Résumé du cours du Samedi 11 Octobre 2014 - groupe débutant.

I) Divisibilité dans $\mathbb{Z}$.

1) Notion de diviseurs et multiples.

Définition. Soient a et b deux entiers relatifs, $a \neq 0$.
On dit que a divise b s'il existe un entier relatif k tel que : $b = ka$.
On note : $a|b$. On peut aussi dire : "a est un diviseur de b", "b est un multiple de a", "b est divisible par a".

Propriétés. Soient a, b et c trois entiers relatifs.
1) Réflexivité : a divise lui-même.
2) Transitivité : si a divise b et b divise c alors a divise c.
3) Si a divise b et b divise a alors $a = b$ ou $a = -b$.
4) 1 divise a.
5) a divise 0.
6) Si 0 divise a alors $a = 0$.
7) Tout entier relatif possède au moins deux diviseurs positifs : 1 et lui-même.

Propriété importante. Si un nombre d divise a et b alors il divise toute combinaison linéaire de a et b. Autrement dit, pour tout u, $v \in \mathbb{Z}$, $d|au + bv$.

Preuve. d divise a et b donc il existe deux entiers relatifs k et k' tels que : $a = kd$ et $b = k'd$. Soient u, $v \in \mathbb{Z}$. On a : $au + bv = akd + bk'd = d(ak + bk')$ et $ak + bk' \in \mathbb{Z}$ donc d divise $au + bv$.

2) Nombres premiers.

Définition. Un entier naturel différent de 1 est dit "premier" si ses seuls diviseurs positifs sont 1 et lui-même.

Théorème fondamental de l'arithmétique. Tout entier naturel $n \geq 2$ est décomposable en un produit de nombres premiers. Autrement dit, il existe un nombre fini de nombres premiers : $p_1, ..., p_k$ et un nombre fini d'entiers naturels non nuls $\alpha_1, ..., \alpha_k$ tels que : $n = p_1^{\alpha_1} \times ... \times p_k^{\alpha_k}$. De plus, cette décomposition est unique, à l'ordre près des facteurs.

Exemple. $6936 = 2^3 \times 3 \times 17^2$.

3) Division euclidienne.

Théorème de la division euclidienne. Soient a un entier naturel et b un entier naturel non nul. Alors il existe deux entiers naturels q (quotient) et r (reste) tels que : $a = bq + r$ et $0 \leq r < b$. De plus, q et r sont uniques.

Démonstration.

Existence : Soit E l'ensemble des entiers k tel que $a \geq bk$. On voit que E est non vide car $0 \in E$. De plus, tous les éléments de E sont inférieurs ou égaux à a. L'ensemble E est donc majoré. L'ensemble E est alors une partie non vide et majorée de $\mathbb{Z}$ donc il admet un plus grand élément nommé q. Posons alors $r = a - bq$. Comme $q \in E$, $a \geq bq$ donc $r \geq 0$. Et comme $q + 1 \notin E$, on obtient : $a < b(q + 1) \Rightarrow a - bq < b \Rightarrow r < b$.

Unicité : supposons qu'il existe des entiers naturels q, r, q' et r' tels que : $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$. On a : $-b < -r' \leq 0$ donc $-b < r - r' < b$. Or, comme $bq + r = bq' + r'$, on a : $r - r' = bq' - bq = b(q' - q)$. Donc, $-b < b(q' - q) < b \Rightarrow -1 < q - q' < 1$ (en divisant par $b > 0$). Comme q et q' sont des entiers naturels, $q - q'$ est un entier relatif et le seul entier relatif entre -1 et 1 différent de 1 et de -1 est 0 donc $q - q' = 0$ donc $q = q'$. Ainsi, on a : $bq + r = bq + r'$ donc $r = r'$.

4) Notion de $PGCD$.

Théorème. Soient a et b deux entiers dont l'un des deux au moins est non nul. L'ensemble des diviseurs de a et b admet un plus grand élément et cet élément est appelé : $PGCD$ (Plus Grand Commun Diviseur) de a et b et il est noté : $PGCD(a, b)$.

Définition. Deux entiers naturels a et b sont premiers entre eux si et seulement s'ils ne possèdent aucun diviseur premier commun si et seulement si leur seul diviseur positif commun est 1 si et seulement si $PGCD(a, b) = 1$.

Caractérisation du $PGCD$. Soient a, $b \in \mathbb{N}^*$, $d \in \mathbb{N}^*$.
$d = PGCD(a, b) \Leftrightarrow \exists\ a', b' \in \mathbb{N}$ tq $a = da'$, $b = db'$ et $PGCD(a', b') = 1$.

Démonstration. Supposons $d = PGCD(a, b)$. Alors il existe deux entiers naturels a' et b' tels que : $a = da'$ et $b = db'$. Si $PGCD(a', b') \neq 1$, il existe $d' > 1$ et deux entiers naturels a'' et b'' tels que : $a' = d'a''$ et $b' = d'b''$. Alors $dd' > d$ est un diviseur commun à a et b ce qui est impossible donc $PGCD(a', b') = 1$.
Réciproquement, s'il existe a', $b' \in \mathbb{N}$ tq $a = da'$, $b = db'$ et $PGCD(a', b') = 1$ alors d est un diviseur commun à a et b donc d divise le $PGCD$ de a et b. Ainsi, il existe un entier naturel q tel que : $\delta = PGCD(a, b) = dq$. D'après le sens direct, il existe des entiers naturels a'' et b'', premiers entre eux, tels que : $a = \delta a''$ et $b = \delta b''$. On a alors : $da' = \delta a''$ et $db' = \delta b''$ donc $a' = qa''$ (car $\delta = dq$) et $b' = qb''$. Comme a' et b' sont premiers entre eux et q divise a' et b', on a : $q = 1$ et alors $\delta = d$.

Les méthodes pour déterminer le $PGCD$ de deux nombres sont au programme de 3ème donc elles seront rappelées brièvement à l'oral.

5) Théorèmes de Bézout et de Gauss.

Théorème de Bézout. Soient a et b deux entiers naturels.
a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que : $au + bv = 1$.

Démonstration. Supposons que a et b sont premiers entre eux. On ne peut pas avoir $a = b = 0$. De plus, si $a = 0$ alors $b = 1$ et si $b = 0$ alors $a = 1$. Donc on peut supposer que $a \neq 0$ et $b \neq 0$. On considère les ensembles : E constitué des nombres positifs de la forme $au + bv$ avec u et v entiers et F constitué des nombres strictement positifs de la forme : $au + bv$ avec u et v entiers. L'ensemble F est une partie de $\mathbb{N}$ non vide car il contient a et b donc F admet un plus petit élément : $d = au_0 + bv_0$. Montrons que d divise a. Par la division euclidienne de a par d, il existe des entiers q et r, uniques, tels que : $a = dq + r$ et $0 \leq r < d$. Donc $a = (au_0 + bv_0)q + r$ donc $r = a(1 - qu_0) + b(-qv_0)$ ainsi, $r \in E$. Mais r ne peut pas appartenir à F car $r < d$ et d est le plus petit élément de F donc on a nécessairement : $r = 0$. Par conséquent, d divise a. De même, on montre que d divise b. Ainsi, d divise le $PGCD$ de a et b donc d divise 1 ainsi, $d = 1$ ou $d = -1$ mais $d > 0$ donc $d = 1$. On a alors trouvé deux entiers u_0 et v_0 tels que $au_0 + bv_0 = 1$.
Réciproquement, s'il existe deux entiers u et v tels que $au+bv = 1$ alors $PGCD(a, b)$ divise 1 donc $PGCD(a, b) = 1$ et a et b sont premiers entre eux.

Théorème de Gauss. Soient a, b et c trois entiers naturels non nuls. Si a divise bc et a et b sont premiers entre eux alors a divise c.

Démonstration. $a|bc$ donc il existe un entier k tel que : $bc = ka$. De plus, a et b sont premiers entre eux donc d'après le théorème de Bézout, il existe deux entiers u et v tels que : $au + bv = 1$. On a alors, $auc + bcv = c \Rightarrow auc + kav = c \Rightarrow a|c$.

Exercice 1. Soit p un entier naturel. Montrer que si p est pair alors p^2 est pair. La réciproque est-elle vraie ?

Solution de l'exercice 1. On suppose que p est pair donc il existe un entier k tel que : $p = 2k$. On a alors : $p^2 = 4k^2 = 2 \times 2k^2$ et $2k^2$ est entier, donc p^2 est pair.
La réciproque est vraie, on peut la démontrer par contraposée : supposons que p est impair alors il existe un entier k tel que : $p = 2k + 1$. On a donc : $p^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ et $2k^2 + 2k$ est un entier. Ainsi, p^2 est impair. Par conséquent, par contraposée, si p^2 est pair alors p est pair.

Exercice 2. Pour quelles valeurs de l'entier naturel n, $n+2$ divise-t-il n^3-2n^2-5n+7 ?

Solution de l'exercice 2. On écrit : $\forall\, n \in \mathbb{N}, n^3-2n^2-5n+7 = n^3-2n^2-5n+6+1 = (n-1)(n+2)(n-3)+1$. Donc si d est un diviseur commun à $n+2$ et à n^3-2n^2-5n+7, d divise 1 donc le $PGCD$ de n^3-2n^2-5n+7 et de $n+2$ est 1. Par conséquent, n^3-2n^2-5n+7 et $n+2$ sont premiers entre eux pour tout entier naturel n. Ainsi, pour tout entier naturel n, $n+2$ ne divise pas n^3-2n^2-5n+7.

II) Equations diophantiennes linéaires à deux inconnues.

Définition. On appelle : "équation diophantienne linéaire à deux inconnues" une équation de la forme : $ax+by=c$ où a, b, c, x et y sont des entiers. Les nombres x et y sont les inconnues (entières !).
Résoudre une telle équation, c'est trouver tous les couples d'entiers (x,y) tels que : $ax+by=c$.

1) Etude d'exemples.

Exemples. Résoudre les équations suivantes.

a) $6x+8y=1$; b) $2x+3y=1$.

2) Généralisation.

Théorème. On considère une équation diophantienne linéaire à deux inconnues x et y de la forme : $ax+by=c$ a, b, c, x, $y \in \mathbb{Z}$. Cette équation a au moins un couple d'entiers solution si et seulement si $PGCD(a,b)|c$.

Démonstration. Supposons que l'équation : $ax+by=c$ ait des solutions entières. Alors, il existe un couple (x_0,y_0) tel que : $ax_0+by_0=c$. Le $PGCD$ de a et b divise ax_0+by_0 donc il divise c.
Réciproquement, suppsons que $d=PGCD(a,b)|c$. Alors il existe un entier c' tel que : $c=dc'$. Par caractérisation de d, il existe deux entiers a' et b' tels que $a=da'$ et $b=db'$ et $PGCD(a',b')=1$. Comme a' et b' sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que : $a'u+b'v=1$. Ainsi, $da'u+db'v=d$ donc $au+bv=d$ ainsi, $ac'u+bc'v=dc' \Rightarrow ac'u+bc'v=c$ donc l'équation $ax+by=c$ admet au moins 1 couple d'entiers solution.

Remarque. Les méthodes des exemples a) et b) peuvent être généralisées pour résoudre n'importe quelle équation diophantienne linéaire à deux inconnues.

III) Congruences.

Définition. Soient a, b et n trois entiers, $n \geq 2$. On dit que a est congru à b modulo n si n divise $a-b$.

Remarque. On peut écrire que : $a \equiv b \pmod{n} \Leftrightarrow n|a-b \Leftrightarrow \exists k \in \mathbb{Z}, a-b=kn$. De plus, $a \equiv 0 \pmod{n} \Leftrightarrow n|a \Leftrightarrow \exists k \in \mathbb{Z}, a=kn$.

Quelques propriétés résultent de la définition :

Propriétés. Soient a, b, c, a', b' et n des entiers, $n \geq 2$.
1. (Réflexivité) $a \equiv a \pmod{n}$.
2. (Symétrie) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.
3. (Transitivité) $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
4. $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n} \Rightarrow a+b \equiv a'+b' \pmod{n}$.
5. $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n} \Rightarrow ab \equiv a'b' \pmod{n}$.
6. Si $a \equiv b \pmod{n}$ alors pour tout entier naturel $q \geq 1$, $a^q \equiv b^q \pmod{n}$.

Théorème. Soient n et a des entiers avec $n \geq 2$. Alors a est congru modulo n à exactement un des entiers $0, 1, 2, ..., n-1$.

Démonstration. Par division euclidienne de a par n, on peut écrire qu'il existe des entiers q et r tels que : $a = nq+r$ avec $0 \leq r \leq n-1$. Comme $a - r = nq$, on en déduit que : n divise $a - r$ donc $a \equiv r \pmod{n}$ donc a est congru à un des nombres $0, 1, ..., n-1$.
Supposons maintenant que a est congru à deux nombres s et t parmi $0, 1, ..., n-1$. Par symétrie et par transitivité, on peut en déduire que $s \equiv t \pmod{n}$ donc il existe $k \in \mathbb{Z}$ tel que : $s = nk + t \Rightarrow s - t = nk$. Or, on a : $0 \leq s < n$ et $-n < -t \leq 0$ donc $-n < s - t < n$ et en divisant par $n \geq 2$ (donc non nul), on obtient : $-1 < k < 1$ (car $s - t = nk$). Comme k est un entier, on a : $k = 0$ et ainsi, $s = t$.

Exercice 3. Montrer que le carré d'un entier est congru à 0 ou 1 modulo 4.

Solution de l'exercice 4. Soit n un entier. L'entier n est congru à 0 ou 1 ou 2 ou 3 modulo 4 (par le théorème précédent) donc n^2 est congru à 0 ou 1 modulo 4.

Exercice 4. Soit n un entier.
1) Montrer que si n est pair, $n^2 \equiv 0 \pmod{8}$ ou $n^2 \equiv 4 \pmod{8}$ et que si n est impair, $n^2 \equiv 1 \pmod{8}$.
2) Montrer que si n est impair, $n^4 \equiv 1 \pmod{8}$.

Solution de l'exercice 5.
1) Si n est pair alors il existe un entier k tel que $n = 2k$. Donc $n^2 = 4k^2$. Si k est pair, alors il existe un entier p tel que $k = 2p$. Ainsi, on a : $n^2 = 16p^2 = 8 \times 2p^2$ et $2p^2$ est un entier donc 8 divise n^2 ainsi, $n^2 \equiv 0 \pmod{8}$, si k est pair.
Si k est impair, alors il existe un entier m tel que $k = 2m + 1$ et alors : $n^2 = 4(2m + 1)^2 = 4(4m^2 + 4m + 1) = 16m^2 + 16m + 4 = 8(2m^2 + 2m) + 4$ donc $n^2 \equiv 4 \pmod{8}$ si k est impair.
Si n est impair alors il existe un entier k tel que $n = 2k + 1$. Donc $n^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. Le produit $k(k + 1)$ est le produit de deux entiers consécutifs donc il est pair. Ainsi, 2 divise $k(k + 1)$ donc 8 divise $4k(k + 1)$. D'où, $n^2 \equiv 1 \pmod{8}$.
2) D'après la question précédente, si n est impair, alors $n^2 \equiv 1 \pmod{8}$. Ainsi, $n^4 \equiv 1 \pmod{8}$.

Exercice 5. Déterminer le chiffre des unités de 1789^{1789}.

Solution de l'exercice 6. On a : $1789 \equiv 9 \pmod{10} \Rightarrow 1789^{1789} \equiv 9^{1789} \pmod{10}$.
Regardons les puissances de 9 modulo 10. On a : $9^0 \equiv 1 \pmod{10}$, $9^1 \equiv 9 \pmod{10}$, $9^2 \equiv 1 \pmod{10}$, $9^3 \equiv 9 \pmod{10}$ etc. On a alors pour tout entier naturel k, $9^{2k} \equiv 1 \pmod{10}$ (en effet, $9^{2k} = 81^k$ et $81 \equiv 1 \pmod{10}$) et $9^{2k+1} \equiv 9 \pmod{10}$ (en effet, $9^{2k+1} = 9^{2k} \times 9$ et $9^{2k} \equiv 1 \pmod{10}$). Comme 1789 est impair, on en déduit que : $9^{1789} \equiv 9 \pmod{10}$. Ainsi, le chiffre des unités de 1789^{1789} est 9.

Exercice 6. Démontrer que la somme des cubes de trois entiers consécutifs est divisible par 9.

Solution de l'exercice 8. Soit n un entier. Calculons : $n^3 + (n + 1)^3 + (n + 2)^3$.
On a : $n^3 + (n + 1)^3 + (n + 2)^3 = n^3 + n^3 + 3n^2 + 3n + 1 + n^3 + 6n^2 + 12n + 8 = 3n^3 + 9n^2 + 15n + 9 = 3n(n^2 + 5) + 9(n^2 + 1)$. Ainsi, pour montrer que 9 divise $n^3 + (n + 1)^3 + (n + 2)^3$, il suffit de démontrer que 9 divise $3n(n^2 + 5)$ i.e : que 3 divise $n(n^2 + 5)$. Si $n \equiv 0 \pmod{3}$, c'est bien sûr vrai. Si $n \equiv 1 \pmod{3}$, alors $n^2 \equiv 1 \pmod{3}$ et $5 \equiv 2 \pmod{3}$ donc 3 divise $n(n^2 + 5)$. Enfin, si $n \equiv 2 \pmod{3}$ alors $n^2 \equiv 1 \pmod{3}$ et $5 \equiv 2 \pmod{3}$ donc 3 divise $n(n^2 + 5)$. Donc dans tous les cas, 9 divise $3n(n^2 + 5)$.

Exercices d'approfondissement.

Exercice 7. Montrer que $\sqrt{2}$ est irrationnel.

Solution de l'exercice 7. Raisonnons par l'absurde. Supposons alors que $\sqrt{2}$ est rationnel. Donc il existe des entiers naturels non nuls a et b premiers entre eux tels que $\sqrt{2} = \dfrac{a}{b}$. On a alors, $2 = \dfrac{a^2}{b^2}$ donc $a^2 = 2b^2$. Comme 2 divise $2b^2$, 2 divise a^2 donc a est pair. Ainsi, il existe un entier k tel que $a = 2k$. On a alors, $4k^2 = 2b^2 \Rightarrow 2k^2 = b^2$ donc b^2 est pair d'où b est pair. Les entiers a et b sont tous les deux divisibles par 2, ce qui contredit le fait qu'ils

soient premiers entre eux. Donc $\sqrt{2}$ est irrationnel.

Exercice 8. Résoudre dans $\mathbb{Z}^2$ l'équation diophantienne suivante : $x^2 - 5y^2 = 3$.

Solution de l'exercice 8. On raisonne modulo 5. Comme tout entier n est congru à 0, 1, 2, 3 ou 4 modulo 5, n^2 est congru à 0, 1 ou 4 modulo 5. Si l'équation diophantienne : $x^2 - 5y^2 = 3$ avait une solution (x, y) alors on aurait : $x^2 \equiv 3 \pmod 5$ (car $-5y^2 \equiv 0 \pmod 5$) ce qui est impossible. Donc l'équation diophantienne : $x^2 - 5y^2 = 3$ n'a pas de solutions dans $\mathbb{Z}^2$.

Exercice 9. Soient $a \geq 2$ et $n \geq 2$ des entiers naturels. Montrer que si $a^n - 1$ est premier alors $a = 2$ et n est premier.

Solution de l'exercice 9. Montrons d'abord que $a = 2$. Pour cela, on factorise $a^n - 1$ de la manière suivante : $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + a + 1)$. $a - 1$ est un diviseur strictement positif de $a^n - 1$ et $a^n - 1 \neq a - 1$. Comme $a^n - 1$ est premier, on a nécessairement, $a - 1 = 1$ donc $a = 2$.
Montrons que n est premier. Soit p un diviseur positif de n. Alors il existe un entier naturel q tel que : $n = pq$. On a : $a^n - 1 = 2^{pq} - 1 = (2^p)^q - 1^q = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + ... + 2^p + 1)$. Donc $2^p - 1$ (qui est strictement positif) divise $2^n - 1$ qui est premier (et strictement positif) donc $2^p - 1 = 2^n - 1$ ou $2^p - 1 = 1$ ainsi, $p = n$ ou $p = 1$. Donc les seuls diviseurs positifs de n sont 1 et n donc n est premier.