EXERCÍCIOS DE MATEMÁTICA FINITA - 2016/2017

II- Teoria Elementar de Números

1. Divisão com resto

1. Recorde o Exercicio 2-2) Soma dos n primeiros termos de uma progressão geométrica de razão r: Considere $r \in \mathbb{R}$, $r \neq 1$. Mostre que:

$$\sum_{k=0}^{n} r^k = \frac{r^{n+1} - 1}{r - 1}$$

2. Determine o resto e o quociente das divisões de 340 e de -625 por 13.

3. Sejam $a, b \in \mathbb{N},\ a \neq 0$. Se r é o resto da divisão de b por a , quanto é o resto da divisão de $-b$ por a?

4. Prove que sendo $a, b, c \in \mathbb{Z}$:

   (a) Se $a|b$ e $b|c$ então $a|c$.

   (b) Se $a|b$ e $a|c$ então $a|b + c$ e $a|b - c$.

   (c) Se $a, b > 0$ e $a|b$ então $a \leq b$.

   (d) Se $a|b$ e $b|a$ então $a = b$ ou $a = -b$.

5. Escreva 37 na base 5 e na base 2.

6. Considere os números a e b , definidos em notação binária por: $a = 10101$ e $b = 1111$ determine $a + b$ em notação binária e na base 10.

7. Porque é que qualquer número racional $\frac{p}{q} \in \mathbb{Q}$ é representado por uma dízima finita ou infinita periódica?

8. Escreva em notação decimal as fracções: $\frac{1}{7}$, $\frac{53}{16}$.

9. Escreva na forma de fracção: $0,36$, $3,235$, $0,(23)$, $0,35(63)$ e $0,(9)$

10. Sabendo que $n \in \mathbb{N}$ é um número de 7 algarismos na base 10. O que pode dizer sobre:

    (a) $log_{10}(n)$

    (b) O número de algarismos de n em notação binária?

11. Utilize o Teorema de Stirling ($n! \simeq (\frac{n}{e})^n \sqrt{2\pi n}$) para responder às seguintes perguntas:

    (a) Estime o número de algarismos de 300! e de $100^3 00$.

    (b) Qual dos números é maior: 300! ou 100^{300}?

2. Divisibilidade. Algoritmo de Euclides.

12. Mostre que:

    (a) Qualquer que seja o inteiro a, $a-1|a^2-1$.

    (b) Mais geralmente, qualquer que seja o inteiro a, $a-1|a^n-1$.

13. Prove a seguinte proposição: *Seja* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *é um polinómio de grau* n *na variável* x*, com coeficientes inteiros (i.e.* $a_i \in \mathbb{Z}$*,* $a_n \neq 0$*). Se* $r \in \mathbb{Z}$ *é uma raiz inteira de* $p(x)$ *então* $r|a_0$*".*

14. Verifique se algum dos seguintes polinómios tem raízes inteiras:

    (a) $p(x) = 6x^3 - 5x^2 - 29x + 10$

    (b) $p(x) = 3x^4 - 2x^2 + 6$

15. Mostre que se $n \in \mathbb{N}$ não é um número primo então tem um divisor $d \leq \sqrt{n}$.

16. Os *números de Mersenne* são os números da forma $2^p - 1$ em que p é um número primo.

    (a) Mostre que a notação binária para um número da forma $2^n - 1$ é $\underbrace{11\ldots1}_{p}$

    (b) Verifique que os 4 primeiros números de Mersenne são números primos, mas que $2^{11} - 1$ não é primo.

    (c) Mostre que se $n \in \mathbb{N}$ não for um número primo então $2^n - 1$ não é um número primo.

17. Um número $n \in \mathbb{N}$ é um *números perfeito* (Euclides) se n é igual à soma de todos os seus divisores (positivos) próprios.

(a) Mostre que 6 é um número perfeito.

(b) Mostre que se um número de Mersenne $2^p - 1$ é primo então $2^{p-1}(2^p - 1)$ é um número perfeito.

(c) Dê exemplo de um número perfeito diferente de 6.

(d) Qual a representação binária de um número da forma $2^{p-1}(2^p-1)$?

18. Mostre que se a é um número par e b é um número impar então $mdc(a, b) = mdc(\frac{a}{2}, b)$.

19. Calcule $mdc(a, b)$ e exprima-o como combinação linear inteira de a e b nos seguintes casos:

(a) $a = 35$, $b = 8$.

(b) $a = 114$, $b = 39$.

(c) $a = 3256$, $b = 123$.

20. Sejam $a, b \in \mathbb{Z}$. Mostre que qualquer divisor comum de a e b divide $mdc(a, b)$.

21. Suponha que dispõe de dois recipientes com as seguintes capacidades:

Caso 1 - 5 litros e 22 litros

Caso 2 - 6 litros e 22 litros

(a) Nalgum dos casos poderia obter 1 litro de água? Se sim, como procederia?

(b) Nalgum dos casos poderia obter 8 litros de água? Se sim como procederia?

22. Considere a sucessão de Fibonacci $F_n, n \in \mathbb{N}$ definida por $F_n = F_{n-1} + F_{n-2},\ F_1 = 1,\ F_2 = 1$.

(a) Mostre que $mdc(F_n, F_{n-1}) = 1$.

(b) Quantos passos tem de executar no algoritmo de Euclides para calcular $mdc(F_n, F_{n-1})$?

(c) Prove que se $4|n$ então $3|F_n$.

23. Prove a seguinte proposição :

Proposição. *Sejam* $a, b \in \mathbb{N}$ *e* $d := mdac(a, b)$. *Se* $(x_0, y_0) \in \mathbb{Z}^2$ *satisfaz a igualdade*

$$(*) \quad ax_0 + by_0 = d$$

então (todos) os pares $(x, y) \in \mathbb{Z}^2$ *que satisfazem a igualdade* $(*)$ *são os pares da forma*

$(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t), \quad t \in \mathbb{Z}.$

Interprete geométricamente o resultado.

24. Diga se as iguladades das duas primeiras alíneas ão verdadeiras ou falsas (justifique):

    (a) $\mathbb{Z} = \{4m + 7n : m, n \in \mathbb{Z}\}$

    (b) $2\mathbb{Z} = \{8m + 12n : m, n \in \mathbb{Z}\}$

    (c) Estude o conjunto $A = \{4m + 7n : \ m, n \in \mathbb{N}\}$. Mostre, em particular, que qualquer número natural $a \geq 29$ é um elemento de A.

25. Diga, justificando, se s ao verdadeiras ou falsas as seguintes afirmações em que $a, b \in \mathbb{N}$:

    (a) Se $17|ab$ então $17|a$ ou $17|b$.

    (b) Se $16|ab$ então $16|a$ ou $16|b$.

    (c) Se a, b são primos entre si e $d \in \mathbb{N}$ divide ab então $d|a$ ou $d|b$.

    (d) Se $a = 2^3 \times 5^7 \times 13^{12}$ e $b = 2^5 \times 3^2 \times 13^7$ então $mdc(a, b) = \frac{b}{2^2 \times 3^2}$.

    (e) Se $a = 2^3 \times 5^7 \times 13^{12}$ e $b = 2^5 \times 3^2 \times 13^7$ então $mmc(a, b) = 2^5 \times 3^2 \times 5^7 \times 13^{12}$.

    (f) Se $a = m^2n^4$ e $b = m^4n^2$ onde $m, n \in \mathbb{N}$, então $mdc(a, b) = m^2n^2$

    (g) $ab = mdc(a, b).mmc(a, b)$.

26. Utilize o método do "crivo de Eratóstenes" para listar todos os números primos até 200.

27. Mostre que os números n_k da forma $n_k = k^2 + k + 41, \ k \in \mathbb{N}$ são primos para $k \leq 20$. Dê exemplo de um valor $k \in \mathbb{N}$ para o qual n_k não é primo.

28. Considere o número natural $n = 2^3 \times 3 \times 5^2$. Quantos divisores naturais tem n?

29. Seja n um número natural cuja representação em factores primos é: $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Quantos divisores naturais tem n? E quantos divisores inteiros tem n?

30. Recorde o Teorema dos números primos: Sendo $\pi(n) := n^0 de\ números\ primos \leq n$, $\pi(n) \simeq \frac{n}{ln\ n}$.

    Utilize-o para estimar quantos números primos têm 100 algarismos.

3. Aritmética modular - Congruências

31. Diga, justificando, se as seguintes afirmações são verdadeiras ou falsas:

    (a) $23 \equiv 3(mod\ 5)$

    (b) $3 \equiv -56(mod\ 12)$

    (c) $3^{54} - 1 \equiv 7(mod\ 8)$

    (d) $300 \times 15 - 5^7 - 12 \equiv 3(mod\ 5)$

32. Calcule o resto da divisões de: (i) 12^{23} $por 53$, (ii) 2^{100} por 13.

33. **Critérios de divisibilidade**

    (a) **por 9:** Mostre que um número é divisível por 9 se e s
    'o se a soma dos seus algarismos o é.

    (b) **por 11:** Mostre que um número é divisível por 11 se e s
    'o se a "soma alternada" dos seus algarismos o é.
    ("soma alternada dos algarismos"= soma dos algarismos que ocupam um lugar par - soma dos algarismos queocupam um lugar impar).

34. Calcule os valores das seguintes expressões algébricas em $\mathbb{Z}_{13}$:

    (a) $\overline{4} \times (\overline{11}^2 + \overline{12} - \overline{7})$.

    (b) $\overline{10}^{34}$.

    (c) $\overline{4}^{-1} \times (\overline{2}^5 - \overline{12})$.

Resultados sobre Equações lineares $(mod\ n)$

35. Determine todas as soluções (eventualmente nenhuma) das equações:

    (a) $3x \equiv 9\ (mod\ 12)$.

    (b) $3x \equiv 9\ (mod\ 13)$.

    (c) $30x \equiv 45\ (mod\ 60)$

(d) $25x \equiv\ 45\ (mod\ 60)$

36. Prove o seguinte Teorema:

    Teorema *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Considere-se a equação:*

    $$(E) \qquad ax \equiv\ b\ (mod\ n)$$

    Seja $d = mdc(a, n)$. Então:

    1) Se $d \not| b$ a equação (E) não tem solução.

    2) Se $d|b$ a equação (E) tem exactamente d soluções $(mod\ n)$

37. Deduza do teorema anterior:

    (a) Um resultado sobre o número de soluções distintas da equação $\overline{a}.\overline{x} = \overline{b}$ em $\mathbf{Z_n}$.

    (b) Um resultado sobre o número de inversos de um elemento invertível $\overline{a} \in \mathbf{Z_n}$.

38. Para cada uma das seguintes equações lineares na variável $\overline{x}$, determine todas as soluções em

    (i) $\mathbf{Z_7}$ (ii) $\mathbf{Z_{12}}$

    (a) $\overline{3} + \overline{x} = \overline{0}$.

    (b) $\overline{3}\overline{x} = \overline{1}$.

    (c) $\overline{3}\overline{x} = \overline{0}$.

    (d) $\overline{3}\overline{x} + \overline{4} = \overline{2}$

    (e) $\overline{5}\overline{x} + \overline{2} = \overline{1}$

39. Seja $n \in N$ e $a \in \mathbb{Z}$, $a \not\equiv 0(modn)$ Mostre que:

    (a) Se $n = p$ é um número primo então a equação $\overline{a}x = \overline{0}$ tem como única solução $x = \overline{0}$.

    (b) Se n não é primo mostre que a proposição da alínea anterior é falsa.

    (c) Se n não é primo que condição necessária e suficiente deve satisfazer a para que a equação $\overline{a}x = \overline{0}$ tenha como única solução $x = \overline{0}$?

40. Seja p um número primo.

    (a) Quais os elementos de $\mathbb{Z}_p$ que têm inverso ?

    (b) Quais os elementos $\overline{a} \in \mathbb{Z}_p$ que são inversos de si próprios.

41. (a) Diga , justificando se algum dos seguintes elementos tem inverso em $\mathbb{Z}_{60}$ e caso o tenha calcule-o:

    $\overline{7},\ \overline{22},\ \overline{3},\ \overline{49}$

    (b) Quantos elementos de $\mathbb{Z}_{60}$ têm inversos?

42. a) Prove que qualquer que seja $a \in \mathbb{Z}$ se verifica $a^2 \equiv\ 0, 1\ ou\ \ 4\ (mod\ 8)$.

    b) Mostre que nenhum número natural da forma $8k+7$ pode ser escrito como soma de três quadrados.

43. (exame 2018) Houve um acidente numa fábrica e a polícia está a entrevistar quem estava presente.

    Num dos hangares há uma máquina com dois contadores cujos ponteiros rodam, no sentido dos ponteiros do relógio, com velocidade angular constante, o maior demora 52 minutos a dar uma volta completa e o menor 8 minutos.

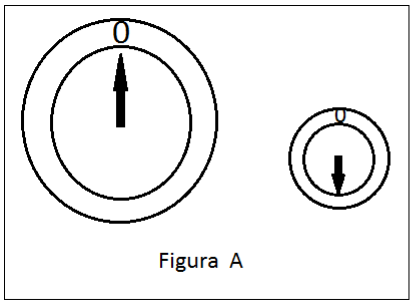

Figura A

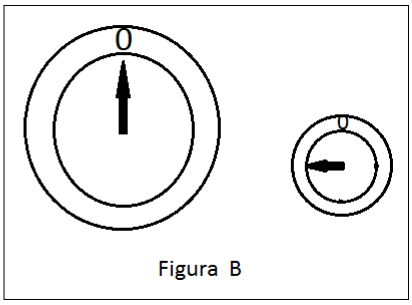

Figura B

    Às 14h 15m , os ponteiros estão na posição da Figura A e o encarregado diz à polícia que ligou a máquina pouco depois das 8h, tendo a máquina começado a funcionar, como é obrigatório, com os dois ponteiros no zero, depoimento corroborado por outros funcionários presentes.

    Um indivíduo, estranho à fábrica, que ali se encontrava disse que passou por ali ao ir à Direção, não se lembra exatamente da hora, mas tem a certeza de que os ponteiros estavam na posição da Figura B.

a) Se são 14h e 15m a que horas foi ligada a máquina?

b) Porque é que a polícia sabe que o indivíduo estranho à fábrica está a mentir?

44. **Camaleões e Congruências** (Terence Tao) :*Numa ilha há* 13 *camaleões verdes,* 15 *camaleões castanhos e* 17 *camaleões encarnados. Se dois camaleões de cores diferentes se encontram mudam ambos para a terceira cor, mas não mudam decor em nenhuma outra situação.*

    Será possível que a certa altura os camaleões fiquem todos da mesma cor?

    Sugestão: analise o resultado de uma mudança de cor de dois camaleões nas populações de cada cor *módulo 3*.

45. (Exame 2017) Determine todos os quádruplos (a, b, c, d) de números naturais, com $a \leq b \leq c \leq d$, que satisfazem a igualdade:

$$2^a + 2^b + 2^c + 2^d = 2^{41}.$$

46. (Exame 2017) Mostre que qualquer que seja o número natural $n \in \mathbb{N}$ existe um múltiplo de n cujos algarismos (na base 10) são $0's$ e $1's$.

    Sugestão: considere os restos da divisão por n dos $(n+1)$ números: 1, 11, 111, ... 1 ... 1.

47. (Exame 2016-2017) Mostre que existe um único número natural N menor do que 100 que dividido por 8 dá resto 3 e por 13 dá resto 6.

48. Determine a forma geral das soluções dos seguintes sistemas de equações.

    (a) $\begin{cases} x \equiv 1 (mod\ 8) \\ x \equiv 4 (mod\ 15) \end{cases}$ (Resposta: $x \equiv 49 (mod\ 8.15)$)

    (b) $\begin{cases} x \equiv 1 (mod\ 3) \\ x \equiv 5 (mod\ 8) \\ x \equiv 11 (mod\ 17) \end{cases}$ (Resposta: $x \equiv 181 (mod\ 3.8.17)$.)

49. Quantas soluções positivas com 3 dígitos têm os sistema de congruências anteriores? E com 6 dgitos?

50. Prove: **Teorema Chinês dos Restos (I)** *Sejam $n_1, n_2 \in \mathbb{N}$ dois números primos entre si. Então quaisquer que sejam $r_1, r_2 \in \mathbb{Z}$ o sistema de equações:*

$$\begin{cases} x & \equiv & r_1 (mod\ n_1) \\ x & \equiv & r_2 (mod\ n_2) \end{cases}$$

tem uma única solução módulo o produto $n_1 n_2$.

51. Deduza da alínea anterior que **Teorema Chinês dos Restos (II)** *Sejam $n_1, \ldots, n_k \in \mathbb{N}$ números primos entre si dois a dois ($mdc(n_i, n_j) = 1,\ i \neq j$). Então quaisquer que sejam $r_1, \ldots, r_k \in \mathbb{Z}$ o sistema de equações:*

$$\begin{cases} x & \equiv & r_1 (mod\ n_1) \\ & \vdots & \\ x & \equiv & r_k (mod\ n_k) \end{cases}$$

tem uma única solução módulo o produto $n_1 \ldots n_k$.

52. (Exame 2018) Se $f(x) = a_k x^k + \ldots a_1 x + a_0$ é um polinómio com coeficientes inteiros as raízes de f em $\mathbb{Z}_n$ são os elementos $\overline{r} \in \mathbb{Z}_n$ que satisfazem a congruência $f(r) \equiv 0 (mod\ n)$.

a) Determine todas as raízes do polinómio $x^2 - 1$ em $\mathbb{Z}_5$ e em $\mathbb{Z}_8$. (Indique os cálculos que fizer).

b) Mostre que se p é um número primo e $f(x) = ax^2 + bx + c$ é um polinómio de grau 2 com coeficientes em $\mathbb{Z}_p$, tal que $a \not\equiv 0 (mod\ p)$ então $f(x)$ tem no máximo duas raízes em $\mathbb{Z}_p$.

Sugestão. No caso de $f(x)$ ter uma raiz $\overline{r}$ em $\mathbb{Z}_p$ estude a equação $f(x) - f(r) \equiv 0 (mod\ p)$.

Comportamento de potências $(mod\ n)$ e função de Euler

53. Prove que $\forall x \in \mathbb{Z}$ se verifica a equação $x^3 \equiv x (mod\ 3)$.

54. Prove que existem $x \in \mathbb{Z}$ para os quais $x^4 \not\equiv x (mod\ 4)$.

55. (a) Determine a factorização em números primos de 1200.

(b) Seja $P(1200) := \{a \in \mathbb{N} :\ a \leq 1200\ e\ mdc(a, 1200) = 1\}$.

Utilize a alímea (a) e o princípio de inclusão-exclusão para determinar $|P(1200)|$.

(c) Quantos elementos de $\mathbb{Z}_{1200}$ são invertíveis?

56. **Função de Euler - $\Phi(n)$**

Dado um número natural $n \in \mathbb{N}$ a função de Euler - $\Phi(n)$ - de n é o número de números naturais menores do que n e primos com n, i.e.:

$$\Phi(n) := |\{a \in \mathbb{N} : \ mdc(a,n) = 1 \ e \ a \leq n\}|.$$

Mostre que:

(a) Se p é um número primo então $\Phi(p) = p - 1$.

(b) Se $n = p_1 p_2$ onde p_1, p_2 são dois números primos distintos, então $\Phi(n) = (p_1 - 1)(p_2 - 1)$.

(c) Utilize o princípio de inclusão- exclusão para mostrar a seguinte proposição:

Se n é um número natural, cuja decomposição em factores primos é da forma:
$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \ \alpha_i \in \mathbb{N}$ *então:*

$$\Phi(n) = n\big(1 - \frac{1}{p_1}\big) \dots \big(1 - \frac{1}{p_k}\big).$$

57. Mostre que se p é um número primo então :

(a) $\forall a \in \mathbb{Z}, a \not\equiv 0 (mod \ p)$ as classes de congruência módulo p dos números $\overline{a}, \overline{2a}, \dots, \overline{(p-1)a}$ são todas diferentes.

(b) Mostre que a proposição da alínea anterior é falsa se n não é um número primo.

58. Mostre que:

(a) Se p é um número primo então $p \mid \left(\begin{array}{c} p \\ k \end{array} \right), \forall k, \ 1 \leq k \leq p-1$.

(b) Se n não é um número primo a proposição da alínea anterior é falsa.

59. Prove por indução e usando o exercício 51 a seguinte versão do **Pequeno Teorema de Fermat** *Se p é um número primo então* $\forall a \in \mathbb{Z},\ a \not\equiv 0(mod\ p)$ *então* $a^p \equiv a(mod\ p)$.

60. Utilize o Pequeno Teorema de Fermat para calcular o inverso de $\overline{5}$ em $\mathbb{Z}_7$.

61. Determine o resto da divisão de 5^{3056} por 328.

4. Sistema de criptografia RSA

62. Considere os números primos $p_1 = 7$, $p_2 = 13$.

    (a) Sendo $n = p_1 p_2$ determine $\Phi(n)$.

    (b) Mostre que $e = 11$ é um expoente de encriptação válido.

    (c) Utlizando o sistema RSA, com $n = p_1 p_2$ e expoente de encriptação $e = 11$, como encripta a mensagem $m = 20$? Indique a mensagem encriptada $E(20)$.

    (d) Determine o coeficiente de desencritação $d :=$*o inverso de* e *em* $\mathbb{Z}_{\Phi(n)}$.

    (e) Justifique a igualdade $E(20)^d = 20$.

    (f) Suponha que recebe a mensagem encriptada $E(m) = 3$. Determine a mensagem m.

63. Considere os números primos $p_1 = 17$, $p_2 = 23$, $n = p_1 p_2$.

    (a) Determine $\Phi(n)$.

    (b) Quantos expoentes de encriptação pode escolher?

    (c) Se o coeficiente de encriptação é $e = 7$ qual é o expoente de desencriptação d?

    (d) Se receber a mensagem encriptada (pelo sistema RSA) $E(m) = 2$ qual é a mensagem m?

64. (Exame 2018) Considere os números $a = 2^5 \times 3^2 \times 5 \times 11^2$ e $b = 2^3 \times 5^7 \times 7$.

a) Escreva a decomposição em factores primos de $mdc(a, b)$ e de $mmc(a, b)$.

b) Quantos divisores positivos de a não dividem b?

c) Considere $d = mdc(a, b)$ e $m = mmc(a, b)$. Verifique se a igualdade seguinte é verdadeira ou falsa:

$$\Phi(a)\Phi(b) = \Phi(m)\Phi(d).$$

d) a alínea anterior é válida para quaisquer $a, b \in \mathbb{N}$?

65. (Exame 2017) Determine a forma geral dos números $a \in \mathbb{N},\ a > 1$ tais que $\Phi(a)$ divide a. São em número finito ou infinito? (justifique)

Geometrias Finitas: afins, projectivas, sistemas ternários de Steiner

66. Estude o conjunto de soluções das seguintes equações lineares em duas variáveis:

(a) $6x + 2y \equiv 0 (mod\ 11)$

(b) $6x + 2y \equiv 5 (mod\ 11)$

(c) $6x + 2y \equiv 0 (mod\ 12)$

(d) $6x + 2y \equiv 5 (mod\ 12)$

67. Considere o plano afim $\mathbb{Z}_{13}^2$. Determine equações vectorial e cartesiana para a reta r definida pelos pontos: $\mathbf{p} = (\overline{5}, \overline{1}),\ \mathbf{q} = (\overline{3}, \overline{10})$

68. Estude o conjunto de soluções em $\mathbb{Z}_{13}^2$ dos seguintes equações lineares e interprete geométricamente o resultado:

(a) $\begin{cases} \overline{2}x + \overline{3}y = \overline{3} \\ \overline{3}x + \overline{4}y = \overline{1} \end{cases}$

(b) $\begin{cases} \overline{2}x & + & \overline{3}y & = \overline{3} \\ \overline{3}x & - & \overline{2}y & = \overline{10} \end{cases}$

(c) $\begin{cases} \overline{2}x & + & \overline{3}y & = \overline{4} \\ \overline{3}x & - & \overline{2}y & = \overline{6} \end{cases}$

69. **Plano afim $\mathbb{Z}_3^2$**

    (a) Represente todos os pares $(\overline{x}, \overline{y}) \in \mathbb{Z}_3^2$ como pontos do reticulado de $\mathbb{R}^2$ com coordenadas (x, y).

    (b) Quantos pontos tem $\mathbb{Z}_3^2$? Quantos pontos tem cada reta?

    (c) $\mathbb{Z}_3^2$ é um plano afim de que ordem ?

    (d) E quantas retas?

    (e) Cada ponto pertence a quantas retas?

    (f) Quantas classes de retas paralelas tem $\mathbb{Z}_3^2$?

    (g) Descreva o plano projectivo $P\mathbb{Z}_3^2$ e responda s alíneas anteriores b) a e) para este plano.

70. Descreva e represente o espaço afim (de dimensão 3), $\mathbb{Z}_2^3$, indicando : n^o de pontos, n^o de retas, n^o de planos. Especifique o n 'umero de pontos de cada reta e de cada plano.

71. (Sistemas ternários de Steiner)

    Um sistema (ternário) de Steiner é um triplo $(C, \mathcal{B}, r)$ em que C é um conjunto, $\mathcal{B}$ uma família de 3-subsconjuntos de conjunto C, *os blocos* do sistema, e $r \in N,\ r \in \mathbb{N}$ que satisfaz as segintes condições:

    (S1) Qualquer elemento $c \in C$, c pertence a exatamente r blocos.

    (S2) Qualquer par de elementos de C está contido num único bloco.

    Considere os números naturais $v := |C|$, $b = |\mathcal{B}$ e r.

    (a) Mostre o plano de Fano ($P\mathbb{Z}_2$ e que o plano afim Z_3^2 são sistemas de Steiner.

    (b) O qe pode dizer sobre os sistemas de Steiner que têm $r = 1$ e $r = 2$?

(c) Mostre quaisquer que sejam os números v, b e r de um sistema ternário de Steiner satisfazem as relações seguintes:

$$(i) 3b = vr \qquad\qquad (ii)\ v - 1 = 2r.$$

(d) Deduza da alínea anterior que $v \equiv 1(mod 6)$ ou que $v \equiv 3(mod 6)$.

(e) Para todos os triplos (v, b, r) satisfazendo as relações da alínea c) existe um sistema de Steiner? (Problema para pensar)