AN IRREDUCIBLE THAT FACTORS MODULO ALL PRIMES

KEITH CONRAD

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

\[
\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \implies \alpha^2 - 5 = 2\sqrt{6} \\
\implies (\alpha^2 - 5)^2 = 24 \\
\implies \alpha^4 - 10\alpha^2 + 25 = 24.
\]

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 \( \mathbb{R} \): \( \sqrt{2} + \sqrt{3} \approx 3.1462, -\sqrt{2} - \sqrt{3} \approx -3.178, -\sqrt{2} + \sqrt{3} \approx .3178 \), and \( -\sqrt{2} - \sqrt{3} \approx -3.1462 \).

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

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

If there were a linear factor in \( \mathbb{Q}[T] \) 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 \( \mathbb{Q}[T] \), then without loss of generality those factors are both monic. 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:

\[
(T - (\sqrt{2} + \sqrt{3}))(T - (\sqrt{2} - \sqrt{3})) = T^2 - 2\sqrt{2}T - 1,
\]

\[
(T - (\sqrt{2} + \sqrt{3}))(T - (-\sqrt{2} + \sqrt{3})) = T^2 - 2\sqrt{3}T + 1,
\]

\[
(T - (\sqrt{2} + \sqrt{3}))(T - (-\sqrt{2} - \sqrt{3})) = T^2 - (5 + 2\sqrt{6}).
\]

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

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

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

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

\[
(T + c)^4 - 10(T + c)^2 + 1 = T^4 + 4cT^3 + (6c^2 - 10)T^2 + (4c^3 - 20c)T + (c^4 - 10c^2 + 1)
\]

\[
= T^4 + 4cT^3 + 2(3c^2 - 5)T^2 + 4c(c^2 - 5)T + (c^4 - 10c^2 + 1)
\]

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 \( c^2 \equiv 1 \) mod 8, so \( c^4 - 10c^2 + 1 \equiv 1 - 10 + 1 \equiv 0 \) mod 8, which contradicts the Eisenstein condition at 2. \( \square \)
Before we show $T^4 - 10T^2 + 1 \mod p$ is reducible for every prime $p$, the data below for $p \leq 43$ support this claim.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$T^4 - 10T^2 + 1 \mod p$</th>
<th>$T^4 - 10T^2 + 1 \mod p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$(T + 1)^4$</td>
<td>$(T^2 + 4)(T^2 + 5)$</td>
</tr>
<tr>
<td>3</td>
<td>$(T^2 + 1)^2$</td>
<td>$(T + 2)(T - 2)(T + 11)(T - 11)$</td>
</tr>
<tr>
<td>5</td>
<td>$(T^2 + 2)(T - 2)$</td>
<td>$(T^2 + 8)(T^2 + 11)$</td>
</tr>
<tr>
<td>7</td>
<td>$(T^2 + T - 1)(T^2 - T - 1)$</td>
<td>$(T^2 + 15T - 1)(T^2 - 15T - 1)$</td>
</tr>
<tr>
<td>11</td>
<td>$(T^2 + T + 1)(T^2 - T + 1)$</td>
<td>$(T^2 + 7T + 1)(T^2 - 7T + 1)$</td>
</tr>
<tr>
<td>13</td>
<td>$(T^2 + 5T + 1)(T^2 - 5T + 1)$</td>
<td>$(T^2 + 7T - 1)(T^2 - 7T - 1)$</td>
</tr>
<tr>
<td>17</td>
<td>$(T^2 + 5T - 1)(T^2 - 5T - 1)$</td>
<td>$(T^2 + 9)(T^2 + 24)$</td>
</tr>
</tbody>
</table>

**Theorem 3.** For each prime $p$, $T^4 - 10T^2 + 1 \mod p$ 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:

\[
T^4 - 10T^2 + 1 = (T^2 - 2\sqrt{2}T - 1)(T^2 + 2\sqrt{2}T - 1),
\]

\[
= (T^2 - 2\sqrt{3}T + 1)(T^2 + 2\sqrt{3}T + 1),
\]

\[
= (T^2 - (5 + 2\sqrt{6}))(T^2 - (5 - 2\sqrt{6})).
\]

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 $2 \equiv 3^2 \mod 7$, 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

\[
(T^2 - (2 \cdot 3)T - 1)(T^2 + (2 \cdot 3)T - 1) = (T^2 + T - 1)(T^2 - T - 1) \mod 7
\]

\[
= T^4 - 3^2 + 1 \mod 7
\]

\[
= T^4 - 10^2 + 1 \mod 7.
\]

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

\[
(T^2 - (5 + 2 \cdot 1))(T^2 - (5 - 2 \cdot 1)) = (T^2 - 7)(T^2 - 3) \mod 5
\]

\[
= T^4 - 10^2 + 21 \mod 5
\]

\[
= T^4 - 10^2 + 1 \mod 5.
\]

In elementary number theory, it can be shown that for each prime $p$ and integers $a$ and $b$, if $a \mod p$ and $b \mod p$ are not squares mod $p$ then $ab \mod p$ 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 $p$, $T^4 - 10T^2 + 1 \mod p$ 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 no prime $p$ does it have an Eisenstein translate at $p$ or is it reducible mod $p$.

\(^1\)This is related to Euler’s criterion for quadratic residues.