Problemes: Aritmètica II. Aritmètica modular.

II.1. Demostreu que, si x i y són dos elements senars de $\mathbb{Z}$, llavors $x^2 + y^2$ no és quadrat de cap enter.

II.2. Quantes solucions tenen aquestes equacions amb congruències? Doneu-ne les solucions.

(a) $26x \equiv 3 \mod 13$
(b) $13x \equiv 3 \mod 26$
(c) $26x \equiv 0 \mod 13$
(d) $9x \equiv -3 \mod 15$
(e) $5x \equiv 4 \mod 7$
(f) $5x \equiv 7 \mod 7$

II.3. Demostreu els criteris de divisibilitat per 3, per 4, per 5, per 7, per 9 i per 11.

II.4. Demostreu que, si $a \equiv b \mod m$, llavors $\mathrm{mcd}(a, m) = \mathrm{mcd}(b, m)$.

II.5. Demostreu que si $ab \equiv ac \mod m$, alesores $b \equiv c \mod \frac{m}{\mathrm{mcd}(a,m)}$.

II.6. Demostreu que si $\begin{cases} a \equiv b \mod m \\ a \equiv b \mod n \end{cases}$ aleshores $a \equiv b \mod \mathrm{mcm}(m, n)$.

II.7. Calculeu $\mathrm{mcd}(48m + 11, 42m + 8)$ en funció de m.

II.8. (a) Demostreu que si p és primer senar i $a \not\equiv 0 \mod p$, aleshores $x^2 \equiv a^2 \mod p$ té dues i només dues solucions.

(b) Demostreu amb exemples que el resultat anterior no és cert si no es compleixen totes les hipòtesis.

II.9. Teorema de Wilson

(a) Demostreu que, si p és primer, aleshores

$$(p-1)! \equiv \Pi_{x \in \{1,\ldots,p-1 : x^2 \equiv 1 \mod p\}} \mod p$$

(b) Demostreu que

$$(p-1)! \equiv -1 \mod p$$

II.10. Digueu quant ha de valdre a per tal que l'equació $ax+4 = 0$ es pugui resoldre a $\mathbb{Z}_6$. Resoleu l'equació per a cada valor possible de a.

II.11. Busqueu un element β de $\mathbb{Z}_{23}$ tal que tot altre element diferent de zero de $\mathbb{Z}_{23}$ es pot escriure com a potència de β.

II.12. Demostreu que, si p és primer, llavors $\mathrm{mcd}(p, (p-1)!) = 1$. Demostreu que, si n no és primer i $n > 4$, llavors $(n-1)! \equiv 0 \mod n$.

II.13. Demostreu que si $x^2 \equiv -1 \mod p$ té solució, aleshores, o bé $p = 2$, o bé $p \equiv 1 \mod 4$.

II.14. Demostreu que, si 7 no divideix n, llavors 7 divideix $n^{12} - 1$.

II.15. Demostreu que $n^{13} - n$ és divisible per 2, 3, 5, 7 i 13, per tot $n \in \mathbb{Z}$.

II.16. Considerem altra vegada els nombres de Fibonacci:

$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5$, etc.,

definits per la recurrència $F_i = F_{i-1} + F_{i-2}$ per $i \geq 2$.

A partir de la Identitat de Bézout de dos nombres de Fibonacci consecutius,

(a) Podem deduir qui és l'invers de F_{i-1} a $\mathbb{Z}_{F_i}$?

(b) Podem deduir quant val $F_{i-1}^2 \mod F_i$, per $i \geq 5$?

(c) Quin és l'ordre de F_{i-1} a $\mathbb{Z}_{F_i}$ per $i \geq 5$?

(d) Què podem dir de $\phi(F_i)$ per $i \geq 5$?

II.17. Qualsevol codi de barres compleix la següent propietat. Si sumem els nombres en posició senar més el triple de la suma dels nombres en posició parell, el resultat és un múltiple de deu, és a dir, és congruent amb zero mòdul 10.

Construïu una funció amb `sage` que detecti si un codi de barres conté algun error.

II.18. (a) Demostreu que donat un enter positiu x, existeix un enter positiu $n(x)$ tal que $\phi^{n(x)}(x) = 1$.

(b) Construïu una funció amb `sage` que donat x retorni $n(x)$.

II.19. (a) Demostreu que, si $d \mid n$, aleshores

$$\#\{b : 1 \leq b \leq n, \mathrm{mcd}(b, n) = d\} = \phi(n/d).$$

Construïu una funció amb `sage` que construeixi el conjunt $\{b : 1 \leq b \leq n, \mathrm{mcd}(b, n) = d\}$ i que calculi quants elements té. Comproveu el resultat que acabeu de demostrar per una varietat de nombres n.

(b) Demostreu que

$$\sum_{d \mid n} \phi(d) = n.$$

Construïu una funció amb `sage` que calculi la suma $\sum_{d \mid n} \phi(d)$. Comproveu el resultat que acabeu de demostrar per una varietat de nombres n.