Département d'Informatique
LICENCE 2ème année
Arithmétique et Cryptographie

Correction : contrôle continu

1 Vrai/Faux

Dire pour chacune des affirmations suivantes si elle est vraie ou fausse en justifiant vos réponses :

1. On a $e \in H \bigcap K$ et si $x, y \in H \cap K$, alors $y' \in H \bigcap K$ et $x \circ y' \in H \bigcap K$. Donc $H \bigcap K$ est un sous-groupe de $(G, \circ)$.

2. Soient $m, n \in \mathbb{Z}$. Si $a = 2 * m + 1$ et $b = 2 * n + 1$, alors $a^2 + b^2 = 4 * (m^2 + n^2 + m + n) + 2$, et donc $a^2 + b^2$ est pair et le reste de la division de $a^2 + b^2$ par 4 est égal à 2.

3. Supposons qu'il existe $p, q \in \mathbb{Z}$ tels que p, q soient premiers entre eux et $\sqrt{3} = \frac{p}{q}$. Donc $p^2 = 3q^2$, et donc 3 divise p, par conséquent $p = 3 * p'$ pour $p' \in \mathbb{N}$, d'où $3 * p'^2 = q^2$, et donc 3 divise q, ce qui est absurde car p et q sont premiers entre eux.

4. a divise $[a; a + 1]$, et donc $[a; a + 1] = a * f$ pour $f \in \mathbb{N}$, et comme $a + 1$ divise $[a; a + 1]$, alors $a + 1$ divise $a * f$, et donc $a + 1$ divise f car a et $a + 1$ sont premiers entre eux, et comme $[a; a + 1] \leq a * (a + 1)$ alors $[a; a + 1] = a * (a + 1)$.

2 PGCD

1. On considère la suite de Fibonacci $(F_n)_{n \geq 0}$ définie par : $F_0 = F_1 = 1$ et pour $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$.

   (a) $F_5 = 8,\ F_7 = 21,\ F_8 = 34,\ F_{11} = 144$ et $F_{13} = 377$.

   (b) Tout D'abord on a :
   $$F_2 F_0 - F_1^2 = 2 - 1 = 1 = (-1)^{1+1}$$
   Supposons que l'on a
   $$F_{n+1} F_{n-1} - F_n^2 = (-1)^{n+1}$$
   Comme
   $$F_{n+2} F_n - F_{n+1}^2 = (F_n + F_{n+1}) F_n - F_{n+1}(F_n + F_{n-1}) = -(F_{n+1} F_{n-1} - F_n^2)$$
   Alors,
   $$F_{n+2} F_n - F_{n+1}^2 = (-1)^{n+2}$$
   Donc pour tout $n \geq 0$, F_n et F_{n+1} sont premiers entre eux.

(c) On a $(13;8) = (8;5) = (5;3) = (3;2) = (2;1) = (1;0) = 1$. Donc $N(13,8) = 4$.
On a $(34;21) = (21;13) = (13;8) = (8;5) = (5;3) = (3;2) = (2;1) = (1;0) = 1$. Donc $N(34,21) = 7$.
On a $(89;55) = (55;34) = (34;21) = (21;13) = (13;8) = (8;5) = (5;3) = (3;2) = (2;1) = (1;0) = 1$. Donc $N(89,55) = 9$.

(d) On a $N(F_2, F_1) = 1$ car $(2;1) = (1;0) = 1$. Supposons que par hypothèse de recurrence que $N(F_n, F_{n-1}) = n-1$ pour un $n \geq 2$. Comme $F_{n+1} = F_n + F_{n-1}$ et $F_{n-1} < F_n$, alors le reste de la division de F_{n+1} par F_n est égal à F_{n-1}. Donc $N(F_{n+1}, F_n) = 1 + N(F_n, F_{n-1}) = 1 + n - 1 = n$.

(e) Effectuons la divion euclidienne de a par b. On a donc $a = q * b + r$ avec $0 \leq r < b$. Comme $a \leq F_{n+1}$ et $F_{n+1} = F_n + F_{n-1}$, alors on a $q * b + r \leq F_n + F_{n-1}$. Deux cas sont alors possibles :

- $q \geq 2$ et on a donc $b \leq F_n$, et par hypothèse de recurrence on a $N(b,r) \leq n-1$, et comme $N(a,b) = 1 + N(b,r)$, alors $N(a,b) \leq n$.

- $q = 1$ et on a donc $b + r < F_n + F_{n-1}$. Si $b \leq F_n$, alors comme $N(a,b) = 1 + N(b,r)$, et par hypothèse de recurrence on a $N(b,r) \leq n-1$, et donc $N(a,b) \leq n$.

  Si $b > F_n$ alors on a nécessairement $r < F_{n-1}$, mais comme $N(a,b) = 1 + N(b,r), N(b,r) = 1 + N(r, b \bmod r)$ et $r < F_{n-1}$, et par hypothèse de recurrence on a $N(b,r) \leq n-2$, alors $N(a,b) \leq n$.
  Comme $F_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}}$ avec $\alpha = \frac{1+\sqrt{5}}{2}$ et $\beta = \frac{1-\sqrt{5}}{2}$.
  Alors $a \leq F_{n+1}$ implique que $a \leq \alpha^{n+2}(\frac{1-(\frac{\alpha}{\beta})^{n+2}}{\sqrt{5}})$. Donc $\ln(a) \leq (n+2)\ln(\alpha) + \ln((\frac{1+(\frac{\alpha}{|\beta|})^{n+2}}{\sqrt{5}}) \leq (n+2)\ln(\alpha) + \ln(\frac{2}{\sqrt{5}})$ car $\frac{\alpha}{|\beta|} < 1$.
  Donc $\ln(a) \leq (n+2)\ln(\alpha)$, ce qui implique que $\log_\alpha(a) \leq n+2$
  et donc $n = \lfloor \log_\alpha(a) \rfloor - 1$ convient.

2. Résoltion dans $\mathbb{Z}$ de l'équation $589x + 817y = 209$.

   Cette équation est équivalente à l'équation $31x + 43y = 11$ où $(43;31) = 1$.
   On a $13 * 31 - 18 * 31 = 1$, et donc $(143, -198)$ est une solution particulière de l'équation.

   Donc $\{(143,-198) + k(43,-31) \mid k \in \mathbb{Z}\}$ est l'ensemble de toutes les solutions de l'équation.