Semana 7: Divisibilidad II

1. El teorema fundamental de la aritmética

Comenzaremos esta sección describiendo una importante clasificación numérica. Mostraremos su importancia y sus propiedades, la más relevante de todas exhibe que estos números son, bajo cierta óptica, la estructura fundamental detrás de los enteros.

Definición 7.1. Decimos que un entero $p > 1$ es *un número primo* si sus únicos divisores son 1 y p.

A simple vista no parecerían tener mucha importancia estos números, sin embargo son la piedra angular de los enteros. Consideremos por ejemplo un número $a > 1$ que no sea primo, en se caso éste debe admitir un divisor distinto de 1 y de a. Esto quiere decir que existe un entero b que satisface $1 < b < a$ y además $a = bc$ para algún otro número c. Este otro número c es por supuesto otro divisor de a por lo que $1 \leq c \leq a$; sin embargo, es imposible que $c = 1$ o $c = a$ (en esos caso tendríamos $a < a$). Esto indica que a se *puede descomponer en los factores b y c*. Usemos esto para formular el siguiente lema y la definición que le sigue.

Lema 7.1. *Si un número entero $a > 1$ no es primo, entonces existen números $1 < b < a$ y $1 < c < a$ tales que*

$$a = bc.$$

Definición 7.2. Un número que no es primo, se dice *compuesto*.

Ahora, podríamos aplicar el tratamiento del lema 7.1 a los números b y c, los números resultantes decrecen y en algún punto esta descomposición involucrará únicamente números primos. Este argumento intuitivo se puede formalizar sin mucho problema.

Teorema 7.2. *Para cualquier entero $a > 1$ existen primos $p_1, p_2, \ldots p_{k-1}$ y p_k de forma que*

$$a = p_1 \cdots p_k.$$

En otras palabras, a se puede expresar como el producto de primos.

Demostración. Usaremos inducción fuerte sobre el enunciado «a se puede expresar como el producto de primos». El caso base será $a = 2$ y como 2 es primo, entonces se puede expresar como el producto de primos. Supongamos entonces que cualquier entero menor que a se puede expresar como el producto de primos. Si a es primo, entonces no hay nada que probar y el resultado sigue. Si por otro lado a es compuesto, entonces se puede expresar como $a = bc$ para algunos enteros $1 < b < a$ y $1 < c < a$ y por hipótesis de inducción, debemos tener

$$b = p_1 \ldots p_k$$

y

$$c = q_1 \dots q_l$$

para algunos primos $p_1, \dots, p_k, q_1, \dots, q_{l-1}$ y q_l; en ese caso tenemos que

$$a = p_1 \dots p_k q_1 \dots q_l$$

y en consecuencia a se puede expresar como el producto de primos. Por inducción fuerte, el resultado sigue. ■

Vamos a dar ejemplos de esta factorización que hemos tratado únicamente en abstracto:

$$42 = 2 \cdot 3 \cdot 7,$$

$$36 = 2 \cdot 2 \cdot 3 \cdot 3,$$

$$15,400 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7 \cdot 11.$$

Estos ejemplos nos permiten observar un par de situaciones, la primera es que los factores que forman la expresión pueden estar repetidos, la segunda es las expresiones no dependen del orden sin embargo la enumeración de los factores parece depender del orden, lo que parece indicar que las factorizaciones no son únicas. Pero al ser el producto conmutativo, no tendría sentido imponer una diferencia entre la expresión $2 \cdot 3$ y la expresión $3 \cdot 2$. Si se aprecia con cuidado, hemos usado la palabra factorización de manera libre, pero la observación anterior nos instiga a definir esta expresión de manera que nos sea útil.

Definición 7.3. Por *una factorización prima de un entero positivo a*, entenderemos un conjunto formado por números primos $\{p_1, p_2, \dots p_k\}$ de forma que $a = p_1 p_2 \dots p_k$.

Esta definición nos permite afirmar las factorizaciones primas de 42,

$$42 = 2 \cdot 3 \cdot 7 = 7 \cdot 3 \cdot 2,$$

son la misma en virtud de que los conjuntos $\{2, 3, 7\}$ y $\{7, 3, 2\}$ coinciden. En general, esto nos permite afirmar que cambiar el orden de los factores, no cambia la factorización. Esto es algo que deseábamos y que nos permite volver a explorar la pregunta, ¿son las factorizaciones primas únicas? La respuesta se formula en el importante *teorema fundamental de la aritmética* (teorema 7.5).

Lema 7.3 (Euclides)**.** *Si p es un número primo y $p|ab$, entonces $p|a$ o $p|b$. De manera más general, si $p|a_1 \dots a_n$, entonces, para algún $1 \leq i \leq n$, p divide al número a_i.*

Demostración. Si $p \mid a$, entonces el resultado es inmediato, supongamos entonces que $p \nmid a$. Debemos notar que al ser p primo, cualquier divisor común de p y a es o 1 o p pero por hipótesis $p \nmid a$ por lo que debemos concluir que el único divisor común entre a y p es 1. Así, debemos concluir de igual forma $(p, a) = 1$.

Como $(p, a) = 1$, la identidad de Bézout garantiza la existencia de enteros s y t de forma que

$$sp + ta = 1,$$

en ese caso debemos tener que

$$b = sbp + tab.$$

De esta forma hemos expresado b como una combinación lineal de p y ab. Por otro lado, $p \mid p$ y por hipótesis $p \mid ab$, por lo que p debe dividir a cualquier combinación lineal de estos números, en particular $p \mid b$. La segunda parte de la prueba se presenta al resolver el ejercicio 7.9 y se puede obtener usando inducción. ■

Corolario 7.4. *Si un entero $m > 1$ satisface que, $m \mid ab$ siempre implica que $m|a$ o $m|b$, entonces m es primo.*

Demostración. Usaremos contraposición para mostrar que si m es compuesto, entonces no sigue necesariamente que m divida un producto implica que divide a alguno de sus factores.

Supongamos que m es compuesto y que $m = ab$ para algunos enteros $1 < a, b < m$. En ese caso, tenemos que $m \mid ab$, pero si $m \mid a$ o $m \mid b$, entonces $m \leq a$ o $m \leq b$ lo cual contradice las desigualdades que definen a a y b. Entonces, si m es compuesto, es falso que $m \mid ab$ implica $m \mid a$ o $m \mid b$. Por contraposición, el resultado que buscamos sigue. ■

Teorema 7.5. *Cualquier entero $a > 1$ posee una factorización prima única.*

Demostración. En el teorema 7.2 se ha probado que a tiene una factorización prima. Supongamos entonces que $a = p_1 \dots p_k$ y $a = q_1 \dots q_l$ son factorizaciones primas de a, en otras palabras

$$p_1 \dots p_k = q_1 \dots q_l.$$

Debemos mostrar para todo k y para todo l, que el conjunto formado por los números $p_1, \dots, p_{k-1}$ y p_k coincide con el formado por los números $q_1, \dots, q_l$ y q_l. Usaremos inducción sobre k para probar el enunciado anterior.

Para $k = 1$, debemos suponer $p_1 = q_1 \dots q_l$. En ese caso, $k = l = 1$ y $p_1 = q_1$, en otro caso p_1 sería el producto de primos en contradicción con ser éste primo. Por lo tanto, como los conjuntos de factores coinciden, las factorizaciones primas son iguales.

Supongamos para un natural k que, las factorizaciones coinciden siempre que su producto coincida. Si $p_1 \dots p_k p_{k+1} = q_1 \dots q_l$, entonces $p_{k+1} \mid q_1 \dots q_l$ y, por el lema de Euclides, p_{k+1} debe dividir alguno de los factores q_j, en otras palabras $p_{k+1} = 1$ o $p_{k+1} = q_j$ por ser q_j un número primo, pero p_{k+1} es también un número primo y por tanto $p_{k+1} \neq 1$, por lo que nos vemos obligados a concluir que $p_{k+1} = q_j$ para algún $1 \leq j \leq l$. Esto nos permite afirmar que

$$p_1 \dots p_{k+1} = q_1 \dots q_{j-1} p_{k+1} q_{j+1} \dots q_l$$

y por la ley de cancelación del producto, esto implica que

$$p_1 \dots p_k = q_1 \dots q_{j-1} q_{j+1} \dots q_l.$$

Con la igualdad anterior, la hipótesis de inducción nos permite garantizar que

$$\{p_1, \dots, p_k\} = \{q_1, \dots, q_{j-1} q_{j+1} \dots q_l\}$$

lo cual implica a su vez que

$$\{p_1, \dots, p_{k+1}\} = \{q_1, \dots, q_l\},$$

i.e., las factorizaciones primas coinciden, como buscábamos.

Por inducción, la afirmación realizada en el primer párrafo sigue y ésta indica solamente que no pueden existir dos factorizaciones primas distintas, salvo el orden en que aparecen los factores. ■

Podemos arreglar un poco la expresión de un número como el producto de números primos, aglutinando los factores comunes con una notación exponencial.

Corolario 7.6. *Para $a > 1$, existe un único conjunto de primos distintos entre sí $p_1, \ldots, p_{k-1}$ y p_k, y números naturales $m_1, \ldots, m_{k-1}$ y m_k de forma que*

$$a = p_1^{m_1} \ldots p_k^{m_k}.$$

Este último resultado contiene una expresión que nos permite representar un entero de manera única a través de primos. No sólo eso, podemos ver que cualquier entero $a \neq \pm 1$ se puede expresar como

$$a = u p_1^{m_1} \ldots p_k^{m_k},$$

donde u es una unidad. Este es el significado que nos permite afirmar que los primos son el bloque fundamental en el conjunto de los enteros, pues los enteros se pueden representar de manera única por un conjunto de números primos. Cuando la factorización prima de un entero se expresa de esa manera, se dice escrita *en notación exponencial*.

Ejemplo. Consideremos los números 550 y 154. No es difícil verificar que

$$1100 = 11 \cdot 2^2 \cdot 5^2$$

y

$$616 = 2^3 \cdot 11 \cdot 7$$

podemos comparar su factorizaciones haciendo uso de la notación exponencial observando el conjunto de factores involucrados en ambas y este caso, los enteros 2, 5, 7 y 11. Podemos entonces expresar 1100 y 616 como producto de estos:

$$1100 = 2^2 \cdot 5^2 \cdot 7^0 \cdot 11^1$$

$$616 = 2^3 \cdot 5^0 \cdot 7^1 \cdot 11^1.$$

Podemos ir más lejos tomando el número primo más grande involucrado en ambas factorizaciones, en este caso 11, y expresar los números como factores de todos los primos menores o iguales que éste, en nuestro caso son los números 2,3,5,7 y 11, con lo cual

$$1100 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^1$$

$$616 = 2^3 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1.$$

Teorema 7.7. *El conjunto de los números primos es infinito.*

Demostración. Para probar el resultado, procedemos por contradicción, i.e., supongamos que el conjunto de los números primos es finito, sean entonces $p_1, \ldots, p_{k-1}$ y p_k todos primos distintos y los únicos que hay. Definimos ahora el entero

$$m = p_1 \ldots p_k + 1,$$

el cual al ser mayor que 1, por lo que se puede expresar como un producto de primos. Tomemos q como el menor de los factores primos m; como el número de primos es finito, q debe dividir también a $p_1 \ldots p_k$, al ser uno de los elementos en esa lista y en consecuencia q es también divisor de la diferencia $m - p_1 \ldots p_k = 1$, lo cual resulta imposible pues $q > 1$. Así, el conjunto de los números primos no es finito. ■

2. El algoritmo de Euclides

Una forma de encontrar el máximo común divisor de dos números es listar todos los divisores de ambos, comparar los conjuntos y encontrar el mayor elemento que compartan. Por ejemplo, consideremos los números 20 y 15, por un lado los divisores positivos de 10, son los números 1, 2, 4, 5, 10 y 20; mientras que los de 15 son los números 1, 3, 4, 5 y 15. Los divisores comunes resultan por tanto 1, 4 y 5, lo que nos permite concluir fácilmente que 5 debe ser el máximo común divisor de 20 y 15, i.e., $(20, 15) = 5$. Parece no ser difícil encontrar el máximo común divisor a través de este método, sin embargo si consideramos números mucho más grandes, la tarea se puede volver insoportablemente larga. Vamos a presentar ahora un algoritmo que nos permitirá calcular el máximo común divisor de manera muy sencilla.

Consdieremos un par de enteros posiivos a y $b \neq 0$. Para obtener el máximo común divisor de a y b, comenzamos tomando los enterosq_1 y r_2 como el cociente y el residuo de dividir a entre b, i.e.,

$$a = q_1 b + r_2.$$

Si $r_2 \neq 0$, entonces, procedemos a calcular q_2 y r_3 como el cociente y residuo de dividir, ahora, b entre r_2, i.e.,

$$b = q_2 r_2 + r_3.$$

Si $r_3 \neq 0$, podemos volver a efectuar una división repitiendo el proceso en cada ocasión. Debemos notar que este proceso no puede continuar indefinidamente, pues los residuos son todos números no negativos que satisfacen

$$r_2 > r_3 > \ldots > r_i > \ldots$$

Esto quiere decir que eventualmente encontraremos un residuo r_{n+1} de forma que $r_{n+1} = 0$. Esto quiere decir que en algún punto obtendremos:

$$\begin{aligned}
a &= q_1 b + r_2 \\
b &= q_2 r_2 + r_3 \\
r_1 &= q_3 r_3 + r_4 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \\
r_{n-1} &= q_n r_n.
\end{aligned}$$

Es muy probable que en este punto no quede del todo claro donde encontrar el máximo común divisor en la secuencia, sin embargo, no hay necesidad de alarma, el siguiente lema explica cual de los números anteriores los índica.

Lema 7.8. *Para enteros a, b, q y r que satisfagan $a = qb + r$, se tiene que $(a, b) = (b, r)$.*

Demostración. Vamos a probar que un número d es un divisor común de a y b si y sólo si es un divisor común de b y r. Si este fuera el caso, los conjuntos de divisores comunes coinciden y en consecuencia los máximos de cada conjunto. Es realidad sencillo, sólo debemos notar dos cosas. Primero que r es una combinación lineal de a y b y segundo que a es una combinación lineal de b y r. Por esta razón, si por un lado d es un divisor común de a y b, debe ser divisor también de r; de manera similar, si d es un divisor de b y r, debe serlo también de a. Esto prueba el enunciado que se afirmo en el primer párrafo y de su discusión sigue el resultado. ■

El lema anterior nos permite usar la descripción que hemos usado para concluir

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n.$$

Esta afirmación es precisamente la que buscamos. Aplicar el teorema de la división repetidas veces sobre dos números hasta encontrar el residuo $r_{n+1} = 0$, deriva en encontrar también el máximo común divisor, el cual simplemente será el último residuo no nulo, i.e., r_n.

Ejemplo. Sean $a = 324$ y $b = 98$. Comenzamos utilizando el algoritmo de división para obtener el cociente y residuo de dividir 324 entre 98:

$$324 = 3 \cdot 98 + 30.$$

Eso quiere decir que debemos tomar $q_1 = 3$ y $r_2 = 30$. Efectuamos nuevamente una división, ahora entre 98 y 30, para obtener

$$98 = 3 \cdot 30 + 8.$$

Lo anterior indica la elección $q_2 = 3$ y $r_3 = 8$. Efectuamos una vez más la división, 30 entre 8, para obtener

$$30 = 3 \cdot 8 + 6.$$

Así, tenemos $q_3 = 3$ y $r_4 = 6$. Nuevamente, efectuamos otra división, 8 entre 6, para obtener

$$8 = 1 \cdot 6 + 2$$

y elegir $q_4 = 1$ y $r_5 = 2$. Por último, dividimos 6 entre 2, obteniendo

$$6 = 3 \cdot 2$$

por lo que $q_5 = 3$ y $r_6 = 0$. El algoritmo de Euclides nos permite concluir, en este punto, que $r_5 = 2$ es el máximo común divisor de 324 y 98.

3. Análisis del algoritmo de Euclides

Esta sección puede considerarse una invitación al análisis de algoritmos y quizá algunos de los resultados parezcan demasiado oscuros. No debemos preocuparnos demasiado si las ideas clave no quedan claros en una primera lectura. Antes de continuación habrá que definir algunos conceptos que tomaremos prestados de otros cursos y en los que no se abundará.

Definición 7.4. Sea $a = a_0 + a_1 10 + \cdots + a_{m-1} 10^{m-1}$ un entero positivo expresado de forma tal que cada entero a_i satisface $0 \leq a_i < 10$ y en particular $a_{m-1} \neq 0$. Entonces, los números a_i se dicen *los dígitos de a* y el número m representa *la cantidad de dígitos en a*.

No debe existir duda que cada entero se puede expresar de manera única a través de sus dígitos. Esto nos permite hablar sin ambigüedad de los dígitos de un entero. La discusión de estos conceptos a través de ejemplos es una trivialidad y para muestra un botón.

Ejemplo. Podemos expresar $134 = 4 \cdot 10^0 + 3 \cdot 10^1 + 1 \cdot 10^2$ para darnos cuenta que el entero tiene como sus dígitos a 1, 3 y 4, mostrando además que tiene 3 dígitos.

Lema 7.9. *Sea a un entero positivo con m dígitos. Entonces,*

$$m = \lfloor \log_{10} a \rfloor + 1.$$

Demostración. Para observar esto, expresamos $a = a_0 + a_1 10 + a_2 10^2 + \ldots a_{m-1} 10^{m-1}$ a través de sus dígitos, i.e., garantizando que $0 \leq a_i < 10$ para $1 \leq i \leq m-1$ y $a_{m-1} \neq 0$. Bajo esta descripción, debemos observar que el número a satisface

$$10^{m-1} \leq a < 10^m$$

pues 10^m es el mínimo entero con $m+1$ dígitos. En ese caso, como la función $\log_{10}$ es monótona,

$$m - 1 \leq \log_{10}(a) < m.$$

Esto quiere decir que $m-1$ es el entero más grande y menor que $\log_{10}(a)$ por lo que corresponde a la función piso, en otras palabras $m - 1 = \lfloor \log_{10} a \rfloor$ de lo que se desprende la afirmación del lema. ■

Vamos ahora a establecer con precisión el significado de la sucesión de Fibonacci y una de sus más famosas estimaciones.

Definición 7.5. *La sucesión de Fibonacci* se define de manera recursiva como

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n. \end{aligned}$$

Teorema 7.10. *Sean*

$$\alpha = \frac{1}{2}\left(1 + \sqrt{5}\right) \quad y \quad \beta = \frac{1}{2}\left(1 - \sqrt{5}\right).$$

Entonces, para todo natural n,

$$F_n = \frac{1}{\sqrt{5}}\left(\alpha^n - \beta^n\right).$$

Demostración. Definimos $S_n = \frac{1}{\sqrt{5}}\left(\alpha^n - \beta^n\right)$ por lo que debemos concluir que $F_n = S_n$ para todo natural n. Observemos primero que $S_0 = 0 = F_0$. Afirmamos ahora que para todo natural $n \geq 1$ se cumple $F_n = S_n$. En efecto, por inducción el caso $n = 1$ se reduce simplemente a observar que

$$S_1 = \frac{1}{\sqrt{5}}(\alpha - \beta) = \frac{1}{\sqrt{5}}\left(\sqrt{5}\right) = 1 = F_1.$$

Supongamos ahora que para $n \geq 1$, se tiene $F_k = S_k$ para todo $k \leq n$, entonces

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &= S_n + S_{n-1} \\ &= \frac{1}{\sqrt{5}} \left(\left(\alpha^n + \alpha^{n-1} \right) - \left(\beta^n + \beta^{n-1} \right) \right). \\ &= \frac{1}{\sqrt{5}} \left(\alpha^{n-1} (\alpha + 1) - \beta^{n-1} (\beta + 1) \right). \\ &= \frac{1}{\sqrt{5}} \left(\alpha^{n-1} \left(\alpha^2 \right) - \beta^{n-1} \left(\beta^2 \right) \right). \\ &= \frac{1}{\sqrt{5}} \left(\alpha^{n+1} - \beta^{n+1} \right). \\ &= S_{n+1}, \end{aligned}$$

notando simplemente que $\alpha^2 = \alpha + 1$ y $\beta^2 = \beta + 1$. Por inducción fuerte podemos concluir que $F_n = S_n$ para todo $n \leq 1$ y como $F_0 = S_0$ podemos concluir también la igualdad es cierta para todo natural n incluyendo el 0. ■

Corolario 7.11. *Para todos los enteros $n \geq 1$, se tiene $F_{n+2} > \alpha^n$.*

Demostración. El resultado sigue por inducción y el único paso que requiere comentario es el paso inductivo el cual se resuelve fácilmente como

$$\begin{aligned} F_{n+3} &= F_{n+2} + F_{n+1} \\ &> \alpha^n + \alpha^{n-1} \\ &= \alpha^{n-1}(\alpha + 1) \\ &= \alpha^{n-1}\alpha^2 \\ &= \alpha^{n+1}. \end{aligned}$$

■

Con este par de estimaciones, podemos ahora formular el número de veces que habremos de ejecutar el algoritmo de división para obtener el máximo común divisor utilizando el algoritmo de Euclides.

Definición 7.6. En la ejecución del algoritmo de Euclides entre los números a y b, el número n tal que $r_{n+1} = 0$ se denomina *el número de pasos requeridos para terminar el algoritmo*.

Teorema 7.12 (Teorema de Lamé)**.** *Sean a y b enteros positivos de forma que $a \geq b$ y sea m el número de dígitos de b. Si n es el número de pasos en la ejecución del algoritmo de Euclides para los enteros a y b, entonces*

$$n \leq 5m.$$

Demostración. Consideremos $r_0 = a$ y $r_1 = b$, en ese caso el algoritmo de Euclides produce ecuaciones de la forma

$$r_j = q_{j+1} r_{j+1} + r_{j+2}$$

excepto en la última donde

$$r_{n-1} = q_n r_n.$$

Debemos notar primero que $q_n \geq 2$, pues si no lo fuera $q_n \leq 1$ y tendríamos $r_{n-1} = q_n r_n \leq r_n$ en contradicción con tener $r_n < r_{n-1}$. De manera similar, para $1 \leq j \leq n-1$, se cumple $q_j \geq 1$, de otra forma $q_j = 0$ y obtendríamos que $r_{j-1} = r_{j+1}$ en contradicción con las desigualdades que satsifacen los residuos $r_{j+1} < r_j < r_{j-1}$.

Ahora,

$$r_n \geq 1 = F_2$$

y como $q_n \geq 2$

$$r_{n-1} = r_n q_n \geq 2r_n \geq 2F_2 \geq 2 = F_3.$$

De manera general tenemos

$$r_{n-j} \geq F_{j+2}.$$

Esto se prueba por inducción sobre $j \geq 0$, siendo el paso inductivo como sigue

$$\begin{aligned} r_{n-j-1} &= r_{n-j} q_{n-j} + r_{n-j+1} \\ &\geq r_{n-j} + r_{n-j+1} \\ &\geq F_{j+2} + F_{j+1} \\ &= F_{j+3}. \end{aligned}$$

En ese caso

$$b = r_1 = r_{n-(n-1)} \geq F_{n+1} > \alpha^{n-1}$$

donde $\alpha = \frac{1}{2}\left(1 + \sqrt{5}\right)$ como en el corolario 7.11. Basta ahora observar que $\log_{10}(\alpha) > \frac{1}{5}$ y en ese caso

$$\log_{10}(b) > (n-1)\log_{10}(\alpha) > \frac{n-1}{5};$$

esto es

$$n - 1 < 5\log_{10}(b) < 5m$$

pues de acuerdo al lema 7.9, $m = \lfloor \log_{10}(b) \rfloor + 1$. En ese caso, $n \leq 5m$ como afirma el teorema. ■

Ejemplo. En el ejemplo 2, el número $b = 98$ tiene 2 dígitos por lo que según el teorema, el algoritmo de Euclides se ejecutará en a lo más 10 pasos. En el desarrollo del ejemplo podemos observar que el algoritmo se ejecuta en 5 pasos lo cual es consistente con lo que afirma el teorema.

Es muy interesante que se pueda estimar el número de pasos que requiere el algoritmo de Euclides con tan sólo observar el número de dígitos de una de sus entradas. Historicamente, el algoritmo de Euclides fue unos de los primeros en que se consiguió estimar el número de pasos requeridos a través de algunas propiedad en sus entradas y el resultado fue tan importante que su publicación en 1844, por el matemático francés Gabriel Lamé, se considera el inicio de un área en la matemática conocida como *teoía de la complejidad computacional*.

Ejercicios

Ejercicio 7.1. Encuentra la factorización prima de los siguientes números.

1. 425.
2. 147.
3. 93.
4. 137.

Ejercicio 7.2. Usando las factorizaciones del ejercicio anterior, expresa cada una en forma exponencial evitando tener exponentes nulos.

Ejercicio 7.3. Para un primo p y un entero $a > 1$, muestra que $(p, a) \neq 1$ si y sólo si $p \mid a$.

Ejercicio 7.4. Define por analogía con el concepto de máximo comun divisor, el concepto de mínimo común mútiplo.

Ejercicio 7.5. Demuestra que si $m \mid a$ y $n \mid a$ entonces $[m, n] \mid a$.

Ejercicio 7.6. Si a y b son enteros que dividen a n y tales que $(a, b) = 1$, demuestra que su producto también divide a n.

Ejercicio 7.7. Utilizando el algoritmo de Euclides encuentra el máximo común divisor de los siguientes números.

1. 228 y 348.
2. 15 y 21.
3. 35 y 71.
4. $2n + 1$ y $4n$, para $n \geq 1$.

Ejercicio 7.8. Para un primo p y un entero $a > 1$, demuestra que $(p, a) \neq 1$ si y sólo si $p \mid a$.

Ejercicio 7.9. Prueba la segunda parte del lema 7.3.

Ejercicio 7.10. Si a y b son enteros que dividen a n y tales que $(a, b) = 1$, demuestra que su producto también divide a n.

Ejercicio 7.11. Si $d = (a, b)$, demuestra que a/d y b/d son primos relativos.

Ejercicio 7.12. Sean a y b enteros positivos tales que $(a, b) = 1$. Si ab es un cuadrado perfecto, demuestra que a y b son ambos cuadrados perfectos.

Ejercicio 7.13. Muestra que un entero $m \geq 2$ es un cuadrado perfecto si y sólo si su factorización expresada de forma exponencial, contiene solamente exponentes pares.

Para entregar: Ejercicio 7.13

Referencias

[Chi95] Childs, Lindsay N.: *A concrete introduction to higher algebra*. Springer, 2ª edición, 1995.

[CLRT90] Cárdenas, Humberto, Luis, Emilio, Raggi, Francisco y Tomás, Francisco: *Álgebra Superior*. Editorial Trillas, 1990.

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.