# 18.781 RECIPROCITY QUIZ

**Monday, Nov. 5, 2007**

Name: _____

Numeric Student ID: _____

Instructor's Name: _____

I agree to abide by the terms of the honor code:

Signature: _____

**Instructions:** Print your name, student ID number and instructor's name in the space provided. During the test you may not use notes, books or calculators. Read each question carefully and **show all your work**; full credit cannot be obtained without sufficient justification for your answer unless explicitly stated otherwise. Underline your final answer to each question. There are 3 questions. You have 50 minutes to do all the problems.

| Question | Score | Maximum |
|---|---|---|
| 1 | | 7 |
| 2 | | 7 |
| 3 (BONUS) | | 5 |
| Total | | 14 |

1. Answer "TRUE" or "FALSE" to the following questions. You don't need to show your work. All computations are understood to be occurring in the ring $R = \mathbb{Z}[\omega]$.

   (a) $13 \equiv 0 \pmod{2+3\omega}$

   **Solution:**

   $N(2+3\omega) = 2^2 - 2 \cdot 3 + 3^2 = 7$. If $(2+3\omega)q = 13$ for some $q \in R$, then by multiplicativity of the norm map, $N(2+3\omega)|N(13)$. Clearly, $7 \nmid 13^2$, so FALSE.

   (b) $20 \equiv 41 \pmod{1-\omega}$

   **Solution:**

   The assertion is equivalent to $1-\omega|(41-20) = 21$. Now $N(1-\omega) = 3$, so $(1-\omega)|3|21$, so TRUE.

   (c) 11 is prime (i.e. irreducible) in $R$.

   **Solution:**

   From our classification of primes in $R$, we recall that all (rational) primes $q \equiv 2\ (3)$ remain prime in $R$, so TRUE.

   (d) Given $\alpha, \beta \in R$, let $N$ denote the norm map in $R$. If $N(\alpha)|N(\beta)$, then $\alpha|\beta$.

   **Solution:**

   It is true that if $\alpha|\beta$ then $N(\alpha)|N(\beta)$, but the above assertion (the converse) is FALSE. The simplest counterexample is a pair of primes $\pi, \bar{\pi}$ with $\pi\bar{\pi} = p$, a prime congruent to 1 mod 3. Then $N(\pi) = N(\bar{\pi})$ but $\pi \nmid \bar{\pi}$.

   (e) Given $\pi_1, \pi_2$, two primes in $R$, if $N(\pi_1) = N(\pi_2)$, then $\pi_1|\pi_2$.

   **Solution:**

   The same counterexample in the above question works here as well, showing that the assertion is FALSE.

   (f) Given a prime $\pi$ and an element $\alpha$ in $R$,

   $$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\alpha\omega}{\pi}\right)_3.$$

   **Solution:**

   Because the residue symbol is multiplicative, this amounts to showing whether

   $$\left(\frac{\omega}{\pi}\right)_3 = 1.$$

   This is FALSE, according to the supplementary laws for cubic reciprocity.

(g) Given a prime $\pi$ and an element $\alpha$ in $R$,

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\alpha}{\pi\omega^2}\right)_3.$$

**Solution:**

$\pi|\alpha \iff \pi\omega^2|\alpha$, so the symbols are simultaneously zero or non-zero. If non-zero,

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\pi)-1)/3}\ (\pi),\ \left(\frac{\alpha}{\pi\omega^2}\right)_3 \equiv \alpha^{(N(\pi\omega^2)-1)/3} = \alpha^{(N(\pi)-1)/3}\ (\pi\omega^2).$$

Moreover, for $d = 0, 1, 2$, $\alpha^{(N(\pi)-1)/3} \equiv \omega^d\ (\pi) \iff \alpha^{(N(\pi)-1)/3} \equiv \omega^d\ (\pi\omega^2)$.

2. (a) Given that $5 + 2\omega \mid 19$, factor 19 into primary primes in $\mathbb{Z}[\omega]$.

**Solution:**

Since 19 is a prime congruent to 1 mod 3, we know that it factors into two primes $\pi\bar{\pi} = 19$ in $R$. Hence $(5 + 2\omega)(5 + 2\omega^2) = 19$. It remains to rewrite these as primary primes (primes $\pi \equiv 2\ (3)$) by multiplying by the appropriate units. Now, running through the list of possibilities

$$(5 + 2\omega)(-\omega) = (-5\omega - 2\omega^2) = (-3\omega + 2) \equiv 2\ (3)$$

and hence

$$(5 + 2\omega^2)(-\omega^2) = (-5\omega^2 - 2\omega) = (2 - 3\omega^2) \equiv 2\ (3)$$

where the last can be rewritten as $5 + 3\omega$.

(b) Describe, in detail, the process you would use to determine whether the equation

$$x^3 \equiv 19 \pmod{23}$$

has a solution.

**Solution:**

There are many possible answers here. The simplest is to say that 23 is congruent to 2 mod 3, and so we know all residues mod 23 are cubic residues. Hence, a solution exists. Another way to solve it: apply cubic reciprocity, where we must use the factorization in part (a) to break 19 into primary primes before flipping the cubic residue symbol and reducing the numerator mod the now smaller denominator.

3. **(BONUS)**

(a) Let $g(a,p)$ denote the Gauss sum formed with the quadratic Legendre symbol mod $p$. Evaluate

$$\sum_{a=1}^{p-1} g(a,p)$$

**Solution:**

There are at least two solutions here. First, recall that $g(a,p) = \left(\frac{a}{p}\right) g(1,p)$, so we may rewrite the sum as

$$\sum_{a=1}^{p-1} g(a,p) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) g(1,p)$$

which gives 0 since the sum over residues of the Legendre symbol is 0 (there are equal numbers of residues and non-residues). Alternately, one can use the definition of the Gauss sum as a finite sum to obtain a double sum, and then change the order of summation to get 0:

$$\sum_{a=1}^{p-1} g(a,p) = \sum_{a=1}^{p-1}\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \zeta_p^{am} = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \sum_{a=1}^{p-1} \zeta_p^{am}$$

but the inner sum is always -1. Then we're left with a sum over Legendre symbols in a complete residue class again.

(b) Let $\tau = \frac{-1+i\sqrt{7}}{2}$. Determine (with proof) whether the ring $\mathbb{Z}[\tau]$, the ring generated by $\mathbb{Z}$ and $\tau$, is a Euclidean domain.

**Solution:**

The claim is TRUE, and the proof is to mimic the proof that $\mathbb{Z}[\omega]$ is a Euclidean domain (see notes). There is one detail that is a bit harder: one inequality in the adapted proof needs to be sharper, but the original proof for $R$ is quite sloppy in estimating terms and this is easily fixed.