FAMAF

Álgebra I

Período | 2022-II

Práctico 7

Ej. 1 Sea $n \in \mathbb{N} \uplus \{0\}$. Verificar las siguientes congruencias, aclarando las propiedades que usa en cada paso:

(a) $4! \equiv 4 \pmod 5$
(b) $36^5 \equiv -1 \pmod{37}$
(c) $57^{n+1} - 1 \equiv 2 \pmod 3$
(d) $6^n + 8 \equiv 4 \pmod 5$.
(e) $3^{2n} \equiv 7^{2n} \pmod 8$
(f) $3^{n+1} \equiv 3 \pmod 6$

Ej. 2 Calcular el resto de la división de a por b para los siguientes pares de números, sin realizar la división:

(a) $a = 1599$, $b = 39$
(b) $a = 914$, $b = 31$
(c) $a = 1010$, $b = 11$

Ej. 3 Para cada uno de los siguientes pares de números, encontrar los menores exponentes i y j en $\mathbb{N}$, con $i < j$, tales que $a^i \equiv a^j \pmod n$:

(a) $a = 3$, $n = 5$
(b) $a = 6$, $n = 10$
(c) $a = 11$, $n = 16$
(d) $a = 10$, $n = 12$

Ej. 4 Hallar la cifra de las unidades y la de las decenas del número 7^{15}.

Ej. 5 Demostrar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11 y usarlas para determinar por cuáles de los anteriores números son divisibles los números 12342, 5176, 314573 y 899.

Ej. 6 Hallar el resto en la división de x por n sin realizar la división en los siguientes casos para:

(a) $x = 5^2 + 7^4 + 11^6 + 13^8 + 17^{10} + 19^{12} + 23^{14}$ y $n = 24$
(b) $x = 1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8$ y $n = 5$
(c) $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$ y $n = 7$
(d) $x = \sum_{k=1}^{100} k!$ y $n = 18$

Ej. 7 Sean n y m en los enteros, $n > 0$. Probar:

(a) Todo número de la forma $4^n - 1$ es divisible por 3.
(b) El número $2^n + 1$ es divisible por 3 si y solo si n es un número impar.
(c) El resto de dividir m^2 por 3 es 1 si y solo si m no es múltiplo de 3.
(d) El resto de dividir m^2 por 4 es igual a 0 si m es par y 1 si m es impar.
(e) El resto de dividir m^2 por 8 es 1 si y solo si m es impar.
(f) El número $m^2 + 4m + 6$ no es múltiplo de 5

Ej. 8 Sean a, b, c números enteros, ninguno divisible por 3. Probar que $a^2 + b^2 + c^2$ es divisible por 3.

Ej. 9 Probar que si las longitudes de los lados de un triángulo rectángulo son números enteros, entonces las longitudes de los catetos no pueden ser ambas impares.
[Hint: Teorema de Pitágoras y Ejercicio 7 - inciso (d)]

Ej. 10 Verificar que la cifra de las unidades en la expansión decimal de todo número cuadrado es $0, 1, 4, 5, 6$ o 9 y en consecuencia, explicar porqué ningún número terminado en 2, 3, 7 u 8 (escrito en base 10) puede tener raíz cuadrada exacta.

Congruencias

Ej. 11 Sean m, n números enteros. Probar que $m^2 + n^2$ es múltiplo de 7 si y sólo si m y n son múltiplos de 7.

Ej. 12 Resolver las siguientes ecuaciones lineales de congruencia:

(a) $233x \equiv 0 \pmod{377}$ (b) $13x \equiv 3 \pmod{21}$ (c) $6x \equiv 4 \pmod{10}$ (d) $50x \equiv 1 \pmod{29}$

Ej. 13 Hallar todos los números enteros a tales que $\mathrm{mcd}(2a+1, 3a-2) \neq 1$.

Ej. 14 Dado $u \in \mathbb{Z}$, decimos que u es *inversible módulo* n si existe $v \in \mathbb{Z}$ tal que $u \cdot v \equiv 1 \pmod{n}$, y en este caso decimos que v es **un** inverso de u módulo n.

(a) Probar que u es inversible módulo n si y sólo si $\mathrm{mcd}(u, n) = 1$.

(b) Probar que los inversos son únicos módulo n; es decir, si v y w son inversos de u módulo n, entonces $v \equiv w \pmod{n}$.

Ej. 15 (Opcional) Sean a, b, m, n, r y s números enteros, con m, n, r, s positivos y $r \leq s$. Demostrar:

(a) El sistema de ecuaciones lineales de congruencia

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

tiene solución si y solo si $a \equiv b \pmod{d}$ con $d = \mathrm{mcd}(m, n)$.

(b) Si el sistema de ecuaciones lineales de congruencia

$$\begin{cases} x \equiv a \pmod{n^r} \\ x \equiv b \pmod{n^s} \end{cases}$$

tiene solución, entonces sus soluciones son las mismas de $x \equiv b \pmod{n^s}$.

Ej. 16 Sea $r \in \mathbb{N}$. Hallar todos los $x \in \mathbb{Z}$ que satisfacen los siguientes sistemas de congruencias:

(a) $\begin{cases} x \equiv 5 \pmod{2} \\ x \equiv 3 \pmod{2^r} \end{cases}$ (b) $\begin{cases} x \equiv 5 \pmod{3} \\ x \equiv 2 \pmod{6} \\ x \equiv -1 \pmod{15} \end{cases}$ (c) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$ (d) $\begin{cases} 3x \equiv 1 \pmod{2} \\ 2x \equiv 1 \pmod{3} \\ 3x \equiv 1 \pmod{4} \\ 2x \equiv 1 \pmod{5}. \end{cases}$

Ej. 17 En un grupo de 20 amigos se reparten alfajores entre todos y sobran 7 alfajores. Tres amigos se van, devuelven su parte y se vuelve a repartir el total de alfajores entre los amigos que quedan. Sobran 5 alfajores. ¿Cuántos alfajores, como mínimo, había para repartir?

Ej. 18 La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogida es tal que contando de a 3 sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz dijo que eso era imposible. ¿Quién tiene razón? Justificar.

Ej. 19 Hallar el resto de la división de a por el primo p en los siguientes casos:

(a) $a = (-13)^{2022}$, $p = 3$;
(b) $a = 12^{2023}$, $p = 5$;
(c) $a = 3^{2023}$, $p = 1013$
(d) $a = 5^{2022}$, $p = 1013$
(e) $a = 2^{2022} + 4^{2022}$, $p = 5$
(f) $a = 2^{2023} + 3^{2023} - 7^{2023}$, $p = 11$

Ej. 20 Sea p un primo distinto de 2 y de 5. Probar que existe un número de la forma $99\ldots99$ que es múltiplo de p.

Ej. 21 Hallar todos los primos positivos p tales que $p \mid 2^p + 5$.

Ej. 22 (Opcional) Sean p y q primos positivos distintos. Verificar que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$
[Hint: Una forma de encarar el ejercicio es resolver $p^{q-1} + q^{p-1} \equiv x \pmod{pq}$.]

Ej. 23 (Opcional) Probar que para todo primo $p > 3$ se cumple que $p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.
[Hint: Una manera de abordar al ejercicio es pensar a 2^{p-2}, 3^{p-2} y 6^{p-2} como los *inversos módulo p* de 2, 3 y 6 respectivamente.]

Ej. 24 (Opcional) Encontrar todos los números primos positivos tales que $p^2 \mid \text{mcd}(25^p + 26, (10!)^{p-1} + 54)$

Ej. 25 (Opcional) Sean p y q primos positivos. Probar que si q divide a $2^p - 1$, entonces $q \equiv 1 (\text{mod } p)$.
[Ayuda: Probar primero que q divide a $\text{mcd}(2^p - 1, 2^{q-1} - 1) = 2^{\text{mcd}(p,q-1)} - 1$].

Ej. 26 (Opcional) Sean a y b números enteros tales que $\text{mcd}(3a, 5b) = 6$. Hallar el resto del número $3a^{2020} + 5b^{2021} + 11^{2022}$ cuando se divide por 60.

Ej. 27 Probar la recíproca del teorema de Wilson: si $p > 1$ satisface $(p-1)! \equiv -1 \,(\text{mod } p)$ entonces p es primo.

Ej. 28 (Opcional) Sea p un número primo impar. Probar que

1. $((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.
2. La ecuación $x^2 \equiv -1 \pmod{p}$ tiene solución si y sólo si p es un primo de la forma $4k + 1$.
   [Hint: Una forma es usando el pequeño teorema de Fermat].
3. Usar el inciso anterior para dar una prueba alternativa al Ejercicio 11 de este práctico:

   "Si a y b son enteros entonces $a^2 + b^2$ es divisible por 7 si y sólo si a y b son divisibles por 7."

   Puede plantear una generalización a dicho ejercicio y probarla?

Ej. 29 Para resolver los siguientes ejercicios, es obligatorio usar el teorema de Euler:

(a) Encontrar el dígito de las unidades de 3^{2022} de su expansión decimal.
(b) Determinar el resto de 2^{2022} cuando se divide por 105.
(c) Determinar los enteros que satisfacen la ecuación $19x \equiv 5 \pmod{24}$

Ej. 30 (Opcional) Resolver las siguientes ecuaciones:

(a) $x^2 + 4x + 6 \equiv 0 \pmod{5}$
(b) $x^3 + x + 2 \equiv 0 \pmod{5}$
(c) $x^3 + x + 2 \equiv 0 \pmod{7}$
(d) $x^3 + x + 2 \equiv 0 \pmod{35}$

Ej. 31 (Opcional) Mostrar que las siguientes ecuaciones no tienen soluciones en los números enteros:

(a) $a^2 + 10b^2 = 2$
(b) $a^2 - 10b^2 = 3$
(c) $7x^4 + 2y^3 = 3$
(d) $2x^3 + 27y^4 = 21$
(e) $7x^5 + 3y^4 = 2$
(f) $15x^2 - 7y^2 = 1$

Ej. 32 (Opcional) Hallar todos los enteros positivos a tales que $\text{mcd}(4a^{62} - a, 11a) \neq a$.

Versión para imprimir

1. Sea $n \in \mathbb{N} \uplus \{0\}$. Verificar las siguientes congruencias, aclarando las propiedades que usa en cada paso:

   (a) $4! \equiv 4 \pmod 5$
   (b) $36^5 \equiv -1 \pmod{37}$
   (c) $57^{n+1} - 1 \equiv 2 \pmod 3$
   (d) $6^n + 8 \equiv 4 \pmod 5$.
   (e) $3^{2n} \equiv 7^{2n} \pmod 8$
   (f) $3^{n+1} \equiv 3 \pmod 6$

2. Calcular el resto de la división de a por b para los siguientes pares de números, sin realizar la división:

   (a) $a = 1599$, $b = 39$
   (b) $a = 914$, $b = 31$
   (c) $a = 1010$, $b = 11$

3. Para cada uno de los siguientes pares de números, encontrar los menores exponentes i y j en $\mathbb{N}$, con $i < j$, tales que $a^i \equiv a^j \pmod n$:

   (a) $a = 3$, $n = 5$
   (b) $a = 6$, $n = 10$
   (c) $a = 11$, $n = 16$
   (d) $a = 10$, $n = 12$

4. Hallar la cifra de las unidades y la de las decenas del número 7^{15}.

5. Demostrar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11 y usarlas para determinar por cuáles de los anteriores números son divisibles los números 12342, 5176, 314573 y 899.

6. Hallar el resto en la división de x por n sin realizar la división en los siguientes casos para:

   (a) $x = 5^2 + 7^4 + 11^6 + 13^8 + 17^{10} + 19^{12} + 23^{14}$ y $n = 24$
   (b) $x = 1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8$ y $n = 5$
   (c) $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$ y $n = 7$
   (d) $x = \sum_{k=1}^{100} k!$ y $n = 18$

7. Sean n y m en los enteros, $n > 0$. Probar:

   (a) Todo número de la forma $4^n - 1$ es divisible por 3.
   (b) El número $2^n + 1$ es divisible por 3 si y solo si n es un número impar.
   (c) El resto de dividir m^2 por 3 es 1 si y solo si m no es múltiplo de 3.
   (d) El resto de dividir m^2 por 4 es igual a 0 si m es par y 1 si m es impar.
   (e) El resto de dividir m^2 por 8 es 1 si y solo si m es impar.
   (f) El número $m^2 + 4m + 6$ no es múltiplo de 5

8. Sean a, b, c números enteros, ninguno divisible por 3. Probar que $a^2 + b^2 + c^2$ es divisible por 3.

9. Probar que si las longitudes de los lados de un triángulo rectángulo son números enteros, entonces las longitudes de los catetos no pueden ser ambas impares.
   [Hint: Teorema de Pitágoras y Ejercicio 7 - inciso (d)]

10. Verificar que la cifra de las unidades en la expansión decimal de todo número cuadrado es $0, 1, 4, 5, 6$ o 9 y en consecuencia, explicar porqué ningún número terminado en 2, 3, 7 u 8 (escrito en base 10) puede tener raíz cuadrada exacta.

11. Sean m, n números enteros. Probar que $m^2 + n^2$ es múltiplo de 7 si y sólo si m y n son múltiplos de 7.

12. Resolver las siguientes ecuaciones lineales de congruencia:

    (a) $233x \equiv 0 \pmod{377}$
    (b) $13x \equiv 3 \pmod{21}$
    (c) $6x \equiv 4 \pmod{10}$
    (d) $50x \equiv 1 \pmod{29}$

13. Hallar todos los números enteros a tales que $\operatorname{mcd}(2a + 1, 3a - 2) \neq 1$.

14. Dado $u \in \mathbb{Z}$, decimos que u es *inversible módulo* n si existe $v \in \mathbb{Z}$ tal que $u \cdot v \equiv 1 \pmod n$, y en este caso decimos que v es **un** inverso de u módulo n.

    (a) Probar que u es inversible módulo n si y sólo si $\operatorname{mcd}(u, n) = 1$.
    (b) Probar que los inversos son únicos módulo n; es decir, si v y w son inversos de u módulo n, entonces $v \equiv w \pmod n$.

15. (Opcional) Sean a, b, m, n, r y s números enteros, con m, n, r, s positivos y $r \leq s$. Demostrar:

    (a) El sistema de ecuaciones lineales de congruencia

    $$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

    tiene solución si y solo si $a \equiv b \pmod d$ con $d = \operatorname{mcd}(m, n)$.

    (b) Si el sistema de ecuaciones lineales de congruencia

    $$\begin{cases} x \equiv a \pmod{n^r} \\ x \equiv b \pmod{n^s} \end{cases}$$

    tiene solución, entonces sus soluciones son las mismas de $x \equiv b \pmod{n^s}$.

16. Sea $r \in \mathbb{N}$. Hallar todos los $x \in \mathbb{Z}$ que satisfacen los siguientes sistemas de congruencias:

(a) $\begin{cases} x \equiv 5 \pmod 2 \\ x \equiv 3 \pmod{2^r} \end{cases}$ (b) $\begin{cases} x \equiv 5 \pmod 3 \\ x \equiv 2 \pmod 6 \\ x \equiv -1 \pmod{15} \end{cases}$ (c) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \end{cases}$ (d) $\begin{cases} 3x \equiv 1 \pmod 2 \\ 2x \equiv 1 \pmod 3 \\ 3x \equiv 1 \pmod 4 \\ 2x \equiv 1 \pmod 5. \end{cases}$

17. En un grupo de 20 amigos se reparten alfajores entre todos y sobran 7 alfajores. Tres amigos se van, devuelven su parte y se vuelve a repartir el total de alfajores entre los amigos que quedan. Sobran 5 alfajores. ¿Cuántos alfajores, como mínimo, había para repartir?

18. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogida es tal que contando de a 3 sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz dijo que eso era imposible. ¿Quién tiene razón? Justificar.

19. Hallar el resto de la división de a por el primo p en los siguientes casos:

    (a) $a = (-13)^{2022}$, $p = 3$;
    (b) $a = 12^{2023}$, $p = 5$;
    (c) $a = 3^{2023}$, $p = 1013$
    (d) $a = 5^{2022}$, $p = 1013$
    (e) $a = 2^{2022} + 4^{2022}$, $p = 5$
    (f) $a = 2^{2023} + 3^{2023} - 7^{2023}$, $p = 11$

20. Sea p un primo distinto de 2 y de 5. Probar que existe un número de la forma $99\dots99$ que es múltiplo de p.

21. Hallar todos los primos positivos p tales que $p \mid 2^p + 5$.

22. (Opcional) Sean p y q primos positivos distintos. Verificar que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$
    [Hint: Una forma de encarar el ejercicio es resolver $p^{q-1} + q^{p-1} \equiv x \pmod{pq}$.]

23. (Opcional) Probar que para todo primo $p > 3$ se cumple que $p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.
    [Hint: Una manera de abordar al ejercicio es pensar a 2^{p-2}, 3^{p-2} y 6^{p-2} como los *inversos módulo* p de 2, 3 y 6 respectivamente.]

24. (Opcional) Encontrar todos los números primos positivos tales que $p^2 \mid \mathrm{mcd}(25^p + 26, (10!)^{p-1} + 54)$

25. (Opcional) Sean p y q primos positivos. Probar que si q divide a $2^p - 1$, entonces $q \equiv 1 (\mathrm{mod}\ p)$.
    [Ayuda: Probar primero que q divide a $\mathrm{mcd}(2^p - 1, 2^{q-1} - 1) = 2^{\mathrm{mcd}(p,q-1)} - 1$].

26. (Opcional) Sean a y b números enteros tales que $\mathrm{mcd}(3a, 5b) = 6$. Hallar el resto del número $3a^{2020} + 5b^{2021} + 11^{2022}$ cuando se divide por 60.

27. Probar la recíproca del teorema de Wilson: si $p > 1$ satisface $(p-1)! \equiv -1 \pmod p$ entonces p es primo.

28. (Opcional) Sea p un número primo impar. Probar que

    (a) $((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$.
    (b) La ecuación $x^2 \equiv -1 \pmod p$ tiene solución si y sólo si p es un primo de la forma $4k+1$.
    [Hint: Una forma es usando el pequeño teorema de Fermat].
    (c) Usar el inciso anterior para dar una prueba alternativa al Ejercicio 11 de este práctico:

    "Si a y b son enteros entonces $a^2 + b^2$ es divisible por 7 si y sólo si a y b son divisibles por 7."

    Puede plantear una generalización a dicho ejercicio y probarla?

29. Para resolver los siguientes ejercicios, es obligatorio usar el teorema de Euler:

    (a) Encontrar el dígito de las unidades de 3^{2022} de su expansión decimal.
    (b) Determinar el resto de 2^{2022} cuando se divide por 105.
    (c) Determinar los enteros que satisfacen la ecuación $19x \equiv 5 \pmod{24}$

30. (Opcional) Resolver las siguientes ecuaciones:

    (a) $x^2 + 4x + 6 \equiv 0 \pmod 5$
    (b) $x^3 + x + 2 \equiv 0 \pmod 5$
    (c) $x^3 + x + 2 \equiv 0 \pmod 7$
    (d) $x^3 + x + 2 \equiv 0 \pmod{35}$

31. (Opcional) Mostrar que las siguientes ecuaciones no tienen soluciones en los números enteros:

    (a) $a^2 + 10b^2 = 2$
    (b) $a^2 - 10b^2 = 3$
    (c) $7x^4 + 2y^3 = 3$
    (d) $2x^3 + 27y^4 = 21$
    (e) $7x^5 + 3y^4 = 2$
    (f) $15x^2 - 7y^2 = 1$

32. (Opcional) Hallar todos los enteros positivos a tales que $\mathrm{mcd}(4a^{62} - a, 11a) \neq a$.