• Teoria de números - Ficha 3

21-

a) Seja $a = 3m+1$, para algum $m \in \mathbb{N}$. Admitamos que a é primo

• Pelo algoritmo da divisão temos $m = 2m+r$ com $m \in \mathbb{N}$ $0 \leq r < 2$

Como $m = 2m$ Temos $a = 6m+1$

Caso $m = 2m+1$ Temos $a = 3(2m+1)+1 = 6m+4 = 2(3m+2)$

Logo $2|a$ mas como a é primo e $a > 2$ temos uma contradição

Assim, se $a = 3m+1$ é primo, temos necessariamente

$a = 6m+1$ com $m \in \mathbb{N}$

b) O único primo da forma m^2+1 é o 7 $(m \in \mathbb{N})$

• 7 é primo e da forma m^3-1 (basta considerar $m=2$)

Seja p primo tal que $p \neq 7$. Queremos provar que $p \neq m^3-1$ para todo o $m \in \mathbb{N}$

• No sentido de fazer prova por redução ao absurdo admitamos que $p = m^3-1$ para algum $m \in \mathbb{N}$. Então $p = (m-1)(m^2+m+1)$

• Uma vez que p é primo, os únicos divisores positivos de p são 1 e p

Logo $m-1 = 1$ ou $m^2+m+1 = 1$

Caso $m-1 = 1$, $m = 2$, pelo que $p = 7$ (contradição)

Caso $m^2+m+1 = 1$. Para todo o $m \in \mathbb{N}$ temos $m^2+m+1 \neq 1$

∴ Assim não existe qualquer $p \in \mathbb{N}$ tal que p seja primo, $p \neq 7$ e $p = m^3-1$, $m \in \mathbb{N}$

23-

- Seja $a > 1$. Se a é um nº composto então a admite um divisor primo menor ou igual a $\sqrt{a}$

- Temos $26^2 < 701 < 27^2$

$$\text{Logo } 26 < \sqrt{701} < 27$$

- Os números primo menores ou iguais a $\sqrt{701}$ são 2, 3, 5, 7, 11, 13, 17, 19, 23

Nenhum destes primos divide o 701, logo 701 é um número primo.

• Dados $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Diz-se que a é congruente com b módulo m se a e b têm o mesmo resto na divisão por m, escreve-se $a \equiv_m b$

Temos $a \equiv_m b$ sse $m | a-b$

a) $91 \equiv_7 0$ → $7 | (91-0)$ logo concluímos que $91 \equiv_7 0$

b) $-2 \equiv_8 2$

• Temos que $-2 = (-1) \times 8 + 6$, $0 \leq 6 < 8$ o resto de -2 na divisão por 8 é 6

• $2 = 0 \times 8 + 2$, $0 \leq 2 < 8$ logo o resto de 2 na divisão por 8 é 2

∴ Uma vez que 2 e −2 não têm o mesmo resto na divisão por 8 concluímos $-2 \not\equiv_8 2$

→ Resolução alternativa

• Uma vez que $8 \nmid (-2-2)$ $(-4) = (-1) \times 8 + 4$, $0 < 4 < 8$

concluímos que $-2 \not\equiv_8 2$

c) $17 \equiv_2 13$

• $17 = 8 \times 2 + 1$, $0 \leq 1 < 2$ o resto de 17 na divisão por 2 é 1

• $13 = 6 \times 2 + 1$, $0 \leq 1 < 2$ o resto de 13 na divisão por 2 é 1

• Uma vez que 13 e 17 têm o mesmo resto na divisão por 2 concluímos que $17 \equiv_2 13$

25 -

Temos $25 \equiv_m 4$ sse $m | \underbrace{(25-4)}_{21}$ sse $m \in \{(1, 3, 7, 21)\}$

26. $a^2 \equiv_m b^2$ não implica $a \equiv_m b$

$5^2 \equiv_6 1$ mas $5 \not\equiv_6 1$

27-

• Seja $m \in \mathbb{N}_0$. Diz-se que um conjunto S com m inteiros é um sistema completo de resíduos módulo m se S tem exatamente um representante de cada classe de congruência módulo m

a) $\{-2, -1, 0, 1, 2\}$

• $-2 = (-1) \times 5 + 3$, $0 \leq 3 < 5$, Logo $-2 \equiv_5 3$ $[-2] = [3]_5$

• $-1 = (-1) \times 5 + 4$, $0 \leq 4 < 5$ Logo $-1 \equiv_5 4$ $[-1] = [4]_5$

• $0 = 0 \times 5 + 0$, $0 \leq 0 < 5$

• $1 = 0 \times 5 + 1$, $0 \leq 1 < 5$ ~~Logo~~

• $2 = 0 \times 5 + 2$, $0 \leq 2 < 5$

• O conjunto é um sistema completo de resíduos módulo 5 pois temos exatamente um representante de cada uma das classes de congruência módulo 5

b) $S = \{0, 5, 10, 15, 20\}$

• S não é um sistema completo de resíduos módulo 5 pois tem mais do que um representante da classe $[0]_5$

c) $S = \{5, 11, 2, 13, 29\}$

• $5 = 1 \times 5 + 0$, $0 \leq 0 < 5$; $[5]_5 = [0]_5$

• $11 = 2 \times 5 + 1$, $0 \leq 1 < 5$, $[11]_5 = [1]_5$

• $2 = 0 \times 5 + 2$; $0 \leq 2 < 5$ $[2]_5$

• $13 = 2 \times 5 + 3$; $0 \leq 3 < 5$ $[13]_5 = [3]_5$

Cont

e) cont.

• $29 = 5\times5+4$, $0\leq4<5$ $[29]_5=[4]_5$

• Logo o conjunto é um sistema completo de resíduos módulo 7 pois tem exatamente um representante de cada classe de congruência módulo 5

d) $\{-6,-3,0,3,6\}$

• $-6=(-2)\times5+4$, $0\leq4<5$ $[-6]_5=[4]_5$

• $-3=(-1)\times5+2$, $0\leq2<5$ $[-3]_5=[2]_5$

• $0=0\times5+0$, $0\leq0<5$

• $3=0\times5+3$, $0\leq3<5$

• $6=1\times5+1$, $0\leq1<5$ $6\equiv_5 1$ $[6]_5=[1]_5$

∴ O conjunto ...

28 –

a) $[-22]_{15}\cap[8]_{15}$

• Temos $(-22)=(-2)\times15+8$, $0\leq8<15$

Logo $[-22]_{15}=[8]_{15}$ Assim $[-22]_{15}\cap[8]_{15}=[8]_{15}$

b) $[20]_{15}\times([39]_{15}+[-80]_{15})$ tais que $-40\leq x<0$ e $y>80$

• Temos $[20]_{15}=[5]_{15}$, $[39]_{15}=[9]_{15}$, $[-80]=[10]_{15}$

Logo $[20]_{15}\times([39]_{15}+[-80]_{15})=[5]_{15}\times([9]_{15}+[10]_{15})$

$=[5]_{15}\times[19]_{15}$ $([19]_{15}=[4]_{15})$

$=[5]_{15}\times[4]_{15}$

$=[20]_{15}=[5]_{15}$

• Seja $x = 5 + (-1) \times 15 = -10 \in [5]_{15}$: $\{x \in \{-10, -25\}$

o elemento pode ser 5, 20, 35

c) $x \equiv_{12} 6$, x é primo

• Um numero que satisfaça estas condições tem de ser do tipo $6k + 12$ e um numero assim nunca seria primo

$2357 \times 1036 + 499$ por 11

· Temos

$2357 = 214 \times 11 + 3$ logo $2357 \equiv_{11} 3$

$1036 = 94 \times 11 + 2$ logo $1036 \equiv_{11} 2$

$499 = 45 \times 11 + 4$ logo $499 \equiv_{11} 4$

logo $\underbrace{2357 \times 1036 + 499}_{a} \equiv_{11} 3 \times 2 + 4 = 10$

Uma vez que $0 \leq 10 < 11$, então o resto da divisão de a por 11 é 10

30-

· Temos $p \equiv_5 3$ logo $p^2 + 2p - 1 \equiv_5 3^2 + 2 \times 3 - 1 = 14$ e

$14 = 2 \times 5 + 4$, $0 \leq 4 < 5$

Assim $14 \equiv_5 4$ portanto o resto de $p^2 + 2p - 1$ na divisão por 5 é 4