1 Llista Exercicis Entrega Tema 1, Aritmètica, curs 2023-24

Recordem que U denota la unitat, D la desena i C la centena del vostre NIU. A cada alumne assignaré alguns exercicis per a entregar.

1. Troba totes les solucions de $X^2+Y^2=Z^2$ amb $(x,y,z)\in\mathbb{F}_q[T]^3$ on $\mathbb{F}_q[T]$ denota l'anell de polinomis en la variable T a coefficients en el cos finit $\mathbb{F}_q$ on $q=p^n$ amb p primer senar.

2. Troba totes les solucions de $X^2+Y^2=Z^2$ amb $(x,y,z)\in\mathbb{F}_{2^n}[T]^3$ on $\mathbb{F}_{2^n}[T]$ denota l'anell de polinomis en la variable T a coefficients en el cos finit $\mathbb{F}_{2^n}$, $n\geq 1$.

3. Considerem l'equació $X^2-Y^2=1$. Justifiqueu una parametrització via el sinh i cosh. Demostreu que si pensem l'equació $X^2-Y^2=1$ amb $x,y\in K$ on K és un cos amb $car(K)\neq 0$ llavors té infinites solucions i calculeu-les totes.

4. Demostreu que existeix un paràmetre t complint que $\mathbb{R}(\sinh(x),\cosh(x))=\mathbb{R}(t)$. Useu aquest t per a calcular $\int(\sinh(x)+\cosh(x))dx$.

5. Considerem l'equació $C: X^2-3*(U+1)XY+3Y^2+(D+1)*X-2Y-1=0$ (escrivim $C: f(X,Y)=0$ amb $f\in\mathbb{R}[X,Y]$). Intenta fer un canvi de variables on s'escrigui l'equació com $a(X')^2+b(Y')^2=1$ per certes constants a i b i variables X',Y'. Intenteu donar una paremetrització de la corba. Estudieu si $L:=\mathbb{R}(X)[Y]/f(X,Y)$ és un cos, i en cas de ser-ho, decidiu si existeix t on $L=\mathbb{R}(t)$. Podem fer el mateix enunciat i preguntes amb $\mathbb{Q}$ enlloc de $\mathbb{R}$?

6. En l'antiga cultura babilònica, ha arribat una taula escrita amb els costats de triangles rectangles amb longitud dels costats i diagonals nombres naturals. A la taula que ens ha arribat a dalt de tot de la llista hi havia el que el ratio x/y de $x^2+y^2=z^2$ fos més proper a 1 i es troba en aquest document a dalt de tot

   $$119^2+120^2=169^2$$

   amb 119/120 el més proper a 1 de tota la llista donada.

   Trobeu un triangle rectangle amb la longitud dels costats i diagonal nombres enters: a,c,d on $a^2+b^2=d^2$ de manera que $|(a/c)-1|<(1/(120+(10C+D+5U)))$. (Podeu usar Magma o SageMath per a calcular-la introduïnt el codi usat en la vostra resposta).

7. Considera l'equació $Y^2-\mathfrak{d}X^2=4$ amb $\mathfrak{d}>0$ natural que no és un quadrat. Demostreu que la solució general $(x,y)\in\mathbb{Z}^2$ de l'equació és de la forma:

   $$\frac{y+x\sqrt{\mathfrak{d}}}{2}=\pm(\frac{t+u\sqrt{\mathfrak{d}}}{2})^n$$

per n enter on $(u,v) \in \mathbb{N}^2$ és solució de $Y^2 - \mathfrak{d}X^2 = 4$ amb $u > 0$, $v > 0$ i en la component de la variable X minimal respecte valor arquimedià dels racionals.

8. Considera l'equació $Y^2 - pX^2 = -1$ amb p un primer congruent amb 1 modul 4. Demostreu que l'equació té infinites solucions a $\mathbb{Z}$. Indicació: considera (u,v) solució entera amb u més petita de $Y^2 - pX^2 = 1$, on $u \equiv 0, v \equiv 1 mod 2$. Escriviu $\frac{v+1}{2} \cdot \frac{v-1}{2} = p(\frac{u}{2})^2$.

9. Considera l'equació $X^4 - X^2Y^2 + Y^4 = Z^2$. Les solucions enteres de l'equació amb $mcd(x,y) = 1$ pertanyen al conjunt següent:

$$\{(1,0),(-1,0),(0,1),(0,-1),(1,1),(1,-1),(-1,1),(-1,-1)\}.$$

   Indicació: escriviu equació via $(X^2 - Y^2)^2 + X^2Y^2 = Z^2$ i useu la solució donada per a $X^2 + Y^2 = Z^2$.

10. Trobeu 3 quadrats en progressió aritmètica en els enters. Demostreu que no hi ha 4 quadrats en progressió aritmètica en els enters. Indicació: sigui x^2, y^2, z^2, w^2 aquests 4 quadrats, com $x^2 + z^2 = 2y^2$ i $2z^2 = y^2 + w^2$ obtenim $x^2w^2 = x^2(2z^2 - y^2) = w^2(2y^2 - z^2)$, i useu el problema anterior.

11. Estudieu les solucions enteres de $X^2 + 3Y^2 = p$ on n lliure de quadrats i p un primer fix.

12. Estudieu les solucions enteres de $X^2 - 3Y^2 = 2p$ on n lliure de quadrats i p un primer fix.

13. Estudieu les solucions enteres de $X^2 - 5Y^2 = p$ on n lliure de quadrats i p un primer fix.

14. Estudieu les solucions enteres de $X^2 + 5Y^2 = 2p$ on n lliure de quadrats i p un primer fix.

15. Estudieu les solucions enteres de $X^2 + 2Y^2 = p$ on n lliure de quadrats i p un primer fix.

16. Estudieu les solucions enteres de $X^2 - 2Y^2 = p$ on n lliure de quadrats i p un primer fix.

17. Considerem en el cos finit $\mathbb{F}_{p^n}$ l'equació $X^{p^n} + Y^{p^n} = Z^2$. Proveu que té solució a $\mathbb{F}_q$ i proveu que si $(x,y,z) \in \mathbb{F}_{p^n}^3$ és solució de l'equació llavors z varia dins un subconjunt de $\mathbb{F}_{p^n}^*$ amb $(p^n+1)/2$ elements si p és senar. Què succeeix si p és 2?

18. Doneu criteris per solucionar a $\mathbb{F}_p$ l'equació $X^n + Y^n = Z^n$.

19. Teorema de Sophie Germain. Sigui p un primer senar i considerem un altre primer senar q que compleixi simultàneament les dues condicions següents:

- l'equació $X^p + Y^p + Z^p = 0 \; mod \; q$ implica que x o y o z tenen residu zero en dividir-los per q,
- l'equcació $n^p = n(mod \; q)$ no té solució.

Demostreu llavors que qualsevol solució entera de $X^p + Y^p = Z^p$ té la propietat que un dels x, y, z és divisible per p.

20. Un primer p senar s'anomena de (Sophie) Germain si $2p + 1$ és també un primer. Demostreu que si p és un primer de Germain llavors en cas d'existir solucions $(x, y, z) \in \mathbb{Z}^3$ amb $mcd(x, y, z) = 1$ de l'equació de Fermat $X^p + Y^p = Z^p$ s'ha de complir que p divideix xyz.

21. Sigui K un cos amb $car(K) = p > 0$ amb $p \neq 2$. Proveu que l'equació $aX^2 + bY^2 = Z^2$ amb $a, b \in \mathbb{F}_p$ té una solució diferent a la $(0, 0, 0)$.

22. Sigui a un enter, i n un enter positiu senar, escrivim $n = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$ amb p_i primers diferents. Definim el simbol de Jacobi $\left(\frac{a}{n}\right)$ mitjançant:

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{n_i}.$$

Proveu que $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right)$ amb m, n enters senars positius. Observeu que el simbol de Jacobi no distingueix residues quadràtics, per exemple si $n = p_1 p_2$ producte de dos primers diferents senars i x coprimer amb N sempre $\left(\frac{x}{N}\right) = 1$.

23. Test de primalitat de Solovay-Strassen. Considereu els morfismes de grups $\chi_i : (\mathbb{Z}/N)^* \to (\mathbb{Z}/N)^*$ per $i = 1, 2$ via $\chi_1(x) = x^{\frac{N-1}{2}} mod \; N$ and $\chi_2(x) = \left(\frac{x}{N}\right)$, i escrivim $\chi_0 := \chi_2/\chi_1$. Proveu que χ_0 és trivial si N és un nombre primer. Demostreu que si N és senar i no primer llavors existeix $x \in (\mathbb{Z}/N)^*$ amb $\chi_0(x) \neq 1$.

24. Doneu un criteri per existir l'arrel quadrada de $-(U + 3)$ en un cos finit $\mathbb{F}_p$.

25. Doneu un criteri per a $\left(\frac{5}{p}\right), \left(\frac{7}{p}\right), \left(\frac{-3}{p}\right)$.

26. Escriu el nombre $-(D + U)$ com nombre enter p-adic $\sum_{i=0}^{\infty} a_i p^i$ amb $a_i \in \{0, 1, \ldots, p - 1\}$ explicitant els a_i's.

27. Sigui p un primer $p \geq 11$ Descriu els nombres de $\mathbb{Q}_p$ que es troben dins la bola unitat tancada del nombre $\beta := \sum_{i=-2}^{\infty} (U+1)p^i$. Descriu els nombres de $\mathbb{Q}_p$ de la bola oberta unitat al voltant de β.

28. Trobeu una successió de nombres racionals que convergeixin a $(U+1)(C+1)$ a $\mathbb{Q}_p$ però no convergeixi als nombres reals.

29. Trobeu una successió de nombres racionals que convegeixi a 1 als reals i a 0 a $\mathbb{Q}_p$.

30. Trobeu una successió de nombres racionals que convergeixi a 1 en $\mathbb{Q}_{p_1}$ i a 0 a $\mathbb{Q}_{p_2}$ on p_1, p_2 dos primers diferents.

31. Calculeu $|4^n - 1|_3$ Indicació: useu exponencial i logaritme en el cos 3-àdic.

32. Proveu un isomorfisme d'anells:

$$\mathbb{Z}_p \cong Hom(\mathbb{Z}[1/p]/\mathbb{Z}, (\mathbb{Z}[1/p]/\mathbb{Z}).$$

33. Proveu que $(\mathbb{Q}_p/\mathbb{Z}_p, +)$ és un grup abelià, on l'ordre de qualsevol element és una potència de p. És un grup finit generat?

34. Proveu que $(\mathbb{Z}_p, +)$ és un grup abelià, sense torsió. És finit generat?

35. Proveu que si p és senar tenim un isomorfisme de grups $\mathbb{Q}_p^* \cong \mathbb{Z} \oplus \mathbb{Z}/(p-1) \oplus \mathbb{Z}_p$, provant

    - tot element de $\mathbb{Q}_p^*$ s'escriu per $p^n u$ amb $u \in \mathbb{Z}_p^*$ de manera única.
    - proveu que $\mathbb{Z}_p^*$ és la suma directa de $1+p\mathbb{Z}_p$ amb $G = \{x \in \mathbb{Z}_p^* | x^{p-1} = 1\}$
    - Si $p \neq 2$ el grup multiplicatiu $1 + p\mathbb{Z}_p$ és isomorf a $(\mathbb{Z}_p, +)$ (penseu logaritme/exponencial).

36. Demostreu que $\mathbb{Q}_2^* \cong \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}_2$. Indicació: seguiu els mateixos passos que exercici anterior però aquí $1 + 4\mathbb{Z}_2 \cong \mathbb{Z}_2$.

37. Escrivint $a \in \mathbb{Q}_p^*$ amb $a = p^n u$ amb n enter i $u \in \mathbb{Z}_p^*$, tenim $a \in (\mathbb{Q}_p^*)^2$ si i només si satisfà les dues condicions següents:

    - n és parell,
    - si $p \neq 2$ $umod\ p\mathbb{Z}_p$ és un quadrat en $\mathbb{F}_p^*$, si $p = 2$, $u \equiv 1\ mod 8\mathbb{Z}_2$.

38. Trieu el primer més petit p complint $p > (C + D + U * 10)$ i calculeu els enters a que son un quadrat en $\mathbb{Q}_p$.

39. Trobeu TOTES les extensions quadràtiques de $\mathbb{Q}_p$ amb el primer p que useu en l'exercici anterior.

40. Trobeu Totes les extensions quadràtiques de $\mathbb{Q}_2$ (són un nombre finit).

41. Sigui G un grup abelià topològic, i.e. suma i pas a l'oposat siguin funcions continues. Observeu que si U és un entorn del zero llavors $a + U$ és un entorn de a per a $a \in G$. Si H denota la intersecció de tots els entorns del zero de G llavors:

    - H és un subgrup de G
    - H és l'adherència de $\{0\}$
    - G/H és Hausdorff

- G és Hausdorff si i només si $H = 0$.

42. Donat un grup topològic abelià G, on $0 \in G$ té un sistema fonamental d'entorns. Una successió de Cauchy en G es (x_v) d'elements de G on per cada entorn U de 0 existeix un enter $s(U)$ amb la propietat que

$$x_v - x_w \in U \text{ per a tot } v, w \geq s(U)$$

i dues successions de Cauchy son equivalents si $x_v - y_v \to 0$ en G. El conjunt de totes les classes d'equivalentia de successions de Cauchy en G forma un grup que es diu el completat de G i s'anota per $\hat{G}$, i tenim un morfime de grups $\phi : G \to \hat{G}$ on proveu que ϕ és injectiva si i només si G és Hausdorff.

Suposem que $0 \in G$ té un sistema fonamental d'entorns format per subgrups, és a dir

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n \supseteq \ldots$$

i $U \subseteq G$ és un entorn del zero si i només si conté algun G_n.

Observem que tenim morfismes projecció $\phi_{n,n-1} : G/G_n \to G/G_{n-1}$ i tenim un morfisme natural de G al limit projectiu de $(G/G_n, \phi_{n,n-1}) =: lim_{\leftarrow} G/G_n$. Proveu que $\tilde{G} \cong lim_{\leftarrow} G/G_n$

43. Suposem tenim tres sistemes inversos $(A_n, \phi_{A,n,n-1})$, $(B_n, \phi_{B,n,n-1})$ i $(C_n, \phi_{C,n,n-1})$, (pensem cadascún almenys grups abelians) de manera que per cada $n \in \mathbb{N}$ tenim una successió exacta curta:

$$0 \to A_n \to^{\alpha_n} B_n \to^{\beta_n} C_n \to 0$$

complint per a tot n que $\phi_{B,n,n-1} \circ \alpha_n = \alpha_{n-1} \circ \phi_{A,n,n-1}$ i $\phi_{C,n,n-1} \circ \beta_n = \beta_{n-1} \circ \phi_{B,n,n-1}$.

Llavors hi ha una successió entre els limits inversos:

$$0 \to lim_{\leftarrow} A_n \to^{\alpha} lim_{\leftarrow} B_n \to^{\beta} lim_{\leftarrow} C_n,$$

on α és injectiva, i $Im(\alpha) = Ker(\beta)$. A més si $\phi_{A,n,n-1}$ són exhaustives per tot n llavors β és exhaustiva i tenim una successió exacta curta:

$$0 \to lim_{\leftarrow} A_n \to^{\alpha} lim_{\leftarrow} B_n \to^{\beta} lim_{\leftarrow} C_n \to 0$$

44. Sigui $0 \to H \to G \to^{proj} G' \to 0$ una successió exacta de grups abelians. Si G té la topologia definida per una successió de subgrups G_n i donem a H i a G' les topologies induides, per base entorn del zero donada per $\{G' \cap G_n\}$ i $\{proj(G_n)\}$ llavors tenim una successió exacta:

$$0 \to \hat{H}' \to \hat{G} \to \hat{G}' \to 0$$

Proveu $(\hat{\hat{G}}) \cong \hat{G}$. És diu que un grup topològic és complet si $\hat{G} \cong G$ via ϕ.

45. Donat $a, b \in \mathbb{Q}_2$, escrivim $a = 2^i u$ i $b = 2^j v$ amb $u, v \in \mathbb{Z}_2^*$, i observeu que $u, v \equiv 1(mod\ 2)$, i considereu $r = (-1)^{ij} u^j v^{-i} \in \mathbb{Z}_2^*$, i observeu $r^2 \equiv 1(mod\ 8)$. Considerem $\alpha, \beta \in \mathbb{Z}$ on $\alpha \equiv (\frac{r^2-1}{8}) mod\ 2$ i $\beta = (\frac{u-1}{2})(\frac{v-1}{2}) mod\ 2$. Definim el simbol de Hilbert a $\mathbb{Q}_2$ mitjançant:

$$(a, b)_2 := (-1)^\alpha (-1)^\beta.$$

Demostreu les següents propietats amb $a, b \in \mathbb{Z}_2^*$:

- $(a, b)_2 = \begin{cases} 1 & if\ a \equiv 1 mod\ 4,\ or\ b \equiv 1\ mod\ 4 \\ -1 & if\ a \equiv b \equiv -1\ mod\ 4 \end{cases}$
- $(a, 2b)_2 = \begin{cases} 1 & if\ a \equiv 1\ mod\ 8,\ or\ a \equiv 1 - 2b\ mod\ 8 \\ -1 & otherwise \end{cases}$

46. Donat $a, b \in \mathbb{Q}^*$, llavors per quasi tot p primer (i.e. per tot nombre primer llevat d'un número finit de primers) el simbol de Hilbert $(a, b)_p$ és 1. I sempre tenim

$$\prod_{v \in Spec(\mathbb{Z}) \cup \{\infty\}} (a, b)_v = 1$$

on $Spec(A)$ és el conjunt ideals primers de l'anell commutatiu A.

47. Donada l'equació $aX^2 + bY^2 = 1$ amb $a, b \in \mathbb{Q}_2$. Es té que té infinites solucions a $\mathbb{Q}_2$ si i només si $(a, b)_2 = 1$.

48. Estudieu per a quins $\mathbb{Q}_v$ amb $v \in Spec(\mathbb{Z}) \cup \{\infty\}$ té solució $15(U+1)X^2 - 36 = Y^2$.

49. Proveu que $X^2 + Y^2 + Z^2 = -2$ té solució a $\mathbb{Q}_p$ per a tot p primer.

50. Proveu que existeixen $x, y \in \mathbb{Q}$ satisfent $p = x^2 + y^2$ amb p primer, s i només si $p \equiv 1\ mod\ 4$ o $p = 2$.

51. Sigui p primer. Existeixen $x, y \in \mathbb{Q}$ satisfent $x^2 + 5y^2 = p$ si i només si $p \equiv 1\ o\ 9\ mod\ 20$ o $p = 5$.

52. Sigui p un primer. Demostreu: existeixen $x, y \in \mathbb{Q}$ satisfent que $p = x^2 + 26y^2$ si i nomes si $p \equiv 1$ o $3\ mod\ 8$ i $p \equiv 1, 3, 4, 9, 10$ o $12\ mod\ 13$.