Olimpiada Básica de Matemáticas en Guanajuato

@OBMGuanajuato | 16 de septiembre

Congruencias con módulos

Emilio Toscano Oneto

1 Módulos

En problemas de teoría de números, el concepto de congruencias abre muchas oportunidades en el momento de resolver un problema, pues es un tema que permite relacionar a los números enteros con clases de equivalencia, es decir, que se pueden pensar que 2 enteros son "iguales" bajo estas ideas y los cuáles resultan muy útiles en la resolución de problemas acerca de divisibilidad.

Nota 1.1. *Como notación, cuando escribamos $a \mid b$, decimos que a divide a b o equivalentemente, b es múltiplo de a. Decimos también que un número n es natural si n es un entero positivo (no incluye al 0).*

Definición 1.2. *Sea n un número natural. Si a y b son enteros cualesquiera (no necesariamente positivos), decimos que $a \equiv b \pmod{n}$ si $n \mid a-b$.*

Nota 1.3. *Cuando escribimos $a \equiv b \pmod{n}$, decimos que "a es congruente a b, módulo n".*

Ejemplo 1.4. *Para los enteros 124, 3201 y 26, se observa que*

$$124 - 4 = 120 = 6 \times 20$$
$$3201 - 3 = 3198 = 6 \times 533$$
$$26 - 2 = 24 = 6 \times 4$$

Es decir, $124 \equiv 4 \pmod{6}$, $3201 \equiv 3 \pmod{6}$ y $26 \equiv 2 \pmod{6}$. Más aún, si n es múltipo de 6, entonces $n-0$ es múltiplo de 6, por lo que $n \equiv 0 \pmod{6}$.

Proposición 1.5. *Sea n un número natural y sean a y b enteros. Supongamos que $a = nq_1 + r_1$ y que $b = nq_2 + r_2$, con q_1, q_2, r_1 y r_2 enteros tales que $0 \leq r_1, r_2 < n$. Entonces $a \equiv b \pmod{n}$ si y sólo si $r_1 = r_2$.*

Demostración de Proposición 1.5 : Si $a \equiv b \pmod{n}$, entonces supongamos que $r_1 \geq r_2$ y observemos que $a-b = n(q_1-q_2)+(r_1-r_2)$, pero $n \mid a-b$, por lo que $n \mid r_1-r_2$. Sin embargo, $0 \leq r_1 - r_2 \leq r_1 < n$ y necesariamente ocurre que $r_1 = r_2$. El caso de $r_1 \leq r_2$ es completamente analogo si se observa que $n \mid a-b$ implica que $n \mid b-a$, pues $-(b-a) = a-b$.

Supongamos ahora que $r_1 = r_2$. Al considerar al número $a-b$, se obtiene que $a-b = n(q_1-q_2) + (r_1-r_2) = n(q_1-q_2)$, es decir, $a-b$ es múltiplo de n y así $a \equiv b \pmod{n}$.
■

Observación 1.6. *Notemos a partir de la Proposición 1.5, para un natural dado n, si $a \equiv b \pmod{n}$, entonces si $0 \leq b < n$ podemos escribir al entero a como $a = nk + b$ para algún k entero.*

Ejemplo 1.7. *Veamos que dos enteros a y b son congruentes módulo 2 entre sí cuando ambos son o bien pares o impares. Si a y b son pares, entonces son múltiplos de 2, es decir $a = 2a'$ y $b = 2b'$ para ciertos a' y b' enteros, por lo tanto, $a - b = 2a' - 2b' = 2(a' - b')$ es múltiplo de 2 y así concluimos que $a \equiv b \pmod 2$. En caso contrario, cuando a y b son impares, entonces podemos escribir $a = 2p_1 + q_1$ y $b = 2p_2 + q_2$ con p_1, p_2, q_1 y q_2 enteros, con q_1 y q_2 impares (pues en caso contrario a y b no serían impares). De esta manera, notemos que $a - b = 2(p_1 - p_2) + (q_1 - q_2)$, pero sabemos que resta de números impares es par, por lo tanto $a - b$ es par, es decir, 2 lo divide y así $a \equiv b \pmod 2$.*

Proposición 1.8. *Sea n un número natural. Para a, b, c y d enteros cualesquiera, se cumple lo siguiente:*
(i) La congruencia es reflexiva. $a \equiv a \pmod n$.
(ii) La coongruencia es simétrica. $a \equiv b \pmod n$ implica que $b \equiv a \pmod n$.
(iii) La congruencia es transitiva. Si $a \equiv b \pmod n$ y $b \equiv c \pmod n$, entonces $a \equiv c \pmod n$.
(iv) Si $a \equiv b \pmod n$ y $c \equiv d \pmod n$, entonces $a + c \equiv b + d \pmod n$.
(v) Si $a \equiv b \pmod n$ y $c \equiv d \pmod n$, entonces $ac \equiv bd \pmod n$.

Demostración de Proposición 1.8 : (i) En efecto, $a - a = 0 = 0 \times n$ y así $a \equiv a \pmod n$.
(ii) Si $a \equiv b \pmod n$, entonces $a - b = nk$ para algún entero k, y así $b - a = n(-k)$, de donde $b \equiv a \pmod n$.
(iii) Se tiene que $(a - b)$ y $(b - c)$ son múltiplos de n, por lo tanto $(a - b) + (b - c) = a - c$ es múltiplo de n, es decir, $a \equiv c \pmod n$.
(iv) Notemos que $(a - b)$ y $(c - d)$ son múltiplos de n, por lo tanto, $(a - b) + (c - d) = (a + c) - (b + d)$ es múltiplo de n, y así $a + c \equiv b + d \pmod n$.
(v) Notemos que $(a - b)c + (c - d)b = ac - bc + bc - bd = ac - bd$, de donde $(a - b)$ y $(c - d)$ son múltiplos de n, por lo tanto $ac \equiv bd \pmod n$.
■

A pesar que dichas propiedades puedan parecer obvias o intuitivas, presentan una idea básica de como operar dentro de las clases de congruencias.

Ejemplo 1.9. *Encuentra el residuo módulo 5 del número $37^8 - 49 \times 803 + 975$.*

Notemos que $37 - 2 = 35 = 5 \times 7$, de donde $37 \equiv 2 \pmod 5$. Por el numeral (i) y (5), se observa que $37^2 \equiv 2^2 \equiv 4 \pmod 5$, como consecuencia $37^4 \equiv 4 \times 4 \equiv 16 \equiv 1 \pmod 5$, luego $37^8 \equiv 1^2 \equiv 1 \pmod 5$. Como 975 es múltiplo de 5, entonces es congruente a 0 módulo 5, y además $49 \equiv 4 \pmod 5$ y $803 \equiv 3 \pmod 5$, por lo tanto, al usar el numeral $(iii), (iv)$ y (v) de la proposición anterior, se concluye que

$$37^8 - 49 \times 803 + 975 \equiv 1 - 4 \times 3 + 0 \equiv 1 - 12 \equiv 1 - 2 \equiv -1 \pmod 5$$

En ciertos casos resulta útil trabajar con residuos negativos, sin embargo, en este problema particular buscamos que sea positivo y basta con notar que $-1 - 4 = -5$, luego $-1 \equiv 4 \pmod 5$ es el residuo del número con el que empezamos.

Principio de Sustitución: *Para sumar y multiplicar en una congruencia, cualquier número puede sustituirse por otro a la que éste sea congruente sin alterar la validez de la congruencia.*

Este Principio es lo que hace a las congruencias especialmente útiles, pues basta con reducir los enteros a los residuos y operar con ellos para sacar conclusiones de algún problema dado.

Nota 1.10. *El Principio de sustitución aplica únicamente para los operadores de suma (o resta) y multiplicación (pero no división). Ejemplos como los exponentes fallan, pues $8 \equiv 3 \pmod 5$, pero $8^2 \equiv 1 \pmod 5$ mientras que $3^2 \equiv 4 \pmod 5$.*

Proposición 1.11. *Para a y b enteros, y n natural, se cumplen las siguientes afirmaciones:*
(i) Si d es un divisor de n, y $a \equiv b \pmod{n}$, entonces $a \equiv b \pmod{d}$.
(ii) Si n_1 y n_2 son naturales tales que n es su mínimo común múltiplo, y se dan las congruencias $a \equiv b \pmod{n_1}$ y $a \equiv b \pmod{n_2}$, entonces $a \equiv b \pmod{n}$.

Demostración de Proposición 1.11 : (i) De la congruencia, sabemos que $n \mid a - b$, pero si $d \min n$, entonces $d \mid a - b$, es decir, $a \equiv b \pmod{d}$.
(ii) Nuevamente, de las congruencias se sigue que $a - b$ es múltiplo de n_1 y de n_2, por lo tanto, debe ser múltiplo de su mínimo común múltiplo n, y $n \mid a - b$, es decir, $a \equiv b \pmod{n}$.
■

A partir de esta Proposición, se tiene el siguiente resultado que junto a 1.11 son de gran utilidad en resolución de problemas relacionados con congruencias.

Teorema 1.12. *Sea $n = p_1^{k_1} p_2^{k_2} ... p_m^{k_m}$ la descomposición de n de potencias de primos distintos. Entonces la congruencia $a \equiv b \pmod{n}$ es equivalente a las congruencias*

$$\begin{aligned} a &\equiv b \pmod{p_1^{k_1}} \\ a &\equiv b \pmod{p_2^{k_2}} \\ &\vdots \\ a &\equiv b \pmod{p_m^{k_m}} \end{aligned}$$

Demostración de Teorema 1.12 : Supongamos que $a \equiv b \pmod{n}$. En este caso, cada $p_i^{k_i}$ con $i = 1, ..., m$, es divisor de n, por lo que del numeral (i) de la Proposición 1.11 se concluye que $a \equiv b \pmod{p_i^{k_i}}$ para cualquier $1 \leq i \leq m$.

En caso contrario, si a y b satisfacen el sistema de congruencias, entonces por el numeral (ii) de la Proposición 1.11, se tiene que como $\text{mcm}(p_1^{k_1}, p_2^{k_2}, ..., p_m^{k_m}) = n$, entonces $a \equiv b \pmod{n}$ de donde se concluye el resultado.
■

Ejemplo 1.13. *Veamos que la ecuación $x^2 - 7 = 45y$ no tiene soluciones (x, y) enteras. Si hubiese una solución, entonces se debe cumplir que $x^2 - 7 \equiv 0 \pmod{45}$, o equivalentemente $x^2 \equiv 7 \pmod{45}$. Puesto que $45 = 5 \times 3^2$, entonces por el Teorema 1.12, basta con verificar que $x^2 \equiv 7 \pmod{5}$ y $x^2 \equiv 7 \pmod{9}$. Por el Principio de sustitución, basta con verificar los casos para $x = 0, 1, 2, 3, 4$ en el caso de la congruencia con 5, pues los demás casos son equivalentes y así observamos que*

x	x^2	$\pmod 5$
0	0	0
1	1	1
2	4	4
3	9	4
4	16	1

Por lo tanto, puesto que $7 \equiv 2 \pmod{5}$, podemos observar que x^2 nunca es congruente a 2 módulo 5, por lo que no existen soluciones a la ecuación $x^2 - 7 = 45y$.

Proposición 1.14. *Sea n un natural.*
(i) Si a es un entero primo relativo con n (esto es, $\mathrm{mcd}(a,n)=1$), entonces existe un entero b tal que $ab \equiv 1 \pmod{n}$. (Cuando esto ocurre, diremos que a es invertible y b es el inverso de a módulo n.)
(ii) El recíproco también se cumple, es decir, si $ab \equiv 1 \pmod{n}$, entonces a y n son primos relativos.

Demostración de Proposición 1.14 : (i) Si a y n son primos relativos, entonces existen enteros x y y tales que $ax+ny=1$, bajo congruencias esto es equivalente a

$$1 \equiv ax+ny \equiv ax+0 \equiv ax \pmod{n}.$$

De esta forma, al tomar un entero que cumpla que $b \equiv x \pmod{n}$, cumple lo que queríamos demostrar.
(ii) De la congruencia dada, se tiene que $n \mid ab-1$, es decir, existe un entero m tal que $nm=ab-1$, o equivalentemente, $1=ab+n(-m)$, es decir, se obtiene una combinación lineal de a y n que da 1, lo cual implica que a y n son primos relativos.
■

Ejemplo 1.15. *Veamos que si $\mathrm{mcd}(a,n)=d>1$, entonces existe un entero k con $k \not\equiv 0 \pmod{n}$ tal que $ak \equiv 0 \pmod{n}$.*

Si $\mathrm{mcd}(a,n)=d$, entonces $a=da'$ y $n=dn'$ para ciertos enteros a' y n'. De este modo, notemos que $an'=da'n'=na'$, es decir, $an'-0=na'$ y $an' \equiv 0 \pmod{n}$, y en particular $n' \not\equiv 0 \pmod{n}$, pues $0<n'<n$, entonces basta con tomar a $k=n'$.

Proposición 1.16. *Si $d=\mathrm{mcd}(a,n)$ y $ax \equiv c \pmod{n}$:*
(i) Existe una solución x si $d \mid c$ y además como $a=da'$, $c=dc'$ y $n=dn'$, entonces la congruencia anterior se puede reescribir como $a'x \equiv c' \pmod{n'}$.
(ii) Si $d \nmid c$, entonces no existe una solución x para dicha congruencia.

Demostración de Proposición 1.16 : (i) Notemos que $ax-c=d(a'x-c')$ y por la congruencia dada, se sigue que n divide a $a'x-c'$ si y sólo si $n' \mid a'x-c'$, por lo tanto, la congruencia es equivalente a $a'x \equiv c' \pmod{n'}$ y así mismo, como $\mathrm{mcd}(a',n')=1$, entonces por la Proposición 1.14 sabemos que existe una solución para x.
(ii) Procediendo por contradicción, supongamos que existe x_1 que satisface $ax_1 \equiv c \pmod{n}$. Como consecuencia, se tiene que $n \mid ax_1-c$ y así existe m entero tal que $ax_1-c=mn$, sin embargo, puesto que d divide a a y a n, entonces debe dividir a c, lo cuál contradice que $d \nmid c$ y la congruencia no tiene solución para x.
■

Ejemplo 1.17. *Encuentra todos los enteros x tales que $4x+20 \equiv 27x-1 \pmod{5}$. Por el Principio de Sustitución, podemos reducir la congruencia a $4x \equiv 2x-1 \pmod{5}$, más aún, se sigue que $2x \equiv -1 \pmod{5}$. Se observa que $\mathrm{mcd}(2,5)$, por lo tanto, existe el inverso de 2 en módulo 5, y trás prueba y error se verifica que $2 \times 3 \equiv 1 \pmod{5}$. De esta manera, al mutiplicar por 3 en la congruencia, se sigue que $x \equiv -3 \pmod{5}$ o equivalentemente, $x \equiv 2 \pmod{5}$ y en general las soluciones están dadas por $x=5k+2$ para k entero.*

Teorema 1.18. ***(Teorema Chino del Residuo.)*** *Para k entero positivo, si $n_1, n_2, ..., n_k$ son k naturales primos relativos por parejas (esto es, para cada pareja (i,j) con $i \neq j$ se cumple que $\mathrm{mcd}(n_i,n_j)=1$ para*

$1 \leq i, j \leq k$). *Si* $b_1, b_2, ..., b_k$ *son enteros, entonces el sistema*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

tiene solución y es única respecto al módulo $N = n_1 n_2 ... n_k$, *es decir, existe al menos una solución y para dos soluciones* x_1, x_2 *se satisface que* $x_1 \equiv x_2 \pmod{N}$.

Demostración de Teorema 1.18 : Definamos a $a_i = \frac{N}{n_i}$ para cada $1 \leq i \leq k$. Tenemos que a_i es entero, por definición de N y además $\text{mcd}(a_i, n_i) = 1$, entonces por la Proposición 1.14 se sigue que cada a_i tiene un inverso, digamos c_i, en el módulo n_i para cada $1 \leq i \leq k$. Definamos al entero x_0 como

$$x_0 = a_1 b_1 c_1 + a_2 b_2 c_2 + ... + a_k b_k c_k,$$

y veamos que es solución del sistema de congruencias. Por definición de a_i, se tiene que $n_j \mid a_i$ para j distinto de i y como consecuencia, $a_i b_i c_i \equiv 0 \pmod{n_j}$ para cualquier $1 \leq j \leq k$ excepto para $j = i$, luego, $x_0 \equiv a_i b_i c_i \pmod{n_i}$, sin embargo, como c_i es inverso de a_i en módulo n_i, entonces $x_0 \equiv b_i \pmod{n_i}$ y en efecto x_0 es solución del sistema.

Por la Proposición 1.11, se tiene que si x_1 también es solución del sistema, entonces como $N = \text{mcm}(n_1, n_2, ..., n_k)$, se sigue que como $x_0 \equiv x_1 \equiv b_i \pmod{n_i}$ para $1 \leq i \leq k$, entonces $x_0 \equiv x_1 \pmod{N}$. Recíprocamente, por la misma proposición se puede notar que cualquier entero de la forma $x_0 + Nm$ para m entero será solución del sistema.
■

A pesar de que parezca enredado, el Teorema Chino del Residuo es de gran utilidad para garantizar la unicidad de nuestras soluciones e inclusive la demostración muestra una forma explícita de como calcular una de las soluciones y por tanto todas las demás. También es importante observar que el recíproco del Teorema no necesariamente es cierto, es decir, no necesariamente debe de ocurrir que los módulos sean primos relativos entre sí para que exista una solución, sin embargo, cuando sucede siempre se garantiza la existencia de dicha solución.

Ejemplo 1.19. *Resuelve el siguiente sistema de congruencias*

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 0 \pmod{9} \\ x &\equiv 4 \pmod{10}. \end{aligned}$$

Notemos que $7, 9$ *y* 10 *no comparten factores, y por tanto son primos relativos entre sí, entonces por el Teorema Chino del Residuo existe una solución. Veamos que una forma de calcular la solución es analoga a la demostración, entonces tomemos a* $a_1 = 90$, $a_2 = 70$ *y* $a_3 = 63$, *de donde sus inversos son* $c_1 = 6$, $c_2 = 4$ *y* $c_3 = 7$ *en los módulos* $7, 9$ *y* 10, *respectivamente, por lo tanto una solución está dada por*

$$\begin{aligned} x_0 &= a_1 b_1 c_1 + a_2 b_2 c_2 + a_3 b_3 c_3 \\ &= 90 \cdot 2 \cdot 6 + 70 \cdot 0 \cdot 4 + 63 \cdot 4 \cdot 7 = 2844. \end{aligned}$$

De esta forma, todos los enteros de la forma $x_0 + 630m$ *son las únicas soluciones del sistema.*

Una manera que en ciertas situaciones resulta más práctica, es considerando al entero $y_n = 10n + 4$ *para* n *natural. La motivación de tomar a dicho número viene del hecho de la tercera congruencia, pues dicho módulo es el mayor, y la estrategia es considerar distintos valores de* n *hasta encontrar algún* y_n *que cumpla con las congruencias del sistema, de las cuales sabemos que en algún momento debemos de encontrar dicho valor de* n *por el Teorema Chino del Residuo, así vemos que al intentar distintos valores de* n*,*

$$\begin{aligned} y_1 &= 14, \quad y_2 = 24 \\ y_3 &= 34, \quad y_4 = 44 \\ y_5 &= 54. \end{aligned}$$

En particular, y_4 *es múltiplo de* 9 *y cumple con dos de las congruencias pero no con la primera, entonces ahora tomamos a* $z_n = 54 + 90n$ *y haciendo el mismo procedimiento se observa*

$$z_1 = 144, \quad z_2 = 234, \quad z_3 = 324.$$

De donde se sigue que $z_3 = 7(46) + 2$*, por lo tanto* 324 *satisface el sistema de congruencias y además se comprueba que* $324 \equiv 2844 \pmod{630}$*, pues* $324 + 4(630) = 2844$*.*

Ejemplo 1.20. *Probar que para cualquier entero positivo* n*, existen* n *números consecutivos tal que cada número es divisible entre el cuadrado de un entero mayor a* 1*.*

Consideremos a n *números primos distintos* $p_1, p_2, ..., p_n$*, y puesto que se buscan enteros consecutivos, consideremos al sistema de congruencias*

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2} \\ x &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -n \pmod{p_n^2}. \end{aligned}$$

Puesto que son primos, entonces sus cuadrados son primos relativos entre sí y por el Teorema Chino del Residuo, existe una solución del sistema, digamos x_0*, y dicho entero satisface que* $p_1^2 \mid x_0 + 1$*,* $p_2^2 \mid x_0 + 2$*,...,* $p_n^2 \mid x_0 + n$*, que es lo se quería demostrar.*

Teorema 1.21. ***(Teorema de Wilson.)*** *Si* p *es un primo, entonces* $(p-1)! \equiv -1 \pmod{p}$*.*

Demostración de Teorema 1.21 : Por ser un número primo, cualquier entero no múltiplo de p tiene inverso multiplicativo módulo p. Para el producto $(p-1)!$, cada que un factor se junte con su inverso, entonces ambos se cancelan, sin embargo, puede ocurrir el caso en el que un factor x sea su mismo inverso, es decir cuando $x^2 \equiv 1 \pmod{p}$.

Esto último implica que $(x+1)(x-1) \equiv 0 \pmod{p}$ lo cual es equivalente a que $p \mid (x+1)$ o $p \mid (x-1)$, pues p es primo. Por lo tanto, $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$ y el 1 y -1 son los únicos residuos del producto $(p-1)!$ que no se pueden cancelar, y así $(p-1)! \equiv -1 \pmod{p}$.
■

2 Ejericios

La siguiente lista de ejercicios no siguen ningún orden de dificultad en particular, por lo que se recomienda intentarlos todos.

Ejercicio 2.1. *Demuestra el criterio de divisibilidad del* 3 *usando congruencias.*

Ejercicio 2.2. *Demuestra que para cualquier colección de* 7 *números enteros siempre se pueden escoger a* 2 *de ellos cuya suma o resta es divisible entre* 11*.*

Ejercicio 2.3. *Demuestra que si un triángulo rectángulo tiene lados* a, b *y* c *y además son enteros, entonces el producto* abc *es múltiplo de* 30*.*

Ejercicio 2.4. *Sea* $p > 3$ *un número primo. Encuentra* $\text{mcd}((p-1)! + 1, p!)$*.*

Ejercicio 2.5. *Para* n *y* m *enteros, prueba que* $2n + 3m$ *es divisible entre* 17 *si y sólo si* $9n + 5m$ *también lo es.*

Ejercicio 2.6. *Demuestra que para* p *primo y* a, b *enteros, entonces* $(a+b)^p \equiv a^p + b^p \pmod{p}$*.*

Ejercicio 2.7. *La sucesión de Fibonacci* $F_1, F_2, F_3, ...$ *se define como sigue: los dos primeros términos son* 1*, es decir* $F_1 = F_2 = 1$*, y para* $n \geq 3$ *se toma a* $F_n = F_{n-1} + F_{n-2}$*. Demuestra que hay infinitos términos de la sucesión de Fibonacci que son múltiplos de* 9*.*

Ejercicio 2.8. *Encuentra todas las tercias de números naturales en progresión aritmética de diferencia* 2 *tales que la suma de sus cuadrados sea un número de cuatro cifras iguales.*

Ejercicio 2.9. *Encuentra el residuo de* $16^{15} - 8^{15} - 4^{15} - 2^{15} - 1^{15}$ *módulo* 96*.*

Ejercicio 2.10. *Determina todos los enteros* $a, b, c, d \geq 0$ *que satisfacen* $4^a + 5^b + 6^c = 7^d$*.*

Ejercicio 2.11. *Demuestra que para cualquier entero* n*, la fracción*

$$\frac{n^2 + n - 1}{n^2 + 2n}$$

es irreducible (en otras palabras, el numerador y denominador son primos relativos.)

Ejercicio 2.12. *Para cualquier entero* n *demuestra que* $22k + 7$ *y* $33k + 5$ *son primos relativos.*

Ejercicio 2.13. *Encuentra todos los enteros* x *tales que* $5x^3 - 2x^2 + 1 \equiv 0 \pmod{6}$*.*

Ejercicio 2.14. *Usando congruencias, demuestra que para n y m enteros, $(n-1)^2 \mid n^m - 1$ si y sólo si $n-1 \mid k$.*

Ejercicio 2.15. *Calcula el residuo de 333^{333} módulo 33.*

Ejercicio 2.16. *¿Para cuántas parejas de números enteros a y b entre 0 y 1993 se satisface que a^2-ab-1 es múltiplo de 1994?*

Ejercicio 2.17. *Sean a y b enteros tales que $a+5b$ y $5a-b$ son ambos divisibles entre 2002. Demuestra que a^2+b^2 es múltiplo de 2002.*

Ejercicio 2.18. *Sean n natural y a entero, demuestra que si $a^t \equiv 1 \pmod{n}$ para algún entero $t \geq 1$, entonces $\text{mcd}(a,n) = 1$.*

Ejercicio 2.19. *Encuentra todos los números de 4 cifras que no tengan ceros y que al elevarlos al cuadrado terminen en las mismas 4 cifras (en el mismo orden).*

Ejercicio 2.20. *(Regional Noroeste 2019) José y María juegan el siguiente juego: María escribe 2019 enteros positivos distintos en el pizarrón. José borra algunos de ellos (posiblemente ninguno, pero no todos) y escribe a la izquierda de cada uno de los números restantes un signo $+$ o un signo $-$. Después se calcula la suma escrita en el pizarrón. Si el resultado es múltiplo de 2019, José gana el juego; si no, gana María. Determina cuál de los dos tiene una estrategia ganadora.*

Ejercicio 2.21. *Sean x y y enteros positivos impares tales que $xy^2+x = 2x^{2018}+y^2+3$. Encuentra todos los posibles valores de $\frac{y}{x}$.*

Ejercicio 2.22. *Demuestra que para cualquier natural n, el número $2(n^2+1)-n$ no es un cuadrado perfecto.*

Ejercicio 2.23. *¿Para qué enteros positivos a, b y c se satisface que $1+2^a+3^b = 6^c$?*

Ejercicio 2.24. *Sean m y n enteros positivos. Demuestra que si el último dígito de m^2+mn+n^2 es cero, entonces sus últimos dos dígitos son ceros.*

Ejercicio 2.25. *Demuestra que en la sucesión de números $11, 111, 1111, ...$ no existe ningún número que sea la quinta potencia de un entero (es decir, no existe un entero n tal que $n^5 = 11...11$ para cierta cantidad de $1's$).*

Ejercicio 2.26. *(OMM 1997) Encuentra todos los primos positivos p tales que $8p^4-3003$ también sea un número primo.*

Ejercicio 2.27. *Encuentra todos los enteros positivos n y m tales que $n!+8 = 2^m$.*

Ejercicio 2.28. *Determina todos los primos distintos p, q, r y s tales que $p+q+r+s$ es un número primo y los números p^2+qs y p^2+qr son ambos cuadrados perfectos.*

Ejercicio 2.29. *Sea n un entero positivo mayor a 1. Encuentra el mínimo valor de n para el cual se tiene que el promedio de los números $1^2, 2^2, 3^2, ..., n^2$ es un cuadrado perfecto.*

Ejercicio 2.30. *Demuestra que no existen enteros p, q y k, con p y q primos, tales que $p-q=2$ y $pq+10^k$ sea un número primo.*