18.781, Fall 2007
Performing Cubic Reciprocity

In this note, we expand our in-class discussion of solutions to the congruence:

$$x^3 \equiv (3-\omega) \pmod 5$$

Recall that we are working in the ring $\mathbb{Z}[\omega]/5\mathbb{Z}[\omega]$ for this congruence, where $\omega = \frac{-1+i\sqrt{3}}{2}$. Then it suffices to compute:

$$\left(\frac{3-\omega}{5}\right)_3,$$

the cubic residue symbol mod 5, which is 1 if and only if $3-\omega$ is a cubic residue mod 5. We'd like to apply cubic reciprocity to this symbol, but unfortunately, the statement of cubic reciprocity we gave requires both primes to be "primary" – that is, both primes must be congruent to 2 mod 3. (Recall that we know $3-\omega$ is prime, as it has norm 13.)

So we seek a unit $u \in \{\pm 1, \pm\omega, \pm\omega^2\}$ with $u(3-\omega) \equiv 2\ (3)$.

Taking $u = \omega^2$, we get

$$\omega^2(3-\omega) = -1 + 3\omega^2 = -1 - 3 - 3\omega = -4 - 3\omega \equiv 2\ (3)$$

So now,

$$\left(\frac{3-\omega}{5}\right)_3 = \left(\frac{\omega^2}{5}\right)_3^{-1} \left(\frac{-4-3\omega}{5}\right)_3$$

Using cubic reciprocity on the latter symbol composed of two PRIMARY primes, this is

$$= \left(\frac{\omega^2}{5}\right)_3^{-1} \left(\frac{5}{-4-3\omega}\right)_3$$

Now we must reduce 5 mod $-4-3\omega$. This is:

$$\frac{5}{-4-3\omega} = \frac{5\overline{(-4-3\omega)}}{-4-3\omega\overline{(-4-3\omega)}} = \frac{-20-15\omega^2}{13}$$

Since an element of $\mathbb{Z}[\omega]$ close to this fraction is $-2-\omega^2 = -1+\omega$, we compute

$$5 - (-4-3\omega)(-2-\omega^2) = -2 - 2\omega = 2\omega^2$$

and hence

$$\begin{aligned}\left(\frac{3-\omega}{5}\right)_3 &= \left(\frac{\omega^2}{5}\right)_3^{-1} \left(\frac{2\omega^2}{-4-3\omega}\right)_3 = \left(\frac{\omega^2}{5}\right)_3^{-1} \left(\frac{\omega^2}{-4-3\omega}\right)_3 \left(\frac{-4-3\omega}{2}\right)_3 \\ &= \left(\frac{\omega}{5}\right)_3^{-2} \left(\frac{\omega}{-4-3\omega}\right)_3^{2} \left(\frac{-\omega}{2}\right)_3 = (\omega^2)^{-2}(\omega)^2(\omega) = \omega^2\end{aligned}$$

so $3-\omega$ is not a cubic residue mod 5.