ALGEBRA 2 – MICHAELMAS 2015
TUTORIAL 4

Finding inverses in $F[x]/I$ using the Euclidean algorithm

Example: Let $R = (\mathbb{Z}/7)[x]$, and $I = (x^4 + \overline{5}x + \overline{3})_R$. Use the Euclidean algorithm to find the multiplicative inverse of $(\overline{2}x^2 + \overline{1}) + I$ in the quotient $(\mathbb{Z}/7)[x]/I$.

(I've changed the handout to make the polynomial generating I monic.)

Note: The generator $x^4 + \overline{5}x + \overline{3}$ of I is irreducible. (Why?) So I is maximal, and R/I is a field. (Why?)

Solution: Work in $R = (\mathbb{Z}/7)[x]$, and apply the division algorithm to divide $x^4 + \overline{5}x + \overline{3}$ by $\overline{2}x^2 + \overline{1}$. We get

$$\begin{aligned} x^4 + \overline{5}x + \overline{3} &= q(x) \cdot (\overline{2}x^2 + \overline{1}) + r(x) \\ &= (\overline{4}x^2 + \overline{5}) \cdot (\overline{2}x^2 + \overline{1}) + (\overline{5}x + \overline{5}) \,. \end{aligned}$$

Take the old divisor $\overline{2}x^2 + \overline{1}$ to be the new dividend, and the old remainder $\overline{5}x + \overline{5}$ to be the new divisor. Divide $\overline{2}x^2 + \overline{1}$ by $\overline{5}x + \overline{5}$ to get

$$\overline{2}x^2 + \overline{1} = (\overline{6}x + \overline{1}) \cdot (\overline{5}x + \overline{5}) + (\overline{3}) \,.$$

Keep doing this, taking the old divisor to be the new dividend and the old remainder to be the new divisor. When the remainder is zero, stop. To summarise we obtain

$$\begin{aligned} x^4 + \overline{5}x + \overline{3} &= (\overline{4}x^2 + \overline{5}) \cdot (\overline{2}x^2 + \overline{1}) + (\overline{5}x + \overline{5}) && (1) \\ \overline{2}x^2 + \overline{1} &= (\overline{6}x + \overline{1}) \cdot (\overline{5}x + \overline{5}) + (\overline{3}) && (2) \\ \overline{5}x + \overline{5} &= (\overline{4}x + \overline{4}) \cdot (\overline{3}) + \overline{0} && (3) \end{aligned}$$

The last non-zero remainder is the GCD of the original polynomials. Here we see that

$$\gcd(x^4 + \overline{5}x + \overline{3}, \overline{2}x^2 + \overline{1}) = \overline{3} \,.$$

But since $\overline{3}$ is a unit in $(\mathbb{Z}/7)[x]$ (it is a non-zero constant), we can *normalise* it to $\overline{1}$ by multiplying by $\overline{3}^{-1}$. So the polynomials are coprime.

Claim: By reading backwards, through these calculations, we can write

$$\overline{3} = a(x)(x^4 + \overline{5}x + \overline{3}) + b(x)(\overline{2}x^2 + \overline{1}) \,,$$

for some $a(x), b(x) \in (\mathbb{Z}/7)[x]$.

This is done as follows. Rearranging the second to last equation, equation 2, shows that

$$\overline{3} = (\overline{2}x^2 + \overline{1}) - (\overline{6}x + \overline{1}) \cdot (\overline{5}x + \overline{5})$$

Then equation 1 shows that

$$\overline{5}x+\overline{5}=(x^4+\overline{5}x+\overline{3})-(\overline{4}x^2+\overline{5})\cdot(\overline{2}x^2+\overline{1})$$

Substitute this into the previous to get

$$\begin{aligned}\overline{3}&=(\overline{2}x^2+\overline{1})-(\overline{6}x+\overline{1})\cdot\Big((x^4+\overline{5}x+\overline{3})-(\overline{4}x^2+\overline{5})\cdot(\overline{2}x^2+\overline{1})\Big)\\&=-(\overline{6}x+\overline{1})(x^4+\overline{5}x+\overline{3})+(\overline{3}x^3+\overline{4}x^2+\overline{2}x+\overline{6})\cdot(\overline{2}x^2+\overline{1})\,.\end{aligned}\tag{4}$$

Do not multiply out completely! Just figure out the coefficients of the polynomials $x^4+\overline{5}x+\overline{3}$ and $\overline{2}x^2+\overline{1}$ used in that step of the procedure.

We can keep going, solving for the remainder in the previous step, and substituting in. Do this until we are back to the first step with the original polynomials. In this example, we are already there. So equation 4 write the GCD as a linear combination of the original polynomials.

Multiply both sides of equation 4 by $\overline{3}^{-1}=\overline{5}$ to write

$$\overline{1}=-(\overline{2}x+\overline{5})(x^4+\overline{5}x+\overline{3})+(x^3+\overline{6}x^2+\overline{3}x+\overline{2})\cdot(\overline{2}x^2+\overline{1})\,.$$

Now if we reduce modulo I, the first term on the RHS is 0, and we get

$$\overline{1}+I=((x^3+\overline{6}x^2+\overline{3}x+\overline{2})+I)\cdot((\overline{2}x^2+\overline{1})+I)\,.$$

So we have found the that the inverse of $(\overline{2}x^2+\overline{1})+I$ in $(\mathbb{Z}/7)[x]/I$ is given by

$$(x^3+\overline{6}x^2+\overline{3}x+\overline{2})+I$$

The same algorithm works in $\mathbb{Z}/p$ to find inverses. To find $\overline{a}^{-1}$ modulo p start by applying the division algorithm to divide p by a and write

$$p=qa+r\,.$$

Repeat until $r=0$. The previous remainder will be $1=\gcd(p,a)$, so read backwards and substitute in to write

$$1=xp+ya\,,$$

for some $x,y\in\mathbb{Z}$. Then modulo p, we have

$$\overline{1}=\overline{0}+\overline{y}\,\overline{a}=\overline{y}\,\overline{a}\,,$$

so $\overline{a}^{-1}=\overline{y}$.

It even works in $\mathbb{Z}/n$, since $\overline{a}$ has an inverse if and only if $\gcd(n,a)=1$.

Exercise:

- Find $\overline{4}^{-1}$ in $\mathbb{Z}/79$.
- Find $\overline{15}^{-1}$ in $\mathbb{Z}/1009$.