Math 3240 (Roby) **HW #6** **Due in MSB 230**
4 Dec. 2012, 8 PM

Mathematics is not a careful march down a well-cleared highway, but a journey into a strange wilderness, where the explorers often get lost. Rigour should be a signal to the historian that the maps have been made, and the real explorers have gone elsewhere.— W.S. Anglin

- *Required Reading*: Text Chapter 11, Handouts on *Squares mod p, parts I–III,*.
- *Optional Reading*: Handouts on *Square Applications, parts I–II.*

1. *Numerical Problems*

   (a) Find a solution in $\mathbf{Z}[i]$ to the pair of congruences

   $$\alpha \equiv 1 - i \bmod 2 + 3i, \quad \alpha \equiv 2 + 4i \bmod 5 - 2i.$$

   Use the same methods as in $\mathbf{Z}$. When you need to invert a Gaussian integer in modular arithmetic, use Euclid's algorithm and back-substitution.

   (b) Use quadratic reciprocity to compute the following Legendre symbols. (257 is prime but the numerators in the Legendre symbols might not be prime, so factor the numerators first). Show all your work!

   $$\left(\frac{94}{257}\right), \quad \left(\frac{103}{257}\right), \quad \left(\frac{-221}{257}\right), \quad \left(\frac{91}{257}\right).$$

2. *Proving Square Patterns* In class it was shown how the law of quadratic reciprocity (main law and supplementary laws) implies the numerical patterns we found for $(\frac{3}{p})$, $(\frac{-3}{p})$, and $(\frac{5}{p})$. Use quadratic reciprocity to prove the following additional rules, which you found before numerically:

   $$\left(\frac{7}{p}\right) = 1 \iff p \equiv 1, 3, 9, 19, 25, 27 \bmod 28,$$
   $$\left(\frac{-15}{p}\right) = 1 \iff p \equiv 1, 2, 4, 8 \bmod 15.$$

3. *Arithmetic in* $\mathbf{Z}[\sqrt{2}]$

   (a) Adapt the algebraic method of division with remainder in $\mathbf{Z}[i]$ to the following example in $\mathbf{Z}[\sqrt{2}]$: find γ and ρ in $\mathbf{Z}[\sqrt{2}]$ such that

   $$17 + \sqrt{2} = (8 + 9\sqrt{2})\gamma + \rho, \quad |\,\mathrm{N}(\rho)| < |\,\mathrm{N}(8 + 9\sqrt{2})| = 98.$$

   Here $\mathrm{N}(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. In place of conjugation in $\mathbf{Z}[i]$ ($\overline{a + bi} = a - bi$) in your computations, use conjugation in $\mathbf{Z}[\sqrt{2}]$ ($\overline{a + b\sqrt{2}} = a - b\sqrt{2}$).

(b) Adapt the algebraic proof of division with remainder in $\mathbf{Z}[i]$ from the handout on Gaussian integers to prove $\mathbf{Z}[\sqrt{2}]$ admits division with remainder: for all α and β in $\mathbf{Z}[\sqrt{2}]$ with $\beta \neq 0$, there are γ and ρ in $\mathbf{Z}[\sqrt{2}]$ such that

$$\alpha = \beta\gamma + \rho, \quad |\,\mathrm{N}(\rho)| < |\,\mathrm{N}(\beta)|.$$

We need to use the absolute value since the norm on $\mathbf{Z}[\sqrt{2}]$ can be negative.

(c) Because there is division with remainder in $\mathbf{Z}[\sqrt{2}]$, it has unique factorization into primes. With this in mind, explain why the following three prime factorizations of 7 in $\mathbf{Z}[\sqrt{2}]$ do *not* violate unique factorization in $\mathbf{Z}[\sqrt{2}]$:

$$7 = (5+3\sqrt{2})(5-3\sqrt{2}) = (27+19\sqrt{2})(27-19\sqrt{2}) = (75+53\sqrt{2})(75-53\sqrt{2}).$$

(These are all prime factorizations in $\mathbf{Z}[\sqrt{2}]$ since each factor has norm 7, a prime in $\mathbf{Z}$.)

4. *Exploration: Solving quadratics mod prime powers*

(a) Suppose we want to solve $x^2 \equiv 69 \pmod{125}$. We know any solution mod 125 has to also work mod 5, so it's **necessary** that $x^2 \equiv 4 \pmod 5 \iff x \equiv 2, 3 \pmod 5$. Write $x = 2 + 5\ell$ and try to solve $x^2 = (2+5\ell)^2 \equiv 69 \pmod{25}$. What values can ℓ (hence x) have? Now repeat this with $x = 3 + 5\ell$.

(b) You should now have two solutions (call them b_1, b_2) to $x^2 \equiv 69 \pmod{25}$. As above, write $x = b_1 + 5\ell$, plug into the original equation, and solve for ℓ. Can you see how to get two solutions to the original equation mod 125? What are they?

(c) Use the method above to solve the congruence $x^2 \equiv 148 \pmod{11^3}$. Check your answer!

(d) PODASIP: The equation $x^2 \equiv a \pmod{p^k}$ has a solution $\iff \left(\frac{a}{p}\right) = 1$, for any positive odd prime p and any $k \in \mathbf{Z}^+$.

5. *Solving Quadratics over Fields*

(a) Let F be any field in which $2 \neq 0$. (Examples include $F = \mathbf{R}, \mathbf{Q}$, and $\mathbf{F}_p$ for $p \neq 2$.) Prove the quadratic formula is valid in $F[T]$: a polynomial $f(T) = aT^2 + bT + c \in F[T]$ with $a \neq 0$ has roots in F if and only if the discriminant $b^2 - 4ac$ is a *square* in F, and if $r \in F$ squares to $b^2 - 4ac$ then the roots of $f(T)$ in F are $(-b \pm r)/2a$.

Remark. A high-school derivation of the quadratic formula over $\mathbf{R}$ should still work, but please *do not* use a square root sign, as that is ambiguous in fields other than $\mathbf{R}$.

(b) Use you know or we've conjectured about squares mod p in class to decide whether $T^2 + T + 1$ has a root in $\mathbf{F}_p$ for the following primes p: 523, 691, 1093, 3511. Then do the same for the polynomial $T^2 + T + 3$. (The point is to explain clearly *from the square patterns* whether the polynomial has roots in $\mathbf{F}_p$.)

6. *Extra Credit Exploration: units in polynomial mods*

Determine the units in $\mathbf{F}_2[T]/(T^2)$, $\mathbf{F}_2[T]/(T^2+T+1)$, and $\mathbf{F}_2[T]/(T^2(T^2+T+1))$. That is, in each case write down a set of representatives for the congruence classes and determine which representatives are relatively prime to the modulus. (You don't have to use Euclid's algorithm; factoring is okay too.) Determine in which cases there is a generator for the units. What should we say $\varphi(T^2)$, $\varphi(T^2+T+1)$, and $\varphi(T^2(T^2+T+1))$ are? What similarities or contrasts do you notice with the classical Euler φ-function on $\mathbf{Z}$?