67 inteiros

(feito no computador)

① a) 3958 / 18 — Quociente: 219 — Resto: 16
-3958 / 18 — Quociente: -219 — Resto: -2
3958 / -18 — Quociente: -219 — Resto: 2
-3958 / -18 — Quociente: 219 — Resto: -16

b) Que nos casos em que o quociente é negativo, o dividendo reconstruído não é equivalente ao original.

c) (feito no computador)

② (feito no computador)

Binário: 11100000010001011_2

Octal: 160213_8

Hexadecimal: $E08B_{16}$

③ a) $N = a_{m-1} \times b^{m-1} + a_{m-2} \times b^{m-2} + \ldots + a_0 \times b^0$

$b^{m-1} \leq N \leq (b-1) \times (b^{m-1} + b^{m-2} + \ldots + b^0)$

$b^{m-1} \leq N \leq (b-1) \times \frac{1-b^m}{1-b} = (b-1) \times \frac{b^m - 1}{b-1} = b^m - 1$

$b^{m-1} \leq N < b^m$ Sabendo que log é monótona crescente:

$\log_b b^{m-1} \leq \log_b N < \log_b b^m \Leftrightarrow m-1 \leq \log_b N < m$

$\lfloor \log_b N \rfloor = m-1 \Leftrightarrow m = \lfloor \log_b N \rfloor + 1$

b) $m = \lfloor \log_{10} 2^{64} \rfloor + 1 = 19 + 1 = 20$

c) $m = \lfloor \log_2 5000000000 \rfloor + 1 = 32 + 1 = 33$

④ (feito no computador)

Como o maior divisor comum entre 17369 e 5472 é 1, estes números são primos entre si. $m = -2647$; $m = 8402$.

⑤

21340	2		88	2	$21340 = 2^2 \times 5 \times 11 \times 97$ $\quad 88 = 2^3 \times 11$
10670	2		44	2	
5335	5		22	2	$m.d.c = 2^2 \times 11 = 4 \times 11 = 44$
1067	11		11	11	
97	97		1		$m.m.c. = 2^3 \times 5 \times 11 \times 97 = 42680$
1					

⑥ 13331, uma vez que este número é primo.

⑦ a) Seja $a = f_1^3 \times f_2^2 \times f_3$ a decomposição em fatores primos de a, por exemplo.

Seja $b = f_3^2 \times f_0 \times f_4$ a decomposição em fatores primos de b, por exemplo.

$mdc(a,b) = f_2 \times f_3$ $\quad mmc(a,b) = f_1^3 \times f_2^2 \times f_3^2 \times f_4$

$mdc(a,b) \times mmc(a,b) = f_1^3 \times f_2^2 \times f_3 \times f_3^2 \times f_0 \times f_4 = |a \times b|$, c.q.p.

b) $mdc(1575, 231) = 21$ (pelo excel)

$mmc = \frac{1575 \times 231}{21} = 17325$

⑧ a) $3x \equiv 4 \pmod 6$ $\quad m.d.c(3,6) = 3$

$3 \nmid 4$, logo não tem solução.

b) $4x \equiv 3 \pmod 7$ m.d.c.$(4,7)=1$

$1 \mid 3$, logo tem solução única $(d=1)$

$4 \equiv -3$, logo $-3x \equiv 3 \pmod 7 \Leftrightarrow x \equiv -1 \Rightarrow x = 6$ R: $x=6$

e) $2x \equiv 18 \pmod{50}$ m.d.c.$(2,50)=2$

$2 \mid 18$, logo existem 2 soluções. $d=2$ (até $d-1$)

$2x \equiv 18 \pmod{50} \Leftrightarrow x \equiv 9 \pmod{25} \Leftrightarrow x = 9 + k \times 25,\ k = 0,1$

$x = 9 \vee x = 9+25 \Leftrightarrow x = 9 \vee x = 34$

⑨ $5x \equiv 1 \pmod 7$ m.d.c.$(5,7)=1$

$1 \mid 1$, logo tem solução única $d=1$

$5x \equiv 1 \pmod 7 \Leftrightarrow 1 = 5x + 7K$ (algoritmo de Euclides dá solução)

$1 = 5 \times 3 + 7 \times (-2)$ Logo, o inverso de 5 $(\bmod 7)$ é 3; R: $x=3$

— // —

$500x \equiv 1 \pmod{8191}$ m.d.c.$(500,8191)=1$

$1 \mid 1$, logo tem solução única

$500x \equiv 1 \pmod{8191} \Leftrightarrow 1 = 500x + 8191K$ (algoritmo de Euclides dá solução.)

$1 = 500 \times 1458 + 8191 \times (-89)$ Logo, o inverso é 1458 R: $x=1458$

⑩ a) $\begin{cases} 2x+3y \equiv 4 \pmod 5 \\ 4x-y \equiv 1 \pmod 5 \end{cases} \Leftrightarrow \begin{cases} \text{———} \\ -x-y \equiv 1 \pmod 5 \end{cases} \Leftrightarrow$

$\Leftrightarrow \begin{cases} 2x-2y \equiv 4 \pmod 5 \\ \text{———} \end{cases} \Leftrightarrow \begin{cases} 2x+2x+2 \equiv -1 \pmod 5 \\ y \equiv -x-1 \pmod 5 \end{cases} \Leftrightarrow$

$\Leftrightarrow \begin{cases} -x \equiv -3 \pmod 5 \\ y \equiv -x-1 \pmod 5 \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \\ y \equiv -4 \equiv 1 \end{cases}$ R: $x=3$ e $y=1$

b) $\begin{cases} 3x+y \equiv 1 \pmod 4 \\ 2x-2y \equiv 2 \pmod 4 \end{cases} \Leftrightarrow \begin{cases} y \equiv 1-3x \pmod 4 \\ 2x+6x-2 \equiv 2 \pmod 4 \end{cases} \Leftrightarrow$

$\Leftrightarrow \begin{cases} \text{———} \\ 8x \equiv 4 \pmod 4 \end{cases} \Leftrightarrow \begin{cases} \text{———} \\ 0x \equiv 0 \pmod 4 \end{cases}$

↑ qualquer x é solução

Se $x=0$, $y=1$
Se $x=1$, $y \equiv -2 \equiv 2$
Se $x=2$, $y \equiv -5 \equiv -1 \equiv 3$
Se $x=3$, $y \equiv -8 \equiv 0$

4 pares de soluções.

(11) a) $(579)^{39} \pmod{59} = (590-11)^{39} \pmod{59} \equiv (-11)^{39} \pmod{59} =$

$= (\underbrace{(-11)^2}_{121 \equiv 3})^{19} \times (-11) \pmod{59} \equiv 3^{19} \times (-11) \pmod{59} = (3^5)^3 \times 3^4 \times (-11) \pmod{59} =$

$= (243)^3 \times 3^4 \times (-11) \pmod{59} \equiv 7^3 \times 3^4 \times (-11) \pmod{59} = 49 \times 7 \times 3^4 \times (-11) \pmod{59} =$

$\equiv 48 \times 22 \times (-11) \equiv (-11)^2 \times 22 \equiv 3 \times 22 = 66 \equiv 7 \pmod{59}$ R: 7

b) $18^{8970} \pmod{8971}$ PTF:

8971 é primo e $8971 \nmid 18$, logo: Se p é primo e $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$

$18^{8970} \equiv 1 \pmod{8971}$ R: 1

c) $18^{8971} + 18^{8974} \pmod{8971} \equiv 18 \times 1 + 18^4 \times 1 = 18 + 18^4 \equiv$

$\equiv 5850 \equiv 104994 \equiv 6313$ R: 6313

(12) Calcular a sequência $c, 2c, 3c, 4c, 5c, 6c, 7c, 8c, 9c, 10c \pmod{11}$

	para c = 5:	para c = 15:
c	5	4
2c	10	8
3c	4	1
4c	9	5
5c	3	9
6c	8	2
7c	2	6
8c	7	10
9c	1	3
10c	6	7

$c^{p-1} = 5^{10} = 9765625 \equiv 1 \pmod{11}$

$c^{p-1} = 15^{10} \equiv 4^{10} \pmod{11} \equiv 1 \pmod{11}$

47 + 56 = 103 184 187 205

(13) $0 + 2\times1 + 3\times3 + 4\times6 + 5\times0 + 6\times2 + 7\times0 + 8\times7 + 9\times9 + 10a_{10} \equiv 0 \pmod{11}$

$\Leftrightarrow 184 + 10a_{10} \equiv 0 \pmod{11} \Leftrightarrow -a_{10} \equiv -184 \pmod{11} \Leftrightarrow a_{10} \equiv 184 \equiv 8 \pmod{11}$

O dígito de verificação para o novo livro é 8.

$0 + 2\times1 + 3\times3 + 4\times6 + 5\times9 + 6\times2 + 7\times0 + 8\times7 + 9\times9 + 10\times8 \equiv 0 \pmod{11}$

$\Leftrightarrow 309 \equiv 0 \pmod{11}$. Ora, isto é falso, pois $309 \equiv 1 \pmod{11}$.

(14) a) $9\times1 + 8\times5 + 7\times4 + 6\times5 + 5\times8 + 4\times4 \times 3\times9 + 2\times0 + 8 \equiv 0 \pmod{11}$

$\Leftrightarrow 198 \equiv 0 \pmod{11}$, o que é verdade.

Logo, o NIF está correto.

b) $9\times5+8\times0+7\times1+6\times4+5\times1+4\times3+3\times1+2\times9+c\equiv0 \pmod{11} \Leftrightarrow$

$\Leftrightarrow 114+c\equiv0 \pmod{11} \Leftrightarrow 4+c\equiv0 \pmod{11} \Leftrightarrow c\equiv-4 \pmod{11} \Leftrightarrow$

$\Leftrightarrow c\equiv7 \pmod{11}$ R: $c=7$.

(15) $x\equiv21 \pmod{25}$ $x\equiv48 \pmod{49}$ $x\equiv88 \pmod{121}$

$1=-49+2\times25$ (pelo algoritmo de Euclides)

$x=21\times(-49)+2\times25\times48=1371 \pmod{25\times49}\equiv146 \pmod{1225}$

$x\equiv88 \pmod{121}$ $x\equiv146 \pmod{1225}$

$1=-8\times1225+81\times121$ (pelo algoritmo de Euclides).

$x\equiv88\times(-8)\times1225+146\times81\times121 \pmod{121\times1225}\equiv568596 \pmod{148225}\equiv$

$\equiv123871 \pmod{148225}$ R: $x=123\,871$

(16) a) $a=s^{-1} \pmod{p-1}$ $mdc(p-1,s)=mdc(126,11)=1$

$1=-2\times126+23\times11\equiv23\times11 \pmod{126}$ Logo, $a=23$

$b=s^{-1} \pmod{q-1}$ $m.d.c.(q-1,s)=mdc(130,11)=1$

$1=5\times130-59\times11\equiv-59\times11 \pmod{130}=71\times11 \pmod{130}$ Logo, $b=71$

b) chave pública $(r=pq,s)=(16637,11)$

chave privada $(p,q,a,b)=(127,131,23,71)$

abrame → 010218011305 Como este número é superior a r, repartimos a mensagem em 2 números.

abrame → 10218|011305

$M=10218$ $E\equiv M^s \pmod{r}\equiv10218^{11} \pmod{16637}\equiv393$

$M=11305$ $E\equiv M^s \pmod{r}\equiv11305^{11} \pmod{16637}\equiv9414$

O criptograma a enviar é $E=3939414$

c) $E=9414$ $E^a \pmod{p}=9414^{23} \pmod{127}\equiv2 \pmod{127}$

$mdc(131,127)=1=-33\times127+32\times131$ $E^b \pmod{q}=9414^{71} \pmod{131}\equiv39 \pmod{131}$

$M=39\times(-33)\times127+32\times131\times2=-155065\equiv11305 \pmod{16637}$

$E=393$ $E^a \pmod{p}=393^{23} \pmod{127}\equiv58 \pmod{127}$ $E^b \pmod{q}=393^{71} \pmod{131}\equiv0 \pmod{131}$

$M=0\times(-99)\times127+58\times32\times131\equiv10218 \pmod{16637}$. $M=010218011305=$ abrame.