A POLYNOMIAL RESISTANT TO IRREDUCIBILITY TESTS

TIM SMITS

For a monic polynomial $f(T) \in \mathbb{Z}[T]$, Gauss's lemma says that $f(T)$ is irreducible in $\mathbb{Z}[T]$ if and only if $f(T)$ is irreducible in $\mathbb{Q}[T]$. There are several standard tests for determining when such a polynomial is irreducible:

- If $\deg(f) = 2$ or 3, then $f(T)$ is irreducible in $\mathbb{Q}[T]$ if and only if $f(T)$ has no root in $\mathbb{Q}$. This is usually combined with the rational root theorem, to narrow down the possible roots of $f(T)$.
- If $f(T)$ is irreducible mod p for some prime p, then $f(T)$ is irreducible in $\mathbb{Q}[T]$.
- If $f(T)$ satisfies the Eisenstein condition for some prime p, then $f(T)$ is irreducible in $\mathbb{Q}[T]$.

We will give an example of a polynomial $f(T) \in \mathbb{Z}[T]$ where all of these tests *fail*, yet $f(T)$ is irreducible nonetheless.

Proposition 1. *Let $f(T) = T^4 - 10T^2 + 1$. Then $f(T)$ is irreducible in $\mathbb{Q}[T]$.*

Proof. By the rational root theorem, the only possible roots of $f(T)$ are ± 1, and clearly neither of these work. Therefore if $f(T)$ is reducible, it must factor as a product of quadratics. By Gauss's lemma, if $f(T)$ has a factorization in $\mathbb{Q}[T]$, then it admits such a factorization in $\mathbb{Z}[T]$ as well. Write $T^4 - 10T^2 + 1 = (T^2 + aT + b)(T^2 + cT + d) = T^4 + (a + c)T^3 + (ac + b + d)T^2 + (ad + bc)T + bd$ for some $a, b, c, d \in \mathbb{Z}$. Comparing coefficients, we have $a + c = 0, ac + b + d = -10, ad + bc = 0, bd = 1$. The first equation says that $a = -c$, so plugging this in says that $c^2 - 10 = b + d$, $c(b - d) = 0$, and $bd = 1$. The last equation says that $b = d = 1$ or $b = d = -1$ (which means the second equation is automatically satisfied). Therefore, we must have either $c^2 = 12$, or $c^2 = 8$, neither of which are solvable in the integers. Therefore, no such factorization exists, so $f(T)$ is irreducible in $\mathbb{Q}[T]$. $\square$

The first of our listed irreducibility tests obviously does not apply to $f(T)$, because $\deg(f) = 4$. Eisenstein's criterion can't apply either, because the constant term of $f(T)$ is 1. However, we've seen that even if the condition doesn't apply to $f(T)$ directly, it's sometimes possible to apply the test to a *translate* of $f(T)$ to show irreducibility.

Example 0.1. The Eisenstein criterion cannot apply to the polynomial $f(T) = T^2 + T + 1$, because the coefficients are all 1. However, the polynomial $f(T+1) = T^2+3T+3$ *is* Eisenstein (at the prime 3), and therefore irreducible. Since a factorization $f(T) = g(T)h(T)$ would give rise to a factorization $f(T + 1) = g(T + 1)h(T + 1)$, this means that $f(T)$ is also irreducible.

Definition 0.2. Let $f(T) \in \mathbb{Z}[T]$. If the polynomial $f(T+c)$ satisfies the Eisenstein criterion for some prime p and some $c \in \mathbb{Z}$, we say that $f(T)$ has an **Eisenstein translate** at c.

Proposition 2. *The polynomial $f(T) = T^4 - 10T^2 + 1$ has no Eisenstein translate.*

Proof. For any $c \in \mathbb{Z}$, we compute that $f(T + c) = T^4 + 4cT^3 + (6c^2 - 10)T^2 + (4c^3 - 20)T + (c^4 - 10c^2 + 1)$. Suppose that $f(T + c)$ is Eisenstein at some prime p. Then $p \mid 4c$ means $p = 2$ or $p \mid c$. First, suppose that $p = 2$. In this case, $c^4 - 10c^2 + 1 \equiv 0 \bmod 2$ means that

$c \equiv 1 \bmod 2$. Therefore, $c \equiv 1, 3 \bmod 4$. In either case, we have $c^4 - 10c^2 + 1 \equiv 0 \bmod 4$, so that $4 \mid c^4 - 10c^2 + 1$. This contradicts that $f(T + c)$ is Eisenstein at 2. This means that we must have $p \mid c$. We then see that $c^4 - 10c^2 + 1 \equiv 1 \not\equiv 0 \bmod p$, so that $p \nmid c^4 - 10c^2 + 1$, again contradicting that $f(T + c)$ is Eisenstein at p. Therefore, $f(T)$ has no Eisenstein translate. □

Proposition 3. *The polynomial $f(T) = T^4 - 10T^2 + 1$ is reducible mod p for all primes p.*

Proof. First, we handle the case $p = 2$: then $\bar{f}(T) \in (\mathbb{Z}/2\mathbb{Z})[T]$ factors as $(T + 1)^4$. Now, let p be an odd prime, and consider $\bar{f}(T)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$. By the factor theorem, $\bar{f}(T)$ has a root in $\mathbb{Z}/p\mathbb{Z}$ if and only if $\bar{f}(T)$ is divisible by a linear factor. Suppose that $c \in \mathbb{Z}/p\mathbb{Z}$ is a root of $\bar{f}(T)$. Then c satisfies $c^4 - 10c^2 + 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$, so $u = c^2$ satisfies $u^2 - 10u + 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Since p is odd, 2 is invertible in $\mathbb{Z}/p\mathbb{Z}$, so the quadratic formula says the roots of the polynomial $T^2 - 10T + 1$ in $(\mathbb{Z}/p\mathbb{Z})[T]$ are given by $5 \pm 2\sqrt{6}$. In particular, this says that if $\bar{f}(T)$ has a linear factor, then $\sqrt{6} \in \mathbb{Z}/p\mathbb{Z}$, and if $\sqrt{6} \in \mathbb{Z}/p\mathbb{Z}$, we have $\bar{f}(T) = (T^2 - 5 - 2\sqrt{6})(T^2 - 5 + 2\sqrt{6})$ says that $\bar{f}(T)$ is reducible.

Now, assume that $\sqrt{6} \notin (\mathbb{Z}/p\mathbb{Z})[T]$, so that $\bar{f}(T)$ has no linear factors. Therefore if $\bar{f}(T)$ factors in $(\mathbb{Z}/p\mathbb{Z})[T]$, it must be a product of two quadratics. Since $\bar{f}(T)$ is monic, we may assume it's a product of monic quadratics: $T^4 - 10T^2 + 1 = (T^2 + aT + b)(T^2 + cT + d)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$. From the work in proposition 1, we see that such a factorization is possible if $c^2 = 12$ or $c^2 = 8$ in $\mathbb{Z}/p\mathbb{Z}$. We can rewrite this condition as $(c/2)^2 = 3$ or $(c/2)^2 = 2$, so that this is is the same as saying $\sqrt{2}$ or $\sqrt{3} \in \mathbb{Z}/p\mathbb{Z}$. As it so turns out, at least one of $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Z}/p\mathbb{Z}$ for any p. Since we assumed $\sqrt{6} \notin \mathbb{Z}/p\mathbb{Z}$, one of the other two are, which is what we needed. □

To explain the last line of the proof, we need to know a little bit about the structure of $\mathbb{Z}/p\mathbb{Z}$.

Theorem 0.3. *Let p be a prime. There is $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that for any $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $x = g^k$ for some $k \geq 0$. In other words, $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group.*

The proof is a counting argument that relies on the fact that a polynomial of degree d over a field has at most d roots. We won't prove this theorem, but it can be found in any abstract algebra textbook. Once we know this, we can easily prove the following, which is what we need:

Corollary 0.4. *Let $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then at least one of a, b, ab must be a square in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. By the above theorem, we can write $a = g^n$ and $b = g^m$ for some $n, m \in \mathbb{Z}$ and some $g \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then $ab = g^{m+n}$. At least one of the integers $m, n, m + n$ must be even. □

Applying this to our specific case says for p odd, at least one of $2, 3, 6$ must be a square in $\mathbb{Z}/p\mathbb{Z}$.

Remark 0.5. Using algebraic number theory, one can actually say quite a lot about how the polynomial $\bar{f}(T) = T^4 - 10T^2 + 1$ factors in $(\mathbb{Z}/p\mathbb{Z})[T]$. It turns out there are four possible different types of factorization: $\bar{f}(T)$ can factor into a product of four distinct linear factors, a product of two irreducible distinct quadratic factors, a square of an irreducible quadratic factor, or a fourth power of a linear factor. These factorization types are witnessed by $p = 23, 5, 3, 2$ respectively. The last two types only happen for $p = 3, 2$ and the former two occur for infinitely many primes p.