Exercise 2

(1) (a) $|(\mathbb{Z}/15\mathbb{Z})^\times| = \varphi(15) = \varphi(3\cdot 5) = \varphi(3)\,\varphi(5) = 2\times 4 = \boxed{8}$

(b) $|(\mathbb{Z}/25\mathbb{Z})^\times| = \varphi(25) = \varphi(5^2) = 5^2 - 5 = \boxed{20}$

(c) $|(\mathbb{Z}/100\mathbb{Z})^\times| = \varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\,\varphi(5^2) = (2^2-2)(5^2-5)$
$= \boxed{40}$

(d) $|(\mathbb{Z}/1000\mathbb{Z})^\times| = \varphi(10^3) = \varphi(2^3 5^3) = (2^3-2^2)(5^3-5^2) = \boxed{400}$

(2) $|(\mathbb{Z}/100\mathbb{Z})^\times| = \varphi(100) = 40$. Since $\gcd(3,100)=1$,

$3^{125} = 3^{40\cdot 3+5} \equiv 3^5 \bmod 100 \equiv 243 \bmod 100 \equiv \boxed{43} \bmod 100$

$3^{9999} = 3^{40\cdot 249+39} \equiv 3^{39} \bmod 100 \equiv 3^{-1} \bmod 100$

Euclidean: 100 3 1
33; 3 $\Rightarrow (-33)\times 3 \equiv 1 \bmod 100$

$\Rightarrow \boxed{67}\times 3 \equiv 3^{-1} \equiv 1 \bmod 100$

(3) We'll compute 2^{9999} in $\mathbb{Z}/4\mathbb{Z}$ and in $\mathbb{Z}/25\mathbb{Z}$.

$2^{9999} \equiv 2^{2\cdot 4999+1} \bmod 4 \equiv 4^{4999}\cdot 2 \bmod 4 \equiv 0 \bmod 4$

$\varphi(25) = 20 \Rightarrow 2^{9999} = 2^{20\cdot 499+19} \equiv 2^{19} \bmod 25$

Euclidean: 25 2 1
12; 2 $\Rightarrow (-12)\times 2 \equiv 13\times 2 \equiv 1 \bmod 25$

Therefore, $2^{9999} \equiv 0 \bmod 4$ and $2^{9999} \equiv 13 \bmod 25$.

Now, we'll find x such that $x \equiv 0 \bmod 4$ and $x \equiv 13 \bmod 25$.

$x \equiv 0 \bmod 4 \Rightarrow 4y \equiv 13 \bmod 25$

$$\begin{array}{ccc} 25 & 4 & 1 \\ 6; & 4 & \end{array} \Rightarrow 4 \times (-6) \equiv 1 \bmod 25 \Rightarrow 4 \times 19 \equiv 1 \bmod 25$$

$y \equiv 19 \times 13 \equiv 247 \equiv 22 \bmod 25 \Rightarrow x = 4 \times 22 = \boxed{88}$

(5) $7^{403} \equiv 7^{400+3} \equiv 7^3 \bmod 1000$ since $\varphi(1000) = 400$

$\Rightarrow 7^{403} \equiv 7^3 \bmod 1000 \equiv \boxed{343} \bmod 1000$

(4) $45 = 3^2 \times 5$, $3^{25} = 3^{23} 3^2 \Rightarrow 3^{25} \equiv 0 \bmod 3^2$

$3^{25} \equiv 3^{4 \cdot 6} 3 \bmod 5 \equiv 3 \bmod 5$

Find x: $x \equiv 0 \bmod 9$ and $x \equiv 3 \bmod 5 \Rightarrow x = 9y$

$9y \equiv 3 \bmod 5$

Note: $9 \times 4 = 36 \equiv 1 \bmod 5 \Rightarrow y \equiv 4 \times 3 \bmod 5 \equiv 2 \bmod 5$

$\Rightarrow x = 9 \cdot 2 = \boxed{18}$

Exercise 4

(1)

$$
\begin{array}{r}
x^2 - 2x + 4 \\
3x+1 \,\big|\, \overline{3x^3 - 5x^2 + 10x - 3} \\
\underline{-3x^3 - x^2} \\
-6x^2 \\
\underline{+6x^2 + 2x} \\
12x \\
\underline{-12x - 4} \\
-7
\end{array}
$$

$$\Rightarrow \boxed{\begin{array}{l} q(x) = x^2 - 2x + 4 \\ r(x) = -7. \end{array}}$$

(2) $b(x) = x^8 + x^7 + x^5 + x^3 + x^2 + 1$

$a(x) = x^5 + x^4 + x^3 + 2x^2 + 1$ $\qquad q_0(x) = x^3 - x$ $\qquad x^3 - x + \frac{1}{x-1}$

$r_0(x) = x^4 + 2x^3 + x^2 + x + 1$ $\qquad q_1(x) = x - 1 \quad \rightarrow \quad \frac{1}{x-1}$

$r_1(x) = 2x^3 + 2x^2 + 2$ $\qquad q_2(x) = \frac{1}{2}x + \frac{1}{2}$

$r_2(x) = 0$

gcd

$$x^3 - x + \frac{1}{x-1} = \frac{x^4 - x^3 - x^2 + x + 1}{x-1} \Rightarrow a(x)\overbrace{(x^4 - x^3 - x^2 + x + 1)}^{s(x)} + b(x)\overbrace{[-(x-1)]}^{t(x)}$$

$$= \gcd[a(x), b(x)]$$

(3) Since $a(x) - b(x) = 1$, we automatically get

$s(x) = 1$ and $t(x) = -1$.

$\gcd[a(x), b(x)] = 1$; no need for Euclidean.