Introducción a la teoría de números

José Cuevas Barrientos

21 de abril de 2019

1 Introducción

Para el siguiente artículo supondremos que el lector está familiarizado con los distintos tipos de números (naturales $\mathbb{N} = \{0, 1, 2, 3, \dots\}$[1], enteros $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ y racionales $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z} \wedge b \neq 0\}$) al igual que las operaciones básicas de suma, resta, multiplicación y división. Al contrario de otros de mis escritos, el presente es independiente de otras lecturas, de forma que no se piden requisitos avanzados ni será este una lectura obligatoria para la comprensión de otro. La finalidad principal es el de la preparación introductiva al tema para afrontar problemas olímpicos.

2 Divisibilidad

En orden para continuar con nuestras demostraciones debemos primero introducir un axioma local[2]:

Axioma del Buen Orden: Todo subconjunto no vacío S de los naturales $\mathbb{N}$ posee elemento mínimo.

Teorema 2.1 (Algoritmo de la división): Dados cualesquiera $a, b \in \mathbb{Z}$ con $a > 0$, existen unos únicos números $q, r \in \mathbb{Z}$ tales que

$$b = aq + r, \quad 0 \leq r < a$$

Proof: Vamos a definir un conjunto

$$S = \{x \in \mathbb{N} : x = b - an, \quad n \in \mathbb{Z}\}$$

[1] En algunos casos se decide no incluir al "0", sin embargo, al estudiar la matemática formalmente, aquel elemento es indispensable.

[2] Con esto nos referimos a que es demostrable en sistemas que no partan desde los axiomas de Peano.

y veremos que es no vacío.

Si $b \geq 0$ entonces para $n = 0$ se obtiene $x = b - a \cdot 0 = b \geq 0$ luego $b \in S$.

Si $b < 0$ entonces, como a es entero positivo, luego $a \geq 1$, multiplicando por $-b$ obtenemos

$$-ab \geq -b \implies x = b - ab \geq 0,$$

finalmente $x \in S$, es decir, S es siempre no vacío.

Por axioma del buen orden, S posee mínimo al que denotaremos como

$$r = b - aq.$$

Ahora hemos de probar la desigualdad con r. Supongamos que (como r es natural) por contradicción $r \geq a$, luego $r - a = b - aq - a = b - a(q+1) \geq 0$, por lo tanto, $r - a \in S$, lo que contradice el que nuestro r sea el mínimo elemento.

Finalmente probaremos la unicidad suponiendo que existen múltiples r_1, r_2 y q_1, q_2 que satisfacen, la ecuación, luego

$$aq_1 + r_1 = aq_2 + r_2,$$

supongamos que $r_2 \geq r_1$ es positivo, luego

$$r_2 - r_1 = a(q_1 - q_2)$$

como a es positivo y entero, $q_1 - q_2$ debe ser también entero positivo. Luego $r_2 - r_1$ debe ser múltiplo de a, sin embargo, como

$$0 \leq r_1 \leq r_2 < a,$$

entonces debe ser cero; con lo cual se concluye que $q_1 = q_2$. □

A tal q en el algoritmo se le dice "cociente", mientras que a r se le denomina "resto".

Definición 2.2 (Divisibilidad): Sean $a, b \in \mathbb{Z}$ (léase "a y b enteros"), escribiremos $a \mid b$ (léase "a divide a b" o "b es múltiplo de a") si y sólo si existe un entero q tal que $b = aq$.

Por ejemplo $2 \mid 10$ o $3 \mid 6$.

Teorema 2.3: Sean $a, b, c \in \mathbb{Z}$ con $a \neq 0$ entonces:

1. $a \mid 0$, $a \mid ka$ y $1 \mid a$ para todo $k \in \mathbb{Z}$.

2. $a \mid b$ y $c \mid d$ implican $ac \mid bd$.

3. $a \mid b$ y $b \mid c$ implican $a \mid c$.

4. $a \mid b$ y $a \mid c$ implican $a \mid ub + vc$, donde $u, v \in \mathbb{Z}$.

5. $a \mid b$ con a, b positivos implica $a \leq b$.

6. $a \mid b$ y $b \mid a$ implican $|a| = |b|$.

PROOF: Probaremos el 4:
Por construcción existen $q_1, q_2 \in \mathbb{Z}$ tales que $b = aq_1$ y $c = aq_2$, finalmente $ub + vc = uaq_1 + vaq_2 = a(uq_1 + vq_2)$. □

Definición 2.4 (Máximo común divisor): Dados $a, b \in \mathbb{Z}$ definimos el máximo común divisor $M = (a; b)$ como aquel que satisface:

a) $M \mid a$ y $M \mid b$.

b) Si $c \mid a$ y $c \mid b$ entonces $c \leq M$.

Cabe destacar que el máximo común divisor no es una *función ordenada*, es decir, $(a; b) = (b; a)$.

Teorema 2.5: Sean $a, b, k \in \mathbb{Z}$ no nulos, entonces

a) $(a; b) = (-a; b) = (-a; -b) = (|a|; |b|)$.

b) $(ak; bk) = |k|(a; b)$.

c) $(a; b) = d$. $(a/d; b/d) = 1$.

Lema 2.6: Sean $a, b \in \mathbb{Z}$ tales que $b = aq + r$, entonces $(a; b) = (a; r)$.

PROOF: Sean $k = (a; b)$ y $l = (a; r)$. Es fácil ver que como $r = b - aq$, entonces $k \mid r$ por definición $k \leq l$. Asimismo, se deduce que $k \geq l$; con lo cual $k = l$. □

Teorema 2.7 (Algoritmo de Euclides): Sean $a, b \in \mathbb{Z}$, una forma de calcular $(a; b)$ es a través del siguiente método:

$$b = aq_1 + r_1, \quad 0 < r_1 < a$$

$$\begin{aligned} a &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_n &= r_{n+1} q_{n+2}, \end{aligned}$$

dónde $r_{n+1} = (a; b)$.

Tomemos dos números cualesquiera: 288 y 560, e intentemos aplicar al método de Euclides:

$$\begin{aligned} 560 &= 288 \cdot 1 + 272 \\ 288 &= 272 \cdot 1 + 16 \\ 272 &= 16 \cdot 17 \end{aligned}$$

por lo tanto $16 = (288; 560)$.

Teorema 2.8 (Identidad de Bezout): Para todo $a, b \in \mathbb{Z}$ existen $x, y \in \mathbb{Z}$ tales que $(a; b) = ax + by$.

PROOF: Definamos el conjunto

$$S = \{z > 0 : z = ax + by, \quad x, y \in \mathbb{Z}\}$$

veamos que no es vacío. Pues $a^2 + b^2 \in S$. Por principio del buen ordenamiento posee mínimo $g = ax_0 + by_0$.

Podemos ver que g divide a a y a b pues

$$a = qg + r, \quad 0 \leq r < g$$

con lo cual

$$\begin{aligned} r &= a - qg \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + by_0 \in S \end{aligned}$$

Si $r \neq 0$ entonces se contradice con que g era el menor.

Como g es un divisor común de a, b se concluye que $g \leq d = (a; b)$.

Como $d \mid a$, $d \mid b$, entonces $d \mid ax_0 + by_0 = g$. Al ser ambos positivos, $d \leq g$. Por antisimetría $d = g$. □

Teorema 2.9: Si se encuentran $u, v \in \mathbb{Z}$ tales que

$$ua + vb = 1,$$

entonces $(a; b) = 1$.

PROOF: Considere la prueba anterior, demostramos que el mínimo del conjunto equivale al máximo común divisor, como dicho conjunto admite únicamente valores positivos, el mínimo valor posible es 1, de ser obtenido, es inmediato que equivale al mcd. □

Teorema 2.10 (Lema de Euclides): Sea $a \mid bc$ y $(a; b) = 1$ entonces $a \mid c$.

PROOF: Por identidad de Benzout, $1 = ax_0 + by_0$, por lo tanto, $c = ax_0c + by_0c$. Evidentemente $a \mid ax_0c$ y por construcción $a \mid y_0bc$, luego $a \mid ax_0c + by_0c = c$. □

Teorema 2.11: Sea $(a; b) = 1$ y $(a; c) = 1$, entonces $(a; bc) = 1$.

PROOF: Digamos que $d = (a; bc)$. Como $d \mid a$ y $(a; b) = 1$, se obtiene que $(d; b) = 1$. Por lema de Euclides $d \mid c$. Y como $(a; c) = 1$ entonces $d = 1$. □

Definición 2.12 (Números coprimos y primos): Decimos que $a, b \in \mathbb{Z}$ son *coprimos* syss $(a; b) = 1$. Un número primo p es aquel que es positivo y sólo posee dos divisores naturales: el 1 y p. Los números que son el producto de números primos son llamados *compuestos*.

Teorema 2.13: Sea p primo tal que $p \nmid a$ entonces $(p; a) = 1$.

PROOF: Por definición $d = (p; a)$ cumple $d \mid p$, luego $d \mid 1$ o $d \mid p$. Como $d \mid a$ y $p \nmid a$ entonces $d \nmid p$, es decir, $d \mid 1$. □

Esto podríamos haberlo utilizado como definición auxiliar de *primo*.

Teorema 2.14: Sea p primo tal que $p \mid ab$ entonces $p \mid a$ o $p \mid b$. Más generalmente si $p \mid a_1 \cdots a_n$ entonces divide a por lo menos uno de los a_i.

PROOF: Probaremos la primera proposición. Si $p \mid ab$ pero $p \nmid a$, lo que implica $(p; a) = 1$, por lema de Euclides, $p \mid b$. El resto es por inducción. □

Teorema 2.15 (Teorema fundamental de la aritmética): Todo número natural mayor que 1 puede escribirse como un único producto de números de primos.

PROOF: Primero probaremos que todo número o es primo o es compuesto. Supongamos que tenemos el siguiente conjunto

$$S = \{n \in \mathbb{N} : n > 1 \text{ y } n \text{ es primo o compuesto}\},$$

probaremos que contiene a todo $n > 1$ por inducción. Evidentemente $2 \in S$. Si $n+1$ es primo entonces pertenece a S, sino, puede escribirse como $n+1 = ab$ donde como $a \mid n+1$ se cumple que $a \leq n+1$ y $b \leq n+1$, luego $a, b \in S$; es decir, a, b o son primos o son producto de primos, por lo tanto, $n+1$ es compuesto.

Ahora probaremos que la descomposición prima es única. Supongamos que no lo fuese y hubiesen dos posibles descomposiciones primas:

$$n = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_n$$

donde $p_1 \leq p_2 \leq \cdots \leq p_n$ y $q_1 \leq q_2 \leq \cdots \leq q_n$. Luego $p_1 \mid q_1 q_2 \cdots q_n$. Por ser primo, $p_1 \mid q_i$ para algún $1 \leq i \leq n$, es decir, $p_1 \leq q_1$. Por simetría $q_1 \mid p_1 \cdots p_n$ y $q_1 \leq p_1$. Como $p_1 = q_1$. Luego podemos aplicar el mismo método sobre

$$\frac{n}{p_1} = p_2 \cdots p_n = q_2 \cdots q_n$$

para ver que, por inducción, $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_n = q_n$. Es decir, la factorización es única. □

Teorema 2.16: Los números primos son infinitos.

PROOF: Supongamos por contradicción que los primos fueran finitos, entonces podríamos hacer una lista de todos ellos como prosigue:

$$P := \{p_1, p_2, \ldots, p_n\},$$

como nos hemos asegurado que p_i es positivo y mayor que 1, es fácil ver que si $p_i \mid c$ entonces $p_i \nmid c+1$. Finalmente el número

$$c = p_1 \cdot p_2 \cdots p_n + 1$$

no sería divisible por ningún de los primos en nuestra lista, y por lo tanto, por ningún otro número más que si mismo y el 1; es decir, c sería primo, contradiciendo que los habíamos organizado en una lista. □

También, suele ser necesario tener que confirmar si un número es primo, por lo cual, hay varias formas, la primera es **la criba de Eratóstenes** que consiste en denotar los números de 2 hasta n y comenzar tachando los múltiplos de los primos, los no tachados resultan ser primos:

		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~~

pero considera que si queremos ver si n es primo debemos comprobar que no sea divisible por ningún número entre 2 y $n-1$ (lo cuál es un proceso terriblemente ineficiente). Por lo cuál, el truco está en probar **sólo** los números primos, del 2 hasta $\sqrt{n}$.

Una identidad muy interesante, y que puede ser de mucho uso es que si $\tau(n)$ es la función que calcula la cantidad de divisores que tiene un natural n.

Teorema 2.17: Sea $n > 1$, por lo que, por TFA tiene una única descomposición prima:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} = \prod_{i=1}^{m} p_i^{\alpha_i},$$

entonces

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1) = \prod_{i=1}^{m} (\alpha_i + 1).$$

3 Aritmética modular

Definición 3.1 (Aritmética modular): Sea $n > 1$, escribiremos $a \equiv b \mod n$ (léase "a y b congruentes en módulo n") syss $n \mid a - b$. Asimismo definiremos $\mathbb{Z}_n = \{0, \ldots, n-1\}$.

Usualmente se explica la aritmética modular con el comportamiento de un reloj, pues se puede comprobar que la idea que dos números son congruentes en un cierto módulo equivale a decir que poseen el mismo resto al aplicarles el algoritmo de la división. En ese sentido $13 \equiv 1 \mod 12$ o $22 \equiv 10 \mod 12$.

En este mismo contexto podemos definir la función $f(x) = \mod(x, n)$ como aquella que le da a todo x el número que le es equivalente en módulo n pero que satisfaga $0 \leq f(x) < n$ (es decir, el resto).

Teorema 3.2: Sea $n > 1$, $a \equiv b \mod n$ y $c \equiv d \mod n$; entonces

a) $a + c \equiv b + d \mod n$.

b) $ac \equiv bd \mod n$.

PROOF: Probaremos la propiedad multiplicativa usando la definición de módulos para ver que $a = nk_1 + b$ y $c = nk_2 + d$, luego

$$ac = (nk_1 + b)(nk_2 + d) = n^2 k_1 k_2 + nk_2 b + nk_1 d + bd \equiv bd \mod n$$

pues todos los múltiplos de n son congruentes con 0 en dicho módulo. □

Corolario 3.2.1: Sea $n > 1$ y $a \equiv b \mod n$ entonces $a^m \equiv b^m \mod n$ con $m \in \mathbb{N} \setminus \{0\}$.

Teorema 3.3 (Pequeño teorema de Fermat): Sea p primo tal que $p \nmid a$, entonces

$$a^{p-1} \equiv 1 \mod p$$

PROOF: La demostración es aquella reescrita por Dirichlet y consta de varios pasos. Primero, consideremos que $(a; b) = 1$, entonces, la ecuación

$$ax \equiv ay \mod b$$

implica

$$x \equiv y \mod b$$

(por lema de Euclides). Consideremos la secuencia

$$a, 2a, 3a, \ldots, (p-1)a;$$

como ningún término es múltiplo de p, ninguno es congruente a 0 en módulo p, y por "ley de la cancelación" nos queda que

$$ka \equiv ma \mod p \iff k \equiv m \mod p$$

por lo que ningún par de términos en la lista es congruente en módulo p. Por lo tanto, la secuencia, en módulo p, puede *reordenarse* en

$$1, 2, \ldots, (p-1);$$

por lo que

$$a \times 2a \times \cdots \times (p-1)a \equiv 1 \times 2 \times \cdot \times (p-1) \mod p$$
$$a^{p-1}(p-1)! \equiv (p-1)! \mod p$$

Finalmente, por "ley de la cancelación" nos queda el enunciado. □

Usualmente se aplica el pequeño teorema de Fermat en la forma

$$a^p \equiv a \mod p$$

4 Problemas

1. Probar que todo primo de la forma $3k+1$ es de la forma $6k+1$.
2. Probar que si x, y son impares entonces $x^2 + y^2$ no es un cuadrado perfecto.
3. ¿Cuál es el exponente de 7 en la descomposición de 2011! en producto de factores primos?
4. ¿Cuántos ceros tiene 2011!?
5. Demuestre que para todo n entero $n^3 - n$ es divisible por 6.
6. (Canguro 2007) Si dividimos 336 en un tal n obtenemos resto 2. ¿Cuál es el resto obtenido al dividir 2007 en dicho n?
7. Probar que todo entero es divisible por 3 syss la suma de sus dígitos es divisible por 3.

8. Probar que para todo primo $p > 2$ y todo natural n se cumple que

$$p \mid 1^{p^n} + 2^{p^n} + \cdots + (p-1)^{p^n}.$$

9. (OIM 1959) Probar que la ecuación

$$\frac{21n+4}{14n+3}$$

es irreductible para todo n entero.

10. (TT 2001) Si en la pizarra está escrito un número natural n, una *operación permitida* consiste en sustituirlo por el producto ab, si a y b son naturales tales que $a + b = n$. Inicialmente está escrito el número 22. ¿Existe una secuencia de operaciones permitidas que nos conduzca al número 2001?

11. (SOMACHI 2018) Encuentre todos los primos p tales que $p^2 + 2$ es primo.

12. (OIM 1999). Halle todos los enteros positivos que son menores que 1000 y cumplen con la siguiente condición: el cubo de la suma de sus dígitos es igual al cuadrado de dicho entero.

13. (SOMACHI 2018) ¿Se pueden elegir cinco enteros positivos tales que la suma de todos los grupos de a tres sea un número primo?

14. (Eötvös 1894) Demuestre que $17 \mid 2m + 3n$ syss $17 \mid 9m + 5n$.

15. Demostrar que $2222^{5555} + 5555^{2222}$ es divisible por 7.

Soluciones*

1. Veamos que dicho k puede escribirse en base 2 como $k = 2q + r$ con $r \in \{0, 1\}$, supongamos que $r = 1$ entonces $p = 3 \cdot (2q + 1) + 1 = 6q + 4 = 2(3q + 2)$, que es creciente con valor mínimo $q = 0$ es decir $p = 4$ lo que es mayor que 2, es decir, siempre será un número par mayor que 2; por ende $r = 0$ y $p = 3k + 1 = 6q + 1$.

2. Como son impares $x = 2a + 1$ e $y = 2b + 1$, luego

$$x^2 + y^2 = 4(a^2 + b^2) + 4(a + b) + 2 = 2(2(a^2 + b^2 + a + b) + 1)$$

   lo que no es un cuadrado perfecto pues a la izquierda tenemos un divisible por 2 (pero no por $4 = 2^2$) y a la derecha un término que no es divisible por 2.

3. Vamos a utilizar un ejemplo, ¿cuál es el máximo exponente de 2 en 3!? Evidentemente cada múltiplo de 2 le suma uno al exponente, por lo cual el resultado es

$$\left\lfloor \frac{3}{2} \right\rfloor = 1.$$

   ¿Y de 4!? Nuestro procedimiento dice $\lfloor 4/2 \rfloor = 2$, pero la respuesta correcta es 3, pues $4 = 2^2$, es decir, la segunda potencia aumenta dos veces el índice, eso lo arreglamos sumando los múltiplos del cuadrado:

$$\left\lfloor \frac{4}{2} \right\rfloor + \left\lfloor \frac{4}{2^2} \right\rfloor = 3.$$

   ¿Y para 8!? Aquí $8 = 2^3$, por lo que también suma otro. En general, el exponente de n en $m!$ es la suma de la función suelo[3] de la división de m con todas las potencias de n menores o iguales a m. Aplicado al problema, nótese que

$$7^1 = 7, \quad 7^2 = 14, \quad 7^3 = 343, \quad 7^4 = 2401 > 2011$$

   por lo que el resultado correcto es

$$\left\lfloor \frac{2011}{7} \right\rfloor + \left\lfloor \frac{2011}{7^2} \right\rfloor + \left\lfloor \frac{2011}{7^3} \right\rfloor = 287 + 41 + 5 = 333.$$

[3] A veces llamada *truncamiento*.

4. Este problema es similar al anterior pero hay que ver que $10 = 5 \cdot 2$, los múltiplos de dos son **demasiado** frecuentes, por lo que se reduce a contar el exponente de 5 (pues es más que evidente que para cada 5 hay al menos un múltiplo de 2). Aplicando la misma lógica vemos que el resultado es

$$\begin{aligned}\left\lfloor \frac{2011}{5} \right\rfloor + \left\lfloor \frac{2011}{5^2} \right\rfloor + \left\lfloor \frac{2011}{5^3} \right\rfloor + \left\lfloor \frac{2011}{5^4} \right\rfloor &= 402 + 80 + 16 + 3 \\ &= 501.\end{aligned}$$

5. $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$, lo que corresponde al producto de tres números consecutivos. Como lema es fácil probar por inducción que en un conjunto de n números consecutivos hay siempre uno que es divisible por n. Con ello vemos que aquí hay por lo menos un múltiplo de 2 y un múltiplo de 3, por lo tanto, el producto entero es un múltiplo de 6.

6. Esto quiere decir que $336 = nq + 2$, o que $334 = nq$. Vemos que los divisores de 334 son 1, 2, 167 y 334. El 1 y el 2 se descartan pues no darían resto 2 con 336. Finalmente si aplicamos algoritmo de la división a 2007 con cualquiera obtenemos

$$2007 = 167 \cdot 12 + 3.$$

7. Veamos que todo número, debido a su expansión decimal, puede ser escrito como

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots$$

Por lo que $3 \mid a_0 + 10a_0 + 10^2 a_2 + \cdots$ syss $3 \mid a_0 + 10a_1 + 10^2 a_2 + \cdots - 9a_1 - 99a_2 - \cdots$, y evidentemente lo último es "valido" puesto que $9 = 3 \cdot 3$, $99 = 33 \cdot 3$ y así sucesivamente.

8. Se obtiene por inducción y con el pequeño teorema de Fermat. Caso $n = 0$:

$$1 + 2 + \cdots + (p-2) + (p-1) = \frac{p-1}{2} \cdot p \equiv 0 \mod p$$

Esto se debe a que $p - 1$ es par puesto que todo primo mayor que 2 es impar. Caso $n + 1$:

$$\begin{aligned}1^{p^{n+1}} + 2^{p^{n+1}} + \cdots + (p-1)^{p^{n+1}} &= (1^p)^{p^n} + (2^p)^{p^n} + \cdots + ((p-1)^p)^{p^n} \\ &\equiv 1^{p^n} + 2^{p^n} + \cdots + (p-1)^{p^n} \mod 7\end{aligned}$$

que es equivalente a 0 en módulo 7 por hipótesis inductiva.

9. Nótese que
$$3(14n+3)-2(21n+4)=1,$$
es decir, siempre serán coprimos.

10. Observe que para todo $n>1$ se cumple que $n=(n-1)+1$ y $1\cdot(n-1)=n-1$, es decir, si obtenemos a n, obtenemos a todos sus antecesores. $22=10+12$, luego $10\cdot 12=120$ y $120=60+60$, con lo que $60\cdot 60=3600$; por lo tanto, podemos obtener a 2001.

11. Nótese que para todo primo p distinto de 3, se puede escribir como $3q+1$ o $3q+2$ y que
$$(3q+1)^2+1=9q^2+6q+1+2=3(3q^2+2q+1),$$
$$(3q+2)^2+2=9q^2+6q+4+2=3(3q^2+2q+2).$$
Como ve, todos son múltiplos de 3, luego no son primos. En cambio $3^2+2=9+2=11$. Es decir, sólo el 3 satisface la condición.

12. Los enteros n pedidos deben satisfacer que n^2 es un cubo perfecto, equivalentemente, n es cubo perfecto. Los cubos perfectos menores a 1000 son 1, 8, 27, 64, 125, 216, 343, 512 y 729; y los únicos de esta lista en satisfacer dicha propiedad son el 1 y el 27.

13. Consideremos un conjunto de tres enteros a,b,c. Si los tres poseen el mismo resto en base 3, entonces su suma será divisible por 3:
$$a+b+c\equiv r+r+r=3r\equiv 0 \mod 3.$$
Por trabajar en módulo 3, los únicos tres restos posibles son 0, 1, 2; si los tres poseen restos distintos su suma es divisible por 3:
$$a+b+c\equiv 0+1+2=3\equiv 0 \mod 3.$$
Finalmente no podemos tomar cinco números sin que al menos en un grupo de a tres todos tengan mismos restos o distintos entre sí.

14. Nótese que $13(2m+3n)-17(m+2n)=9m+5n$, como $(13;17)=1$ (por ser primos) entonces la equivalencia es clara.

15. Primero ver que $2222=317\cdot 7+3$ y $5555=793\cdot 7+4$, por lo que
$$2222^{5555}+5555^{2222}\equiv 3^{5555}+4^{2222} \mod 7,$$

observe $2222 = 370 \cdot 6 + 2$ y $5555 = 925 \cdot 6 + 5$, con teorema de Fermat:

$$\begin{aligned} 3^{5555} + 4^{2222} &= (3^3 70)^6 \cdot 3^2 + (4^9 25)^6 \cdot 4^5 \\ &\equiv 3^2 + 4^5 \mod 7 \\ &= 9 + 1024 \equiv 2 + 5 \equiv 0 \mod 7. \end{aligned}$$

References

1. Andreescu, T., Andrica, D. & Feng, Z. *104 number theory problems: from the training of the USA IMO team* (Springer Science & Business Media, 2007).
2. Ankeny, N. C. Sums of three squares. *Proc. Amer. Math. Soc.* doi:10.1090/S0002-9939-1957-0085275-8 (1957).
3. Clark, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).
4. Cohn, H. A Short Proof of the Simple Continued Fraction Expansion of e. *Amer. Math. Mon.* doi:10.2307/27641837 (2006).
5. Conrad, K. *Fermat's little theorem* https://kconrad.math.uconn.edu/blurbs/ugradnumthy/fermatlittletheorem.pdf.
6. Conrad, K. *Modular Arithmetic* https://kconrad.math.uconn.edu/blurbs/ugradnumthy/modarith.pdf.
7. Conrad, K. *The Division Theorem in $\mathbb{Z}$ and $F[T]$* https://kconrad.math.uconn.edu/blurbs/ugradnumthy/divthmZF%5BT%5D.pdf.
8. Conrad, K. *The infinitude of the primes* https://kconrad.math.uconn.edu/blurbs/ugradnumthy/infinitudeofprimes.pdf.
9. Cuevas, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).
10. Cuevas, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).
11. De Bessy, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).
12. Dedekind, R. Sur la théorie des nombres entiers algébriques. *Bull. Sci. Math. et Astronomiques.* doi:10.1007/978-3-322-98606-1_3 (1876).
13. Dedekind, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).

14. Dickson, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).

15. Dirichlet, P. G. L. *Vorlesungen über Zahlentheorie* (ed Dedekind, R.) (Braunschweig, 1863).

16. Dixon, J. D. π is not Algebraic of Degree One or Two. *Amer. Math. Mon.* doi:10.2307/2310831 (1962).

17. Ebbinghaus, H.-D. *et al. Numbers* (Springer-Veriag New York, 1991).

18. Edwards, H. M. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory Graduate Texts in Mathematics* **50** (Springer-Verlag, 1977).

19. Eggleton, R. B., Lacampagne, C. B. & Selfridge, J. L. Euclidean Quadratic Fields. *Amer. Math. Mon.* doi:10.2307/2324118 (1992).

20. Euler, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125–146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).

21. Euler, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3–40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).

22. Euler, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).

23. Gauss, C. F. *Disquisitiones Arithmeticae* trans. by Ruiz Zúñiga, A. https://archive.org/details/disquisitiones-arithmeticae-carl-f.-gauss-espanol (Universidad de Costa Rica, 1801).

24. Harper, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).

25. Hua, L. K. *Introduction to Number Theory* (Springer-Verlag Berlin Heidelberg, 1982).

26. Khinchin, A. *Continued Fractions* (University of Chicago Press, 1964).

27. Kronecker, L. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. Reine Angew. Math.* doi:10.1515/crll.1882.92.1 (1882).

28. Kummer, E. E. *De Numeris Complexis, Qui Radicibus Unitatis Et Numeris Integris Realibus Constant* (Kessinger Publishing, 1844).

29. Kummer, E. E. Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. *Kgl. Preuss. Akad. Wiss* (1856).

30. Mordell, L. J. *Diophantine Equations* (Academic Press, 1969).

31. Nathanson, M. B. *Elementary Methods in Number Theory* (Springer-Verlag New York, 2000).

32. Niven, I. A simple proof that π is irrational. *Bull. Amer. Math. Soc.* **53.** doi:10.1090/S0002-9904-1947-08821-2 (1947).

33. Niven, I. *Irrational Numbers* (Mathematical Association of America, 1956).

34. Pollack, P. *Not Always Buried Deep* (American Mathematical Society, 2009).

35. Ribenboim, P. *Fermat's Last Theorem for Amateurs* (Springer-Verlag New York, 1999).

36. Weil, A. *Number theory. An approach through history, from Hammurapi to Legendre* (Birkhäuser Boston, 1906).