→ Teoria de números - Ficha 6

51-

• Pequeno Teorema de Fermat: dados um primo p e um inteiro a tal que

$$p \nmid a \quad a^{p-1} \equiv_p 1$$

• Corolário: dados um primo p e um inteiro a: $a^p \equiv_p a$

a) $a^{21} \equiv_{15} a$

obs: 15 não é primo, mas admite a fatorização $15 = 3 \times 5$

• Sabemos que $a^{21} \equiv_{15} a \Rightarrow \begin{cases} a^{21} \equiv_3 a \\ a^{21} \equiv_5 a \end{cases}$

• Como 3 e 5 são primos, pelo corolário do T. Fermat,

$$a^3 \equiv_3 a \quad \text{e} \quad a^5 \equiv_5 a$$

Assim, $a^{21} = a^{3 \times 7} = (a^3)^7 \equiv_3 a^7$

$\downarrow$

$a^3 \equiv_3 a$

Fiz depois 60, 61, 63

Mas, $a^7 = a^3 \times a^3 \times a$

$\equiv_3 a \times a \times a$

$\equiv_3 a^3$

$\equiv_3 a$

• Logo, $a^{21} \equiv_3 a^7$

$\equiv_3 a$, como pretendemos provar

• Além disso, $a^{21} = a^{5 \times 4 + 1} = (a^5)^4 \times a$

$\equiv_5 a^4 \times a = a^5$

$a^5 \equiv_5 a \longleftarrow \equiv_5 a$

• Como $a^{21} \equiv_3 a$ e $a^{21} \equiv_5 a$ podemos concluir que $a^{21} \equiv_{15} a$

b) $a^{13} \equiv_{273} a$

$273 = 3 \times 7 \times 13$

• Temos que $a^{13} \equiv_{273} a \iff \begin{cases} a^{13} \equiv_3 a \\ a^{13} \equiv_7 a \\ a^{13} \equiv_{13} a \end{cases}$

• Sendo 3, 7, 13 primos sabemos que, pelo corolário do T. Fermat, que $a^3 \equiv_3 a$, $a^7 \equiv_7 a$ e $a^{13} \equiv_{13} a$

Assim,

$$a^{13} = (a^3)^4 \times a \equiv_3 a^4 \times a = a^3 \times a^2 \equiv_3 a \times a^2 = a^3 \equiv_3 a$$

$$a^3 \equiv_3 a \Downarrow (a^3)^4 \equiv_3 a^4$$

$$a^3 \equiv a \Downarrow a^3 \cdot a^2 \equiv a \cdot a^2$$

e,

$$a^{13} = a^7 \times a^6 \equiv_7 a \times a^6 = a^7 \equiv_7 a$$

$$a^7 \equiv_7 a \Downarrow a^7 \cdot a^6 \equiv_7 a \cdot a^6$$

Logo, $a^{13} \equiv_{273} a$

c) $a^{12} \equiv_{35} 1$ • Sabemos que $mdc(a, 35) = 1$, pelo que $5 \nmid a$ e $7 \nmid a$

• Pelo T. Fermat temos que

$$a^6 \equiv_7 1 \quad e \quad a^4 \equiv_5 1$$

• Assim, $a^{12} = (a^6)^2 \equiv_7 1^2$
$\equiv_7 1$

e, $a^{12} = (a^4)^3 \equiv_5 1^3$
$\equiv_5 1$

• Como $a^{12} \equiv_{35} 1$ se e só se $a^{12} \equiv_5 1$ e $a^{12} \equiv_7 1$, podemos concluir que $a^{12} \equiv_{35} 1$

52-

- Sabemos que 60 divide a^4+59 se o resto da divisão de a^4+59 por 60 é zero

ou seja, se $a^4+59 \equiv_{60} 0$

Ora,

$$a^4+59 \equiv_{60} 0 \overset{59 \equiv_{60} -1}{\iff} a^4-1 \equiv_{60} 0$$

$$\iff a^4 \equiv_{60} 1 \iff \begin{cases} a^4 \equiv_4 1 \\ a^4 \equiv_3 1 \\ a^4 \equiv_5 1 \end{cases}$$

- Dado que $mdc(a,30)=1$, $2 \nmid a$, $3 \nmid a$, $5 \nmid a$ e $mdc(a,4)=1$

- Pelo T. de Fermat

$$a^{3-1} \equiv_3 1,$$

e $a^{5-1} \equiv_5 1$,

i.e, $a^2 \equiv_3 1$ e $a^4 \equiv_5 1$

- Pelo teorema de Euler, como $mdc(a,4)=1$, $a^{\phi(4)} \equiv_4 1$

ou seja, $a^{2^2-2^1} \equiv_4 1$

i.e, $a^2 \equiv_4 1$

- Assim, $a^4=(a^2)^2 \equiv_3 1^2$
$\equiv_3 1$
, $a^4=(a^2)^2 \equiv_5 1^2$
$\equiv_5 1$

e $a^4=(a^2)^2 \equiv_4 1^2$
$\equiv_4 1$

- De $a^4 \equiv_4 1$, $a^4 \equiv_3 1$ e $a^4 \equiv_5 1$, podemos concluir que $a^4 \equiv_{60} 1$

53-

- Como 7 é primo e $7 \nmid a$ segue que $a^6 \equiv_7 1$, ou seja, $a^6 - 1 \equiv_7 0$

Logo, $7 \mid (a^6 - 1)$, ou seja, $7 \mid (a^3+1)(a^3-1)$. Uma vez que 7 é primo resulta que $7 \mid a^3+1$ ou $7 \mid a^3 - 1$.

54-

- Função de Euler

$$\phi : \mathbb{N} \to \mathbb{N}$$

$m \longmapsto \phi(m) =$ nº de naturais inferiores a m primos com m

m.d.c$(a, m) = 1$

- Propriedades
  - p primo

$$\phi(p) = p - 1$$

$$\phi(p^\alpha) = p^\alpha - p^{\alpha - 1} \quad (\alpha \in \mathbb{N})$$

- $K, m \in \mathbb{N}$ t.q. $mdc(K, m) = 1$

$$\phi(Km) = \phi(K)\,\phi(m)$$

$m \in \mathbb{N}$

$m = p_1^{K_1}\, p_2^{K_2} \cdots p_i^{K_i}$, com p_i primos, $K_i \in \mathbb{N}$

$$\phi(m) = \phi(p_1^{K_1})\ \phi(p_2^{K_2}) \cdots \phi(p_n^{K_n})$$
$$= (p_1^{K_1} - p_1^{K_1 - 1})\,(p_2^{K_2} - p_2^{K_2 - 2}) \cdots (p_2^{K_n} - p_n^{K_n - 1})$$

- $\phi(420)$

$m \in \mathbb{N}$

$\phi(m) =$ nº inteiros positivos menores ou iguais a m que são primos com m

- Fatorizando 420 em nº primos temos $420 = 2^2 \times 3 \times 5 \times 7$

$$\phi(420) = \phi(2^2) \times \phi(3) \times \phi(5) \times \phi(7)$$
$$= (2^2 - 2^1) \times (3^1 - 3^0) \times (5^1 - 5^0) \times (7^1 - 7^0) = 96$$

* Cont.

54- cont.

- $\phi(1001)$

- Fatorizando 1001 em números primos temos $1001 = 7 \times 11 \times 13$

$$\begin{array}{r|l} 1001 & 7 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array}$$

$$\phi(1001) = \phi(7) \times \phi(11) \times \phi(13)$$
$$= (7^1 - 7^0) \times (11^1 - 11^0) \times (13^1 - 13^0) = 720$$

- $\phi(5040)$

- Fatorizando 5040 em nº primos temos $5040 = 2^4 \times 3^2 \times 5 \times 7$

$$\begin{array}{r|l} 5040 & 2 \\ 2520 & 2 \\ 1260 & 2 \\ 630 & 2 \\ 315 & 3 \\ 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

$$\phi(5040) = \phi(2^4) \times \phi(3^2) \times \phi(5) \times \phi(7)$$
$$= \underbrace{(2^4 - 2^3)}_{8} \times \underbrace{(3^2 - 3^1)}_{6} \times (5^1 - 5^0) \times (7^1 - 7^0) = 1152$$

56-

- Teorema de Euler: dados um natural m e um inteiro a t.q. $mdc(a, m) = 1$
$a^{\phi(m)} \equiv_m 1$ onde $\phi(m)$ é o nº de naturais inferiores a m primos com m

- Temos que $mdc(3, 10) = 1$. Pretendemos verificar que $a^{\phi(10)} \equiv_{10} 1$

Ora,

$$\phi(10) = \phi(2 \times 5)$$
$$= \phi(2)\ \phi(5)$$
$$= (2-1)(5-1) = 4$$

- Portanto, pretendemos mostrar que $3^4 \equiv_{10} 1$. Temos que $3^4 = 81$. Logo $3^4 \equiv_{10} 1$

57-

a) • Sabemos que $a^{17} \equiv_{5} a$ se e só se $a^{17} \equiv_{15} a$ e $a^{17} \equiv_{15} a$, vez que $15 = 3 \times 5$ e $mdc(3,5)=1$

• Como $mdc(a,15)=1$, sabemos que $3 \nmid a$ e $5 \nmid a$. Assim, pelo Pequeno T. Fermat,

$$a^{3-1} \equiv_{3} 1 \quad e \quad a^{5-1} \equiv_{5} 1,$$

ou seja, $\quad a^{2} \equiv_{3} 1 \quad e \quad a^{4} \equiv_{5} 1$

Temos que $\quad a^{17} = (a^{2})^{8} \times a \equiv_{3} 1^{8} \times a = a$

e $\quad a^{17} = (a^{4})^{4} \times a \equiv_{5} 1^{4} \times a = a$

• Portanto, $a^{17} \equiv_{3} a$ e $a^{17} \equiv_{5} a$, pelo que $a^{17} \equiv_{15} a$

b) • Como $mdc(a,15)=1$, sabemos, pelo T. de Euler que $a^{\phi(15)} \equiv_{15} 1$

• Ora, $\phi(15) = \phi(3 \times 5) = \phi(3)\,\phi(5) = (3-1)\,(5-1) = 2 \times 4 = 8$

• Assim, $a^{17} = (a^{8})^{2} \times a \equiv_{15} 1^{2} \times a = a$

Logo, $a^{17} \equiv_{15} a$

58-

• Os dois últimos dígitos da representação decimal de 3^{256} correspondem aos dígitos do resto da divisão de 3^{256} por 10

• Pretendemos determinar $b \in \{0, \ldots, 99\}$ tal que

$$3^{256} \equiv_{100} b$$

• Pelo T. Euler. Sejam $a \in \mathbb{Z}$, $m \in \mathbb{N}$ e $mdc(a,m)=1$. Então

$$a^{\phi(m)} \equiv_{m} 1$$

cont

58 - Cont.

- Como $mdc(3, 100) = 1$, então, pelo Teorema de Euler, temos $3^{\phi(100)} \equiv_{100} 1 \quad (1)$

- Fatorizando 100 em números primos temos $100 = 2^2 \times 5^2$
logo $\phi(100) = (2^2 - 2^1)(5^2 - 5^1) = 40$

- De (1) segue que $3^{40} \equiv_{100} 1$

- Como $256 = 6 \times 40 + 16$ temos

$$3^{256} = (3^{40})^6 \times 3^{16} \equiv_{100} 1^6 \times 3^{16} = 3^{16} \qquad 16 = 3 \times 5 + 1$$

- temos $3^5 = 243 \equiv_{100} 43$ logo $3^{16} = (3^5)^3 \times 3 \equiv_{100} 43^3 \times 3$

- Uma vez que $43^2 = 1849 \equiv_{100} 49$ segue que $43^3 \times 3 = 43^2 \times 43 \times 3$
$\equiv_{100} 49 \times 43 \times 3$

- Temos $49 \times 43 \times 3 = 6321 \equiv_{100} 21$

- Como $0 \leq 21 < 100$, então o resto de 3^{256} na divisão por 100 é 21.
Portanto os dois últimos dígitos são o 2 e o 1

59 -

- Seja m um inteiro ímpar não divisível por 5. Então, $2 \nmid m$ e $5 \nmid m$
Admitamos que m é positivo (caso contrário $|m|$ é, se $|m|$ divide um determinado inteiro, também m divide esse inteiro)

- Pelo T. Euler, como $mdc(10, 9m) = 1$

$$10^{\phi(9m)} \equiv_{9m} 1$$

- Assim, $10^{\phi(9m)} - 1 \equiv_{9m} 0$, ou seja, $9m$ divide $10^{\phi(9m)} - 1$

- Note-se que $10^{\phi(9m)} - 1$ é o nº com $\phi(9m)$ dígitos todos iguais a 9

• Logo, $\frac{10^{\phi(9n)}-1}{9}$ é um inteiro com $\phi(9n)$ dígitos todos iguais a 1

• Como $9n$ divide $10^{\phi(9n)}-1$, existe $k \in \mathbb{N}$ tal que $10^{\phi(9n)}-1 = 9nk$.

Logo, $\frac{10^{\phi(9n)}-1}{9} = nk$ e n divide $\frac{10^{\phi(9n)}-1}{9}$

62-

a)

• Teorema de Wilson: Se p é primo então $(p-1)! \equiv_p -1$

• Como 17 é primo, pelo T. Wilson

$16! \equiv_{17} -1$ Logo $16 \times 15! \equiv_{17} -1$ Uma vez que $-1 \equiv_{17} 16$

então $16 \times 15! \equiv_{17} 16$ considerando que $\text{mdc}(16,17)=1$ segue

que $15! \equiv_{17} 1$

• Como $0 \leq 1 < 17$, o resto da divisão de $15!$ por 17 é 1.

b)

• Como 29 é primo, pelo T. Wilson temos

$28! \equiv_{29} -1$ logo $28 \times 27 \times 26! \equiv_{29} -1$

temos $28 \equiv_{29} -1$, $27 \equiv_{29} -2$, portanto $(-2) \times (-1) \times 26! \equiv_{29} -1$

• Assim $2 \times 26! \equiv_{29} -1$ donde resulta $2 \times 26! \equiv_{29} 28$

• Como $0 \leq 28 < 29$, o resto de $2 \times 26!$ na divisão por 29 é 28