AN IRREDUCIBLE THAT FACTORS MODULO ALL PRIMES

KEITH CONRAD

Let $\alpha = \sqrt{2} + \sqrt{3}$. To find a monic polynomial in $\mathbf{Q}[T]$ with root α, start by squaring α:

$$\begin{aligned} \alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} &\Longrightarrow \alpha^2 - 5 = 2\sqrt{6} \\ &\Longrightarrow (\alpha^2 - 5)^2 = 24 \\ &\Longrightarrow \alpha^4 - 10\alpha^2 + 25 = 24. \end{aligned}$$

Thus $\alpha^4 - 10\alpha^2 + 1 = 0$, so $\sqrt{2}+\sqrt{3}$ is a root of $T^4 - 10T^2 + 1$. This polynomial has four roots in $\mathbf{R}$: $\sqrt{2}+\sqrt{3} \approx 3.1462$, $\sqrt{2}-\sqrt{3} \approx -.3178$, $-\sqrt{2}+\sqrt{3} \approx .3178$, and $-\sqrt{2}-\sqrt{3} \approx -3.1462$.

Theorem 1. *The polynomial $T^4 - 10T^2 + 1$ is irreducible in $\mathbf{Q}[T]$.*

Proof. If the polynomial were reducible, it could be expressed as a linear times a cubic in $\mathbf{Q}[T]$ or as a product of two quadratics in $\mathbf{Q}[T]$.

If there were a linear factor in $\mathbf{Q}[T]$ then $T^4 - 10T^2 + 1$ would have a rational root. But the square of every root is $5 \pm 2\sqrt{6}$, which is irrational since $\sqrt{6}$ is irrational.

If $T^4 - 10T^2 + 1$ were a product of two quadratics in $\mathbf{Q}[T]$, then without loss of generality those factors are both monic. There are four roots in $\mathbf{R}$, so by unique factorization in $\mathbf{R}[T]$ a monic quadratic factor in $\mathbf{Q}[T]$ must be $(T - r)(T - s)$ for two of the real roots r and s. Therefore in a factorization into monic quadratics, one of the two factors has root $\sqrt{2} + \sqrt{3}$ and the factor with that root is one of the following:

$$\begin{aligned} (T - (\sqrt{2} + \sqrt{3}))(T - (\sqrt{2} - \sqrt{3})) &= T^2 - 2\sqrt{2}T - 1, \\ (T - (\sqrt{2} + \sqrt{3}))(T - (-\sqrt{2} + \sqrt{3})) &= T^2 - 2\sqrt{3}T + 1, \\ (T - (\sqrt{2} + \sqrt{3}))(T - (-\sqrt{2} - \sqrt{3})) &= T^2 - (5 + 2\sqrt{6}). \end{aligned}$$

All of these have an irrational coefficient, so there are no quadratic factors in $\mathbf{Q}[T]$. This completes the proof that $T^4 - 10T^2 + 1$ is irreducible in $\mathbf{Q}[T]$. $\square$

For $T^4 - 10T^2 + 1$ *neither* standard irreducibility test in $\mathbf{Q}[T]$ – reduction mod p or the Eisenstein criterion – can prove its irreducibility: for each prime p, $T^4 - 10T^2 + 1 \bmod p$ is reducible and for no $c \in \mathbf{Z}$ is $(T + c)^4 - 10(T + c)^2 + 1$ Eisenstein at p.

Theorem 2. *For each $c \in \mathbf{Z}$, $(T + c)^4 - 10(T + c)^2 + 1$ not an Eisenstein polynomial.*

Proof. Suppose for some $c \in \mathbf{Z}$ and prime p that $(T + c)^4 - 10(T + c)^2 + 1$ is Eisenstein at a prime p. Since

$$\begin{aligned} (T + c)^4 - 10(T + c)^2 + 1 &= T^4 + 4cT^3 + (6c^2 - 10)T^2 + (4c^3 - 20c)T + (c^4 - 10c^2 + 1) \\ &= T^4 + 4cT^3 + 2(3c^2 - 5)T^2 + 4c(c^2 - 5)T + (c^4 - 10c^2 + 1) \end{aligned}$$

we have $p \mid 4c$, so $p = 2$ or $p \mid c$. If $p \mid c$ then the constant term $c^4 - 10c^2 + 1$ is not divisible by p, which contradicts the Eisenstein condition at p. Therefore $p = 2$, so $c^4 - 10c^2 + 1$ is even, which implies c is odd. Then $c^2 \equiv 1 \bmod 8$, so $c^4 - 10c^2 + 1 \equiv 1 - 10 + 1 \equiv 0 \bmod 8$, which contradicts the Eisenstein condition at 2. $\square$

Before we show $T^4 - 10T^2 + 1 \bmod p$ is reducible for every prime p, the data below for $p \leq 43$ support this claim.

p	$T^4 - 10T^2 + 1 \bmod p$	p	$T^4 - 10T^2 + 1 \bmod p$
2	$(T+1)^4$	19	$(T^2+4)(T^2+5)$
3	$(T^2+1)^2$	23	$(T+2)(T-2)(T+11)(T-11)$
5	$(T^2+2)(T^2-2)$	29	$(T^2+8)(T^2+11)$
7	$(T^2+T-1)(T^2-T-1)$	31	$(T^2+15T-1)(T^2-15T-1)$
11	$(T^2+T+1)(T^2-T+1)$	37	$(T^2+7T+1)(T^2-7T+1)$
13	$(T^2+5T+1)(T^2-5T+1)$	41	$(T^2+7T-1)(T^2-7T-1)$
17	$(T^2+5T-1)(T^2-5T-1)$	43	$(T^2+9)(T^2+24)$

Theorem 3. *For each prime p, $T^4 - 10T^2 + 1 \bmod p$ is reducible.*

Proof. The polynomial $T^4 - 10T^2 + 1$ has three monic quadratic factorizations in $\mathbf{R}[T]$, found from the monic quadratic factors appearing in the proof of Theorem 2 and their conjugates. Here are the monic quadratic factorizations:

$$\begin{aligned} T^4 - 10T^2 + 1 &= (T^2 - 2\sqrt{2}T - 1)(T^2 + 2\sqrt{2}T - 1), \\ &= (T^2 - 2\sqrt{3}T + 1)(T^2 + 2\sqrt{3}T + 1), \\ &= (T^2 - (5 + 2\sqrt{6}))(T^2 - (5 - 2\sqrt{6})). \end{aligned}$$

For each prime p, at least one of these factorizations *makes sense* mod p. In $\mathbf{F}_p[T]$, the first factorization makes sense if 2 is a square mod p, the second factorization makes sense if 3 is a square mod p, and the third factorization makes sense if 6 is a square mod p.

For example, take $p = 7$. Since $2 \equiv 3^2 \bmod 7$, if we replace $\sqrt{2}$ with 3 in the first quadratic factorization of $T^4 - 10T^2 + 1$ and treat coefficients as elements of $\mathbf{F}_7$ then

$$\begin{aligned} (T^2 - (2\cdot 3)T - 1)(T^2 + (2\cdot 3)T - 1) &= (T^2 + T - 1)(T^2 - T - 1) \bmod 7 \\ &= T^4 - 3^2 + 1 \bmod 7 \\ &= T^4 - 10^2 + 1 \bmod 7. \end{aligned}$$

Taking $p = 5$, since $6 \equiv 1^2 \bmod 5$ we can replace $\sqrt{6}$ with 1 in the third quadratic factorization of $T^4 - 10T^2 + 1$ to get a factorization modulo 5:

$$\begin{aligned} (T^2 - (5 + 2\cdot 1))(T^2 - (5 - 2\cdot 1)) &= (T^2 - 7)(T^2 - 3) \bmod 5 \\ &= T^4 - 10^2 + 21 \bmod 5 \\ &= T^4 - 10^2 + 1 \bmod 5. \end{aligned}$$

In elementary number theory, it can be shown that for each prime p and integers a and b, if $a \bmod p$ and $b \bmod p$ are not squares mod p then $ab \bmod p$ is a square mod p.[1] Taking $a = 2$ and $b = 3$, for each prime p at least one of 2, 3, or 6 has to be a square mod p, and that gives meaning in $\mathbf{F}_p[T]$ to at least one of the monic quadratic factorizations of $T^4 - 10T^2 + 1$. Thus for each prime p, $T^4 - 10T^2 + 1 \bmod p$ is reducible. $\square$

In a similar way, for integers a and b such that a, b ,and ab are all not perfect squares, $\sqrt{a} + \sqrt{b}$ is a root of $T^4 - 2(a+b)T^2 + (a-b)^2$ and this polynomial is irreducible in $\mathbf{Q}[T]$ and for all primes p it has no Eisenstein translate at p and it is reducible mod p.

[1]This is related to Euler's criterion for quadratic residues.