1 Exercice 1

1.1

$a^{p-1} \equiv 1 \mod p \iff a^{p-2}a \equiv 1 \mod p \iff a^{p-2}$ est l'inverse de a modulo p. Donc a^{p-2} est l'inverse de a modulo p.

1.2

Algorithme 1 Calcul de l'inverse de $a \mod p$ à l'aide de l'exponentiation binaire

Entrées: a, p
Sorties: $a^{p-2} \mod p$

$e \leftarrow p - 2$
$m \leftarrow p$
$r \leftarrow 1$
Tant que $e \neq 0$ **Faire**
  Si $e \equiv 1 \mod 2$ **Alors**
    $r \leftarrow r \times m$
  Fin si
  $m \leftarrow m^2$
  $e \leftarrow \lfloor \frac{e}{2} \rfloor$
Fin tant que
Retourner r

1.3

- $\lfloor \log_2(p-2) \rfloor + 1$ mises au carré modulo dans $\mathbb{Z}/p\mathbb{Z}$
- Au maximum $\lfloor \log_2(p-2) \rfloor + 1$ multiplications dans $\mathbb{Z}/p\mathbb{Z}$
- Les modulos et divisions par 2 sont négligeables.

On a donc une complexité algébrique de $2\lfloor \log_2(p-2) \rfloor + 2 \simeq O(\log(p))$

1.4

L'algorithme d'Euclide étendu appliqué à a et p renvoie $pgcd(a, p)$, u, v tels que $au + bp \equiv pgcd(a, p)$ or p est premier donc $pgcd(a, p) = 1$ on a donc : $au + bp \equiv pgcd(a, p) \Rightarrow au \equiv 1 \mod p \iff u$ est l'inverse de a modulo p.

L'algorithme d'Euclide étendu a une complexité algébrique de $O(\log(p)^2)$.

Il existe un algorithme calculant la relation de Bezout (sans le pgcd donc, qui ne sert à rien car nécessairement égal à 1 sauf pour $a = 0$) qui a une complexité algébrique de $\tilde{O}(p)$.

2 Exercice 2

2.1

2.1.1

Soit $N = \prod_{i \in \{1,..,n\}} p_i^{(e_i)}$ avec p_i premiers et $p_i \equiv 1 \mod p^e$, tout diviseurs d de N s'écrit comme produit de puissances de p_i et on a alors :
$d = \prod_{j \in Dec \subset \{1,..,n\}, i \leq e_j} p_j^i \Rightarrow d \equiv \prod_{j \in Dec \subset \{1,..,n\}, i \leq e_j} 1^i \mod p^e \Rightarrow d \equiv 1 \mod p^e$
Il suffit donc de démontrer l'assertion pour d premier.

2.1.2

$a^{N-1} \equiv 1 \mod N \Rightarrow a^{N-1} \equiv 1 \mod d$ (car d divise N), et o le plus petit exposant de a tel que $a^o \equiv 1 \mod d$ donc $o | N-1$

Supposons $o | \frac{N-1}{p}$ on a alors :
$a^{\frac{N-1}{p}} \equiv 1 \mod d \Rightarrow a^{\frac{N-1}{p}} - 1 \equiv 0 \mod d \Rightarrow a^{\frac{N-1}{p}} - 1 = kd$ avec $k \in \mathbb{Z}$.
On a alors $pgcd(a^{\frac{N-1}{p}} - 1, N) \geq d > 1$ ce qui contredis l'hypothèse de départ : $pgcd(a^{\frac{N-1}{p}} - 1, N) = 1$
on a donc bien $o \nmid \frac{N-1}{p}$

2.1.3

Les seuls diviseurs de $N-1$ qui ne divisent pas $\frac{N-1}{p}$ sont de la forme $d \times p^e$ avec $d = \prod_{j \in Dec \subset \{1,..,n\}, i \leq e_j, p_j \neq p} p_j^i$, donc p^e divise o.
$p^e | o, o | d-1 \Rightarrow p^e | d-1 \Rightarrow d = k \times p^e + 1, k \in \mathbb{Z} \Rightarrow d \equiv 1 \mod p^e$

3

3.0.4

$\forall p | F$, p premier on pose $e_{N-1} = v_p(N-1), e_F = v_p(F)$ comme $F | N-1$, on a nécessairement $e_F \leq e_{N-1}$ et donc :

$d \equiv 1 \mod p^{e_{N-1}} \Rightarrow d = 1 + k \times p^{e_{N-1}}$, $k \in \mathbb{Z} \Rightarrow d = 1 + k' \times p^{e_F} \Rightarrow d \equiv 1 \mod p^{e_F}$
D'après le lemme chinois, il existe un unique $d \mod F$ tel que $d \equiv 1 \mod p^{e_F}$, $\forall p|F$, p premier. 1 convient et est donc l'unique solution. On a donc bien $d \equiv 1 \mod F$.

3.0.5

$d \equiv 1 \mod F$ et $d > 1$ donc $d \geq F + 1 \geq \sqrt{N} + 1$, on a bien $d > sqrtN$. Tout les diviseurs de N strictement supérieur à 1 sont supérieurs à $\sqrt{N}$ donc le seul diviseur de N supérieur à 1 est N donc N est premier.

3.1

Tous les éléments a de $\mathbb{Z}$ vérifient $a^{N-1} \equiv 1 \mod N$ si N premier.
$pgcd(a^{\frac{N-1}{p}} - 1, N) = 1 \iff a$ est d'ordre $N-1$, il y a $\phi(N-1)$ éléments de $\mathbb{Z}/N\mathbb{Z}$ d'ordre $N-1$ (si je me goure pas ...), la probabilité de trouver un a tel que a vérifie la propriété 1 est donc de $\frac{1}{\phi(N-1)}$.

4 Problème