Teste 20/21

1. $m = 253$

$\sqrt{m} \simeq 15{,}905$

$s = 16$

$s^2 - m = 16^2 - 253 = 3$

$s \leftarrow s+1$

$s^2 - m = 17^2 - m = 36$ (é quadrado

$t = \sqrt{s^2 - m} = 6$

$a = s - t = 17 - 6 = 11$ $\qquad m = ab = 11 . 23$

$b = s + t = 17 + 6 = 23$ $\qquad$ Logo, 23 e 11 são divisores não triviais de m

2. $m = 377$

$f(x) = x^2 - 1$ e $x_0 = 2$

b $\quad x_1 \equiv f(x_0) = f(2) \equiv 2^2 - 1 \equiv 3 \bmod m$

b $\quad$ a $\quad x_2 \equiv f(f(x_0)) \equiv 8 \bmod m$ $\qquad$ mdc$(8-3, 377) = $ mdc$(5, 377) = 1$

$b = 63$ $\quad$ a $\quad x_3 \equiv f(f(x_2)) = f(63) \equiv 3968 \bmod m$ $\qquad$ mdc$(198-8, 377) =$

$\equiv 198 \bmod m$ $\qquad$ mdc$(190, 377) = 1$

a $\quad x_4 \equiv f(f(x_3)) = f(f(198)) \equiv f(39203)$

$\equiv f(372)$ $\qquad$ mdc$(63-24, m) = 13$

$\equiv 138383 \equiv 24 \bmod m$

Logo, 13 é um fator não trivial de 377.

3. $p = 31$, $r = 3$, $a = 5$

(a) consideremos um s.r.r. $\mathbb{Z}_{31}^{*} = \{1, 2, \ldots, 30\}$

$r = 3$ é raiz primitiva de 31 se e só se ord$_{31} 3 = \varphi(31) = 30$

Sabemos que ord$_{31} 3 \mid \varphi(31)$. Logo,

ord$_{31} 3 \in \{1, 2, 3, 5, 6, 10, 15, 30\}$

Temos que:

$3^1 \equiv 3 \bmod 31 \not\equiv 1 \bmod 31$

$3^2 \equiv 9 \bmod 31 \not\equiv 1 \bmod 31$

$3^3 \equiv 27 \bmod 31 \not\equiv 1 \bmod 31$

$3^5 \equiv 243 \bmod 31 \equiv 26 \bmod 31 \not\equiv 1 \bmod 31$

$3^6 \equiv 729 \bmod 31 \equiv 16 \bmod 31$

$3^{10} \equiv 59049 \bmod 31 \equiv 25 \bmod 31$

$3^{15} \equiv 14348907 \bmod 31 \equiv 30 \bmod 31 \equiv -1 \bmod 31$

$3^{30} = 3^{15} \times 3^{15} \equiv (-1) \times (-1) \bmod 31 \equiv 1 \bmod 31$

$\curvearrowright \equiv 3^5 \bmod p$

(b) $K=4$ $\quad b \equiv \alpha^a \bmod p \qquad p=31,\ \alpha=3$ e $a=5$

$P=6$

Sabemos que para uma dada mensagem,

$x \equiv \alpha^K \bmod p$ e, δ = mensagem . $b^K \bmod p$

E envia-se (x, δ).

Ora, calculemos $x \equiv 3^4 \bmod 31$ e $\delta = 6 \cdot b^4 \bmod p$

consideremos $b = 26$, $x = 19$, então $\delta = 6 \cdot 26^4 \bmod 31$

Logo, envia-se $(19,30)$.

4. $x^2 \equiv 633 \bmod 863$, temos que 863 é número primo.

Ora, se supormos que $\left(\frac{633}{863}\right)=1$, então sabemos que $\exists x : x^2 \equiv 633$ mod 863.

Logo, calculemos $\left(\frac{633}{863}\right) = \left(\frac{3 \cdot 211}{863}\right) = \left(\frac{3}{863}\right)\left(\frac{211}{863}\right)$

$$=\left((-1)^{431}\left(\frac{863}{3}\right)\right)\left((-1)^{105 \cdot 431}\left(\frac{863}{211}\right)\right)$$

$$=\left(-\left(\frac{863}{3}\right)\right)\left(-\left(\frac{863}{211}\right)\right) = \left(\frac{863}{3}\right)\left(\frac{863}{211}\right) = (-1)\left(\frac{863}{211}\right)$$

$$=(-1)\left(\frac{19}{211}\right) = (-1)\ (-1)^{9 \cdot 105}\left(\frac{211}{19}\right) = \left(\frac{211}{19}\right) = \left(\frac{-2}{19}\right) = \left(\frac{17}{19}\right)$$

$= (-1)$

Logo, temos que não existe solução para $x^2 \equiv 633 \bmod 863$.

5. $$\left(\frac{2^5 \cdot 3 \cdot 7^3}{5 \cdot 11 \cdot 17^2}\right) = \left(\frac{2^5}{5 \cdot 11 \cdot 17^2}\right)\left(\frac{3}{5 \cdot 11 \cdot 17^2}\right)\left(\frac{7^3}{5 \cdot 11 \cdot 17^2}\right)$$

$$=\left(\frac{2^5}{5}\right)\left(\frac{2^5}{11}\right)\left(\frac{2^5}{17^2}\right)\left(\frac{3}{5}\right)\left(\frac{3}{11}\right)\left(\frac{3}{17^2}\right)\left(\frac{7^3}{5}\right)\left(\frac{7^3}{11}\right)\left(\frac{7^3}{17^2}\right)$$

$$=\left(\frac{2^5}{5}\right)\left(\frac{-1}{11}\right)\left(\frac{2^5}{17}\right)\left(\frac{2^5}{17}\right)\left(\frac{3}{5}\right)(-1)^5\left(\frac{11}{3}\right)\left(\frac{3}{17}\right)\left(\frac{3}{17}\right)\left(\frac{7^3}{5}\right)\left(\frac{7^3}{11}\right)\left(\frac{7^3}{17}\right)\left(\frac{7^3}{17}\right)$$

$$=(-1)\left(\frac{2^5}{5}\right)\left(\frac{2^5}{17}\right)\left(\frac{2^5}{17}\right)\left(\frac{3}{5}\right)(-1)\left(\frac{-1}{3}\right)\left(\frac{17}{3}\right)\left(\frac{17}{3}\right)\left(\frac{7^3}{5}\right)\left(\frac{7^3}{11}\right)\left(\frac{7^3}{17}\right)\left(\frac{7^3}{17}\right)$$

$$=(-1)\left(\frac{2}{5}\right)\left(\frac{2^5}{17}\right)\left(\frac{2^5}{17}\right)\left(\frac{-1}{3}\right)\underbrace{(-1)\left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right)}_{1}\left(\frac{3}{5}\right)\left(\frac{7^3}{11}\right)\left(\frac{7^3}{11}\right)\left(\frac{7^2}{17}\right)$$

$\overset{(-1)}{=}\left(\frac{2}{5}\right)\left(\frac{2}{17}\right)\left(\frac{2}{17}\right)\left(\frac{2}{17}\right)\left(\frac{2}{17}\right)\left(\frac{2}{17}\right)\left(\frac{2^5}{17}\right)(-1)\left(\frac{-1}{3}\right)\left(\frac{7}{11}\right)\left(\frac{7}{11}\right)\left(\frac{7}{11}\right)\left(\frac{7^3}{17}\right)\left(\frac{7^3}{17}\right)$

$\overset{(-1)}{=}\left(\frac{2}{5}\right)\left(\frac{1}{17}\right)\left(\frac{1}{17}\right)\left(\frac{1}{17}\right)\left(\frac{1}{17}\right)\left(\frac{1}{17}\right)\left(\frac{2^5}{17}\right)\left(\frac{7^3}{17}\right)(-1)\left(\frac{11}{7}\right)(-1)\left(\frac{11}{7}\right)(-1)\left(\frac{11}{7}\right)\left(\frac{7^3}{17}\right)$

$\overset{(-1)}{=}(-1)\left(\frac{2^5}{17}\right)\left(\frac{7^3}{17}\right)\left(\frac{7^3}{17}\right)\left(\frac{11}{7}\right)\left(\frac{11}{7}\right)(-1)\left(\frac{11}{7}\right)$

$\overset{(-1)}{=}\left(\frac{7^3}{17}\right)\left(\frac{7^3}{17}\right)\left(\frac{11}{7}\right)\left(\frac{11}{7}\right)\left(\frac{11}{7}\right)\overset{(-1)}{=}\left(\frac{7}{17}\right)\left(\frac{7}{17}\right)\left(\frac{7}{17}\right)\left(\frac{7^3}{17}\right)\left(\frac{11}{7}\right)\left(\frac{11}{7}\right)\left(\frac{11}{7}\right)$

$\overset{(-1)}{=}\left(\frac{4}{17}\right)\left(\frac{4}{17}\right)\left(\frac{4}{17}\right)\left(\frac{7^3}{17}\right)\left(\frac{11}{7}\right)\left(\frac{11}{7}\right)\left(\frac{11}{7}\right)$

$\overset{(-1)}{=}\left(\frac{2^2}{17}\right)\left(\frac{2^2}{17}\right)\left(\frac{2^2}{17}\right)\left(\frac{7^3}{17}\right)\left(\frac{4}{7}\right)\left(\frac{4}{7}\right)\left(\frac{4}{7}\right)$

$\overset{(-1)}{=}\left(\frac{7^3}{17}\right)\left(\frac{2^2}{7}\right)\left(\frac{2^2}{7}\right)\left(\frac{2^2}{7}\right) = -1$

6. $p = 19$, $r = 2$ $\qquad \varphi(19) = 18$

$ind_2 5 = 16$ e $2^{13} \equiv 3 \bmod p$ $\qquad 2^1 \bmod 19 \leftarrow$

Teorema do índice

$15x^7 \equiv 9 \bmod p \Leftrightarrow ind_2 15x^7 \equiv ind_2 9 \bmod 18$

$\Leftrightarrow ind_2 15 + 7\, ind_2 x \equiv ind_2 9 \bmod 18$

$\Leftrightarrow ind_2 (3\times 5) + 7\, ind_2 x \equiv ind_2 9 \bmod 18$

$\Leftrightarrow ind_2 3 + ind_2 5 + 7\, ind_2 x \equiv ind_2 9 \bmod 18$

$\Leftrightarrow 13 + 16 + 7\, ind_2 x \equiv 8 \bmod 18$

$\Leftrightarrow 29 + 7\, ind_2 x \equiv 8 \bmod 18$

$\Leftrightarrow 7\, ind_2 x \equiv 8 - 29 \bmod 18$

$\Leftrightarrow 7\, ind_2 x \equiv -21 \bmod 18$

$\Leftrightarrow 7\, ind_2 x \equiv 15 \bmod 18$

$\Leftrightarrow 7y \equiv 15 \bmod 18$

$\times 5$ $\Leftrightarrow 35y \equiv 75 \bmod 18 \Leftrightarrow -y \equiv 3 \bmod 18$

$\Leftrightarrow ind_2 x \equiv -3 \bmod 18$

$\Leftrightarrow ind_2 x \equiv 15 \bmod 18$

$\Leftrightarrow x \equiv 2^{15} \bmod 18$

$\Leftrightarrow x = 12$ (o índice de 15 é 12)

$\mathbb{Z}_{19}^*$	$ind_2 a$
1	2
2	4
3	8
4	16
5	13
6	7
7	14
8	9
9	18
10	17
11	15
12	11
13	3
14	6
15	12
16	5
17	10
18	1

7. p primo ímpar e $\left(\frac{a}{p}\right) = 1$.

$ind_2 a \bmod p \Rightarrow$ é par em que r é raiz primitiva de p.

Ora, se $\left(\frac{a}{p}\right) = 1$, então a é uma raiz primitiva, logo existe x tal que $x^2 \equiv a \bmod p$

$\Rightarrow r^{ind_r(x^2)} \equiv r^{ind_r a} \bmod \varphi(p)$, em que $\varphi(p) = p-1$

$\Rightarrow 2 * ind_r x \equiv ind_r a \bmod p-1 \Rightarrow 2 * ind_r x + K(p-1) = ind_r a$

- $2 * ind_r x$ é par
- $K(p-1)$ é par pois $p-1$ é par

Então: $2 * ind_r x + K(p-1)$ é par, logo $ind_r a$ é par.

8. $ax^{11} \equiv 2 \bmod 23$

Como 23 é primo ímpar, então $\left(\frac{x}{p}\right) = 1$ ou -1, ou seja, $x^{\frac{23-1}{2}} \equiv 1 \bmod p$ ou $x^{\frac{23-1}{2}} \equiv -1 \bmod p$.

$(\Leftrightarrow) x^{11} \equiv 1 \bmod p \vee x^{11} \equiv -1 \bmod p$

Então,

$a * x^{11} \equiv 2 \bmod 23$

$(\Leftrightarrow) -a \equiv 2 \bmod p \vee a \equiv 2 \bmod p$

Logo, $a = 21 \vee a = 2$.