# A Quick Note on Testing for Irreducibility in $\mathbb{Q}[x]$

On your homework, you were asked to show that $f(x) = x^4 + 5x^2 + 3x + 2$ is irreducible over $\mathbb{Q}$. We had mentioned the Eisenstein irreducibility criterion in class, but this polynomial isn't immediately $p$-Eisenstein for any selection of $p$. One variation to this approach that we've encountered is applying the Eisenstein criterion to a shifted version of the polynomial, (e.g. apply the Eisenstein criterion to $f(x+a)$ where $a$ is some integer). As it turns out, this doesn't help in this case (no integer shift $-1000 \leq a \leq 1000$ helps).

Below, I've outlined a couple of general approaches and a delightful computational approach that I feel compelled to mention.

## 1 Application of a Reduction Homomorphism

Note that we can gain insight into $f(x)$ by mapping $f(x) \in \mathbb{Z}[x]$ to a corresponding polynomial $\tilde{f}(x) \in \mathbb{Z}_p[x]$ (for some fixed prime $p$) by sending each coefficient of $f(x)$ to its reduction mod $p$. More formally we use the map $\Phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, the ring homomorphism induced by the reduction ring homomorphism $\phi_p : \mathbb{Z} \to \mathbb{Z}_p$, defined so that the monomial $\Phi_p(a_j x^j) = \phi_p(a_j)x^j$. If the polynomial $\tilde{f}(x) = \Phi_p(f(x))$ is of the same degree as $f(x)$ and is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.[1]

This can be used directly if we consider the reduction mod 3, but this approach resolves in an unfortunate argument involving several cases. Another approach is to note that by the contrapositive of the above statement, you have that if $f(x)$ is reducible, then $\Phi_p(f(x))$ is reducible; indeed if $f(x) = h(x)g(x)$ then $\Phi_p(f(x)) = \Phi_p(h(x))\Phi_p(g(x))$.

We proceed by applying $\Phi_2(f(x)) = x^4 + x^2 + x = x(x^3 + x + 1)$. Letting $\tilde{h}(x) = x^3 + x + 1$, we see that $\tilde{h}(x)$ is irreducible in $\mathbb{Z}_2[x]$ (as $\tilde{h}(x)$ is degree 3 and $\tilde{h}(0) = \tilde{h}(1) = 1$, so there are no linear terms). This implies that **if** $f(x)$ is reducible, then it must factor into a linear term and a cubic term. The rational root test shows us that $f(x)$ has no linear terms (as $f(1) \neq 0$, $f(-1) \neq 0$, $f(2) \neq 0$, and $f(-2) \neq 0$), so we conclude that $f(x)$ must be irreducible.

[1] Please note, the converse is not true! For example, the polynomial $x^4 + 1$ is reducible mod every prime, but is (clearly) irreducible over $\mathbb{Q}$.

## 2 A Computational Approach

If $f(x)$ was not irreducible over the rational numbers, then we could write $f(x) = g(x)h(x)$, where the degree of each $g(x)$ and $h(x)$ are degree 1 or greater. In this case, $g(k)$ and $h(k)$ must be always be integer divisors of $f(k)$, for any integer value, $k$. If we found a $k$ so that $f(k)$ is prime, then $g(k)$ is 1 or $-1$, or $h(k)$ is 1 or $-1$. $g(k)$ can be 1 at most $\deg g(x)$ times (as otherwise $g(x) - 1$ would have more than $\deg g(x)$ roots!), and similarly can be $-1$ at most $\deg g(x)$ times. Similarly, the same is true of $h(k)$.

Putting this together, this tells us that if $f(x)$ is reducible, then $f(k)$ can be a prime at most $2\left(\deg g(x) + \deg h(x)\right) = 2\deg f(x)$ times. Thus, if we can locate more than $2\deg f(x)$ prime values for $f(x)$ over the integers, we know that the polynomial must be irreducible over the integers (and thus over the rationals).

We now evaluate the polynomial at a few points:

| $k$ | $f(k)$ |
|---:|---:|
| 0 | 2 |
| −1 | 5 |
| 1 | 11 |
| 3 | 137 |
| 15 | 51797 |
| −19 | 132071 |
| 21 | 196751 |
| −25 | 393677 |
| 27 | 535169 |

The table above has 9 distinct points with prime values, which tells us that $f(x)$ must be irreducible.

This approach may not be appropriate for test situations (as significant computation is required both to evaluate the polynomial and test the resulting value for primality) but it is easy to implement this test in a computer algebra system.