- 1) $x^4 5x^3 + 3x^2 + x = (x^2 + 1)(x^2 5x + 2) + (6x 2)$.
- 2) Since x^2+x+1 is quadratic, either it is irreducible, or it can be factored into linear factors. The only linear polynomials in $\mathbb{Z}_2(X)$ are x and x+1. However, $x^2+x+1=x(x+1)+1$. Therefore, neither x nor x+1 divide x^2+x+1 . Ergo, x^2+x+1 is irreducible.
- 3) If we try to use the Euclidean algorithm, we will fail. In the second division, we would have to invert 29, which we cannot do in the integers. Therefore, we need a different technique for finding the greatest common divisor. We see that b(-1) = 0, and hence x + 1 is a factor of b(x). Therefore, we can factor b(x) as follows:

$$b(x) = (x+1)(x^4 + 2x^2 + 1) = (x+1)(x^2 + 1)^2$$

x+1 and x^2+1 are both irreducible in $\mathbb{Z}[X]$. x+1 does not divide a(x), but x^2+1 does, precisely once.

$$a(x) = (x^2 + 1)(x^2 - 5x + 2)$$

Therefore, the gcd of a(x) and b(x) is $x^2 + 1$.

4) The key to this problem is to note that $\omega^{16} = -1$, and therefore $x + \omega^n = x - \omega^{16+n}$.

The proper ordering of factors is (leftmost column):