info505 : mathématiques pour l'informatique
TD 3 : un peu d'arithmétique

Pierre Hyvernat
Laboratoire de mathématiques de l'université de Savoie
bâtiment Chablais, bureau 22, poste : 94 22
email : Pierre.Hyvernat@univ-savoie.fr
www : http://www.lama.univ-savoie.fr/~hyvernat/
wiki : http://www.lama.univ-savoie.fr/wiki/

Exercice 1 : définitions du cours

Question 1.
- expliquez pourquoi $0 \setminus n$
- est-ce que $0 \setminus 0$?
- quels sont les multiples de -1 ?
- pourquoi est-ce que $\text{pgcd}(0,0)$ est indéfini

Question 2. Appliquez l'algorithme d'Euclide pour calculer les nombres de Bezout associés à
- $\text{pgcd}(5,9)$
- $\text{pgcd}(8,38)$
- $\text{pgcd}(6,21)$
- $\text{pgcd}(22,75)$

Question 3.
- on a $1 = 3 \times 7 - 4 \times 5$, que pouvez-vous déduire sur 3, 7, 4 et 5 ?
- on a $4 = 6 \times 9 - 5 \times 10$, que pouvez-vous déduire sur 6, 9, 5 et 10 ?

Question 4. Les nombres 537138 et 412923 ont les représentations suivante comme produits de facteurs premiers :

$$537138 = 2 \times 3^2 \times 7^3 \times 29 \quad \text{et} \quad 412923 = 3 \times 7^2 \times 53$$

Quel est leur pgcd ?

Exercice 2 : calcul modulo

Question 1. Les équations suivantes ont-elles des solutions ? Si oui, donnez l'ensemble des solutions...
- $3x \equiv 5 \pmod 7$
- $2x - 3 \equiv 0 \pmod 4$
- $5x + 2 \equiv 0 \pmod 6$

Question 2. Montrez que $(3^{77} - 1)/2$ est un nombre impair. Montrez que ce même nombre est divisible par $(3^7 - 1)/2$ pour conclure qu'il n'est pas premier.

Montrez que si k n'est pas premier, alors $2^k - 1$ (nombre de Mersenne) n'est pas premier non plus.

Question 3. Quand est-ce que $2^n - 1$ est un multiple de 3 ?

Question 4. "Pour savoir si un nombre est divisible par 9, il suffit de vérifier si la somme de ces chiffres est divisible par 9".

Expliquer pourquoi cette règle par 9 fonctionne.

Exercice 3 : échange de clé de Diffie-Hellman

Question 1. Faites tourner l'algorithme d'échange de clé de Diffie-Hellman avec les valeurs suivantes

- $p = 11$ comme nombre premier
- $g = 2$ comme générateur de $\mathbf{Z}/p\mathbf{Z}$
- $a = 4$ comme nombre secret choisi par Alice
- $b = 8$ comme nombre secret pour Bob

Détaillez les calculs en mettant en avant les messages échangés par Alice et Bob. Quelle est la clé ainsi obtenue ?

Question 2. Vérifiez que 2 est bien un élément générique de $\mathbf{Z}/p\mathbf{Z}$. Est-ce que 3 est générique ? Que se passe-t'il si g n'est pas générique ?

Question 3. Que se passe-t'il si le canal de communication est compromis et qu'un observateur malveillant (Eve) écoute les communications ?

Question 4. Pouvez-vous généraliser le protocole d'échange pour partager une clé entre trois personnes ? Entre quatre ?