Acerca de los números de Carmichael

David José Fernández Bretón

Universidad Michoacana de San Nicolás de Hidalgo
Instituto de Matemáticas UNAM, campus Morelia

XLI Congreso Nacional de la SMM
Valle de Bravo, Méx.

Motivación

Teorema (Pequeño teorema de Fermat)

Si p es un número primo, entonces $p \mid a^p - a \ \ \forall\, a \in \mathbb{Z}$.

De manera natural, surge la pregunta acerca del recíproco de este teorema: si se tiene un $n \in \mathbb{Z}$ tal que $n \mid a^n - a \ \ \forall\, a \in \mathbb{Z}$, ¿Implica esto que n es un número primo? Fermat pensó que sí. De hecho, Fermat propuso que, dado $n \in \mathbb{Z}$, una buena forma de evaluar si n es o no primo consistía en tomar unos cuantos enteros a al azar y verificar si $n \mid a^n - a$ (test de primalidad de Fermat).

Motivación

Teorema (Pequeño teorema de Fermat)

Si p es un número primo, entonces $p \mid a^p - a \ \ \forall\, a \in \mathbb{Z}$.

De manera natural, surge la pregunta acerca del recíproco de este teorema: si se tiene un $n \in \mathbb{Z}$ tal que $n \mid a^n - a \ \ \forall\, a \in \mathbb{Z}$, ¿Implica esto que n es un número primo? Fermat pensó que sí. De hecho, Fermat propuso que, dado $n \in \mathbb{Z}$, una buena forma de evaluar si n es o no primo consistía en tomar unos cuantos enteros a al azar y verificar si $n \mid a^n - a$ (test de primalidad de Fermat).

Motivación

Teorema (Pequeño teorema de Fermat)

Si p es un número primo, entonces $p \mid a^p - a \ \ \forall\, a \in \mathbb{Z}$.

De manera natural, surge la pregunta acerca del recíproco de este teorema: si se tiene un $n \in \mathbb{Z}$ tal que $n \mid a^n - a \ \ \forall\, a \in \mathbb{Z}$, ¿Implica esto que n es un número primo? Fermat pensó que sí. De hecho, Fermat propuso que, dado $n \in \mathbb{Z}$, una buena forma de evaluar si n es o no primo consistía en tomar unos cuantos enteros a al azar y verificar si $n \mid a^n - a$ (test de primalidad de Fermat).

¿Qué tan bueno es el test de primalidad de Fermat

Definición

Sea n un número compuesto, y $a \in \mathbb{N}\backslash\{0\}$. Decimos que n es un ***pseudoprimo de base*** *a si $n \mid a^n - a$.*

En otras palabras, un pseudoprimo de base a es un número compuesto capaz de “aprobar" el test de primalidad de Fermat si de pura casualidad le toca ser evaluado con el entero a en dicho test.

J.H. Jeans y E.B. Escott demostraron que, para cualquier $a \in \mathbb{N}$, existen los pseudoprimos de base a. De hecho, Schinzel notó en 1958 que, si m_a denota al mínimo pseudoprimo de base a, entonces $m_a \leq 561$.

¿Qué tan bueno es el test de primalidad de Fermat

Definición

Sea n un número compuesto, y $a \in \mathbb{N}\backslash\{0\}$. Decimos que n es un ***pseudoprimo de base*** *a si $n \mid a^n - a$.*

En otras palabras, un pseudoprimo de base a es un número compuesto capaz de “aprobar" el test de primalidad de Fermat si de pura casualidad le toca ser evaluado con el entero a en dicho test.

J.H. Jeans y E.B. Escott demostraron que, para cualquier $a \in \mathbb{N}$, existen los pseudoprimos de base a. De hecho, Schinzel notó en 1958 que, si m_a denota al mínimo pseudoprimo de base a, entonces $m_a \leq 561$.

¿Qué tan bueno es el test de primalidad de Fermat

Definición

Sea n un número compuesto, y $a \in \mathbb{N}\backslash\{0\}$. Decimos que n es un ***pseudoprimo de base*** *a si $n \mid a^n - a$.*

En otras palabras, un pseudoprimo de base a es un número compuesto capaz de “aprobar" el test de primalidad de Fermat si de pura casualidad le toca ser evaluado con el entero a en dicho test.

J.H. Jeans y E.B. Escott demostraron que, para cualquier $a \in \mathbb{N}$, existen los pseudoprimos de base a. De hecho, Schinzel notó en 1958 que, si m_a denota al mínimo pseudoprimo de base a, entonces $m_a \leq 561$.

¿Qué tan bueno es el test de primalidad de Fermat

Definición

Sea n un número compuesto, y $a \in \mathbb{N}\backslash\{0\}$. Decimos que n es un ***pseudoprimo de base*** *a si $n \mid a^n - a$.*

En otras palabras, un pseudoprimo de base a es un número compuesto capaz de “aprobar" el test de primalidad de Fermat si de pura casualidad le toca ser evaluado con el entero a en dicho test.

J.H. Jeans y E.B. Escott demostraron que, para cualquier $a \in \mathbb{N}$, existen los pseudoprimos de base a. De hecho, Schinzel notó en 1958 que, si m_a denota al mínimo pseudoprimo de base a, entonces $m_a \leq 561$.

Más acerca de los pseudoprimos

Ejemplos

- $341(= 11 \cdot 31)$ *es un pseudoprimo de base 2, pero no de base 3. En efecto, es posible realizar el cálculo y ver que* $341 \mid 2^{341} - 2$*; sin embargo,* $341 \nmid 3^{341} - 3$ *debido a que* $31 \nmid 3^{341} - 3$*, pues* $3^{341} - 3 \equiv 10 \mod 31$*.*
- $91(= 7 \cdot 13)$ *es un pseudoprimo de base 3, pero no de base 2; pues* $91 \mid 3^{91} - 3$*, pero* $91 \nmid 2^{91} - 2$ *ya que* $13 \nmid 2^{91} - 2$*, dado que* $2^{91} - 2 \equiv 9 \mod 13$

Definición

Un ***número de Carmichael*** *es un número compuesto* n *tal que* $n \mid a^n - a \ \forall\ a \in \mathbb{Z}$*, es decir, tal que* n *es un pseudoprimo de base* $a \ \forall\ a \in \mathbb{Z}$*.*

Más acerca de los pseudoprimos

Ejemplos

- $341(= 11 \cdot 31)$ *es un pseudoprimo de base 2, pero no de base 3. En efecto, es posible realizar el cálculo y ver que* $341 \mid 2^{341} - 2$*; sin embargo,* $341 \nmid 3^{341} - 3$ *debido a que* $31 \nmid 3^{341} - 3$*, pues* $3^{341} - 3 \equiv 10 \mod 31$*.*
- $91(= 7 \cdot 13)$ *es un pseudoprimo de base 3, pero no de base 2; pues* $91 \mid 3^{91} - 3$*, pero* $91 \nmid 2^{91} - 2$ *ya que* $13 \nmid 2^{91} - 2$*, dado que* $2^{91} - 2 \equiv 9 \mod 13$

Definición

Un ***número de Carmichael*** *es un número compuesto* n *tal que* $n \mid a^n - a \ \forall\ a \in \mathbb{Z}$*, es decir, tal que* n *es un pseudoprimo de base* $a \ \forall\ a \in \mathbb{Z}$*.*

Más acerca de los pseudoprimos

Ejemplos

- $341(= 11 \cdot 31)$ *es un pseudoprimo de base 2, pero no de base 3. En efecto, es posible realizar el cálculo y ver que* $341 \mid 2^{341} - 2$*; sin embargo,* $341 \nmid 3^{341} - 3$ *debido a que* $31 \nmid 3^{341} - 3$*, pues* $3^{341} - 3 \equiv 10 \mod 31$*.*
- $91(= 7 \cdot 13)$ *es un pseudoprimo de base 3, pero no de base 2; pues* $91 \mid 3^{91} - 3$*, pero* $91 \nmid 2^{91} - 2$ *ya que* $13 \nmid 2^{91} - 2$*, dado que* $2^{91} - 2 \equiv 9 \mod 13$

Definición

Un ***número de Carmichael*** *es un número compuesto* n *tal que* $n \mid a^n - a \ \forall\, a \in \mathbb{Z}$*, es decir, tal que* n *es un pseudoprimo de base* $a \ \forall\, a \in \mathbb{Z}$*.*

Más acerca de los pseudoprimos

Ejemplos

- $341(= 11 \cdot 31)$ *es un pseudoprimo de base 2, pero no de base 3. En efecto, es posible realizar el cálculo y ver que* $341 \mid 2^{341} - 2$*; sin embargo,* $341 \nmid 3^{341} - 3$ *debido a que* $31 \nmid 3^{341} - 3$*, pues* $3^{341} - 3 \equiv 10 \mod 31$*.*
- $91(= 7 \cdot 13)$ *es un pseudoprimo de base 3, pero no de base 2; pues* $91 \mid 3^{91} - 3$*, pero* $91 \nmid 2^{91} - 2$ *ya que* $13 \nmid 2^{91} - 2$*, dado que* $2^{91} - 2 \equiv 9 \mod 13$

Definición

Un ***número de Carmichael*** *es un número compuesto* n *tal que* $n \mid a^n - a \ \forall\, a \in \mathbb{Z}$*, es decir, tal que* n *es un pseudoprimo de base* $a \ \forall\, a \in \mathbb{Z}$*.*

Más acerca de los pseudoprimos

Ejemplos

- $341(= 11 \cdot 31)$ *es un pseudoprimo de base 2, pero no de base 3. En efecto, es posible realizar el cálculo y ver que* $341 \mid 2^{341} - 2$*; sin embargo,* $341 \nmid 3^{341} - 3$ *debido a que* $31 \nmid 3^{341} - 3$*, pues* $3^{341} - 3 \equiv 10 \mod 31$*.*
- $91(= 7 \cdot 13)$ *es un pseudoprimo de base 3, pero no de base 2; pues* $91 \mid 3^{91} - 3$*, pero* $91 \nmid 2^{91} - 2$ *ya que* $13 \nmid 2^{91} - 2$*, dado que* $2^{91} - 2 \equiv 9 \mod 13$

Definición

Un ***número de Carmichael*** *es un número compuesto* n *tal que* $n \mid a^n - a \ \ \forall\, a \in \mathbb{Z}$*, es decir, tal que* n *es un pseudoprimo de base* $a \ \ \forall\, a \in \mathbb{Z}$*.*


Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p - 1 \mid n - 1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*

$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.

$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0, 1, 2\}$.

$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.

Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \mathrm{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.

Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p - 1 \mid n - 1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*

$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.

$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0, 1, 2\}$.

$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.

Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \mathrm{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.

Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p - 1 \mid n - 1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*

$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.

$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0, 1, 2\}$.

$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.

Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \text{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.

Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p - 1 \mid n - 1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*

$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.

$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0, 1, 2\}$.

$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.

Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \text{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.

Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p - 1 \mid n - 1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*
$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.
$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0, 1, 2\}$.
$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.
Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \text{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.

Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p - 1 \mid n - 1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*
$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.
$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0, 1, 2\}$.
$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.
Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \mathrm{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.

Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p-1 \mid n-1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*
$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.
$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0,1,2\}$.
$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.
Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \mathrm{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.


Números de Carmichael

Teorema (Criterio de Korselt)

Sea $n \in \mathbb{N}\backslash\{1\}$. *Entonces,* $n \mid a^n - a \ \forall\, a \in \mathbb{Z} \iff n$ *es libre de cuadrado y* $p-1 \mid n-1$ *para cualquier divisor primo* p *de* n.

Definición

La ***función*** λ ***de Carmichael*** *es la siguiente:*
$\lambda(p^a) = \phi(p^a)$ *si* p *es un número primo impar,* $a \in \mathbb{N}$.
$\lambda(2^a) = \phi(2^a)$ *si* $a \in \{0,1,2\}$.
$\lambda(2^a) = \frac{1}{2}\phi(2^a)$ *si* $a \geq 3$.
Finalmente, $\lambda(2^a p_1^{a_1} \cdots p_k^{a_k}) = \mathrm{M.C.M}\{\lambda(2^a), \lambda(p_1^{a_1}), \ldots, \lambda(p_k^{a_k})\}$ *si* $p_1, \ldots, p_k$ *son números primos impares distintos;* $a_1, \ldots, a_k \in \mathbb{N}$ *y* $a \in \mathbb{N} \cup \{0\}$.

La función λ

Lema

Si p es un número primo, $a \in \mathbb{Z}\backslash\{0\}$ y $(x, p^a) = 1$, entonces $x^{\lambda(p^a)} \equiv 1 \mod p^a$.

Con ayuda de este lema, se demuestra el siguiente teorema.

Teorema

Sea $n \in \mathbb{N}$, $x \in \mathbb{Z}$ con $(x, n) = 1$. Entonces, se cumple que $x^{\lambda(n)} \equiv 1 \mod n$.

Este teorema es análogo al teorema de Euler, si reemplazamos la función ϕ de Euler por la función λ de Carmichael.

La función λ

Lema

Si p es un número primo, $a \in \mathbb{Z}\backslash\{0\}$ y $(x, p^a) = 1$, entonces $x^{\lambda(p^a)} \equiv 1 \mod p^a$.

Con ayuda de este lema, se demuestra el siguiente teorema.

Teorema

Sea $n \in \mathbb{N}$, $x \in \mathbb{Z}$ con $(x, n) = 1$. Entonces, se cumple que $x^{\lambda(n)} \equiv 1 \mod n$.

Este teorema es análogo al teorema de Euler, si reemplazamos la función ϕ de Euler por la función λ de Carmichael.

La función λ

Lema

Si p es un número primo, $a \in \mathbb{Z}\backslash\{0\}$ y $(x, p^a) = 1$, entonces $x^{\lambda(p^a)} \equiv 1 \mod p^a$.

Con ayuda de este lema, se demuestra el siguiente teorema.

Teorema

Sea $n \in \mathbb{N}$, $x \in \mathbb{Z}$ con $(x, n) = 1$. Entonces, se cumple que $x^{\lambda(n)} \equiv 1 \mod n$.

Este teorema es análogo al teorema de Euler, si reemplazamos la función ϕ de Euler por la función λ de Carmichael.

La función λ

Lema

Si p es un número primo, $a \in \mathbb{Z}\backslash\{0\}$ y $(x, p^a) = 1$, entonces $x^{\lambda(p^a)} \equiv 1 \mod p^a$.

Con ayuda de este lema, se demuestra el siguiente teorema.

Teorema

Sea $n \in \mathbb{N}$, $x \in \mathbb{Z}$ con $(x, n) = 1$. Entonces, se cumple que $x^{\lambda(n)} \equiv 1 \mod n$.

Este teorema es análogo al teorema de Euler, si reemplazamos la función ϕ de Euler por la función λ de Carmichael.

La función λ

Lema

Si p es un número primo, $a \in \mathbb{Z}\backslash\{0\}$ y $(x, p^a) = 1$, entonces $x^{\lambda(p^a)} \equiv 1 \mod p^a$.

Con ayuda de este lema, se demuestra el siguiente teorema.

Teorema

Sea $n \in \mathbb{N}$, $x \in \mathbb{Z}$ con $(x, n) = 1$. Entonces, se cumple que $x^{\lambda(n)} \equiv 1 \mod n$.

Este teorema es análogo al teorema de Euler, si reemplazamos la función ϕ de Euler por la función λ de Carmichael.

La función λ

Lema

Si p es un número primo, $a \in \mathbb{Z}\backslash\{0\}$ y $(x, p^a) = 1$, entonces $x^{\lambda(p^a)} \equiv 1 \mod p^a$.

Con ayuda de este lema, se demuestra el siguiente teorema.

Teorema

Sea $n \in \mathbb{N}$, $x \in \mathbb{Z}$ con $(x, n) = 1$. Entonces, se cumple que $x^{\lambda(n)} \equiv 1 \mod n$.

Este teorema es análogo al teorema de Euler, si reemplazamos la función ϕ de Euler por la función λ de Carmichael.


λ-raíces primitivas

Definición

- *Sean $a, n \in \mathbb{N}\backslash\{1\}$, $(a, n) = 1$. Si $\lambda(n)$ es el mínimo entero tal que $a^{\lambda(n)} \equiv 1 \mod n$, entonces diremos que a es una* ***λ-raíz primitiva módulo*** *n.*
- *Para distinguir, a las raíces primitivas usuales las llamaremos* ***ϕ-raíces primitivas módulo n.***

Proposición

Si $n \in \mathbb{Z}$ es una potencia de primo, entonces hay λ-raíces primitivas módulo n.

λ-raíces primitivas

Definición

- *Sean* $a, n \in \mathbb{N}\backslash\{1\}$, $(a, n) = 1$. *Si* $\lambda(n)$ *es el mínimo entero tal que* $a^{\lambda(n)} \equiv 1 \mod n$, *entonces diremos que* a *es una* λ***-raíz primitiva módulo*** n.
- *Para distinguir, a las raíces primitivas usuales las llamaremos* ϕ***-raíces primitivas módulo n.***

Proposición

Si $n \in \mathbb{Z}$ *es una potencia de primo, entonces hay* λ*-raíces primitivas módulo* n.

λ-raíces primitivas

Definición

- *Sean* $a, n \in \mathbb{N}\backslash\{1\}$, $(a, n) = 1$. *Si* $\lambda(n)$ *es el mínimo entero tal que* $a^{\lambda(n)} \equiv 1 \mod n$, *entonces diremos que* a *es una* λ***-raíz primitiva módulo*** n.
- *Para distinguir, a las raíces primitivas usuales las llamaremos* ϕ***-raíces primitivas módulo n***.

Proposición

Si $n \in \mathbb{Z}$ *es una potencia de primo, entonces hay* λ*-raíces primitivas módulo* n.

λ-raíces primitivas

Definición

- *Sean* $a, n \in \mathbb{N}\backslash\{1\}$, $(a, n) = 1$. *Si* $\lambda(n)$ *es el mínimo entero tal que* $a^{\lambda(n)} \equiv 1 \mod n$, *entonces diremos que* a *es una* λ***-raíz primitiva módulo*** n.
- *Para distinguir, a las raíces primitivas usuales las llamaremos* ϕ***-raíces primitivas módulo n***.

Proposición

Si $n \in \mathbb{Z}$ *es una potencia de primo, entonces hay* λ*-raíces primitivas módulo* n.

λ-raíces primitivas

Definición

- *Sean $a, n \in \mathbb{N}\backslash\{1\}$, $(a, n) = 1$. Si $\lambda(n)$ es el mínimo entero tal que $a^{\lambda(n)} \equiv 1 \mod n$, entonces diremos que a es una λ-**raíz primitiva módulo** n.*
- *Para distinguir, a las raíces primitivas usuales las llamaremos ϕ-**raíces primitivas módulo n**.*

Proposición

Si $n \in \mathbb{Z}$ es una potencia de primo, entonces hay λ-raíces primitivas módulo n.

Números de Carmichael

Teorema

Dada la congruencia $X^{\lambda(n)} \equiv 1 \mod n,\ (X,n) = 1$, existe una solución g que es una λ-raíz primitiva; y, para cualquiera de estas soluciones g, hay $\phi(\lambda(n))$ λ-raíces primitivas congruentes con potencias de g.

R.D. Carmichael fue el primero en encontrar un número de Carmichael, con la ayuda de la teoría de la función λ. Enseguida veremos cómo lo hizo.

Teorema (Carmichael)

Sea $n \in \mathbb{Z}$. Entonces, $n \mid a^n - a\ \forall\, a \in \mathbb{Z} \iff \lambda(n) \mid n - 1$.

Números de Carmichael

Teorema

Dada la congruencia $X^{\lambda(n)} \equiv 1 \mod n,\ (X,n) = 1$, existe una solución g que es una λ-raíz primitiva; y, para cualquiera de estas soluciones g, hay $\phi(\lambda(n))$ λ-raíces primitivas congruentes con potencias de g.

R.D. Carmichael fue el primero en encontrar un número de Carmichael, con la ayuda de la teoría de la función λ. Enseguida veremos cómo lo hizo.

Teorema (Carmichael)

Sea $n \in \mathbb{Z}$. Entonces, $n \mid a^n - a\ \forall\, a \in \mathbb{Z} \iff \lambda(n) \mid n - 1$.

Números de Carmichael

Teorema

Dada la congruencia $X^{\lambda(n)} \equiv 1 \mod n,\ (X,n) = 1$, *existe una solución* g *que es una* λ*-raíz primitiva; y, para cualquiera de estas soluciones* g, *hay* $\phi(\lambda(n))$ λ*-raíces primitivas congruentes con potencias de* g.

R.D. Carmichael fue el primero en encontrar un número de Carmichael, con la ayuda de la teoría de la función λ. Enseguida veremos cómo lo hizo.

Teorema (Carmichael)

Sea $n \in \mathbb{Z}$. *Entonces,* $n \mid a^n - a\ \forall\, a \in \mathbb{Z} \iff \lambda(n) \mid n-1$.

Números de Carmichael

Teorema

Dada la congruencia $X^{\lambda(n)} \equiv 1 \mod n,\ (X,n) = 1$, *existe una solución* g *que es una* λ*-raíz primitiva; y, para cualquiera de estas soluciones* g, *hay* $\phi(\lambda(n))$ λ*-raíces primitivas congruentes con potencias de* g.

R.D. Carmichael fue el primero en encontrar un número de Carmichael, con la ayuda de la teoría de la función λ. Enseguida veremos cómo lo hizo.

Teorema (Carmichael)

Sea $n \in \mathbb{Z}$. *Entonces,* $n \mid a^n - a\ \ \forall\ a \in \mathbb{Z} \iff \lambda(n) \mid n-1$.

Propiedades de los números de Carmichael

Así, si n es un número de Carmichael, entonces n es impar. En efecto, para $n \geq 2$, se tiene que $\lambda(n)$ es par, y dado que por el teorema de Carmichael $\lambda(n) \mid n-1$, entonces $n-1$ será también par, con lo cual n será impar.

Ahora bien, si p es un número primo tal que $p \mid n$, entonces $p-1 \mid n-1 = (n/p)(p-1) + (n/p) - 1$, por consiguiente, $p-1 \mid (n/p) - 1$.

Es decir, si $n = p_1 p_2 \cdots p_k$, los p_i primos distintos, entonces,

$$p_i - 1 \mid p_1 \cdots p_{i-1} p_{i+1} \cdots p_k - 1, \quad \forall \ 1 \leq i \leq k$$

Por ejemplo, no puede tenerse que $k = 2$. Si $n = p_1 p_2$, entonces por la condición anterior se tendrá que $p_1 - 1 \mid p_2 - 1$ y $p_2 - 1 \mid p_1 - 1$, con lo cual $p_1 - 1 = p_2 - 1$ y $\therefore p_1 = p_2$, lo cual es absurdo.

Propiedades de los números de Carmichael

Así, si n es un número de Carmichael, entonces n es impar. En efecto, para $n \geq 2$, se tiene que $\lambda(n)$ es par, y dado que por el teorema de Carmichael $\lambda(n) \mid n-1$, entonces $n-1$ será también par, con lo cual n será impar.

Ahora bien, si p es un número primo tal que $p \mid n$, entonces $p-1 \mid n-1 = (n/p)(p-1) + (n/p) - 1$, por consiguiente, $p-1 \mid (n/p) - 1$.

Es decir, si $n = p_1 p_2 \cdots p_k$, los p_i primos distintos, entonces,

$$p_i - 1 \mid p_1 \cdots p_{i-1} p_{i+1} \cdots p_k - 1, \quad \forall \ 1 \leq i \leq k$$

Por ejemplo, no puede tenerse que $k = 2$. Si $n = p_1 p_2$, entonces por la condición anterior se tendrá que $p_1 - 1 \mid p_2 - 1$ y $p_2 - 1 \mid p_1 - 1$, con lo cual $p_1 - 1 = p_2 - 1$ y $\therefore p_1 = p_2$, lo cual es absurdo.

Propiedades de los números de Carmichael

Así, si n es un número de Carmichael, entonces n es impar. En efecto, para $n \geq 2$, se tiene que $\lambda(n)$ es par, y dado que por el teorema de Carmichael $\lambda(n) \mid n-1$, entonces $n-1$ será también par, con lo cual n será impar.

Ahora bien, si p es un número primo tal que $p \mid n$, entonces $p-1 \mid n-1 = (n/p)(p-1) + (n/p) - 1$, por consiguiente, $p-1 \mid (n/p) - 1$.

Es decir, si $n = p_1 p_2 \cdots p_k$, los p_i primos distintos, entonces,

$$p_i - 1 \mid p_1 \cdots p_{i-1} p_{i+1} \cdots p_k - 1, \quad \forall \ 1 \leq i \leq k$$

Por ejemplo, no puede tenerse que $k = 2$. Si $n = p_1 p_2$, entonces por la condición anterior se tendrá que $p_1 - 1 \mid p_2 - 1$ y $p_2 - 1 \mid p_1 - 1$, con lo cual $p_1 - 1 = p_2 - 1$ y $\therefore p_1 = p_2$, lo cual es absurdo.

Propiedades de los números de Carmichael

Así, si n es un número de Carmichael, entonces n es impar. En efecto, para $n \geq 2$, se tiene que $\lambda(n)$ es par, y dado que por el teorema de Carmichael $\lambda(n) \mid n-1$, entonces $n-1$ será también par, con lo cual n será impar.

Ahora bien, si p es un número primo tal que $p \mid n$, entonces $p-1 \mid n-1 = (n/p)(p-1) + (n/p) - 1$, por consiguiente, $p-1 \mid (n/p) - 1$.

Es decir, si $n = p_1 p_2 \cdots p_k$, los p_i primos distintos, entonces,

$$p_i - 1 \mid p_1 \cdots p_{i-1} p_{i+1} \cdots p_k - 1, \quad \forall \ 1 \leq i \leq k$$

Por ejemplo, no puede tenerse que $k = 2$. Si $n = p_1 p_2$, entonces por la condición anterior se tendrá que $p_1 - 1 \mid p_2 - 1$ y $p_2 - 1 \mid p_1 - 1$, con lo cual $p_1 - 1 = p_2 - 1$ y $\therefore p_1 = p_2$, lo cual es absurdo.

Propiedades de los números de Carmichael, un ejemplo

Todo lo dicho anteriormente puede resumirse de la manera siguiente.

Proposición

Si n es un número de Carmichael, entonces n es un producto de al menos tres números primos impares distintos.

Ejemplo (Chernick)

Sea $m \in \mathbb{N}$ tal que $6m+1$, $12m+1$ y $18m+1$ son todos ellos primos. Entonces, $n := (6m+1)(12m+1)(18m+1)$ es un número de Carmichael. En efecto, $\lambda(n) = 18m$, y $n - 1 = 1296m^3 + 396m^2 + 36m$. De ahí que $\lambda(n) \mid n-1$ y, por consiguiente, n es de Carmichael.

Propiedades de los números de Carmichael, un ejemplo

Todo lo dicho anteriormente puede resumirse de la manera siguiente.

Proposición

Si n es un número de Carmichael, entonces n es un producto de al menos tres números primos impares distintos.

Ejemplo (Chernick)

Sea $m \in \mathbb{N}$ tal que $6m+1$, $12m+1$ y $18m+1$ son todos ellos primos. Entonces, $n := (6m+1)(12m+1)(18m+1)$ es un número de Carmichael. En efecto, $\lambda(n) = 18m$, y $n - 1 = 1296m^3 + 396m^2 + 36m$. De ahí que $\lambda(n) \mid n-1$ y, por consiguiente, n es de Carmichael.


Propiedades de los números de Carmichael, un ejemplo

Todo lo dicho anteriormente puede resumirse de la manera siguiente.

Proposición

Si n es un número de Carmichael, entonces n es un producto de al menos tres números primos impares distintos.

Ejemplo (Chernick)

Sea $m \in \mathbb{N}$ tal que $6m+1$, $12m+1$ y $18m+1$ son todos ellos primos. Entonces, $n := (6m+1)(12m+1)(18m+1)$ es un número de Carmichael. En efecto, $\lambda(n) = 18m$, y $n - 1 = 1296m^3 + 396m^2 + 36m$. De ahí que $\lambda(n) \mid n-1$ y, por consiguiente, n es de Carmichael.


Propiedades de los números de Carmichael, un ejemplo

Todo lo dicho anteriormente puede resumirse de la manera siguiente.

Proposición

Si n es un número de Carmichael, entonces n es un producto de al menos tres números primos impares distintos.

Ejemplo (Chernick)

Sea $m \in \mathbb{N}$ tal que $6m+1$, $12m+1$ y $18m+1$ son todos ellos primos. Entonces, $n := (6m+1)(12m+1)(18m+1)$ es un número de Carmichael. En efecto, $\lambda(n) = 18m$, y $n - 1 = 1296m^3 + 396m^2 + 36m$. De ahí que $\lambda(n) \mid n-1$ y, por consiguiente, n es de Carmichael.

Ejemplo de un número de Carmichael

Ejemplo

En particular, cuando $m = 1$, entonces $6m + 1$, $12m + 1$ y $18m + 1$ son todos números primos, con lo cual su producto $7 \cdot 13 \cdot 19 = 1729$ es un número de Carmichael.

De acuerdo con una conjetura de Hardy y Littlewood, existirían una infinidad de números m tales que $6m + 1$, $12m + 1$ y $18m + 1$ son todos ellos primos, lo cual nos daría una infinidad de números de Carmichael.

Ejemplo de un número de Carmichael

Ejemplo

En particular, cuando $m = 1$, entonces $6m + 1$, $12m + 1$ y $18m + 1$ son todos números primos, con lo cual su producto $7 \cdot 13 \cdot 19 = 1729$ es un número de Carmichael.

De acuerdo con una conjetura de Hardy y Littlewood, existirían una infinidad de números m tales que $6m + 1$, $12m + 1$ y $18m + 1$ son todos ellos primos, lo cual nos daría una infinidad de números de Carmichael.

Ejemplo de un número de Carmichael

Ejemplo

En particular, cuando $m = 1$, entonces $6m + 1$, $12m + 1$ y $18m + 1$ son todos números primos, con lo cual su producto $7 \cdot 13 \cdot 19 = 1729$ es un número de Carmichael.

De acuerdo con una conjetura de Hardy y Littlewood, existirían una infinidad de números m tales que $6m + 1$, $12m + 1$ y $18m + 1$ son todos ellos primos, lo cual nos daría una infinidad de números de Carmichael.

El cálculo de Carmichael

Supóngase que $n = pqr$, $p < q < r$ primos distintos, y n de Carmichael. Entonces, por la condición vista anteriormente, se tiene que $p - 1 \mid qr - 1$, $q - 1 \mid pr - 1$ y $r - 1 \mid pq - 1$. Si por ejemplo $p = 7$, entonces la condición $r - 1 \mid 7q - 1$, por lo cual $(7q - 1)/(r - 1) = m \in \mathbb{Z}$, en donde además $2 \leq m \leq 6$. Despejando r, tenemos que

$$r = \frac{7q + m - 1}{m}$$

Como $q - 1 \mid pr - 1$, entonces $(pr - 1)/(q - 1) \in \mathbb{Z}$ Con esta condición se inspeccionan los valores posibles de q. Algunos valores se descartan debido a la condición de que r es primo, otros permanecen. Por último, estos valores se ponen a prueba mediante el teorema de Carmichael. Se encuentra que los números $7 \cdot 19 \cdot 67$, $7 \cdot 13 \cdot 31$, $7 \cdot 31 \cdot 73$ y $7 \cdot 13 \cdot 19$ son de Carmichael.

Los números de Carmichael más pequeños

Los primeros números de Carmichael son:
$561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$,
$2821 = 7 \cdot 13 \cdot 31$, $6601 = 7 \cdot 23 \cdot 41$, $8911 = 7 \cdot 19 \cdot 67$, $10585 = 5 \cdot 29 \cdot 73$,
$15841 = 7 \cdot 31 \cdot 73$, $29341 = 13 \cdot 37 \cdot 61$, $41041 = 7 \cdot 11 \cdot 13 \cdot 41$,
$46657 = 13 \cdot 37 \cdot 97$, $52633 = 7 \cdot 73 \cdot 103$, $62745 = 3 \cdot 5 \cdot 47 \cdot 89$,
$63973 = 7 \cdot 13 \cdot 19 \cdot 37$, $75361 = 11 \cdot 17 \cdot 31$, $101101 = 7 \cdot 11 \cdot 13 \cdot 101$,
$115921 = 13 \cdot 37 \cdot 241$, $126217 = 7 \cdot 13 \cdot 19 \cdot 73$, $162401 = 17 \cdot 41 \cdot 233$,
$172081 = 7 \cdot 13 \cdot 31 \cdot 61$, $188461 = 7 \cdot 13 \cdot 19 \cdot 109$, $252601 = 41 \cdot 61 \cdot 101$.

Algunas estimaciones de la cantidad de números de Carmichael

Sea $C(x) = \#\{n \leq x \big| n \text{ es de Carmichael}\}$

Pomerance, Selfridge y Wagstaff Jr. demostraron que

$$C(x) \leq x^{1-\{1+o(1)\}\log\log\log x/\log\log x}$$

Alford, Granville y Pomerance demostraron que, para x suficientemente grande,

$$C(x) \geq x^{2/7}$$

lo cual nos dice que existe una infinidad de números de Carmichael.

Algunas estimaciones de la cantidad de números de Carmichael

Sea $C(x) = \#\{n \leq x \big| n \text{ es de Carmichael}\}$

Pomerance, Selfridge y Wagstaff Jr. demostraron que

$$C(x) \leq x^{1-\{1+o(1)\}\log\log\log x/\log\log x}$$

Alford, Granville y Pomerance demostraron que, para x suficientemente grande,

$$C(x) \geq x^{2/7}$$

lo cual nos dice que existe una infinidad de números de Carmichael.

Algunas estimaciones de la cantidad de números de Carmichael

Sea $C(x) = \#\{n \leq x \big| n \text{ es de Carmichael}\}$

Pomerance, Selfridge y Wagstaff Jr. demostraron que

$$C(x) \leq x^{1-\{1+o(1)\}\log\log\log x/\log\log x}$$

Alford, Granville y Pomerance demostraron que, para x suficientemente grande,

$$C(x) \geq x^{2/7}$$

lo cual nos dice que existe una infinidad de números de Carmichael.

Bibliografía

- W.R. Alford, Andrew Granville y Carl Pomerance, “There are infinitely Carmichael numbers"; *Annals of Mathematics* **140** (1994), 703-722.
- R.D. Carmichael, “Note on a new number theory function"; *Bulletin of the American Mathematical Society* **16** (1910), 232-238.
- R.D. Carmichael, “On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \mod P$"; *American Mathematical Monthly*; **19** (1912), 22-27.
- Ireland, Kenneth y Rosen, Michael, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1990.
- C. Pomerance, J.L. Selfridge y S.S. Wagstaff Jr., “Thepseudoprimes to 25×10^9"; *Mathematics of Computation* **35** (1980), 1003-1026.

Bibliografía

- W.R. Alford, Andrew Granville y Carl Pomerance, “There are infinitely Carmichael numbers"; *Annals of Mathematics* **140** (1994), 703-722.
- R.D. Carmichael, “Note on a new number theory function"; *Bulletin of the American Mathematical Society* **16** (1910), 232-238.
- R.D. Carmichael, “On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \mod P$"; *American Mathematical Monthly*; **19** (1912), 22-27.
- Ireland, Kenneth y Rosen, Michael, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1990.
- C. Pomerance, J.L. Selfridge y S.S. Wagstaff Jr., “Thepseudoprimes to 25×10^9"; *Mathematics of Computation* **35** (1980), 1003-1026.

Bibliografía

- W.R. Alford, Andrew Granville y Carl Pomerance, “There are infinitely Carmichael numbers"; *Annals of Mathematics* **140** (1994), 703-722.
- R.D. Carmichael, “Note on a new number theory function"; *Bulletin of the American Mathematical Society* **16** (1910), 232-238.
- R.D. Carmichael, “On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \mod P$"; *American Mathematical Monthly*; **19** (1912), 22-27.
- Ireland, Kenneth y Rosen, Michael, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1990.
- C. Pomerance, J.L. Selfridge y S.S. Wagstaff Jr., “Thepseudoprimes to 25×10^9"; *Mathematics of Computation* **35** (1980), 1003-1026.

Bibliografía

- W.R. Alford, Andrew Granville y Carl Pomerance, “There are infinitely Carmichael numbers"; *Annals of Mathematics* **140** (1994), 703-722.
- R.D. Carmichael, “Note on a new number theory function"; *Bulletin of the American Mathematical Society* **16** (1910), 232-238.
- R.D. Carmichael, “On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \mod P$"; *American Mathematical Monthly*; **19** (1912), 22-27.
- Ireland, Kenneth y Rosen, Michael, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1990.
- C. Pomerance, J.L. Selfridge y S.S. Wagstaff Jr., “Thepseudoprimes to 25×10^9"; *Mathematics of Computation* **35** (1980), 1003-1026.

Bibliografía

- W.R. Alford, Andrew Granville y Carl Pomerance, “There are infinitely Carmichael numbers"; *Annals of Mathematics* **140** (1994), 703-722.
- R.D. Carmichael, “Note on a new number theory function"; *Bulletin of the American Mathematical Society* **16** (1910), 232-238.
- R.D. Carmichael, “On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \mod P$"; *American Mathematical Monthly*; **19** (1912), 22-27.
- Ireland, Kenneth y Rosen, Michael, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1990.
- C. Pomerance, J.L. Selfridge y S.S. Wagstaff Jr., “Thepseudoprimes to 25×10^9"; *Mathematics of Computation* **35** (1980), 1003-1026.