Corrections of exercises 2-4

Exercise 2

a) $X-1$ divides X^4-1 because
$$X^4-1=(X-1)(X^3+X^2+1)$$
thus
$$\text{gcd }(X^4-1,X-1)=X-1$$

b) Apply Euclid's algorithm :
$$3X^3+2X+1=(3X+12)(X^2-4X)+50X+1$$
$$X^2-4X=(\frac{1}{50}X-\frac{201}{50})(50X+1)+\frac{201}{50}$$
Thus the last non zero residue in Euclid's algorithm is $\frac{201}{50}$ which proves that
$$\text{gcd}(3X^3+2X+1,X^2-4X)=1$$
Alternative proof : $X^2-4X=X(X-4)$ thus a non constant divisor of X^2-4X has either 0 or 4 as a root. None of them is a root of $3X^3+2X+1$ thus the can't have a non constant common divisor.

Exercise 3

a) In $\mathbb{F}_p$ any non-zero element is invertible thus the group of units has $p-1$ elements. Thus Lagrange's theorem implies that for any unit $a\in\mathbb{F}_p-\{0\}$,
$$a^{p-1}=1$$
i.e. $a^p=a$ that is, a is a root of X^p-X. As 0 is also obviously a root of X^p-X, this normalized polynomial of degree p has exactly p different roots in $\mathbb{F}_p$ and thus factorizes as
$$X^p-X=\prod_{a\in\mathbb{F}_p}(X-a)$$

1. In $\mathbb{F}_3[X]$, since $3=0$ and $2=-1$,
$$X(X-1)(X-2)=X(X^2-3X+2)=X(X^2+2)=X^3+2X=X^3-X$$
2. As already said in *a*), for any a in $\mathbb{F}_p$,
$$a^p-a=0$$
Thus evaluating X^p-X+1 on a gives 1 which doesn't equal 0, so this polynomial has no root in $\mathbb{F}_p$.

Exercise 4

(a) $\mathbb{F}_7^*=\{1,2,3,4,5,6\}$ endowed with multiplication is a cyclic group of order 6 so it's generators are elements which have order exactly 6 and we know from cyclicity (identification with $(\mathbb{Z}/6\mathbb{Z},+)$) that there must be two of them, one being the inverse of the other. 1 has order 1 so it's not a generator. $2^3=8=1=64=4^3$ so 2 and 4 have order two so they are not generators. $6^2=36=1$ so 6 has order 2 and is not a generator. Thus the generators must be 3 and 5. Notice that $3\times5=15=1$ so we recover that one is the inverse of the other.

b) We have seen that $1=6^2$ is a square. Let's compute directly all squares of non-zero elements of $\mathbb{F}_7$:
- $6^2=1$ so 1 is a square,
- $5^2=25=4$ so 4 is a square,
- $4^2=16=2$ so 2 is a square,
- $3^2=9=2$, nothing new,
- $2^2=4$ so nothing new,
- $1^2=1$ ....

We see that there are 3 squares in $\mathbb{F}_7^*$ which are 2, 4 and 1.
Notice that $a\mapsto a^2$ is a group homomorphism from $\mathbb{F}_7^*$ to istelf. It's kernel is a subgroup of $\mathbb{F}_7^*$ so it has order 1, 2, 3 or 6. Since X^2-1 has at most two roots in $\mathbb{F}_7$, this kernel has in fact order two, it is $\{1,6\}$ Thus we recover that the image (i.e. the subgroup of squares) has order $6/2=3$.