Teoría de Números 7

Temas

Teorema de Fermat (demostración)

Recordemos el Teorema de Fermat:

> Sea p primo, $a \in Z$ y $mcd(a,p) = 1$ entonces se cumple que:
>
> $$a^{p-1} \equiv 1 \ \ mod(p)$$

Sea $P = \{0, 1, \dots, p-1\}$ un SRC módulo p, luego, como $mcd(a,p) = 1 \implies$ al multiplicar cada elemento de P por a el resultado será un conjunto P' que seguirá siendo un SRC módulo $p \implies P' = \{0, a, 2a, \dots, (p-1)a\}$

Al multiplicar todos los elementos de P' excepto el cero obtenemos $a * 2a * 3a * \cdots * (p-1)a \equiv \ 1 * 2 * \cdots * (p-1) \ mod(p) \implies a^{p-1}(p-1)! \equiv (p-1)! \ mod(p)$ y como p es primo entonces es primo relativo con todos los números menores que él $\implies mcd(p,(p-1)!) = 1 \implies a^{p-1} \equiv 1 \ mod(p)$

Teorema de Wilson (demostración)

Recordemos el Teorema de Wilson:

> Sea $p \in \mathrm{N}$. Se cumple que p es primo $\iff p \div (p-1)! + 1$

Demostración

- $\Leftarrow$

Sea $p \div (p-1)! + 1$ y supongamos que existe $d \div p$ tal que $1 < d < p \implies d \div (p-1)!$ pero d no divide a 1 por tanto d no divide a $(p-1)! + 1$, de donde $d = 1$ o $d = p$ \implies p$ es primo

- $\implies$

Sea $P = \{1, 2, \dots, p-1\}$ un SRC exceptuando el cero, nótese que cada elemento posee un inverso módulo p distinto en el conjunto P porque cada $a \in P$ cumple que $mcd(a, p) = 1$. Analicemos el caso en que un elemento sea su mismo inverso:

$$a^2 \equiv 1 \ mod(p)$$
$$(a+1)(a-1) \equiv 0 \ mod(p)$$

De donde $a = 1$ o $a = p - 1$, por lo que en el conjunto $\{2, 3, \dots, p-2\}$ cada número posee un inverso distinto de él mismo, por lo que se cumple que:

$$2 * 3 * \cdots * (p-2) \equiv 1 \ mod(p)$$
$$2 * 3 * \cdots * (p-2) * (p-1) \equiv (p-1) \ mod(p)$$
$$(p-1)! \equiv -1 \ mod(p)$$
$$(p-1)! + 1 \equiv 0 \ mod(p)$$

Que es lo que queríamos demostrar

Función aritmética

> Una función es aritmética si está definida en Z_+

Sea $\varphi(n)$ una función aritmética que retorna la cantidad de números menores que n que son coprimos con n

Sistema Reducido de Restos

> Sistema reducido de restos módulo m es un conjunto de $\varphi(m)$ enteros positivos que son primos relativos con m, de modo que todo par de ellos es incongruente módulo m.

Si $r_1, r_2, \dots, r_{\varphi(n)}$ es un sistema reducido de restos módulo n y a es un entero positivo tal que $mcd(a, n) = 1$, entonces $ar_1, ar_2, \dots, ar_{\varphi(n)}$ también es un sistema reducido de restos módulo n.

Demostración

Debemos demostrar que los $ar_1, ar_2, \dots, ar_{\varphi(n)}$ son distintos modularmente y primos relativos con n.

- Supongamos que para algún r_k se cumple que $mcd(n, ar_k) = d > 1 \implies$ existe p primo tal que $p \div n$ y $p \div ar_k$ pero como $mcd(a, n) = 1 \implies p \div r_k$ contradicción porque $mcd(n, r_k) = 1$
- Supongamos que para algún i, j se cumple que $ar_i \equiv ar_j \ mod(n)$, luego, como $mcd(a, n) = 1 \implies r_i \equiv r_j \ mod(n)$ contradicción porque r_i, r_j pertenecen a un SRR

Teorema de Euler

> Sean $a, n \in Z_+$, si se cumple que $mcd(a, n) = 1 \implies a^{\varphi(n)} \equiv 1 \ mod(n)$

Demostración

Sea $r_1, r_2, \dots, r_{\varphi(n)}$ un SRR módulo n, entonces se cumple que al multiplicarlo por a tal que $mcd(a,n) = 1$ también tenemos otro SRR y por tanto:

$$(ar_1)(ar_2)\cdots(ar_{\varphi(n)}) \equiv r_1 r_2 \cdots r_{\varphi(n)} \ mod(n)$$
$$a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \ mod(n)$$

Y como cada r_i es coprimo con n por propiedad de SRR entonces concluimos que:

$$a^{\varphi(n)} \equiv 1 \ mod(n)$$

Funciones multiplicativas

> Una función aritmética es multiplicativa si $\forall n, m \in \mathbb{Z}$ primos relativos se cumple que $f(nm) = f(n) * f(m)$.

> Una función aritmética es totalmente multiplicativa si $\forall n, m \in \mathbb{Z}$ se cumple que $f(nm) = f(n) * f(m)$.

> Si f es multiplicativa y $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ con p_i primos se cumple que $f(n) = f(p_1^{e_1}) * f(p_2^{e_2}) * \cdots f(p_k^{e_k})$

Función $\varphi(n)$

> La función $\varphi(n)$ es mutiplicativa

Para demostrar este teorema haremos uso de los siguientes lemas:

> **Lema 1:**
>
> Sean $a, b, m \in \mathbb{N} \implies$ se cumple que $mcd(ab, m) = 1 \iff mcd(a,m) = 1$ y $mcd(b,m) = 1$

La demostración en el sentido $\impliedby$ es obvia. En el otro caso, supongamos que no se cumple, sin pérdida de generalidad sea $mcd(a,m) = d > 1 \implies \exists\, p$ primo tal que $p \div m$ y $p \div a \implies p \div ab \implies p \div mcd(ab,m)$ contradicción porque $mcd(ab,m) = 1$

> **Lema 2:**
>
> Sean $a, b \in \mathbb{Z}_+^*$ coprimos, entonces se cumple que $mcd(ax, b) = 1 \iff mcd(x,b) = 1$

($\implies$) Supongamos que $mcd(ax,b) = 1$ y $mcd(x,b) = d > 1 \implies \exists\, p$ primo tal que $p \div b$ y $p \div x \implies p \div ax \implies p \div mcd(ax,b)$ contradicción porque $mcd(ax,b) = 1$. Por tanto $d = 1$

($\impliedby$) Supongamos que $mcd(x,b) = 1$ y $mcd(ax,b) = d > 1 \implies \exists\, p$ primo tal que $p \div b$ y $p \div ax$, pero como $mcd(a,b) = 1 \implies p \div x$ porque p no puede dividir a a. Luego $p \div mcd(b,x) = 1$ contradicción, por lo que $d = 1$

> **Lema 3:**
>
> Sean $k, l \in \mathbb{Z}_+^*$ coprimos. Si x y y recorren respectivamente sistemas completos de restos módulos k y l, entonces $xl + yk$ recorre un sistema completo de restos módulo kl

No es díficil ver que existen exactamente kl números de la forma $xl + yk$. Supongamos que $xl + yk$ no recorre el sistema completos de restos módulo kl, entonces:

$$x_1 l + y_1 k \equiv x_2 l + y_2 k \ mod(kl)$$

Por propiedades de congruencia se cumple que:

$$\begin{gathered} x_1 l + y_1 k \equiv x_2 l + y_2 k \ mod(k) \\ x_1 l \equiv x_2 l \ mod(k) \end{gathered}$$

Como $mcd(k, l) = 1$ entonces:

$$x_1 \equiv x_2 \ mod(k)$$

Contradicción porque x recorre un SRC módulo k. Análogamente se hace el análisis con l

> **Lema 4:**
>
> Sean $a, n \in \mathbb{N}$. Se cumple que $mcd(a, n) = 1 \iff mcd(x, n) = 1$ siendo $a \equiv x \ mod(n)$

Nótese que ambas expresiones son análogas, ya que $a \equiv x \ mod(n)$ es equivalente a $x \equiv a \ mod(n)$ por lo que basta demostrar en un solo sentido de la doble implicación.

Supongamos que dado $mcd(a, n) = 1$ se cumpe que $mcd(x, n) = d > 1 \implies \exists\, p$ primo tal que $p \div x$ y $p \div n$ pero como $a \equiv x \ mod(n)$ se cumple que $n \div (a - x) \implies p \div (a - x)$ y como $p \div x \implies p \div a \implies p \div mcd(a, n) = 1$ contradicción porque $mcd(a, n) = 1$

Demostración (Somoza)

Agrupemos los números desde 1 hasta mn de la siguiente forma:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ m & 2m & 3m & \cdots & nm \end{array}$$

Según el **Lema 1** para saber cuántos números hay coprimos con mn basta calcular cuántos números son coprimos con m y coprimos con n simultáneamente.

Nótese que en una fila, si un elemento deja resto k módulo m entonces todos los elementos de esa fila dejan resto k módulo n

Por cada columna tenemos un SRC módulo m, en el cual hay $\varphi(m)$ números primos relativos con m, ya que su resto módulo m es primo relativo con m

Analicemos ahora las filas, nótese que si tenemos un SRC módulo n, al multiplicarlo por m, como son coprimos seguiremos teniendo un SRC, y al sumarle una constante k igual el resultado será un SRC, luego, si en la matriz buscamos en la fila k observamos que es exactamente lo que tenemos, por lo cual, en cada fila de la matriz hay un SRC módulo n, en el cual hay $\varphi(n)$ números primos relativos con n

Por último, como tenemos en cada columna $\varphi(m)$ coprimos con m y en cada fila $\varphi(n)$ primos relativos con n, la cantidad total de números coprimos con m y n a la vez son $\varphi(m)\varphi(n)$

Demostración (Temas escogidos de Teoría de Números)

Sean a y b enteros positivos coprimos. Supongamos que x y y recorren sistemas completos de restos módulos a y b respectivamente. Por el **Lema 3** $xb + ya$ recorre un sistema completo de restos módulo ab, luego aplicando el **Lema 1** y **Lema 2** se cumple que:

$$(xb + ya, ab) = 1 \iff (xb + ya, a) = 1, (xb + ya, b) = 1 \iff (xb, a) = 1, (ya, b) = 1 \iff (x, a) = 1, (y, b) =$$

Esto significa que $xb + ya$ es primo relativo con ab si y solo si x es coprimo con a y y es primo relativo con b, entonces $\varphi(ab) = \varphi(a)\varphi(b)$

Demostración (Youtube)

Queremos probar que la función $\varphi(n)$ es multiplicativa, o sea, $\varphi(mn) = \varphi(m)\varphi(n)$.

Sean $M = \{m_1, m_2, \ldots, m_p\}$ y $N = \{n_1, n_2, \ldots, n_q\}$ los sistemas de restos reducidos de m y n respectivamente. Si hallamos una función f biyectiva entre el producto cartesiano de ambos conjuntos y los números que son primos relativos con mn menores que mn habríamos demostrado que la cardinalidad tanto del producto cartesiano ($\varphi(m)\varphi(n)$) como la de $\varphi(mn)$ son iguales.

Apoyándonos en el **Lema 1** y **Lema 4** basta encontrar todos restos primos relativos con m y con n y los números que cumplen con esos restos simultáneamente, por lo que serán coprimos con mn, por tanto, nuestra función f será sobreyectiva. Utilizando el *Teorema Chino del Resto* dados m_i, n_j restos de m, n respectivamente, como $mcd(m, n) = 1 \implies$ el sistema de congruencia:

$$\begin{gathered} x \equiv m_i \ mod(m) \\ x \equiv n_j \ mod(n) \end{gathered}$$

Tiene solución y es única, por tanto, garantizamos que la función f es total (abarca todos los elementos del producto cartesiano de ambos conjuntos) y es inyectiva (porque la solución proporcionada por el *Teorema Chino del Resto* es única). Por tanto, podemos concluir que la función f es biyectiva, lo que implica que el producto cartesiano tiene tantos elementos como coprimos menores que $mn \implies \varphi(mn) = \varphi(m)\varphi(n)$

Expresión de $\varphi(n)$

> Sean $p, k \in \mathbb{Z}_+$ con p primo. Se cumple que:
>
> $$\varphi(p^k) = p^k(1 - \frac{1}{p})$$

Nótese que los números menores que p^k coprimos con este son los que no contienen ningún factor p por tanto, como $p^k = p(p^{k-1})$ entonces en los primeros p^k números hay p^{k-1} números que contienen un factor $p \implies \varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$

> Sea $n \in \mathbb{Z}$ con $n \geq 2$ y $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ entonces se cumple que:
>
> $$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

Orden a módulo n

Definición

> Sea $a, n \in Z_{+}$ y $mcd(a, n) = 1$. El menor entero positivo k tal que $a^k \equiv 1\ mod(n)$ se llama orden de a módulo n y se denota $ord_n a$

Propiedad

> Sea $a, n \in Z_{+}$,$mcd(a, n) = 1$ y $ord_n a = e \implies a^t \equiv 1\ mod(n) \iff e \div t$

($\Longleftarrow$) Supongamos que $e \div t$ entonces $t = eq \implies a^t = (a^e)^q$ por tanto:

$$a^e \equiv 1\ mod(n)$$
$$(a^e)^q \equiv 1\ mod(n)$$
$$a^t \equiv 1\ mod(n)$$

Vía Alvarito

($\implies$) Sea $t = eq + r$ entonces se cumple que como $a^t \equiv 1\ mod(n)$:

$$a^{eq+r} \equiv 1\ mod(n)$$
$$(a^e)^q * a^r equiv 1\ mod(n)$$

Y como $a^e \equiv 1\ mod(n)$ entonces:

$$a^r \equiv 1\ mod(n)$$

Lo cuales falso porque $ord_n a = e$ y $r < e$

Otra vía

Como se cumple que:

$$a^t \equiv 1\ mod(n)$$
$$a^e \equiv 1\ mod(n)$$

Entonces siendo $t = eq + r$ ocurre que $n \div a^t - a^e \implies n \div a^e(a^{e(q-1)+r} - 1)$ y como $a^e \equiv 1\ mod(n)$ entonces $n \div a^{e(q-1)+r} - 1$ de donde $a^{e(q-1)+r} \equiv 1\ mod(n)$. Luego:

$$a^{e(q-1)+r} \equiv 1\ mod(n)$$
$$a^e \equiv 1\ mod(n)$$

Por lo que $n \div a^{e(q-1)+r} - a^e \implies n \div a^e(a^{e(q-2)+r} - 1)$ y por el razonamiento anterior $n \div a^{e(q-2)+r} - 1$

Repitiendo este algoritmo q veces legamos a que $n \div a^{e(q-q)+r} - 1$ cumpliéndose que:

$$a^r \equiv 1\ mod(n)$$

Lo cuales falso porque $ord_n a = e$ y $r < e$

Raiz primitiva

> Sean $a, n \in Z_+$ y $mcd(a, n) = 1$ decimos que a es raíz primitiva módulo n si se cumple que $ord_n a = \varphi(n)$

Ejercicios

Problema 1

> Sean a, n enteros positivos con $a > 1$. Prueba que $n \div \varphi(a^n - 1)$

Solución

Nótese que $a^n - 1 \equiv 0\ mod(a^n - 1) \implies a^n \equiv 1\ mod(a^n - 1)$

Sea $k \in Z_+^*$ con $k < n \implies a^k \in$ SRC módulo $a^n - 1$, y como $k = 0$ entonces no existe valor de k tal que $a^k \equiv 1\ mod(a^n - 1)$ (no puede ser cero porque k es entero positivo y el poren se define siempre positivo)

Luego n es el menor entero positivo que cumple la condición, por tanto $ord_{a^n-1} a = n$. Pero como $mcd(a, a^n - 1) = 1$ se cumple que $a^{\varphi(a^n-1)} \equiv 1\ mod(a^n - 1) \implies n \div \varphi(a^n - 1)$

Problema 2

> Sea p primo mayor que 5. Prueba que $(p - 1)! + 1$ tiene 2 divisores primos diferentes.

Solución

Por el Teorema de Wilson se cumple que $p \div ((p - 1)! + 1)$, luego debemos demostrar que $(p - 1)! + 1$ no es una potencia de p, o sea, hay otro primo en su descomposición.

Supongamos que $(p - 1)! + 1 = p^t$ para algún $t > 1$, cumpliéndose que $t < p - 1$ porque $(p - 1)! + 1 < p^{p-1}$. Luego $p^t - 1 = (p - 1)!$, pero $p^t - 1 = (p - 1)(p^{t-1} + p^{t-2} + ... + p + 1)$, si dividimos entre $p - 1$ resulta en $p^{t-1} + p^{t-2} + ... + p + 1 = (p - 2)!$, nótese que como $p - 1$ es par $\implies$ es compuesto, luego $p - 1 \div (p - 2)!$, entonces $p^{t-1} + p^{t-2} + ... + p + 1 \equiv 0\ mod(p - 1)$, pero como $p \equiv 1\ mod(p - 1) \implies p^{t-1} + p^{t-2} + ... + p + 1 \equiv t\ mod(p - 1)$, entonces debe cumplirse que $t \equiv 0\ mod(p - 1)$, y esto no se cumple porque $t < p - 1$.

Entonces $(p - 1)! + 1$ no es una potencia de p, y como es mayor que p entonces tiene como factor otro primo distinto de p.

Problema 3

> Sea n entero positivo. Prueba que $\sum_{k=1}^{n} \varphi(k) * \lfloor \frac{n}{k} \rfloor = \frac{n(n-1)}{2}$

Solución

Nótese que $\frac{n(n-1)}{2} = 1 + 2 + \cdots + n$ y esto podemos verlo como la cantidad de fracciones $\frac{p}{q}$ tal que $p \leq q$ y $q \leq n$

Por cada denominador q desde 1 hasta n contamos la cantidad de fracciones propias irreducibles la cual es una cantidad $\varphi(q)$, y luego debemos generar todas las fracciones propias tal que $q \leq n$ con cada fracción irreducible, las cuales, por cada q hay $\lfloor \frac{n}{q} \rfloor$.

Por tanto $\frac{n(n-1)}{2} = \sum_{q=1}^{n} \varphi(q) * \lfloor \frac{n}{q} \rfloor$

Problema 4

> Calcule el $mcd(n! + 1, (n+1)!)$

Solución

Sea $mcd(n! + 1, (n+1)!) = d > 1 \implies \exists\, p$ primo tal que $p \div n! + 1 \implies p$ es coprimo con cada $k \leq n$ y como $p \div (n+1)! \implies p \div (n+1)$. Luego pueden darse dos casos:

- $(n+1)$ es compuesto $\implies p < (n+1) \implies p \div n!$ contradicción porque $p \div (n! + 1)$
- $(n+1)$ es primo $\implies p \div (n+1)$ y por el *Teorema de Wilson* $p \div n! + 1$

Por tanto, si $(n+1)$ es compuesto $mcd(n! + 1, (n+1)!) = 1$, de lo contrario $mcd(n! + 1, (n+1)!) = n + 1$

Problema 5

> Demuestra que si n es compuesto se cumple que $\varphi(n) \leq n - \sqrt{n}$

Solución (Alvarito)

Notemos que la cantidad de números coprimos con n es $n - m$ siendo m la cantidad de números que no son coprimos con n, luego, sustituyendo $\varphi(n) = n - m$ en la expresión resulta que debemos probar que $m \geq \sqrt{n}$.

Sea p_1 el menor primo que divide a n, luego, todo q desde 1 hasta $\sqrt{n}$ cumple que $p_1 q \leq n$ entonces al menos hay $\sqrt{n}$ números que no son coprimos con n

Problema 6

> Sea p primo mayor que 2. Demuestra que todo divisor de $2^p - 1$ es de la forma $2kp + 1$ con $k \in Z$

Solución

Notemos que basta analizar los divisores primos de $2^p - 1$ porque si dos divisores primos cumplen la condición, su producto también la cumplirá:

$$(2k_1p+1)(2k_2p+1) = 2p(2k_1k_2p + k_1 + k_2) + 1$$

Sea $q \in \mathbb{Z}_+^*$ primo tal que $q \div (2^p - 1) \implies 2^p \equiv 1 \ mod(q)$. Analicemos los siguientes casos:

- $p \div (q-1)$

Se cumple entonces que existe un $k \in \mathbb{Z}$ tal que $q - 1 = kp \implies q = kp + 1$ y como q es primo distinto de 2 entonces k es par, por lo que q cumple la condición del problema.

- p no divide a $q-1$

Notemos que en este caso $mcd(p, q-1) = 1$ por lo que existe x tal que $(q-1)x \equiv 1 \ mod(p) \implies \exists t \in \mathbb{Z}: \ (q-1)x = tp + 1$. Luego, utilizando el *Pequeño Teorema de Fermat* se cumple que $2^{q-1} \equiv 1 \ mod(q)$, por lo que $2^{(q-1)x} \equiv 1 \ mod(q)$, y también como $2^p \equiv 1 \ mod(q) \implies 2^{pt} \equiv 1 \ mod(q)$ por tanto, teniendo en cuenta que $(q-1)x = tp + 1$:

$$2^{pt+1} \equiv 1 \ mod(q)$$
$$2^{pt} * 2 \equiv 1 \ mod(q)$$

Pero como $2^{pt} \equiv 1 \ mod(q)$ contradicción, por tanto p siempre divide a todo divisor primo $q \implies$ todo divisor de $2^p - 1$ es de la forma $2kp + 1$ con $k \in \mathbb{Z}$

Ejercicios Extra

Problema 1

> Probar que $\frac{1}{2}\sqrt{n} \leq \varphi(n) \leq n$ para todo $n \in \mathbb{N}$

Soluciones de ejercicios extra

Solución 1

Para resolver el ejercicio vamos a apoyarnos en las siguientes desigualdades que podríamos probar fácilmente:

$$p - 1 > \sqrt{p}$$

Sea n primo $\implies \varphi(n) = n - 1$, luego, por las desigualdades anteriores se cumple que:

$$\frac{1}{2}\sqrt{n} < \sqrt{n} < n - 1 < n$$

Supongamos que n no es primo $\implies$

$$n = 2^{e_0}p_1^{e_1}\cdots p_k^{e_k}$$
$$n = 2^{e_0}p_1^{e_1-1}\cdots p_k^{e_k-1}p_1\cdots p_k$$
$$\varphi(n) = 2^{e_0-1}p_1^{e_1-1}\cdots p_k^{e_k-1}(p_1-1)(p_2-1)\cdots(p_k-1)$$

$$\frac{1}{2}\sqrt{n}=\frac{1}{2}2^{\frac{e_0}{2}}p_1^{\frac{e_1-1}{2}}\cdots p_k^{\frac{e_k-1}{2}}\sqrt{p_1}\cdots \sqrt{p_k}$$

Luego, démonos cuenta que:

$$\frac{1}{2}2^{\frac{e_0}{2}}=2^{\frac{e_0}{2}-1}\leq 2^{e_0-1}$$
$$p_1^{\frac{e_1-1}{2}}\leq p_1^{e_1-1}$$
$$\ldots$$
$$p_k^{\frac{e_k-1}{2}}\leq p_k^{e_k-1}$$
$$\sqrt{p_1}\leq (p_1-1)$$
$$\ldots$$
$$\sqrt{p_k}\leq (p_k-1)$$

Por tanto si n es compuesto entonces se cumple que: $\frac{1}{2}\sqrt{n}\leq \varphi(n)\leq n$