Bilan TD1.

1. Définition de la division euclidienne dans $\mathbb{Z}$
2. Pour démontrer P ou Q, on suppose non$P$ et on démontre Q.
3. Définition : soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$. On dit que a divise b (ou a est un diviseur de b ou b est un multiple de a) si :
$$\exists k \in \mathbb{Z} \quad b = ka.$$
4. Le raisonnement par récurrence
5. Soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$.
Si a divise b et a divise c alors a divise $b + c$ et a divise $b - c$
6. Soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ si a divise b alors a divise $-b$.
7. Un nombre premier est premier avec tout entier qu'il ne divise pas. Autrement dit si p est premier et ne divise pas a, alors p est premier avec a.
8. Théorème de Bezout
9. Algorithme d'Euclide pour trouver un pgcd et les coefficients de l'identité de Bezout
10. Théorème de Gauss (exercice 4.)
11. Pour démontrer qu'un nombre n est premier, on prend un diviseur d de n et on prouve que $d = 1$ ou $d = n$
12. $(a-1)(\sum_{i=0}^{n-1} a^i) = a^n - 1$
13. Les congruences :
    (a) définition : $a \equiv b\ [n]$ signifie n divise $a - b$
    Autrement dit $a \equiv b\ [n]$ signifie $\exists k \in \mathbb{Z}\ a = b + kn$
    (b) propriétés (entre autres) :
    1.si r est le reste de la division de a par n, alors $a \equiv r\ [n]$
    2. si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a + c \equiv b + d\ [n]$
    3. si $a \equiv b\ [n]$ alors $\forall k \in \mathbb{N}\ a^k \equiv b^k\ [n]$
14. Si n est pair alors $\exists k \in \mathbb{N}\ n = 2k$
15. Si n est impair alors $\exists k \in \mathbb{N}\ n = 2k + 1$
16. Le produit $n(n + 1)$ est divisible par 2