f) $5x \equiv 7 \mod 8$

Exo 10

1) $(7777)^{7777} \equiv (7)^{7777 \pmod{10}} \pmod{10}$

$7^2 \equiv 49 \equiv -1 \pmod{10}$

$7^4 \equiv (-1)^2 \equiv 1 \pmod{10}$

$7777 = 4 \times 1944 + 1$

$(7)^{7777} \equiv (7)^{4 \times 1944 + 1} \equiv (7^4)^{1944} \times 7 \equiv (1)^{1944} \times 7 \equiv 7 \pmod{10}$

2) $900^{200} \mod 13$

$900 = 69 \times 13 + 3$

donc $900^{200} \equiv 3^{200} \mod 13$

$3^2 \equiv 9 \mod 13$

$3^3 \equiv 1 \mod 13$

$200 = 3 \times 66 + 2$

$(900)^{200} \equiv 3^{200} \equiv 3^{3 \times 66 + 2} \equiv (3^3)^{66} \times 3^2 \equiv 1^{66} \times 3^2 \equiv 9 \pmod{13}$

$(101)^{(102^{103})} \mod 13$

$101 = 7 \times 13 + 10$

$(101)^{(102^{103})} \equiv (10)^{(102^{103})} \pmod{13}$

$10^2 \equiv 9 \pmod{13}$

$10^3 \equiv 9 \times 10 \pmod{13}$
$\equiv -1 \pmod{13}$

$10^6 \equiv (-1)^2 \equiv 1 \pmod{13}$

On cherche $(102)^{103} \mod 6$

$102 = 6 \times 17$

donc $(102)^{103} \equiv 0^{103} \equiv 0 \mod 6$

donc $(101)^{(102^{103})} \equiv 10^{(102^{103})} \pmod{13}$
$\equiv 0 \pmod{13}$

3) $31^{(32^{33})} \mod 7$

$31 = 4 \times 7 + 3$

$31^{(32^{33})} \equiv 3^{(32^{33})} \mod 7$

$3^2 \equiv 2 \mod 7$

$3^3 \equiv -1 \mod 7$

$3^6 \equiv 1 \mod 7$

$32^{33} \equiv (2^5)^{33} \equiv 2^{5 \times 33} \mod 6$

$2^2 \equiv -2 \mod 6$

$2^3 \equiv 2 \mod 6$

Affirmons $2^{2n} \equiv -2 \mod 6$ $\quad P(n)$ $\qquad 2^{n-1} \equiv 2 \mod 6$ $\quad Q(n)$

Par récurrence :

$2^{2\times 1} \equiv 2^2 \equiv -2 \mod 6 \rightarrow P(1)$

$2^{2\times 1 - 1} \equiv 2^1 \equiv 2 \mod 6 \rightarrow Q1$

Hérédité : Soit $n \geq 1$

On suppose $P(n)$ et $Q(n)$ vrai

On a : $2^{2(n+1)} \equiv 2^{2n} \times 2^2 \equiv (-2)(-2) \equiv -2 \mod 6$ $\quad P(n+1)$

$2^{2(n+1)-1} \equiv 2^{2(n-1)} \times 2^2 \equiv 2 \times (-2) \equiv 2 \mod 6$ $\quad Q(n+1)$

Par récurrence, $P(n)$ et $Q(n)$ sont vraies $\forall n \geq 1$

donc $2^{5 \times 3^3} \equiv 2 \mod 6$ donc $(31)^{(32^{33})} \equiv 3^{(32^{33})}$

$\equiv 3^2 \mod 7$

$\equiv 2 \mod 7$

Exercice 9

1) Rq. $\forall a, b \in \mathbb{R}$, $n \in \mathbb{N}^*$

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$$

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = a\sum_{k=0}^{n-1} a^k b^{n-1-k} - b\sum_{k=0}^{n-1} a^k b^{n-1-k}$$

$$= \sum_{k=0}^{n-1} a^{k+1} b^{n-(k+1)} - \sum_{k=0}^{n-1} a^k b^{n-k}$$

$$= \sum_{k=1}^{n} a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} = a^n - b^n$$

2) $a \geq 2$

Soient $m, n \in \mathbb{N}$

Rq : $a^m - 1 \mid a^n - 1 \iff m \mid n$

$\Leftarrow$ Si $m \mid n$, $\exists l$ tq $n = lm$

$A = a^m \qquad B = 1$

Pour 1) $a^n - 1 = A^l - 1^l = (A-1) \underbrace{\sum_{k=0}^{l-1} A^k}_{\in \mathbb{N}^*}$

donc $a^m - 1 = A - 1 \mid a^n - 1$

$\Rightarrow$ Si $a^m - 1 \mid a^n - 1$

$n = mq + r$ avec $0 \leq r < m$

$a^n - 1 = a^{mq+r} - a^r + a^r - 1$

$= a^r (a^{mq} - 1) + a^r - 1$

par 1) $a^m - 1 \mid a^{mq} - 1$

On en déduit que $a^m - 1 \mid a^r - 1$

Or $r < m$ donc $a^m > a^r$ donc $a^m - 1 > a^r - 1$

donc $a^m - 1 \mid a^r - 1 \Rightarrow a^r - 1 = 0$

donc $r = 0$

3) $(a^n - 1) = a^n - 1^n = (a-1) \left(\sum_{k=0}^{n-1} a^k \right)$

Si $a > 2$ $(a-1) \geq 1$ $(a-1) \mid a^n - 1$

4) Rq si $2^n - 1$ est premier alors n est premier

par contraposée : si $n = pq$ $p > 1$ $q > 1$

alors $\underbrace{2^p - 1}_{\neq 1} \mid 2^n - 1$

par 2) donc $2^n - 1$ pas premier