Solution to Problem 25: Division of $x^7+x^6+x^2+x+1$ by $x^7+x^5+x^4+x^2+1$ yields

$$x^7+x^6+x^2+x+1=(x^7+x^5+x^4+x^2+1)+(x^6+x^5+x^4+x)$$

Division of $x^7+x^5+x^4+x^2+1$ by $x^6+x^5+x^4+x$ yields

$$x^7+x^5+x^4+x^2+1=(x+1)(x^6+x^5+x^4+x)+(x^5+x+1).$$

Division of $x^6+x^5+x^4+x$ by x^5+x+1 yields

$$x^6+x^5+x^4+x=(x+1)(x^5+x+1)+(x^4+x^2+x+1).$$

Division of x^5+x+1 by x^4+x^2+x+1 yields

$$x^5+x+1=x(x^4+x^2+x+1)+(x^3+x^2+1).$$

Division of x^4+x^2+x+1 by x^3+x^2+1 yields

$$x^4+x^2+x+1=(x+1)(x^3+x^2+1).$$

Thus a greatest common divisor of $f=x^7+x^6+x^2+x+1$ and $g=x^7+x^5+x^4+x^2+1$ is $d(x)=x^3+x^2+1$. In order to express d as a combination of f and g we work backwards (recall that $-1=1$ in the field $\mathbb{F}_2$):

$$d=x^5+x+1-x(x^4+x^2+x+1)=x^5+x+1+x[(x^6+x^5+x^4+x)-(x+1)(x^5+x+1)]=$$

$$=x(x^6+x^5+x^4+x)+(x^2+x+1)(x^5+x+1)=$$

$$=x(x^6+x^5+x^4+x)+(x^2+x+1)[x^7+x^5+x^4+x^2+1-(x+1)(x^6+x^5+x^4+x)]=$$

$$=(x^3+x+1)(x^6+x^5+x^4+x)+(x^2+x+1)(x^7+x^5+x^4+x^2+1)=$$

$$=(x^3+x+1)[(x^7+x^6+x^2+x+1)-(x^7+x^5+x^4+x^2+1)]+(x^2+x+1)(x^7+x^5+x^4+x^2+1)=$$

$$=(x^3+x+1)(x^7+x^6+x^2+x+1)+(x^3+x^2)(x^7+x^5+x^4+x^2+1).$$

Solution to Problem 26: i) Let us note first the following very useful observation:

Let F be a field. Any polynomial of degree 1 in $F[x]$ is irreducible. A polynomial of degree 2 or 3 is not irreducible in $F[x]$ iff it has a root in F.

In fact, if a polynomial $f \in F[x]$ is not irreducible then it can be factored into two non-invertible polynomials $f = gh$. Since polynomials of degree 0 (i.e. non-zero constants) are invertible, both g and h have positive degree. In particular, $\deg f = \deg g + \deg h \geq 2$, i.e. degree 1 polynomials are irreducible. Also, if $degf$ is 2 or 3 then at least one of $\deg g$, $\deg h$ must be 1. But any polynomial of degree 1 has a root in F, so f has a root in F. Conversely, if r is a root of f (and $\deg f > 1$) then $f = (x - r)q(x)$ for some q of degree at least 1, so f is not irreducible.

In $\mathbb{F}_3$ we have 9 monic polynomials of of degree 2:

$$x^2, x^2+1, x^2+2, x^2+x, x^2+x+1, x^2+x+2, x^2+2x, x^2+2x+1, x^2+2x+2$$

Note that 0 is a root of the polynomials x^2, x^2+x, x^2+2x, 1 is a root of x^2+2, x^2+x+1 and 2 is a root of x^2+2x+1. Thus these polynomials are not irreducible. None of 0, 1, 2 is a root of any of the remaining three polynomials, so they are irreducible. Thus x^2+1, x^2+x+2, x^2+2x+2 are the only irreducible monic polynomials of degree 2 in $\mathbb{F}_3[x]$.

ii) Let $f \in \mathbb{F}_3[x]$ be a polynomial of degree 4 or 5 which has no roots. Then f has no divisors of degree 1. Thus every irreducible factor of f has degree at least 2. Suppose that f is not irreducible. Then it has at least two irreducible factors. Since the sum of the degrees of the factors is equal to $\deg f$, we see that f has exactly two factors and at least one of them is of degree 2. Since every non-zero polynomial over a field is associated to a monic polynomial of the same degree, f has a monic irreducible factor of degree 2.

Remark. Note that the observation in ii) holds for polynomials over any field.

iii) Consider the polynomial $f = x^5 - x + 1 \in \mathbb{F}_3[x]$. Easy inspection shows that it does not have any roots in $\mathbb{F}_3$. If f was reducible, it would have a monic irreducible factor of degree 2 by ii). In i) we found all monic irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$. A simple calculation using division algorithm shows that none of them divides f. Thus f is irreducible. Since $\mathbb{F}_3[x]$ is a PID, we know that every irreducible element is prime and every non-zero prime ideal is maximal. Thus $f\mathbb{F}_3[x]$ is a maximal ideal and therefore $\mathbb{F}_3[x]/f\mathbb{F}_3[x]$ is a field. Note now that if $h \in \mathbb{F}_3[x]$ and if $r(x)$ is the remainder of h modulo f then $h + f\mathbb{F}_3[x] = r + f\mathbb{F}_3[x]$. This shows that every coset of $f\mathbb{F}_3[x]$ can be represented by a polynomial of dgeree at most 4. Conversly, two different polynomials p, q of degree at most 4 represent the same cosets iff $f|p-q$ which is only possible when $p = q$. Thus the cosets of $f\mathbb{F}_3[x]$ are in bijective correspondence with polynomials of degree at most 4. The number of such polynomials is $3^5 = 243$. This proves that the field $\mathbb{F}_3[x]/f\mathbb{F}_3[x]$ has 243 elements. Since $x + f\mathbb{F}_3[x]$ is a non-zero element of $\mathbb{F}_3[x]/f\mathbb{F}_3[x]$, it is invertible. We are asked to find its inverse. Note that $f = x(x^4 - 1) + 1$, so $1 = (1 - x^4)x + f$. It follows that

$$1+f\mathbb{F}_3[x] = ((1-x^4)x+f)+f\mathbb{F}_3[x] = (1-x^4)x+f\mathbb{F}_3[x] = ((1-x^4)+f\mathbb{F}_3[x])(x+f\mathbb{F}_3[x]).$$

This shows that the inverse of $x + f\mathbb{F}_3[x]$ is $(1 - x^4) + f\mathbb{F}_3[x]$.

Solution to Problem 31: i) There are only 4 polynomials of degree 2 in $\mathbb{F}_2[x]$:

$$x^2, x^2 + 1, x^2 + x, x^2 + x + 1.$$

The first three polynomials have a root in $\mathbb{F}_2$ so they are not irreducible. The last polynomials does not have any roots in $\mathbb{F}_2$ so it is irreducible (we use the general observation discussed in the solutiuon to problem 26).

ii) There are eight polynomials of degree 3 in $\mathbb{F}_2[x]$:

$$x^3, x^3 + x, x^3 + x^2, x^3 + x^2 + x, x^3 + 1, x^3 + x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1.$$

The first four polynomials have root 0, the next two have root 1 so none of them is irreducible. Neither 0 nor 1 is a root of the last two polynomials, so they are the only cubic irreducible polynomials in $\mathbb{F}_2[x]$.

iii) Note that a reducible polynomial of degree 6 must have an irreducible factor of dgeree at most 3. By i) and ii) we have five irreducible polynomials of degree at most 3:

$$x, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1.$$

Thus a polynomial of degree 6 which is not divisible by any of these 5 polynomials is irreducible. It is now easy to check (using division algorithm) that none of these five polynomials divides $x^6 + x^5 + 1$. Similarly, $x^6 + x + 1$ is not divisible by any of the five polynomials. Thus both $x^6 + x^5 + 1$ and $x^6 + x + 1$ are irreducible.

Remark. It can be proved that there are 9 irreducible polynomials of degree 6 in $\mathbb{F}_2[x]$. There are 6 irreducible polynomials of degeree 5 and 3 irreducible polynomials of degree 4.