Correction de l'examen MA02.

Exercice 1

1. $3^6 \equiv 1$ modulo 7 d'après le petit théorème de Fermat.
   $182 = 6 \times 30 + 2$. Donc $3^{182} = (3^6)^{30} \times 3^2$, d'où $3^{182} \equiv 3^2$ modulo $7 \equiv 2$ modulo 7.
   Le reste de la division euclidienne de 3^{182} par 7 est 2.

2. $$\left\{\begin{array}{l} x \equiv 3[15] \\ x \equiv 6[11] \end{array}\right. \Leftrightarrow \exists k \in \mathbb{Z} \left\{\begin{array}{l} x = 3 + 15k \\ 3 + 15k \equiv 6[11] \end{array}\right.$$

   De plus,
   $$3 + 15k \equiv 6[11] \Leftrightarrow 4k \equiv 3[11]$$
   .
   On remarque que $4 \times 3 \equiv 1[11]$. Puisque 3 et 11 sont premiers entre eux,
   $$4k \equiv 3[11] \Leftrightarrow 3 \times 4k \equiv 3 \times 3[11] \Leftrightarrow k \equiv 9[11]$$

   D'où, en remplaçant k par $9 + 11k'$ où k' décrit $\mathbb{Z}$, les solutions de ce problème chinois sont
   $$x = 138 + 165k', k' \text{décrit } \mathbb{Z}$$
   .

3. 7 et 5 sont premiers entre eux donc il existe α et β deux entiers relatifs tels que l'on ait la relation de Bézout : $7\alpha + 5\beta = 1$. Par exemple: $7 \times 3 - 5 \times 4 = 1$.
   On a dans ce cas :
   $$7x + 5y = 1 \Leftrightarrow 7x + 5y = 7 \times 3 - 5 \times 4 \Leftrightarrow 7(x - 3) = -5(y + 4)$$
   D'après le théorème de Gauss, puisque 5 et 7 sont premiers entre eux et que 5 divise $7(x - 3)$, 5 divise $x - 3$: il existe donc k entier relatif tel que $x = 3 + 5k$, et en reportant dans l'équation, on trouve $y = -4 - 7k$.
   Réciproquement, on vérifie que pour tout $k \in \mathbb{Z}$, $(x = 3+5k, y = -4-7k)$ est solution de l'équation initiale.
   $7a + 5b = 3 \Leftrightarrow 7a + 5b = 7 \times 9 - 5 \times 12 \Leftrightarrow 7(a - 9) = -5(b + 12)$
   Par un raisonnement analogue au précédent, les solutions sont $(a = 9 + 5k, b = -12 - 7k)$ où k décrit $\mathbb{Z}$.

Exercice 2

1. Soit d le pgcd de a^2 et b^2, supposons $d \neq 1$, il existe donc p premier divisant d.
   p divisant a^2, il divise a (conséquence du lemme d'Euclide par exemple : si p premier divise un produit,p divise l'un au moins des facteurs).
   De même p divise b.
   p divise donc le pgcd de a et b, à savoir 1. Absurde. Donc $d = 1$.

2. Par récurrence sur n. Soit $\mathcal{P}_n : S_n = (\frac{n(n+1)}{2})^2$.
   Pour $n = 1$, la propriété s'écrit : $S_1 = 1$, ce qui est vrai.
   Soit n un entier naturel non nul quelconque, supposons $\mathcal{P}_n$ vraie,
   $$S_{n+1} = S_n + (n+1)^3 = (\frac{n(n+1)}{2})^2 + (n+1)^3 = (n+1)^2(\frac{n^2}{2^2} + n + 1) = \left(\frac{(n+1)(n+2)}{2}\right)^2$$
   .

3. Lorsque n est pair.
   (a) $S_{2k} = k^2(2k+1)^2$ et $S_{2k+1} = (2k+1)^2(k+1)^2$, donc
   pgcd(S_{2k}, S_{2k+1})=pgcd($(2k+1)^2k^2, (2k+1)^2(k+1)^2) = (2k+1)^2$ pgcd$(k^2, (k+1)^2)$.

(b) Or k et $k+1$ sont premiers entre eux (en effet, si d divise k et $k+1$, d divise $(k+1)-k$, c'est à dire 1). Donc $\text{pgcd}(k^2,(k+1)^2)=1$ d'après un résultat précédent.
D'où : $\text{pgcd}(S_{2k},S_{2k+1})$ $=(2k+1)^2$.

4. Lorsque n est impair, $S_{2k+1}=(2k+1)^2(k+1)^2$ et $S_{2k+2}=(k+1)^2(2k+3)^2$.
On a : $\text{pgcd}(2k+1,2k+3)=1$ car si d entier naturel divise $2k+1$ et $2k+3$, il divise leur différence : 2. Puisque $2k+1$ est impair, d ne peut être égal à 2, et ainsi $d=1$.
Comme précédemment on aboutit à : $\text{pgcd}(S_{2k+1},S_{2k+2})$ $=(k+1)^2$.

5. Pour tout k non nul, S_{2k} et S_{2k+1} ne sont pas premiers entre eux car $(2k+1)^2>1$
Soit k quelqconque, S_{2k+1} et S_{2k+2} sont premiers entre eux ssi $(k+1)^2=1$, soit pour $k=0$.
$S_1=1$ et $S_2=5$ sont donc premiers entre eux.

Exercice 3

1. (a) p divise $a(a+b)-ab$ donc p divise a^2. Puisque p est premier, il divise donc a.
De même p divise b.
   (b) D'après la question précédente, p divise pgcd(a,b).
De plus, tout diviseur commun à a et b divise $a+b$ et ab, donc divise le pgcd de $a+b$ et de ab, c'est à dire p : ainsi, $\text{pgcd}(a,b)$ divise p.
Bilan : $\text{pgcd}(a,b)=p$.

2. pgcd(10,15) = 5, pgcd(10+15, 10 $\times$ 15)=25 $\neq 5$. La réciproque est donc fausse.

3. pgcd(a,b)= 5 si et seulement si il existe a' et b' premiers entre eux tels que $a=5a'$, $b=5b'$.
On a : ppcm(a,b)=$5a'b'$.
De là, $a'b'=\frac{170}{5}=34$. On obtient les couples $(a'=1,b'=34)$ et $(a'=2,b'=17)$ et leurs "symétriques"', d'où les couples solutions $(a=5,b=5\times 34=180)$, $(a=5\times 2=10,b=5\times 17=85)$ et leurs symétriques.

4. **Si** a et b vérifient $\text{pgcd}(a+b,ab)=5$, **alors**, d'après ce qui précède, pgcd(a,b)= 5, et les couples (a,b) sont à chercher parmi les solutions du problème précédent. Après calculs, seul $(a=10,b=85)$ satisfait le système donné.

Exercice 4

1. 3, 7 et 11

2. (a) α est impair donc n'est pas divisible par 2.
   (b) p est un nombre premier différent de 2 : il est donc impair.
   (c) Si p est congru à 3 modulo 4, $p\in E$.
Alors, $\alpha\equiv -1$ modulo p. Or $\alpha\equiv 0$ modulo p. Absurde car -1 n'est pas divisible par p.
   (d) Ainsi, tout diviseur premier de α est congru à 1 modulo 4. Or un produit de facteurs congrus à 1 modulo 4 est congru à 1 modulo 4, d'où $\alpha\equiv 1$ modulo 4. C'est absurde car on a aussi $\alpha\equiv -1$ modulo 4, et 1 et -1 ne sont pas congrus modulo 4.