

Tips and Remarks for Homework 6: Section 4.4 and 5.1

page 104 #5

Tip: Use the Factor Theorem with $a = 1_F$.

page 104 #15 Prove that $x^2 + 1$ is reducible in $\mathbb{Z}_p[x]$ if and only if there exists integers a and b such that $p = a + b$ and $ab \equiv 1 \pmod p$.

Be very careful when you write your arguments for this problem that you distinguish between elements of \mathbb{Z}_p and elements of \mathbb{Z} . Distinguishing between the two sets by using different notation. Before you begin your proofs, introduce your new notation for elements of \mathbb{Z}_p : if $a \in \mathbb{Z}$, then denote the congruence class of $a \pmod p$ by $[a]$. (You can also use \bar{a} if you prefer.)

Use your notation any time you write your polynomial. Write $[1]x^2 + [1]$ to emphasize that your coefficients are in \mathbb{Z}_p .

" \Rightarrow " Suppose that $[1]x^2 + [1]$ is reducible in \mathbb{Z}_p . We will show that there exists integers a and b such that $p = a + b$ (note that this is equality, not congruence) and $ab \equiv 1 \pmod p$.

Remark: Let F be a field. If you have a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in F[x]$$

that is reducible, then there exist nonconstant polynomials $g(x)$ and $h(x)$ of degree less than n such that $f(x) = g(x)h(x)$. *Question: can we assume that $g(x)$ and $h(x)$ are monic?* if $g(x) = b_mx^m + \dots + b_0$ and $h(x) = c_kx^k + \dots + c_0$, then the leading coefficient of $g(x)h(x)$ is b_mc_k . Since $g(x)h(x) = f(x)$ and the leading coefficient of $f(x)$ is 1_F , we must have $b_mc_k = 1_F$. Since F is a field, b_m and c_k have inverses. So:

$$\begin{aligned} f(x) &= g(x)h(x) = (b_mx^m + \dots + b_0)(c_kx^k + \dots + c_0) \\ &= b_mc_k(x^m + b_m^{-1}b_{m-1}x^{m-1} + \dots + b_m^{-1}b_0)(x^k + c_k^{-1}c_{k-1}x^{k-1} + \dots + c_k^{-1}c_0) \\ &= (x^m + b_m^{-1}b_{m-1}x^{m-1} + \dots + b_m^{-1}b_0)(x^k + c_k^{-1}c_{k-1}x^{k-1} + \dots + c_k^{-1}c_0) \end{aligned}$$

Answer: yes, if $f(x)$ is monic and reducible, then $f(x)$ is the product of two monic polynomials of degree less than n .

In the future, you may just use the fact we discussed in the above remark. In this problem, you should explain the proof back to me in this setting.

Make this argument: $f(x) = [1]x^2 + [1]$ is reducible, there exist nonconstant polynomials $g(x)$ and $h(x)$ of degree less than 2 such that $f(x) = g(x)h(x)$. Explain why the degrees of $g(x)$ and $h(x)$ must actually be 1. When you write out $g(x)$ and $h(x)$, use the notation for elements of $\mathbb{Z}_p[x]$. For example, a general polynomial in $\mathbb{Z}_p[x]$ would be $[a_n]x^n + \dots + [a_1]x + [a_0]$. Explain why $g(x)$ and $h(x)$ can be assumed to be monic, using an argument like that given in the remark above, except using your degree 1 polynomials.

Now you have shown that $f(x)$ is a product of monic polynomials $g(x)$ and $h(x)$ of degree 1. Rename your variables as follows: Let $g(x) = [1]x + [a]$ and $h(x) = [1]x + [b]$,

where $a, b \in \mathbb{Z}$ and $0 \leq a, b \leq p - 1$. Now prove that the integers a and b have the properties $p = a + b$ and $ab \equiv 1 \pmod{p}$.

Tip: To show $p = a + b$, use the fact that $0 \leq a, b \leq p - 1$.

“ \Leftarrow ” Suppose that there exists integers a and b such that $p = a + b$ and $ab \equiv 1 \pmod{p}$. We will show that $[1]x^2 + [1]$ is reducible in \mathbb{Z}_p . Let $g(x) = [1]x + [a]$ and $h(x) = x + [b]$. Prove that $f(x) = g(x)h(x)$.

page 123 #13 Suppose that $f(x), g(x) \in \mathbb{R}[x]$ and $f(x) \equiv g(x) \pmod{x}$. What can be said about the graphs of $y = f(x)$ and $y = g(x)$?

Show that the graphs of $y = f(x)$ and $y = g(x)$ have the same y -intercept.