Rappel de cours

Exercice 1

Exercice 1.1

$a = 5n+1$ et $b = 2n+1$. On a $d|a \Leftrightarrow kd = a = 5n+1$, donc $n = \frac{kd-1}{5}$ et $d|b \Leftrightarrow k'd = b = 2n+1$. $n = \frac{k'd-1}{2}$.

$$\frac{kd-1}{5} = \frac{k'd-1}{2}$$
$$2(kd-1) = 5(k'd-1)$$
$$d(2k-5k') = 3$$

Donc $d|3$.

Exercice 1.2

- Prenons $n \equiv 0 \mod 3$ donc $n = 3m$

$$pgcd(a,b) = pgcd(5(3m)+1, 2(3m)+1) = pgcd(15m+1, 6m+1) = pgcd(9m, 6m+1)$$
$$= pgcd(3m-1, 6m+1) = pgcd(3m-1, 3m+2) = pgcd(3m-1, 3) = 1$$

- Prenons $n \equiv 1 \mod 3$ donc $n = 3m+1$

$$pgcd(a,b) = pgcd(5(3m+1)+1, 2(3m+1)+1) = pgcd(15m+6, 6m+3) = pgcd(9m+3, 6m+3)$$
$$= pgcd(3m, 6m+3) = pgcd(3m, 3m+3) = pgcd(3m, 3) = 3$$

- Prenons $n \equiv 2 \mod 3$ donc $n = 3m+2$

$$pgcd(a,b) = pgcd(5(3m+2)+1, 2(3m+2)+1) = pgcd(15m+11, 6m+5) = pgcd(9m+6, 6m+3)$$
$$= pgcd(3m+3, 6m+3) = pgcd(3m+3, 3m) = pgcd(3m, 3) = 3$$

Exercice 2

on a $8k+7 \equiv 7 \mod 8$. et on cherche si il existe a, b, c tel que $a^2+b^2+c^2 = 8k+7$ ou $a^2+b^2+c^2 \equiv 7 \mod 8$. Tout entier peut s'écrire sous la forme $8k+i$ avec $0 \geq i \geq 7$. Et on a

$(8k)^2 \mod 8$	0
$(8k+1)^2 \mod 8$	1
$(8k+2)^2 \mod 8$	4
$(8k+3)^2 \mod 8$	1
$(8k+4)^2 \mod 8$	0
$(8k+5)^2 \mod 8$	1
$(8k+6)^2 \mod 8$	4
$(8k+7)^2 \mod 8$	1

Si $a_1 \equiv a_2 \mod n$ et $b_1 \equiv b_2 \mod n$ alors $a_1+b_1 \equiv a_2+b_2 \mod n$. En ce basant sur la table précédente, il n'existe pas de combinaison possible pour avoir $a^2+b^2+c^2 \equiv 7 \mod 8$

Exercice 3

$$666^9 99 \mod 13 = (666 \mod 13)^9 99 = 1^9 99 = 1$$

Exercice 4

Soit $a = a_1^2 + a_2^2 = (a_1+ia_2)(a_1-ia_2)$ et $b = b_1^2+b_2^2 = (b_1+ib_2)(b_1-ib_2)$, on a .

$$ab = (a_1+ia_2)(a_1-ia_2)(b_1+ib_2)(b_1-ib_2) = (a_1+ia_2)(b_1+ib_2)(a_1-ia_2)(b_1-ib_2)$$
$$= (a_1b_1 - a_2b_2 + i(a_2b_1+a_1b_2))(a_1b_1 - a_2b_2 - i(a_2b_1+a_1b_2)) = (a_1b_1-a_2b_2)^2 + (a_2b_1+a_1b_2)^2$$

QED