Teoría de Números II

José de Jesús Lavalle Martínez

Benemérita Universidad Autónoma de Puebla
Facultad de Ciencias de la Computación
Estructuras Discretas CCOS 009

Contenido

Motivación I

- En la sección 3.1 estudiamos el concepto de divisibilidad de números enteros.

Motivación I

- Un concepto importante basado en la divisibilidad es el de un número primo.

Motivación I

- Un primo es un número entero mayor que 1 que no es divisible por ningún entero positivo que no sea 1 y él mismo.

Motivación I

- El estudio de los números primos se remonta a la antigüedad.

Motivación I

- Hace miles de años se sabía que hay infinitos números primos; la prueba de este hecho, que se encuentra en las obras de Euclides, es famosa por su elegancia y belleza.

Motivación II

- Describiremos algunos de los resultados sobre números primos encontrados por matemáticos en los últimos 400 años.

Motivación II

- En particular, presentaremos un teorema importante, el teorema fundamental de la aritmética.

Motivación II

- Este teorema, que afirma que todo entero positivo puede escribirse de forma única como producto de números primos en orden no decreciente, tiene muchas consecuencias interesantes.

Motivación II

- En esta sección también estudiaremos el máximo común divisor de dos enteros, así como el mínimo común múltiplo de dos enteros.

Motivación II

- Desarrollaremos un algoritmo importante para calcular los máximos divisores comunes, llamado algoritmo euclidiano.

Números Primos

Definición 1

Un entero p mayor que 1 se llama *primo* si los únicos factores positivos de p son 1 y p. Un número entero positivo que es mayor que 1 y no es primo se llama *compuesto*.

Números Primos

Observación 1

El número entero 1 no es primo porque sólo tiene un factor positivo. Tenga en cuenta también que un número entero n es compuesto si y sólo si existe un número entero a tal que $a|n$ y $1 < a < n$.

Ejemplo 1

Ejemplo 1

El número entero 7 es primo porque sus únicos factores positivos son 1 y 7, mientras que el número entero 9 es compuesto porque es divisible por 3.

□

Teorema Fundamental de la Aritmética

Teorema 1

TEOREMA FUNDAMENTAL DE LA ARITMÉTICA Todo número entero mayor que 1 puede escribirse únicamente como un primo o como el producto de dos o más primos, donde los factores primos se escriben en orden de tamaño no decreciente. ■

Ejemplo 2

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$

Ejemplo 2

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$
$$641 = 641,$$

Ejemplo 2

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$
$$641 = 641,$$
$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$$

Ejemplo 2

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$
$$641 = 641,$$
$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$$
$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$$

□

División por Ensayo I

- A menudo es importante mostrar que un número entero dado es primo.

División por Ensayo I

- Por ejemplo, en criptología, los números primos grandes se utilizan en algunos métodos para hacer que los mensajes sean secretos.

División por Ensayo I

- Un procedimiento para demostrar que un número entero es primo se basa en la siguiente observación.

Teorema 2 I

Teorema 2

Si n es un entero compuesto, entonces n tiene un divisor primo menor o igual que $\sqrt{n}$.

■

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.
- Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.
- Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.
- Demostraremos que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.
- Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.
- Demostraremos que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $ab > \sqrt{n} \cdot \sqrt{n} = n$, lo cual es una contradicción.

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.
- Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.
- Demostraremos que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $ab > \sqrt{n} \cdot \sqrt{n} = n$, lo cual es una contradicción.
- En consecuencia, $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.
- Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.
- Demostraremos que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $ab > \sqrt{n} \cdot \sqrt{n} = n$, lo cual es una contradicción.
- En consecuencia, $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Debido a que tanto a como b son divisores de n, vemos que n tiene un divisor positivo que no excede a $\sqrt{n}$.

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.
- Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.
- Demostraremos que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $ab > \sqrt{n} \cdot \sqrt{n} = n$, lo cual es una contradicción.
- En consecuencia, $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Debido a que tanto a como b son divisores de n, vemos que n tiene un divisor positivo que no excede a $\sqrt{n}$.
- Este divisor es primo o, por el teorema fundamental de la aritmética, tiene un divisor primo menor que él.

Teorema 2 II

Demostración:

- Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$.
- Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.
- Demostraremos que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $ab > \sqrt{n} \cdot \sqrt{n} = n$, lo cual es una contradicción.
- En consecuencia, $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
- Debido a que tanto a como b son divisores de n, vemos que n tiene un divisor positivo que no excede a $\sqrt{n}$.
- Este divisor es primo o, por el teorema fundamental de la aritmética, tiene un divisor primo menor que él.
- En cualquier caso, n tiene un divisor primo menor o igual que $\sqrt{n}$.

División por Ensayo II

- Del teorema 2 se deduce que un número entero es primo si no es divisible por ningún primo menor o igual que su raíz cuadrada.
- Esto conduce al algoritmo de fuerza bruta conocido como **división por ensayo**.
- Para usar la división por ensayo, dividimos n por todos los primos que no excedan a $\sqrt{n}$ y concluimos que n es primo si no es divisible por ninguno de estos primos.

Ejemplo 3

Muestre que 101 es primo.

Ejemplo 3

Muestre que 101 es primo.

Solución:

- Los únicos números primos que no exceden a $\sqrt{101}$ son 2, 3, 5 y 7.

Ejemplo 3

Muestre que 101 es primo.

Solución:

- Los únicos números primos que no exceden a $\sqrt{101}$ son 2, 3, 5 y 7.
- Dado que 101 no es divisible entre 2, 3, 5 o 7 (el cociente de 101 y cada uno de estos números enteros no es un número entero), se sigue que 101 es primo.

□

División por Ensayo III

- Debido a que cada entero tiene una factorización prima, sería útil tener un procedimiento para encontrar esta factorización prima.

División por Ensayo III

- Considere el problema de encontrar la factorización prima de n.

División por Ensayo III

- Comience por dividir n entre primos sucesivos, comenzando con el primo más pequeño, 2.

División por Ensayo III

- Si n tiene un factor primo, entonces por el Teorema 2 se encontrará un factor primo p que no exceda a $\sqrt{n}$.

División por Ensayo III

- Así, si no se encuentra un factor primo que no exceda a $\sqrt{n}$, tenemos que n es primo.

División por Ensayo III

- De otro modo si se encuentra un factor primo p, continue factorizando n/p.

División por Ensayo III

- Tenga en cuenta que n/p no tiene factores primos menores que p.

División por Ensayo III

- Nuevamente, si n/p no tiene un factor primo mayor o igual a p y que no excede a su raíz cuadrada, entonces es primo.

División por Ensayo III

- De lo contrario, si tiene un factor primo q, continúe factorizando $n/(pq)$. Este procedimiento se continúa hasta que la factorización se ha reducido a un primo.

Ejemplo 4

Encuentre la factorización prima de 7007.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- Para encontrar la factorización prima de 7007, primero realice divisiones de 7007 entre números primos sucesivos, comenzando con 2.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- Ninguno de los primos 2, 3 y 5 divide 7007. Sin embargo, 7 divide 7007, con $7007/7 = 1001$.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- A continuación, divida 1001 entre primos sucesivos, comenzando con 7.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- Se ve inmediatamente que 7 también divide 1001, porque $1001/7 = 143$.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- Continúe dividiendo 143 entre primos sucesivos, comenzando con 7.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- Aunque 7 no divide 143, 11 divide 143 y $143/11 = 13$.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- Como 13 es primo, el procedimiento se completa.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- De ello se deduce que $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$.

Ejemplo 4

Encuentre la factorización prima de 7007.

Solución:

- En consecuencia, la factorización prima de 7007 es $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

La criba de Eratóstenes I

- Tenga en cuenta que los números enteros compuestos que no excedan 100 deben tener un factor primo que no exceda 10.

La criba de Eratóstenes I

- Debido a que los únicos números primos menores que 10 son 2, 3, 5 y 7, los números primos que no exceden 100 son estos cuatro primos y los números enteros positivos mayores que 1 que no exceden a 100 que no son divisibles por 2, 3, 5, o 7.

La criba de Eratóstenes I

- La criba de Eratóstenes se usa para encontrar todos los números primos que no excedan un número entero positivo especificado.

La criba de Eratóstenes I

- Por ejemplo, el siguiente procedimiento se usa para encontrar los números primos que no excedan 100.

La criba de Eratóstenes I

- Comenzamos con la lista de todos los números enteros entre 1 y 100.

La criba de Eratóstenes II

- Para comenzar el proceso de cribado, se eliminan los números enteros que son divisibles por 2, distintos de 2.

La criba de Eratóstenes II

- Debido a que 3 es el primer número entero mayor que 2 que queda, se eliminan todos los números enteros divisibles por 3 que no sean 3.

La criba de Eratóstenes II

- Como 5 es el siguiente número entero que queda después de 3, se eliminan los números enteros divisibles por 5 que no sean 5.

La criba de Eratóstenes II

- El siguiente número entero que queda es 7, por lo que se eliminan los números enteros divisibles por 7 que no sean 7.

La criba de Eratóstenes III

- Debido a que todos los números enteros compuestos que no excedan de 100 son divisibles entre 2, 3, 5 o 7, todos los números enteros restantes excepto 1 son primos.

La criba de Eratóstenes III

- En la Tabla 1, los paneles muestran los números enteros eliminados en cada etapa, donde cada entero divisible por 2, distinto de 2, está subrayado en el primer panel,

La criba de Eratóstenes III

- cada entero divisible por 3, distinto de 3, está subrayado en el segundo panel,

La criba de Eratóstenes III

- cada el entero divisible por 5, distinto de 5, está subrayado en el tercer panel,

La criba de Eratóstenes III

- y cada entero divisible por 7, distinto de 7, está subrayado en el cuarto panel.

La criba de Eratóstenes IV

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Tabla 1: La criba de Eratóstenes para los primos menores que 100.

Infinitud de Primos I

- Se sabe desde hace mucho tiempo que hay infinitos números primos.

Infinitud de Primos I

- Esto significa que siempre que $p_1, p_2, \ldots, p_n$ son los n primos más pequeños, sabemos que hay un primo mayor que no aparece en la lista.

Infinitud de Primos I

- Demostraremos este hecho usando una demostración dada por Euclides en su famoso texto de matemáticas, *Los Elementos*.

Infinitud de Primos I

- Muchos matemáticos consideran que esta demostración simple, pero elegante, se encuentra entre las demostraciones más hermosas de las matemáticas.

Infinitud de Primos I

- Es la primera prueba presentada en el libro *Proofs from THE BOOK*, donde EL LIBRO se refiere a la colección imaginaria de pruebas perfectas que el legendario matemático Paul Erdős afirma que Dios resguarda.

Infinitud de Primos I

- Por cierto, hay una gran cantidad de pruebas diferentes de que hay una infinidad de números primos, y se publican nuevas con una frecuencia sorprendente.

Teorema 3

Hay infinitos números primos.

Teorema 3

Hay infinitos números primos.

Demostración:

- Probaremos este teorema usando una prueba por contradicción.

Teorema 3

Hay infinitos números primos.

Demostración:

- Suponemos que sólo hay un número finito de primos, $p_1, p_2, \ldots, p_n$.

Teorema 3

Hay infinitos números primos.

Demostración:

- Suponemos que sólo hay un número finito de primos, $p_1, p_2, \ldots, p_n$.
- Sea

$$Q = p_1 p_2 \cdots p_n + 1.$$

Teorema 3

Hay infinitos números primos.

Demostración:

- Suponemos que sólo hay un número finito de primos, $p_1, p_2, \ldots, p_n$.
- Sea
$$Q = p_1 p_2 \cdots p_n + 1.$$
- Según el teorema fundamental de la aritmética, Q es primo o puede escribirse como el producto de dos o más primos.

Teorema 3

Hay infinitos números primos.

Demostración:

- Suponemos que sólo hay un número finito de primos, $p_1, p_2, \ldots, p_n$.
- Sea
$$Q = p_1 p_2 \cdots p_n + 1.$$
- Según el teorema fundamental de la aritmética, Q es primo o puede escribirse como el producto de dos o más primos.
- Sin embargo, ninguno de los primos p_j divide a Q, porque si $p_j | Q$, entonces p_j divide $Q - p_1 p_2 \cdots p_n = 1$, por lo tanto, hay un primo que no está en la lista $p_1, p_2, \ldots, p_n$.

Teorema 3

Hay infinitos números primos.

Demostración:

- Suponemos que sólo hay un número finito de primos, $p_1, p_2, \ldots, p_n$.
- Sea
$$Q = p_1 p_2 \cdots p_n + 1.$$
- Según el teorema fundamental de la aritmética, Q es primo o puede escribirse como el producto de dos o más primos.
- Sin embargo, ninguno de los primos p_j divide a Q, porque si $p_j | Q$, entonces p_j divide $Q - p_1 p_2 \cdots p_n = 1$, por lo tanto, hay un primo que no está en la lista $p_1, p_2, \ldots, p_n$.
- Este primo o es Q, si es primo, o un factor primo de Q.

Teorema 3

Hay infinitos números primos.

Demostración:

- Suponemos que sólo hay un número finito de primos, $p_1, p_2, \ldots, p_n$.
- Sea
$$Q = p_1 p_2 \cdots p_n + 1.$$
- Según el teorema fundamental de la aritmética, Q es primo o puede escribirse como el producto de dos o más primos.
- Sin embargo, ninguno de los primos p_j divide a Q, porque si $p_j | Q$, entonces p_j divide $Q - p_1 p_2 \cdots p_n = 1$, por lo tanto, hay un primo que no está en la lista $p_1, p_2, \ldots, p_n$.
- Este primo o es Q, si es primo, o un factor primo de Q.
- Esto es una contradicción porque asumimos que hemos enumerado todos los números primos.

Infinitud de Primos II

Observación 2

¡Tenga en cuenta que en esta demostración no declaramos que Q sea primo! Además, en esta prueba, hemos dado una prueba de existencia no constructiva de que dados n números primos, hay un primo que no está en esta lista. Para que esta demostración sea constructiva, habríamos tenido que dar explícitamente un primo que no esté en nuestra lista original de n primos.

Infinitud de Primos III

- Debido a que hay infinitos números primos, dado cualquier entero positivo hay primos mayores que este número entero.

Infinitud de Primos III

- Hay una búsqueda en curso para descubrir números primos cada vez más grandes; durante casi todos los últimos 300 años, el número primo más grande conocido ha sido un número entero de la forma especial $2^p - 1$, donde p también es primo.

Infinitud de Primos III

- Tenga en cuenta que $2^n - 1$ no puede ser primo cuando n no es primo.

Infinitud de Primos III

- Estos números primos se llaman números primos de Mersenne, en honor al monje francés Marin Mersenne, que los estudió en el siglo XVII.

Infinitud de Primos III

- La razón por la que el número primo más grande conocido suele ser un número primo de Mersenne es que existe una prueba extremadamente eficiente, conocida como prueba de Lucas-Lehmer, para determinar si $2^p - 1$ es primo.

Infinitud de Primos III

- Además, actualmente no es posible probar tan rápido si son primos números que no sean de esta u otras formas especiales.

Ejemplo 5

Los números $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ y $2^7 - 1 = 127$ son números primos de Mersenne, mientras que $2^{11} - 1 = 2047$ no es un número primo de Mersenne porque $2047 = 23 \cdot 89$.

□

Máximo Común Divisor I

Definición 2

Sean a y b enteros, no ambos cero. El entero más grande d tal que $d|a$ y $d|b$ se llama el *máximo común divisor* de a y b. El máximo común divisor de a y b se denota por $\text{mcd}(a, b)$.

Máximo Común Divisor II

- El máximo común divisor de dos enteros, no ambos cero, existe porque el conjunto de divisores comunes de estos enteros no es vacío y es finito.

Máximo Común Divisor II

- Una forma de encontrar el máximo común divisor de dos enteros es encontrar todos los divisores comunes positivos de ambos enteros y luego tomar el mayor divisor.

Máximo Común Divisor II

- Esto se hace en los Ejemplos 6 y 7.

Máximo Común Divisor II

- Más adelante, se dará un método más eficiente para encontrar el máximo común divisor de dos enteros.

Ejemplo 6

Ejemplo 6

¿Cuál es el máximo común divisor de 24 y 36?

Ejemplo 6

¿Cuál es el máximo común divisor de 24 y 36?

Solución:

- Los divisores comunes positivos de 24 y 36 son 1, 2, 3, 4, 6 y 12.

Ejemplo 6

¿Cuál es el máximo común divisor de 24 y 36?

Solución:

- Los divisores comunes positivos de 24 y 36 son 1, 2, 3, 4, 6 y 12.
- Por lo tanto, $\text{mcd}(24, 36) = 12$.

□

Ejemplo 7

Ejemplo 7

¿Cuál es el máximo común divisor de 17 y 22?

Ejemplo 7

¿Cuál es el máximo común divisor de 17 y 22?

Solución:

- Los números enteros 17 y 22 no tienen divisores comunes positivos distintos de 1, de modo que $\text{mcd}(17, 22) = 1$.

□

Primos relativos I

Definición 3

Los números enteros a y b son *primos relativos* si su máximo común divisor es 1.

Primos relativos I

Ejemplo 8

Del ejemplo 7 se deduce que los números enteros 17 y 22 son primos relativos, porque $\text{mcd}(17, 22) = 1$. □

Primos relativos II

Definición 4

Los enteros $a_1, a_2, \ldots, a_n$ son *primos relativos por pares* si $\text{mcd}(a_i, a_j) = 1$ siempre que $1 \leq i < j \leq n$.

Primos relativos II

Ejemplo 9

Determine si los números enteros 10, 17 y 21 son primos relativos por pares y si los números enteros 10, 19 y 24 son primos relativos por pares.

Primos relativos II

Ejemplo 9

Determine si los números enteros 10, 17 y 21 son primos relativos por pares y si los números enteros 10, 19 y 24 son primos relativos por pares.

Solución:

- Como $\text{mcd}(10, 17) = 1$, $\text{mcd}(10, 21) = 1$ y $\text{mcd}(17, 21) = 1$, concluimos que 10, 17 y 21 son primos relativos por pares.

Primos relativos II

Ejemplo 9

Determine si los números enteros 10, 17 y 21 son primos relativos por pares y si los números enteros 10, 19 y 24 son primos relativos por pares.

Solución:

- Como $\text{mcd}(10, 24) = 2 > 1$, vemos que 10, 19 y 24 no son primos relativos por pares.

Máximo Común Divisor III

- Otra forma de encontrar el máximo común divisor de dos números enteros positivos es usar las factorizaciones primas de estos números enteros.

Máximo Común Divisor III

- Otra forma de encontrar el máximo común divisor de dos números enteros positivos es usar las factorizaciones primas de estos números enteros.
- Suponga que las factorizaciones primas de los enteros positivos a y b son

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

Máximo Común Divisor III

- Otra forma de encontrar el máximo común divisor de dos números enteros positivos es usar las factorizaciones primas de estos números enteros.
- Suponga que las factorizaciones primas de los enteros positivos a y b son

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

- donde cada exponente es un número entero no negativo,

Máximo Común Divisor III

- Otra forma de encontrar el máximo común divisor de dos números enteros positivos es usar las factorizaciones primas de estos números enteros.
- Suponga que las factorizaciones primas de los enteros positivos a y b son

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

- donde cada exponente es un número entero no negativo,
- y donde todos los números primos que ocurren en la factorización prima de a o b se incluyen en ambas factorizaciones, con exponentes cero si es necesario.

Máximo Común Divisor III

- Otra forma de encontrar el máximo común divisor de dos números enteros positivos es usar las factorizaciones primas de estos números enteros.
- Suponga que las factorizaciones primas de los enteros positivos a y b son

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

- donde cada exponente es un número entero no negativo,
- y donde todos los números primos que ocurren en la factorización prima de a o b se incluyen en ambas factorizaciones, con exponentes cero si es necesario.
- Entonces $\text{mcd}(a, b)$ viene dado por

$$\text{mcd}(a, b) = p_1^{\text{mín}(a_1,b_1)} p_2^{\text{mín}(a_2,b_2)} \cdots p_n^{\text{mín}(a_n,b_n)},$$

Máximo Común Divisor III

- Otra forma de encontrar el máximo común divisor de dos números enteros positivos es usar las factorizaciones primas de estos números enteros.
- Suponga que las factorizaciones primas de los enteros positivos a y b son

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

- donde cada exponente es un número entero no negativo,
- y donde todos los números primos que ocurren en la factorización prima de a o b se incluyen en ambas factorizaciones, con exponentes cero si es necesario.
- Entonces $\text{mcd}(a, b)$ viene dado por

$$\text{mcd}(a, b) = p_1^{\text{mín}(a_1,b_1)} p_2^{\text{mín}(a_2,b_2)} \cdots p_n^{\text{mín}(a_n,b_n)},$$

- donde $\text{mín}(x, y)$ representa el mínimo de los dos números x y y.

Máximo Común Divisor IV

- Para demostrar que esta fórmula para $\text{mcd}(a, b)$ es válida, debemos mostrar que el número entero del lado derecho divide tanto a a como a b, y que ningún entero más grande lo hace.

Máximo Común Divisor IV

- Para demostrar que esta fórmula para $\text{mcd}(a, b)$ es válida, debemos mostrar que el número entero del lado derecho divide tanto a a como a b, y que ningún entero más grande lo hace.
- Este número entero divide a a y a b, porque la potencia de cada primo en la factorización no excede la potencia de este primo ni en la factorización de a ni en la de b.

Máximo Común Divisor IV

- Para demostrar que esta fórmula para $\text{mcd}(a, b)$ es válida, debemos mostrar que el número entero del lado derecho divide tanto a a como a b, y que ningún entero más grande lo hace.
- Este número entero divide a a y a b, porque la potencia de cada primo en la factorización no excede la potencia de este primo ni en la factorización de a ni en la de b.
- Además, ningún número entero mayor puede dividir a y b, porque los exponentes de los números primos en esta factorización no se pueden aumentar y no se pueden incluir otros números primos.

Ejemplo 10

Debido a que las factorizaciones primas de 120 y 500 son $120 = 2^3 \cdot 3 \cdot 5$ y $500 = 2^2 \cdot 5^3$, el máximo común divisor es

$$\text{mcd}(120, 500) = 2^{\text{mín}(3,2)} 3^{\text{mín}(1,0)} 5^{\text{mín}(1,3)} = 2^2 3^0 5^1 = 20.$$

□

Mínimo Común Múltiplo I

Definición 5

El *mínimo común múltiplo* de los enteros positivos a y b es el menor entero positivo que es divisible por a y b. El mínimo común múltiplo de a y b se denota mediante el mcm(a, b).

Mínimo Común Múltiplo II

- El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b no está vacío (porque ab pertenece a este conjunto, por ejemplo),

Mínimo Común Múltiplo II

- El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b no está vacío (porque ab pertenece a este conjunto, por ejemplo),
- y cada conjunto no vacío de enteros positivos tiene un elemento mínimo (por la propiedad del buen orden).

Mínimo Común Múltiplo II

- El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b no está vacío (porque ab pertenece a este conjunto, por ejemplo),
- y cada conjunto no vacío de enteros positivos tiene un elemento mínimo (por la propiedad del buen orden).
- Suponga que las factorizaciones primas de a y b son las mismas que antes.

Mínimo Común Múltiplo II

- El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b no está vacío (porque ab pertenece a este conjunto, por ejemplo),
- y cada conjunto no vacío de enteros positivos tiene un elemento mínimo (por la propiedad del buen orden).
- Suponga que las factorizaciones primas de a y b son las mismas que antes.
- Entonces el mínimo común múltiplo de a y b viene dado por

$$\text{mcm}(a,b) = p_1^{\text{máx}(a_1,b_1)} p_2^{\text{máx}(a_2,b_2)} \cdots p_n^{\text{máx}(a_n,b_n)},$$

Mínimo Común Múltiplo II

- El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b no está vacío (porque ab pertenece a este conjunto, por ejemplo),
- y cada conjunto no vacío de enteros positivos tiene un elemento mínimo (por la propiedad del buen orden).
- Suponga que las factorizaciones primas de a y b son las mismas que antes.
- Entonces el mínimo común múltiplo de a y b viene dado por

$$\text{mcm}(a,b) = p_1^{\text{máx}(a_1,b_1)} p_2^{\text{máx}(a_2,b_2)} \cdots p_n^{\text{máx}(a_n,b_n)},$$

- donde $\text{máx}(x,y)$ denota el máximo de los dos números x y y.

Mínimo Común Múltiplo II

- El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b no está vacío (porque ab pertenece a este conjunto, por ejemplo),
- y cada conjunto no vacío de enteros positivos tiene un elemento mínimo (por la propiedad del buen orden).
- Suponga que las factorizaciones primas de a y b son las mismas que antes.
- Entonces el mínimo común múltiplo de a y b viene dado por

$$\text{mcm}(a,b) = p_1^{\text{máx}(a_1,b_1)} p_2^{\text{máx}(a_2,b_2)} \cdots p_n^{\text{máx}(a_n,b_n)},$$

- donde $\text{máx}(x,y)$ denota el máximo de los dos números x y y.
- Esta fórmula es válida porque un múltiplo común de a y b tiene al menos $\text{máx}(a_i,b_i)$ factores de p_i en su factorización prima, y el mínimo común múltiplo no tiene otros factores primos además de los de a y b.

Ejemplo 11

¿Cuál es el mínimo común múltiplo de $2^3 3^5 7^2$ y $2^4 3^3$?

Ejemplo 11

¿Cuál es el mínimo común múltiplo de $2^3 3^5 7^2$ y $2^4 3^3$?

Solución:

- Tenemos que

$$\text{mcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\text{máx}(3,4)} 3^{\text{máx}(5,3)} 7^{\text{máx}(2,0)} = 2^4 3^5 7^2.$$

□

Relación entre mcd y mcm

Teorema 4

Sean a y b enteros positivos. Entonces

$$ab = \text{mcd}(a, b) \cdot \text{mcm}(a, b).$$

El Algoritmo de Euclides I

- Calcular el máximo común divisor de dos números enteros directamente a partir de las factorizaciones primas de estos números enteros es ineficaz.

El Algoritmo de Euclides I

- La razón es que lleva mucho tiempo encontrar las factorizaciones primas.

El Algoritmo de Euclides I

- Daremos un método más eficiente para encontrar el máximo común divisor, llamado algoritmo euclidiano.

El Algoritmo de Euclides I

- Este algoritmo se conoce desde la antigüedad.

El Algoritmo de Euclides I

- Lleva el nombre del antiguo matemático griego Euclides, quien incluyó una descripción de este algoritmo en su libro *Los elementos*.

El Algoritmo de Euclides II

- Antes de describir el algoritmo euclidiano, mostraremos cómo se usa para encontrar mcd$(91, 287)$.

El Algoritmo de Euclides II

- Primero, divida 287, el mayor de los dos enteros, por 91, el menor, para obtener

$$287 = 91 \cdot 3 + 14.$$

El Algoritmo de Euclides II

- Cualquier divisor de 91 y 287 también debe ser un divisor de $287 - 91 \cdot 3 = 14$.

El Algoritmo de Euclides II

- Además, cualquier divisor de 91 y 14 también debe ser un divisor de $287 = 91 \cdot 3 + 14$.

El Algoritmo de Euclides II

- Por lo tanto, el máximo común divisor de 91 y 287 es el mismo que el máximo común divisor de 91 y 14.

El Algoritmo de Euclides II

- Esto significa que el problema de encontrar mcd$(91, 287)$ se ha reducido al problema de encontrar mcd$(91, 14)$.

El Algoritmo de Euclides III

- Luego, divida 91 entre 14 para obtener

$$91 = 14 \cdot 6 + 7.$$

El Algoritmo de Euclides III

- Debido a que cualquier divisor común de 91 y 14 también divide $91 - 14 \cdot 6 = 7$ y cualquier divisor común de 14 y 7 divide 91, se deduce que $\text{mcd}(91, 14) = \text{mcd}(14, 7)$.

El Algoritmo de Euclides III

- Continúe dividiendo 14 entre 7, para obtener

$$14 = 7 \cdot 2.$$

El Algoritmo de Euclides III

- Como 7 divide 14, se deduce que $\text{mcd}(14, 7) = 7$.

El Algoritmo de Euclides III

- Además, dado que

$$\text{mcd}(287, 91) = \text{mcd}(91, 14) = \text{mcd}(14, 7) = 7,$$

el problema original se ha resuelto.

El Algoritmo de Euclides IV

- Ahora describimos cómo funciona el algoritmo euclidiano en general.

El Algoritmo de Euclides IV

- Usaremos divisiones sucesivas para reducir el problema de encontrar el máximo común divisor de dos enteros positivos al mismo problema con enteros más pequeños, hasta que uno de los enteros sea cero.

El Algoritmo de Euclides IV

- El algoritmo euclidiano se basa en el siguiente resultado sobre el máximo común divisor y el algoritmo de división.

El Algoritmo de Euclides V

Lema 1

Sea $a = bq + r$, donde a, b, q y r son números enteros. Entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

El Algoritmo de Euclides V

Lema 1

Sea $a = bq + r$, donde a, b, q y r son números enteros. Entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración:

- Si podemos demostrar que los divisores comunes de a y b son los mismos que los divisores comunes de b y r, habremos demostrado que $\text{mcd}(a, b) = \text{mcd}(b, r)$, porque ambos pares deben tener el mismo máximo común divisor.

El Algoritmo de Euclides V

Lema 1

Sea $a = bq + r$, donde a, b, q y r son números enteros. Entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración:

- Si podemos demostrar que los divisores comunes de a y b son los mismos que los divisores comunes de b y r, habremos demostrado que $\text{mcd}(a, b) = \text{mcd}(b, r)$, porque ambos pares deben tener el mismo máximo común divisor.
- Entonces, suponga que d divide a a y b.

El Algoritmo de Euclides V

Lema 1

Sea $a = bq + r$, donde a, b, q y r son números enteros. Entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración:

- Si podemos demostrar que los divisores comunes de a y b son los mismos que los divisores comunes de b y r, habremos demostrado que $\text{mcd}(a, b) = \text{mcd}(b, r)$, porque ambos pares deben tener el mismo máximo común divisor.
- Entonces, suponga que d divide a a y b.
- Así, se deduce que d también divide $a - bq = r$ (del Teorema 3.1.1 de las notas).

El Algoritmo de Euclides VI

- Por tanto, cualquier divisor común de a y b es también divisor común de b y r.

El Algoritmo de Euclides VI

- Por tanto, cualquier divisor común de a y b es también divisor común de b y r.
- Asimismo, suponga que d divide a b y r.

El Algoritmo de Euclides VI

- Por tanto, cualquier divisor común de a y b es también divisor común de b y r.
- Asimismo, suponga que d divide a b y r.
- Entonces d también divide $bq + r = a$.

El Algoritmo de Euclides VI

- Por tanto, cualquier divisor común de a y b es también divisor común de b y r.
- Asimismo, suponga que d divide a b y r.
- Entonces d también divide $bq + r = a$.
- Por tanto, cualquier divisor común de b y r es también un divisor común de a y b.

El Algoritmo de Euclides VI

- Por tanto, cualquier divisor común de a y b es también divisor común de b y r.
- Asimismo, suponga que d divide a b y r.
- Entonces d también divide $bq + r = a$.
- Por tanto, cualquier divisor común de b y r es también un divisor común de a y b.
- En consecuencia, $\text{mcd}(a, b) = \text{mcd}(b, r)$.

■

El Algoritmo de Euclides VII

- Suponga que a y b son números enteros positivos con $a \geq b$.

El Algoritmo de Euclides VII

- Suponga que a y b son números enteros positivos con $a \geq b$.
- Sea $r_0 = a$ y $r_1 = b$.

El Algoritmo de Euclides VII

- Suponga que a y b son números enteros positivos con $a \geq b$.
- Sea $r_0 = a$ y $r_1 = b$.
- Cuando aplicamos sucesivamente el algoritmo de división, obtenemos

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 &< r_1, \\
r_1 &= r_2 q_1 + r_3 & 0 \leq r_3 &< r_2, \\
&\vdots & &\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n &< r_{n-1}, \\
r_{n-1} &= r_n q_n
\end{aligned}$$

El Algoritmo de Euclides VIII

- Finalmente, se produce un resto de cero en esta secuencia de divisiones sucesivas, porque la secuencia de restos $a = r_0 > r_1 > r_2 > \cdots \geq 0$ no puede contener más de a términos.

El Algoritmo de Euclides VIII

- Finalmente, se produce un resto de cero en esta secuencia de divisiones sucesivas, porque la secuencia de restos $a = r_0 > r_1 > r_2 > \cdots \geq 0$ no puede contener más de a términos.
- Además, del Lema 1 se sigue que

$$\begin{aligned}\text{mcd}(a, b) &= \text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) = \cdots = \text{mcd}(r_{n-2}, r_{n-1}) \\ &= \text{mcd}(r_{n-1}, r_n) = \text{mcd}(r_n, 0) = r_n.\end{aligned}$$

El Algoritmo de Euclides VIII

- Finalmente, se produce un resto de cero en esta secuencia de divisiones sucesivas, porque la secuencia de restos $a = r_0 > r_1 > r_2 > \cdots \geq 0$ no puede contener más de a términos.
- Además, del Lema 1 se sigue que

$$\begin{aligned} \text{mcd}(a, b) &= \text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) = \cdots = \text{mcd}(r_{n-2}, r_{n-1}) \\ &= \text{mcd}(r_{n-1}, r_n) = \text{mcd}(r_n, 0) = r_n. \end{aligned}$$

- Por tanto, el máximo común divisor es el último resto distinto de cero en la secuencia de divisiones.

Ejemplo 12 I

Ejemplo 12

Encuentre el máximo común divisor de 414 y 662 usando el algoritmo euclidiano.

Solución:

- Los usos sucesivos del algoritmo de división dan:

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41. \end{aligned}$$

- Por lo tanto, $\text{mcd}(414, 662) = 2$, porque 2 es el último resto distinto de cero.
- Podemos resumir estos pasos en forma de tabla.

Ejemplo 12 II

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	662	414	1	248
1	414	248	1	166
2	248	166	1	82
3	166	82	2	2
4	82	2	41	0

□

Pseudocódigo del Algoritmo de Euclides

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

Pseudocódigo del Algoritmo de Euclides

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

- En cada etapa del procedimiento, x se reemplaza por y, y y se reemplaza por x mod y, que es el resto cuando x se divide por y.

Pseudocódigo del Algoritmo de Euclides

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

- En cada etapa del procedimiento, x se reemplaza por y, y y se reemplaza por x mod y, que es el resto cuando x se divide por y.
- Este proceso se repite siempre que $y \neq 0$.

Pseudocódigo del Algoritmo de Euclides

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

- En cada etapa del procedimiento, x se reemplaza por y, y y se reemplaza por x mod y, que es el resto cuando x se divide por y.
- Este proceso se repite siempre que $y \neq 0$.
- El algoritmo termina cuando $y = 0$, y el valor de x en ese punto, el último resto distinto de cero en el procedimiento, es el máximo común divisor de a y b.

Ejercicios I

1. Determine si cada uno de estos números enteros es primo.
   1. 19
   2. 93
   3. 107
   4. 27
   5. 101
   6. 113
2. Encuentre la factorización prima de cada uno de estos números enteros.
   1. 39
   2. 81
   3. 101
   4. 143
   5. 289
   6. 899
3. ¿Qué números enteros positivos menores que 12 son primos relativos a 12?
4. Determine si los números enteros de cada uno de estos conjuntos son primos relativos por pares.
   1. 11, 15, 19
   2. 14, 15, 21
   3. 12, 17, 31, 37
   4. 7, 8, 9, 11

Ejercicios II

5. ¿Cuáles son los máximos comunes divisores de estos pares de números enteros?

    1. $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$
    2. $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
    3. $23^{31}, 23^{17}$
    4. $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$
    5. $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$
    6. $1111, 0$

6. ¿Cuál es el mínimo común múltiplo de cada par en el ejercicio 5?
7. Encuentre $\text{mcd}(1000, 625)$ y $\text{mcm}(1000, 625)$ y verifique que

$$\text{mcd}(1000, 625) \cdot \text{mcm}(1000, 625) = 1000 \cdot 625.$$

8. Utilice el algoritmo euclidiano para encontrar

    1. $\text{mcd}(12, 18)$
    2. $\text{mcd}(111, 201)$
    3. $\text{mcd}(1001, 1331)$
    4. $\text{mcd}(12345, 54321)$
    5. $\text{mcd}(1000, 5040)$
    6. $\text{mcd}(9888, 6060)$