Problem 5. As you know, if F is a field and $s(x) \in F[x]$ has degree 2 or degree 3, then $s(x)$ is irreducible if and only if $s(x)$ has no root in F. By inspection, the only irreducible degree 2 polynomial over $\mathbb{Z}_2$ is $x^2 + x + 1 = s(x)$. Observe that $[s(x)]^2 = x^4 + x^2 + 1$.

The polynomial $t(x) = x^4 + x + 1$ has no root in $\mathbb{Z}_2$; hence, it has no factorization into degree 1 polynomial times a degree 3 polynomial. So $t(x)$ is reducible over $\mathbb{Z}_2$ if and only if it is a product of two irreducible degree 2 polynomials. But $x^2 + x + 1$ is the only irreducible degree 2 polynomial over $\mathbb{Z}_2$, and $(x^2 + x + 1)(x^2 + x + 1) \neq x^4 + x + 1$. Thus, $t(x) = x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$, completing the first part of the problem.

For the second part of the problem, you're asked to find $(\theta^2 + 1))^{-1}$, where $\theta = x + (t(x))$, a root of $t(x)$ in $F_1 = \mathbb{Z}_2[x]/(t(x))$.

This would be a good time to review a very important observation concerning inverses of elements in finite dimensional extensions:

For any field F contained in a field K, whenever an element $\beta \in K$, $F(\beta)$ is by definition the least subfield of K containing F and β.

Suppose β is a root of some irreducible polynomial $p(x) \in F[x]$, and let's consider $F[\beta]$, the least ring of K that contains F and β. Since $F[\beta]$ is a subring of K, it is closed under addition and multiplication, so it follows that if $q(x) \in F[x]$, then $q(\beta) \in F[\beta]$. On the other hand, $\{q(\beta) : q(x) \in F[x]\}$ is clearly closed under addition and multiplication, so $\{q(\beta) : q(x) \in F[x]\}$ must be equal to $F[\beta]$. Notice also that $p(\beta) = 0$, so if $q(\beta) = s(\beta)p(\beta) + r(\beta)$, where $\deg(r(x)) < \deg(p(x))$. It follows that $F[\beta] = \{q(\beta) : q(x) \in F[x],\ \deg(q(x)) < deg(p(x))\}$.

If we select $\alpha \in F[\beta] - \{0\}$, since $F[\beta]$ consists of polynomials in β of idegree less than $\deg p(x)$, there exists a polynomial $q(x) \in F[x] - \{0\}$ such that $\alpha = q(\beta)$.

Since $p(x)$ is irreducible and $q(x)$ is non-0 and of lesser degree than $p(x)$, $(p(x), q(x)) = 1$. Since we're operating in a Euclidean domain (see the first couple of pages of Chapter 8), there exists polynomials $s(x), t(x) \in F[x]$ such that $s(x)q(x) + t(x)p(x) = 1$. Evaluate this last equation at $x \to \beta$: we see that $s(\beta)q(\beta) + t(\beta)p(\beta) = 1$. Since β is a root of $p(x)$, $s(\beta)q(\beta) = 1$. But $q(\beta) = \alpha$, and now it is apparent that $s(\beta)$ is the inverse in K of α. It follows that $F[\beta]$ is field! And it must be the least field containing F and β, the field we called $F(\beta)$. Moreover, we have a procedure for finding inverses of elements of $F[\beta] = F(\beta)$, the Euclidean algorithm with backtracking. In 5(b), you're asked to implement that algorithm over $\mathbb{Z}_2$.

So in 5(b), with θ the root of $t(x)$, we're asked to find $(\theta^2+1)^{-1}$, we're asked to to determine $s(x), t(x)$ in $\mathbb{Z}_2[x]$ satsifying

$$s(x)(x^2+1) + t(x)(x^4+x+1) = 1$$

over $\mathbb{Z}_2$.

It is $s(x)$ that will determine the inverse of θ^2+1, and we won't have to be precise about $t(x)$ above.

Applying the Division Algorithm twice (again see the first pages of Chapter 8), we have
(1.) $x^4+x+1 = (x^2+1)(x^2+1)+x$
(2.) $x^2+1 = (x)x+1$, witnessing that $(t(x), x^2+1) = 1$. Now we have to "backtrack" to find $s(x), t(x)$ above.

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

So $s(x) = x^3+x+1$. Thus $(\theta^2+1)^{-1} = \theta^3+\theta+1$.

Check: $(\theta^3+\theta+1)(\theta^2+1) = \theta^5+\theta^3+\theta^2+\theta^3+\theta+1 = \theta^5+\theta^2+\theta+1 = (\theta^2+\theta)+\theta^2+\theta+1 = 1$. (Notice that $\theta^4+\theta+1 = 0$ implies that $\theta^5 = \theta^2+\theta$.)