Problemes d'Aritmètica. Llista 1

1. Sigui $a \geq 2$ un nombre enter, i considerem la successió recurrent determinada per

$$a_0 = a \text{ i } a_{n+1} = a_n^2 - a_n + 1.$$

Demostreu que la successió és estrictament creixent, i que $a_n \equiv 1 \pmod{a_m}$ per a tot $m < n$.

Demostreu que per a tot $n \geq 1$ hi ha algun nombre primer p_n que divideix a_n però no a_m per cap $m < n$.

2. Demostreu el teorema de Wilson: si p és un nombre primer, aleshores

$$(p-1)! \equiv -1 \pmod{p}$$

És cert el recíproc?

3. Donat un nombre enter $n \geq 2$, denotem per $(\mathbb{Z}/n\mathbb{Z})^\times$ els enters invertibles mòdul n i per

$$T(n) := (\mathbb{Z}/n\mathbb{Z})^{\times[2]} = \{a \in \mathbb{Z}/n\mathbb{Z} \mid a^2 \equiv 1 \pmod{n}\}.$$

a) Demostreu que $T(n)$ és un subgrup, i, donats a i $b \in \mathbb{Z}_{\geq 2}$, primers entre si, descriviu un isomorfisme de grups explicit $T(ab) \cong T(a) \times T(b)$.

b) Demostreu que per a tot $m \geq 2$,

$$\prod_{\substack{k=1 \\ \gcd(k,m)=1}}^{m-1} k \equiv \prod_{k \in T(m)} k \pmod{m}$$

c) Demostreu que, per a tot $r \geq 1$ i tot primer senar p, tenim que

$$T(p^r) = \{\pm 1\} \text{ i que } T(2p^r) = \{\pm 1\}.$$

d) Demostreu que, per a tot $r \geq 3$,

$$T(2^r) = \{1, 2^{r-1} - 1, 2^{r-1} + 1, 2^r - 1\}.$$

i deduïu que

$$\prod_{\substack{k=1 \\ \gcd(k,m)=1}}^{m-1} k \equiv 1 \pmod{m} \text{ si } m = 2^r \text{ amb } r \geq 3$$

e) Demostreu, usant els apartats anteriors, que

$$\prod_{\substack{k=1 \\ \gcd(k,m)=1}}^{m-1} k \equiv \begin{cases} -1 \pmod{m} & \text{si } m = 2, 4, p^r, 2p^r \\ 1 \pmod{m} & \text{en cas contrari.} \end{cases}$$

4. Demostreu que si tenim $p_1, ..., p_r$ amb $r > 2$ primers diferents, i $N = p_1 \cdots p_r$, aleshores $\sum_{i=1}^r \frac{N}{p_i}$ és un enter > 1 i que no és divisible per cap dels primers p_i per $i = 1, \cdots, r$. Deduïu d'aquí que hi ha infinits primers.

5. Demostreu que hi ha infinits nombres primers tals que:
   a) $p \equiv 3 \pmod{4}$ (Ajuda: Considereu $N = 4p_1 \cdots p_r + 3$),
   b) $p \equiv 5 \pmod{6}$ (Ajuda: Considereu $N = 6p_1 \cdots p_r + 5$),
   c) $p \equiv 1 \pmod{4}$ (Ajuda: Considereu $N = (n!)^2 + 1$).

6. Sigui $G \subsetneq (\mathbb{Z}/m\mathbb{Z})^\times$ un subgrup del grup multiplicatiu de les unitats de $\mathbb{Z}/n\mathbb{Z}$ (que tenen representants a $\mathbb{Z}$ enters primers amb m).
   a) Demostreu que si $N \in \mathbb{Z}$ és un enter amb $(N, m) = 1$ tal que $\overline{N} \notin G$, aleshores N té un factor primer amb residu que no està a G.
   b) Donat un conjunt $p_1, ..., p_r$ amb $r \geq 1$ de primers diferents que no divideixen m, i una classe residual $a \pmod m$, existeix un enter N amb $N \equiv a \pmod m$ tal que p_i no divideix N per a tot $i = 1, ..., r$.
   c) Demostreu que, donats $p_1, ..., p_r$ amb $r \geq 1$ primers diferents, hi ha algun primer q amb $\overline{q} \notin G$ i $q \neq p_i$ per a tot $i = 1, ..., r$.
   d) Deduïu que el conjunt de primers q amb $q \pmod m \notin G$ és infinit.
   e) Apliqueu-ho per veure que com a mínim dues de les successions aritmètiques

$$\{3 + 8m\}_{m\geq 1} \text{ , } \{5 + 8m\}_{m\geq 1} \text{ i } \{7 + 8m\}_{m\geq 1}$$

   contenen infinits primers.
   f) Que podeu deduïr en el cas $m = 10$?

7. Siguin $a_1, a_2, ..., a_n$ i b enters, quines condicions s'han de complir per què l'equació

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b$$

   tingui solució amb $x_1, ..., x_n$ enters? Com podem obtenir totes les solucions?

8. Contesteu les mateixes preguntes pel sistema d'equacions:

$$\begin{cases} a_{11}\ x_1 + a_{12}\ x_2 + ... + a_{1n}\ x_n = b_1 \\ a_{21}\ x_1 + a_{22}\ x_2 + ... + a_{2n}\ x_n = b_2 \\ \qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = b_m \end{cases}$$

9. a) Vegeu que si $d \geq 1$ divideix un enter n aleshores per a tot enter positiu b es té que $b^d - 1$ divideix $b^n - 1$.
   b) Vegeu que si a més n és senar, aleshores $b^d + 1$ divideix $b^n + 1$ per a tot $b > 0$.
   c) Siguin b i m naturals coprimers, i a i c dos naturals qualssevol, i definim $d = (a, c)$. Vegeu que si $b^a \equiv 1 \pmod m$ i $b^c \equiv 1 \pmod m$ aleshores $b^d \equiv 1 \pmod m$)}.

10. Demostreu que si a, b i c són enters positius, aleshores

$$\gcd\big(c^a - 1, c^b - 1\big) = c^{\gcd(a,b)} - 1.$$

11. Demostreu que no hi ha cap enter positiu $n > 1$ tal que $n \mid (2^n - 1)$. Indicació: proveu d'usar el teorema d'Euler i el problema anterior. Anàlogament, demostreu que no hi ha cap enter senar positiu $n > 1$ tals que $n \mid (3^n + 1)$.

12. Sigui $a \in \mathbb{Z}_{>1}$. Considereu el conjunt

$$S_a := \big\{n \in \mathbb{Z}_{\geq 2} : n \mid (a^n + 1)\big\}.$$

    Demostreu que
    a) si p és un primer senar i $p \mid (a + 1)$, aleshores $p^{k+1} \mid \left(a^{p^k} + 1\right)$ per a tot $k \geq 0$.
    b) si $a > 1$ és un enter senar, i considerem la successió $n_0 := 2$ i $n_{i+1} := a^{n_i} + 1$ si $i > 0$ aleshores $n_i \mid n_{i+1}$ per a tot i.
    c) el conjunt S_a té infinits elements per a tot $a > 1$.

13. Considereu el conjunt

$$S := \{n \in 2\mathbb{Z}_{\geq 1} : n \mid (n^2+2) \text{ i } (n-1) \mid (2^n+1)\}$$

Demostreu que si $n \in S$, aleshores $2^n + 2 \in S$. Deduïu que S té infinits elements.

14. Definim els nombres de Fermat com $F_n = 2^{2^n} + 1$. Tenim que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ són primers. (Fermat va conjecturar que tots ho són…)
    a) Demostreu que si $2^m + 1$ és primer, aleshores $m = 2^n$ per algun $n \in \mathbb{Z}$.
    b) Demostreu que $F_n \mid F_m - 2$ si $n < m$ i deduïu que $(F_n, F_m) = 1$ si $n \neq m$.
    c) Deduïu d'aquest últim fet que hi ha infinits primers.

15. Nombres primers de Mersenne:
    a) Demostreu que si $n > 1$ i $a^n - 1$ és primer, amb $a > 1$ enter, aleshores $a = 2$ i n és primer (aquests primers se'ls anomena primers de Mersenne)
    b) Un nombre enter s'anomena perfecte si és igual a la suma dels seus divisors. Demostreu que si $2^n - 1$ és primer, aleshores $2^{n-1}(2^n - 1)$ és perfecte. (Se sap que tot nombre perfecte parell és d'aquesta forma, i es conjectura que no ni ha de senars).
    c) Demostreu que si p és un primer senar, qualsevol divisor de $2^p - 1$ és de la forma $2kp + 1$, per algun enter positiu k.

16. En aquest exercici analitzem la descomposició en nombres primers dels nombres factorials. Donat un primer p i un enter N, direm que $v_{p(N)} = a \in \mathbb{Z}_{\geq 0}$ si $p^a \mid N$ i $p^{a+1} \nmid N$.
    a) Proveu que $v_{p(n!)} = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor$, i doneu la factorització completa de 100!.
    b) Vegeu que $v_2(n!) = n - s_2(n)$, on $s_2(n)$ és la suma dels digits de n en base 2.
    c) Descobriu una fórmula semblant per $v_{p(n!)}$ per a qualsevol primer p. (Ajuda: escriviu n en base p i utilitzeu la primera fórmula.
    d) Proveu el següent teorema de Kummer: $v_p\left(\binom{n}{m}\right)$ és el nombre de vegades que "ens n'emportem" quan sumem $n - m$ i m en base p.

17. Sigui p un primer tal que $p \mid b^n - 1$ i $p \nmid b^d - 1$ per a tot divisor no trivial d de n. Demostreu que $p \equiv 1 \pmod{n}$, i que si $p > 2$ i n és senar, aleshores que $p \equiv 1 \pmod{2n}$.

18. Sigui p un primer que divideixi $b^n + 1$. Demostreu que o bé p divideix $b^d + 1$ per algun divisor d no trivial de n tal que $\frac{n}{d}$ és senar, o bé $p \equiv 1 \pmod{2n}$. Factoritzeu $16777217 = 2^{24} + 1$.