

Consider the polynomial $p(x) = x^2 - 2x + 2$, which has *no rational roots*. In other words, $p(x)$ is irreducible in $\mathbf{Q}[x]$.

Now the elements of $\mathbf{Q}[x]/p(x)$ are equivalence classes of polynomials of degree less than 2, hence all elements of the form $[ax + b]$. Let $a = 1$ and $b = 0$ and consider the particular equivalence class $[x]$. What happens when we substitute that element in our original polynomial equation?

Note that $[x]^2 - 2[x] + 2$ is equivalent to $[x^2 - 2x + 2]$ by congruence-class arithmetic, but $[x^2 - 2x + 2] = [0]$ (the remainder when $x^2 - 2x + 2$ is divided by our modulus polynomial). In other words, we see that $[x]$ is a *root* of our polynomial – but it's not a root in \mathbf{Q} . It's a root of that polynomial in the new field $\mathbf{Q}[x]/p(x)$.

What's the other root? To make it a little clearer, let's now use a different variable for our polynomial. Thus $p(t) = t^2 - 2t + 2$ and $t = [x]$ is a root in our new field, so $t - [x]$ is a factor. Let's divide $t - [x]$ into $p(t)$. We get

$$\begin{aligned} p(t) &= (t - [x])(t - 2 + [x]) + ([x]^2 - 2[x] + 2) \\ &= (t - [x])(t - 2 + [x]) + 0 \\ &= (t - [x])(t - 2 + [x]), \end{aligned}$$

so the other factor is $t - 2 + [x]$. This yields the *other root*, namely $t = 2 - [x]$.

So the roots of $p(x)$ in our new field are $[x]$ and $2 - [x]$.

Note that for any irreducible $p(x)$, the congruence class $[x]$ will always be a root of the polynomial in the new field $F[x]/(p(x))$, but the other roots, if they exist at all, may be determined by the polynomial $p(x)$. If $p(x)$ is a quadratic, the other root will always exist, but its relation to $[x]$ will be determined by the quadratic.

If the polynomial had been $x^2 - 2$, the roots would be $[x]$ and $-[x]$, but for the polynomial $x^2 - 2x + 2$, the roots are $[x]$ and $2 - [x]$. Can you guess how the relationship between the two roots depends on the quadratic polynomial $p(x)$.