Number Theory Fall 2009
Homework 11
Due: Wed. Nov. 18, start of class

9.8 Proof of quadratic reciprocity

The following exercises are related to our proof of quadratic reciprocity.

Exercise 9.9. *Let p, q be distinct odd primes. Determine the elements $x \in (\mathbb{Z}/pq\mathbb{Z})^\times$ such that $x^2 \equiv 1$ mod pq.* (Hint: think about the Chinese Remainder Theorem). *Using this, prove that $\prod_{x\in(\mathbb{Z}/pq\mathbb{Z})^\times} x \equiv 1$ mod pq in the same way we proved Wilson's Theorem.*

Exercise 9.10. *As in the proof, set*

$$P = \left\{ 1 \leq x \leq \frac{pq-1}{2} | \gcd(x, pq) = 1 \right\}.$$

Deduce from the previous exercise that $\left(\prod_{x\in P} x\right)^2 \equiv 1$ mod pq.

[Note that if one knew $\prod_{x\in P} x \equiv \pm 1$ *mod pq, this would say $\prod_{x\in P} \alpha(x) \equiv \pm(1,1)$ mod (p,q), hence* (3) *would mean $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$, which is* not true. *(In the previous exercise, you determined which elements square to* 1*, and it's not just ± 1 anymore.) As we see from* (4)*, the actual determination of $\prod_{x\in P} \alpha(x)$ (even up to ± 1) is more complicated. This is an example of how working mod pq is more complicated than working mod p.]*

Exercise 9.11. *(Proof of Theorem 9.2) Let $p > 3$ be prime. (i) Show $p = x^2 + 3y^2$ implies $p \equiv 1$ mod 3. (ii) Show $p = X^2 - XY + Y^2$ with $X \equiv Y$ mod 2 if and only if p is not prime in $\mathbb{Z}[\zeta_3]$. (iii) Find half-integers $a, b, c, d \in \frac{1}{2}\mathbb{Z}$ such that $X^2 - XY + Y^2 = x^2 + 3y^2$ where $x = aX + bY$, $y = cX + dY$. (iv) Deduce that $p = x^2 + 3y^2$ if and only if p is not prime in $\mathbb{Z}[\zeta_3]$. (v) Suppose $p \equiv 1$ mod 3. Using quadratic reciprocity, show $p | m^2 + 3$ for some m. Conclude p is of the form $x^2 + 3y^2$.*

10.2 Rings and fields

Exercise 10.1. *Why are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$ not fields? What about $\mathbb{Z}[i]$?*

Exercise 10.2. *In the same way we determined $\mathbb{Z}[\sqrt{2}, \sqrt{3}] = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\right\}$, determine what the rings $\mathbb{Z}[\sqrt{-2}, i]$ and $\mathbb{Z}[\sqrt[3]{2}]$ are, in terms of $\mathbb{Z}$-linear combinations of algebraic numbers. Similarly determine what $\mathbb{Q}(\sqrt{-2}, i)$ and $\mathbb{Q}(\sqrt[3]{2})$ are in terms of $\mathbb{Q}$-linear combinations of algebraic numbers. Prove at least one of your four answers, like we did in the example above. For the other three, you may just state the answer.*

Exercise 10.3. *Let R be a ring, and U be the subset of units. Show that U is a group under multiplication. What are the units of $R = \mathbb{Z}/n\mathbb{Z}$? What about $R = \mathbb{Z}[\sqrt{-n}]$ for $n \in \mathbb{N}$?*

Exercise 10.4. *Let R be a ring. Let u be a unit of R. Show u' is also a unit of R if and only if $u' \sim u$.*

10.3 Algebraic integers

Definition 10.1. *Let $\alpha \in \mathbb{C}$. We say α is an* **algebraic number of degree** $m > 0$ *if*

$$\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha + c_0 = 0$$

for some $c_0, c_1, \ldots, c_m \in \mathbb{Q}$ with $m > 0$ minimal. If each $c_i \in \mathbb{Z}$, we say α is an **algebraic integer**. *The polynomial $p(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$ is called the* **minimum polynomial** *of α.*

Exercise 10.5. *Show the definition of algebraic number and algebraic integer given above coincide with that in the text. Namely show that (i) α is an an algebraic number of degree m if and only if*

$$a_m\alpha^m a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_i \in \mathbb{Z}$ with m minimal; and (ii) α is an algebraic integer if and only if we may take $a_m = 1$.