CONCOURS GÉNÉRAL 2005
Exercice 4
Corrigé détaillé

Samuel Rochetin

Vendredi 23 décembre 2016

Résumé

Ce problème traite du logarithme discret, utilisé en cryptologie. Les techniques d'arithmétique sont classiques et proches du cours de spécialité mathématiques. Les deux dernières questions, indépendantes des autres, se démarquent clairement par leur difficulté et pourraient constituer un exercice à elles seules. Enfin, signalons que les notations du sujet sont inutilement compliquées.

I – Définition du logarithme discret

1. En procédant comme dans les exemples, nous trouvons que $\boxed{\text{les racines primitives modulo 7 sont 3 et 5.}}$

2. (a) Posons $E := \left\{\left(g^k \pmod p\right), k \in [\![0; p-2]\!]\right\}$. Tout d'abord, puisque g est une racine primitive modulo p, nous avons l'inclusion $E \subset \left\{\left(g^k \pmod p\right), k \in \mathbb{N}\right\} = [\![1; p-1]\!]$. Pour montrer que cette inclusion est une égalité, il suffit de montrer que l'ensemble E contient $p-1$ éléments. Supposons que ce n'est pas le cas. Alors il existe $(i,j) \in [\![0; p-2]\!]^2$ tel que $i > j$ et $g^i = g^j \pmod p$. Donc $g^j\left(g^{i-j}-1\right) = 0 \pmod p$, c'est-à-dire p divise $g^j\left(g^{i-j}-1\right)$. Or, $0 < g < p$ et p est premier donc p et g sont premiers entre eux, donc d'après le théorème de Gauss, p divise $g^{i-j}-1$, c'est-à-dire $g^{i-j} = 1 \pmod p$, où $i-j \in [\![1; p-2]\!]$. Soit $k \in \mathbb{N}$. Posons $b := i-j$ et considérons la division euclidienne de k par b : il existe $(q,r) \in \mathbb{N}^2$ tel que $k = bq + r$ et $0 \leq r \leq b-1$. Donc $g^k = \left(g^b\right)^q g^r = g^r \pmod p$. Or, $0 \leq r \leq b-1 \leq p-3$ donc l'ensemble $\left\{\left(g^k \pmod p\right), k \in \mathbb{N}\right\}$ contient au plus $p-2$ éléments. Contradiction. Donc $\boxed{\left\{\left(g^k \pmod p\right), k \in [\![0; p-2]\!]\right\} = [\![1; p-1]\!].}$

   (b) D'après la question précédente, les ensembles $\left\{\left(g^k \pmod p\right), k \in [\![0; p-2]\!]\right\}$ et $[\![1; p-1]\!]$ ont le même cardinal fini non nul, ils sont donc en bijection. Autrement dit, pour tout $A \in [\![1; p-1]\!]$, il existe un unique entier $a \in [\![0; p-2]\!]$ tel que $A = (g^a \pmod p)$.

   (c) Supposons $b \geq a$. Puisque $b = a \pmod{(p-1)}$, il existe $k \in \mathbb{N}$ tel que $b - a = k(p-1)$. Donc $g^{b-a} = \left(g^{p-1}\right)^k \pmod p$. Or, p est premier et ne divise pas g, donc d'après le petit théorème de Fermat, $g^{p-1} = 1 \pmod p$, donc $g^{b-a} = 1 \pmod p$. En multipliant par g^a, il vient $\boxed{\left(g^b \pmod p\right) = (g^a \pmod p).}$ De même si $a \geq b$.

3. (a) entrer p, g, A
   $\ell := 0$
   $k := 0$
   tant que $\left(g^k \pmod p\right) \neq A$
   $k := k + 1$
   $\ell := k$
   fin tant que
   afficher ℓ

   (b) Nous trouvons $\boxed{\ell(40) = 18.}$

II – Calcul du logarithme discret par la méthode d'Adleman

1. $2 = \left(55^{60} \pmod{113}\right)$ et $3 = \left(55^5 \pmod{113}\right)$ donc $54 = 2 \times 3^3 = 55^{60}\left(55^5\right)^3 = 55^{75} \pmod{113}$) donc $\boxed{\ell(54) = 75.}$

2. Nous voulons montrer la réciproque de la question I 2. (c). Commençons par montrer que si $(a,b) \in \mathbb{N}^2$ est tel que $a \geq b$ et $g^a = g^b \pmod p$, alors $g^{a-b} = 1 \pmod p$. Nous avons $g^a = g^b \pmod p$ si et seulement si $g^b\left(g^{a-b}-1\right) = 0 \pmod p$, c'est-à-dire si et seulement si p divise $g^b\left(g^{a-b}-1\right)$. Or, $0 < g < p$ et p est premier donc p et g sont premiers entre eux, donc d'après le théorème de Gauss, p divise $g^{a-b}-1$, c'est-à-dire $g^{a-b} = 1 \pmod p$. Ensuite, montrons que si $x \in \mathbb{N}$ est tel

que $g^x = 1 \pmod p$, alors $p-1$ divise x. Effectuons la division de x par $p-1$: il existe $(q,r) \in \mathbb{N}^2$ tel que $x = (p-1)q + r$ et $0 \leq r \leq p-2$. Donc $1 = g^x = \left(g^{p-1}\right)^q g^r = g^r \pmod p$, en utilisant le petit théorème de Fermat comme à la question 2. (c). Or, d'après la question I 2. (a), $\{(g^r \pmod p), r \in [\![0; p-2]\!]\} = [\![1; p-1]\!]$ et $g^0 = 1 \pmod p$, donc $r = 0$. Donc $x = (p-1)q$, donc $p-1$ divise x. Enfin, précisons que $p-1$ divise $a-b$ si et seulement si $p-1$ divise $b-a$, ce qui règle le cas où $a \leq b$. Conclusion : si $g^a = g^b \pmod p$, alors $p-1$ divise $a-b$. Pour répondre à la question, il suffit donc de montrer que pour tout $i \in [\![1; n]\!], g^{a_i} = g^{e_{i,1}\ell(p_1)+\cdots+e_{i,n}\ell(p_n)} \pmod p$. Or, pour tout $k \in [\![1; n]\!], 1 < p_k < p$, donc par définition du logarithme discret, $\left(g^{\ell(p_k)} \pmod p\right) = p_k$. Donc $g^{\ell(p_k)} = p_k \pmod p$, donc $g^{e_{i,k}\ell(p_k)} = p_k^{e_{i,k}} \pmod p$, donc $g^{e_{i,1}\ell(p_1)} \dots g^{e_{i,n}\ell(p_n)} = p_1^{e_{i,1}} \dots p_n^{e_{i,n}} \pmod p$, donc nous avons bien $g^{e_{i,1}\ell(p_1)+\cdots+e_{i,n}\ell(p_n)} = g^{a_i} \pmod p$. D'après ce qui vient d'être vu, nous avons donc $\boxed{a_i = e_{i,1}\ell(p_1) + \cdots + e_{i,n}\ell(p_n) \pmod{(p-1)}.}$

Remarque : nous avons obtenu une relation logarithmique classique de transformation des produits en sommes puisque $a_i = \ell\left(p_1^{e_{i,1}} \dots p_n^{e_{i,n}}\right) = e_{i,1}\ell(p_1) + \cdots + e_{i,n}\ell(p_n) \pmod{(p-1)}$. Par ailleurs, soulignons que l'indexation par i est inutile dans tout le problème et ne fait que compliquer inutilement la notation.

3. (a) $g^1 = 20 \pmod{53}$ donc $\ell(20) = 1$. Or, $20 = 2^2 \times 5$, donc d'après la question précédente, $2\ell(2) + \ell(5) = 1 \pmod{52}$. De même, $g^3 = 50 \pmod{53}$ et $50 = 2 \times 5^2$ donc $\ell(2) + 2\ell(5) = 3 \pmod{52}$. Nous obtenons donc le système :
$$\begin{cases} 2\ell(2) + \ell(5) = 1 \pmod{52} \\ \ell(2) + 2\ell(5) = 3 \pmod{52} \end{cases}$$
$2L_1 - L_2$ donne $3\ell(2) = 51 \pmod{52}$, c'est-à-dire $3(\ell(2) - 17) = 0 \pmod{52}$. Or, 52 et 3 sont premiers entre eux donc d'après le théorème de Gauss et puisque $17 \in [\![0; 51]\!]$, $\boxed{\ell(2) = 17}$, donc en réinjectant dans L_1, il vient $\boxed{\ell(5) = 19.}$

Remarque : sans l'astuce $51 = 3 \times 17$, nous aurions dû chercher un inverse de 3 modulo 52. Un tel inverse existe car 3 et 52 sont premiers entre eux, donc d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $3u + 52v = 1$, donc $3u \equiv 1 \pmod{52}$, et l'algorithme d'Euclide permet de déterminer une solution particulière (u_0, v_0).

(b) $\ell(40) = \ell\left(2^3 \times 5\right) = 3\ell(2) + \ell(5) = 70 = 18 \pmod{52}$. Donc $\boxed{\ell(40) = 18}$, comme vu à la question I 3. (b).

(c) Si $2^\alpha 5^\beta \in [\![1; 52]\!]$, avec α et β entiers naturels, puisque $5^3 = 125$, nous avons nécessairement $0 \leq \beta \leq 2$. Réciproquement, si $\beta = 2$, alors $0 \leq \alpha \leq 1$, si $\beta = 1$, alors $0 \leq \alpha \leq 3$ et si $\beta = 0$, alors $0 \leq \alpha \leq 5$. Il y a donc $2 + 4 + 6 = \boxed{12 \text{ entiers}}$ de $[\![1; 52]\!]$ pouvant s'écrire sous la forme $2^\alpha 5^\beta$, avec α et β entiers naturels.
Remarque : la connaissance des logarithmes de 2 et 5 permet donc de déterminer les logarithmes de 10 autres entiers de $[\![1; 52]\!]$.

4. (a) Par définition du reste de la division euclidienne par p, l'ensemble des $(g^s A \pmod p)$, pour $s \in [\![0; p-2]\!]$, est inclus dans $[\![0; p-1]\!]$. Or, p est premier avec g^s et premier avec A, donc par contraposée du lemme d'Euclide, p ne divise pas $g^s A$ donc $(g^s A \pmod p)$ ne peut pas prendre la valeur 0. Ainsi, les $p-1$ valeurs de $(g^s A \pmod p)$ sont bien dans $[\![1; p-1]\!]$. Il reste à montrer qu'elles sont distinctes. Supposons qu'elles ne le sont pas. Alors il existe $(i, j) \in [\![0; p-2]\!]^2$ tel que $i \neq j$ et $g^i A = g^j A \pmod p$. Donc $\left(g^i - g^j\right) A = 0 \pmod p$. Or, p et A sont premiers entre eux, donc d'après le théorème de Gauss, p divise $g^i - g^j$, c'est-à-dire $g^i = g^j \pmod p$. D'après la question I 2. (a), nous savons que cela signifie que $i = j$. Contradiction. Donc $\boxed{\text{l'ensemble des } (g^s A \pmod p), \text{ pour } s \in [\![0; p-2]\!], \text{ est } [\![1; p-1]\!].}$

Remarque : ce résultat permet de faire l'hypothèse de la question suivante, c'est-à-dire qu'il existe un entier naturel s tel que $(g^s A \pmod p)$ se factorise à l'aide de $p_1, \dots, p_n$ uniquement.

(b) $A \in [\![1; p-1]\!]$, donc $\left(g^{\ell(A)} \pmod p\right) = A$, donc $A = g^{\ell(A)} \pmod p$ et $g^s A = g^{s+\ell(A)} \pmod p$ en multipliant par g^s, donc nous avons $(g^s A \pmod p) = \left(g^{s+\ell(A)} \pmod p\right)$. Donc, par hypothèse, il existe n entiers naturels $e_1, \dots, e_n$ tels que $\left(g^{s+\ell(A)} \pmod p\right) = p_1^{e_1} \dots p_n^{e_n}$, donc la question II 2. donne $\boxed{\ell(A) = e_1\ell(p_1) + \cdots + e_n\ell(p_n) - s \pmod{(p-1)}.}$

(c) Nous connaissons $\ell(2)$ et $\ell(5)$, donc il suffit de trouver un entier s tel que $(20^s \times 30 \pmod{53})$ soit un entier de $[\![1; 52]\!]$ s'écrivant sous la forme $2^\alpha 5^\beta$, avec α et β entiers naturels. Pour $s = 3$, nous avons $20^3 \times 30 = 16 = 2^4 \pmod{53}$. En posant $A := 30, s := 3, p_1 := 2$, nous avons $(g^s \times A \pmod p) = p_1^4$, donc d'après la question précédente et la question II 3. (a), $\ell(30) = 4\ell(2) - 3 = 65 = 13 \pmod{52}$. Donc $\boxed{\ell(30) = 13.}$

5. *Dans les questions suivantes, nous utiliserons à plusieurs reprises la croissance du logarithme népérien sans le préciser. Par ailleurs, les logarithmes considérés seront positifs ou strictement positifs, puisque tout nombre premier est strictement supérieur à 1.*

(a) Soit α le plus grand entier naturel tel que $p_1^\alpha \leq p-1$. Nous avons donc $\alpha \leq \dfrac{\ln(p-1)}{\ln p_1}$. Or, α est entier, donc $0 \leq \alpha \leq \left\lfloor \dfrac{\ln(p-1)}{\ln p_1} \right\rfloor$. Réciproquement, soit un entier naturel α tel que $0 \leq \alpha \leq \left\lfloor \dfrac{\ln(p-1)}{\ln p_1} \right\rfloor$. Pour tout réel x, nous avons $\lfloor x \rfloor \leq x$, donc $\alpha \leq \dfrac{\ln(p-1)}{\ln p_1}$, donc $p_1^\alpha \leq p-1$. L'ensemble des entiers naturels α tels que $p_1^\alpha \leq p-1$ est donc $\left\{0, \dots, \left\lfloor \dfrac{\ln(p-1)}{\ln p_1} \right\rfloor\right\}$. Donc il y a $\boxed{\left\lfloor \dfrac{\ln(p-1)}{\ln p_1} \right\rfloor + 1 \text{ entiers de } [\![1; p-1]\!] \text{ qui sont une puissance de } p_1.}$

(b) D'après la question II 4. (a), l'ensemble des $(g^s A \pmod p)$, pour $s \in [\![0; p-2]\!]$, est $[\![1; p-1]\!]$, donc la probabilité qu'un entier $s \in [\![0; p-2]\!]$ soit tel que $(g^s A \pmod p)$ soit une puissance de p_1 est égal au nombre de puissances de p_1 dans $[\![1; p-1]\!]$, divisé par le nombre d'entiers dans $[\![1; p-1]\!]$, c'est-à-dire $\boxed{\dfrac{1}{p-1}\left(\left\lfloor \dfrac{\ln(p-1)}{\ln p_1}\right\rfloor + 1\right).}$

(c) Essayons de généraliser la question II 3. (c) et cherchons le nombre N d'entiers de $[\![1; p-1]\!]$ pouvant s'écrire sous la forme $p_1^\alpha p_2^\beta$, avec α et β entiers naturels. Posons $m := \left\lfloor \dfrac{\ln(p-1)}{\ln p_2}\right\rfloor$. D'après la question II 5. (a), m est la plus grande puissance de p_2 dans $[\![1; p-1]\!]$. Soit $i \in [\![0; m]\!]$ fixé. Combien existe-t-il d'entiers naturels α tels que $p_1^\alpha p_2^i \in [\![1; p-1]\!]$, c'est-à-dire tels que $p_1^\alpha \leq \ln\left(\dfrac{p-1}{p_2^i}\right)$? La méthode de la question II 5. (a) permet de conclure qu'il en existe $\left\lfloor \dfrac{\ln\left(\dfrac{p-1}{p_2^i}\right)}{\ln p_1}\right\rfloor + 1$. Puisque i peut prendre chaque valeur de $[\![0; m]\!]$, nous avons $N = \displaystyle\sum_{i=0}^{m}\left(\left\lfloor \frac{\ln\left(\frac{p-1}{p_2^i}\right)}{\ln p_1}\right\rfloor + 1\right)$. Commençons par minorer N. Pour tout réel x, nous avons $\lfloor x\rfloor + 1 > x$, donc $N > \displaystyle\sum_{i=0}^{m}\frac{\ln\left(\frac{p-1}{p_2^i}\right)}{\ln p_1} = \frac{1}{\ln p_1}\sum_{i=0}^{m}\ln\left(\frac{p-1}{p_2^i}\right) = \frac{1}{\ln p_1}\ln\left(\frac{(p-1)^{m+1}}{p_2^{0+1+\cdots+m}}\right) = \frac{1}{\ln p_1}\ln\left(\frac{(p-1)^{m+1}}{p_2^{\frac{m(m+1)}{2}}}\right) = \frac{1}{\ln p_1}\ln\left((p-1)^{\frac{m+1}{2}} \times \frac{(p-1)^{\frac{m+1}{2}}}{p_2^{\frac{m(m+1)}{2}}}\right)$. Par définition de m, nous avons d'une part, $p-1 \geq p_2^m$ donc $(p-1)^{\frac{m+1}{2}} \geq p_2^{\frac{m(m+1)}{2}}$ donc $\dfrac{(p-1)^{\frac{m+1}{2}}}{p_2^{\frac{m(m+1)}{2}}} \geq 1$, et d'autre part, $p_2^{m+1} > p-1$ donc $m+1 > \dfrac{\ln(p-1)}{\ln p_2}$. Il vient donc $N > \dfrac{\ln\left((p-1)^{\frac{m+1}{2}}\right)}{\ln p_1} = (m+1)\dfrac{\ln(p-1)}{2\ln p_1} > \dfrac{\ln^2(p-1)}{2\ln p_1 \ln p_2}$. Ensuite, majorons N. Il suffit de chercher la plus grande valeur des termes de la somme : elle est atteinte pour la plus petite valeur de p_2^i, c'est-à-dire pour $1 = p_2^0$, donc nous avons la majoration classique $N \leq (m+1)\left(\left\lfloor \dfrac{\ln(p-1)}{\ln p_1}\right\rfloor + 1\right) = \left(\left\lfloor \dfrac{\ln(p-1)}{\ln p_1}\right\rfloor + 1\right)\left(\left\lfloor \dfrac{\ln(p-1)}{\ln p_2}\right\rfloor + 1\right) \leq \left(\dfrac{\ln(p-1)}{\ln p_1} + 1\right)\left(\dfrac{\ln(p-1)}{\ln p_2} + 1\right)$. Puisque la probabilité P cherchée vaut $P = \dfrac{N}{p-1}$, nous avons $\boxed{\dfrac{\ln^2(p-1)}{2(p-1)\ln p_1 \ln p_2} \leq P \leq \dfrac{1}{p-1}\left(\dfrac{\ln(p-1)}{\ln p_1} + 1\right)\left(\dfrac{\ln(p-1)}{\ln p_2} + 1\right).}$

Remarque : la majoration de N peut aussi s'obtenir directement avec un raisonnement combinatoire. Soit α le plus grand entier naturel tel que $p_1^\alpha \leq p-1$ et β le plus grand entier naturel tel que $p_2^\beta \leq p-1$. Tout entier de $[\![1; p-1]\!]$ s'écrivant $p_1^a p_2^b$, avec a et b entiers naturels, vérifie nécessairement $0 \leq a \leq \alpha = \left\lfloor \dfrac{\ln(p-1)}{\ln p_1}\right\rfloor$ et $0 \leq b \leq \beta = \left\lfloor \dfrac{\ln(p-1)}{\ln p_2}\right\rfloor$. En effet, si $a > \alpha$, alors, par définition de α et puisque $p_2^b \geq 1$, il vient $p_1^a p_2^b \geq p_1^a \geq p_1^{\alpha+1} > p-1$, ce qui est impossible. Même raisonnement si $b > \beta$. Il y a donc au plus $\left(\left\lfloor \dfrac{\ln(p-1)}{\ln p_1}\right\rfloor + 1\right)\left(\left\lfloor \dfrac{\ln(p-1)}{\ln p_2}\right\rfloor + 1\right)$ entiers de $[\![1; p-1]\!]$ s'écrivant $p_1^a p_2^b$.

(d) La majoration est immédiate à généraliser. En revanche, la minoration, déjà technique avec deux nombres premiers, est délicate à généraliser. En effet, le 2 au dénominateur peut se généraliser de plusieurs façons : n, 2^n ou $n!$. L'aspect multiplicatif de la minoration nous oriente plutôt vers 2^n ou $n!$, et la puissance du logarithme nous rappelle les expressions de la forme $\dfrac{x^n}{n!}$. Commençons par traiter le cas $n = 3$. Soit N le nombre d'entiers de $[\![1; p-1]\!]$ pouvant s'écrire sous la forme $p_1^i p_2^j p_3^k$, avec i, j, k des entiers naturels. Posons $m := \left\lfloor \dfrac{\ln(p-1)}{\ln p_3}\right\rfloor$. Soit $k \in [\![0; m]\!]$. Soit N_k le nombre de couples d'entiers naturels (i, j) tels que $p_1^i p_2^j p_3^k \leq p-1$. Puisque cette inégalité est équivalente à $p_1^i p_2^j \leq \dfrac{p-1}{p_3^k}$, d'après la question précédente, en posant $u_k := \dfrac{p-1}{p_3^k}$, nous avons $N_k \geq \dfrac{\ln^2(u_k)}{2\ln p_1 \ln p_2}$. Précisons que changer $p-1$ en u_k pour appliquer la minoration de la question précédente est licite parce que le fait que $p-1$ soit un entier et le fait que p soit premier n'intervenaient pas dans la preuve de la minoration. Nous avons donc $N = \displaystyle\sum_{k=0}^{m} N_k \geq \frac{1}{2\ln p_1 \ln p_2}\sum_{k=0}^{m}\ln^2(u_k)$. Le carré empêche cette fois de transformer la somme en produit, donc nous poursuivons la minoration à l'aide d'une comparaison série-intégrale. Posons $f : t \mapsto \ln\left(\dfrac{p-1}{p_3^t}\right)$. Nous avons donc $f(k) = \ln^2(u_k)$. La fonction f est décroissante et continue sur $\mathbb{R}^+$, donc pour tout $k \in [\![0; m]\!]$, nous avons $f(k) \geq \displaystyle\int_k^{k+1} f(t)\,\mathrm{d}t$. Cette intégrale se calcule simplement car $f(t) = v^2(t)$, avec $v(t) = \ln\left(\dfrac{p-1}{p_3^t}\right)$, donc $v'(t) = -\ln p_3$, et

nous savons qu'une primitive de $v'(t)v^2(t)$ est $\dfrac{v^3(t)}{3}$. D'où $\int\limits_k^{k+1} f(t)\,\mathrm{d}t = \dfrac{1}{3\ln p_3}\left(\ln^3 u_k - \ln^3 u_{k+1}\right)$. En reconnaissant une somme télescopique, il vient donc $\sum\limits_{k=0}^{m} \ln^2(u_k) = \sum\limits_{k=0}^{m} f(k) \geq \sum\limits_{k=0}^{m} \int\limits_k^{k+1} f(t)\,\mathrm{d}t = \dfrac{1}{3\ln p_3}\sum\limits_{k=0}^{m}\left(\ln^3 u_k - \ln^3 u_{k+1}\right) = \dfrac{1}{3\ln p_3}\left(\ln^3 u_0 - \ln^3 u_{m+1}\right) = \dfrac{\ln^3(p-1)}{3\ln p_3} - \dfrac{1}{3\ln p_3}\ln\left(\dfrac{p-1}{p_3^{m+1}}\right)$. Or, par définition de m, nous avons $p-1 < p_3^{m+1}$ donc $-\ln\left(\dfrac{p-1}{p_3^{m+1}}\right) > 0$, donc $\sum\limits_{k=0}^{m} \ln^2(u_k) > \dfrac{\ln^3(p-1)}{3\ln p_3}$. Nous avons donc $N \geq \dfrac{\ln^3(p-1)}{3\times 2\times \ln p_1 \ln p_2 \ln p_3}$. Nous en déduisons que la minoration se généralise par $\dfrac{\ln^n(p-1)}{n!\ln p_1 \ldots \ln p_n}$. Prouvons-le par récurrence sur n. Initialisation : le cas $n=1$ se déduit de la question II 5. (a) et de la minoration $\lfloor x \rfloor + 1 > x$, valable pour tout réel x. Hérédité : soit N le nombre d'entiers de $[\![1; p-1]\!]$ se factorisant à l'aide de $n+1$ nombres premiers distincts uniquement. Supposons que le nombre d'entiers de $[\![1; p-1]\!]$ se factorisant à l'aide de n nombres premiers distincts $p_1, \ldots, p_n$ uniquement soit supérieur à $\dfrac{\ln^n(p-1)}{n!\ln p_1 \ldots \ln p_n}$. Soit p_{n+1} un nombre premier distinct de $p_1, \ldots, p_n$. Posons $m := \left\lfloor \dfrac{\ln(p-1)}{\ln p_{n+1}} \right\rfloor$. Soit $k \in [\![0; m]\!]$. Soit N_k le nombre d'entiers de $[\![1; p-1]\!]$ s'écrivant sous la forme $p_{n+1}^k X$, où X se factorise à l'aide de $p_1, \ldots, p_n$ uniquement. En posant $u_k := \dfrac{p-1}{p_{n+1}^k}$, par hypothèse de récurrence, nous avons $N_k \geq \dfrac{\ln^n(u_k)}{n!\ln p_1 \ldots \ln p_n}$. Donc $N = \sum\limits_{k=0}^{m} N_k \geq \dfrac{1}{n!\ln p_1 \ldots \ln p_n}\sum\limits_{k=0}^{m} \ln^n(u_k)$. En minorant $\sum\limits_{k=0}^{m} \ln^n(u_k)$ avec une comparaison série-intégrale comme ci-dessus, nous obtenons $\sum\limits_{k=0}^{m} \ln^n(u_k) \geq \dfrac{1}{(n+1)\ln p_{n+1}}\sum\limits_{k=0}^{m}\left(\ln^{n+1} u_k - \ln^{n+1} u_{k+1}\right) = \dfrac{1}{(n+1)\ln p_{n+1}}\left(\ln^{n+1} u_0 - \ln^{n+1} u_{m+1}\right) = \dfrac{\ln^{n+1}(p-1)}{(n+1)\ln p_{n+1}} - \dfrac{1}{(n+1)\ln p_{n+1}}\ln\left(\dfrac{p-1}{p_{n+1}^{m+1}}\right)$. De même que précédemment, la définition de m mène à $-\ln\left(\dfrac{p-1}{p_{n+1}^{m+1}}\right) > 0$, donc $\sum\limits_{k=0}^{m} \ln^n(u_k) > \dfrac{\ln^{n+1}(p-1)}{(n+1)\ln p_{n+1}}$, ce qui donne bien $N \geq \dfrac{\ln^{n+1}(p-1)}{(n+1)!\ln p_1 \ldots \ln p_{n+1}}$. La probabilité P cherchée vérifie donc :

$$\boxed{\frac{\ln^n(p-1)}{n!(p-1)\ln p_1 \ldots \ln p_n} \leq P \leq \frac{1}{p-1}\left(\frac{\ln(p-1)}{\ln p_1}+1\right)\cdots\left(\frac{\ln(p-1)}{\ln p_n}+1\right).}$$

Remarque : interprétons ce résultat. Soient p un nombre premier et g une racine primitive modulo p. Supposons que nous connaissions les logarithmes (de base g modulo p) de n nombres premiers distincts $p_1, \ldots, p_n$ strictement inférieurs à p. Supposons que nous cherchions le logarithme d'un entier $A \in [\![1; p-1]\!]$. Nous savons qu'il existe un entier $s \in [\![0; p-2]\!]$ tel que $(g^s A \pmod p)$ se factorise à l'aide de $p_1, \ldots, p_n$ uniquement. Trouver un tel entier s nous permet de calculer le logarithme de A. Cependant, pour tout entier $n \geq 1$, nous avons $\lim\limits_{p\to+\infty} \dfrac{\ln^n(p-1)}{p-1} = 0$ par croissance comparée, donc plus p est grand, plus la probabilité de trouver par hasard un tel entier s est faible.