, siempre hay soluciones? Lamentablemente no...
Hay muchas formas de numeros imposibles, por ejemplo, si un numero dado b es de la forma $2p^a$, p-primo, $p > 3$ y tal que $2p^a + 1$ es compuesto entonces $\varphi(n) = b$ no tiene solucion.

Valores imposibles de $\Phi(N)$

14	62	90	122	152
26	28	94	124	154
34	74	98	134	158
38	76	114	142	170
50	86	117	146	174

Ejemplo. – Tenemos que $b = 2 \cdot 5^2$ cumple que $5 > 3$ y $2 \cdot 5^2 + 1 = 51 = 3 \cdot 17$ $\therefore$ $b = 2 \cdot 5^2 = 50$ es imposible

2) Dado b ¿Cuantas soluciones hay? *No se sabe...*

Sean $n, b \in \mathbb{Z}^+$ tal que n sea solucion de $\varphi(n) = b$. Entonces sabemos que $\sqrt{n} \leq \varphi(n)$ siempre que $n \neq 2,6 \Rightarrow \; n \leq \varphi^2(n)$ $\Rightarrow \; n \leq b^2$

Entonces, si n es solucion de $\varphi(n) = b$ se tiene que $n \in [1, b^2]$, es decir, siempre habra un numero finito de soluciones. y ademas, seran menores a b^2

b	n t.q $\varphi(n) = b$	b	n t.q $\varphi(n) = b$
4	4	22	2
6	4	24	5
8	5	26	---
10	2	28	2
12	6	30	2
14	---	32	5
16	6	34	---
18	4	36	6
20	5	38	---

Como podemos notar en la tabla, seimpre se tienen al menos 2 soluciones , lo que nos lleva a preguntarnos, ¿Siempre sera asi?
A este problema hoy se le conoce como "La conjetura de Carmichael"

Conjetura de Carmichael

Para cada $n \in \mathbb{N}$, existe $m \in \mathbb{N}$ tal que $\varphi(n) = \varphi(m)$

Robert Daniel Carmichael
(1879 –1967)

Esta conjetura, como muchas otras, se han comprobado para numeros enormes, el propio Carmichael dio un limite para encontrar un contraejemplo. Demostro que si exitiera un contraejemplo, este debia ser mayor a 10^{37}

Hubieron mas cotas para estos contraejemplos, la mas actual fue dada por Kevin Ford en 1998, siendo que si existiera un contraejemplo, este seria mayor a $10^{10^{10}} = 10^{10,000,000,000}$

Gracias por su atencion :)