

From Bridge magazine in Britain:

Q: "Do you have to be a brilliant mathematician to play bridge?"

A: "No. The truth of the matter is that bridge is much more about inference, deduction, and judgement, than it is about mathematics."

- *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

$$\alpha \equiv 1 - i \pmod{2 + 3i}, \quad \alpha \equiv 2 + 4i \pmod{5 - 2i}.$$

Use the same methods as in **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 $\left(\frac{3}{p}\right)$, $\left(\frac{-3}{p}\right)$, and $\left(\frac{5}{p}\right)$. Use quadratic reciprocity to prove the following additional rules, which you found before numerically:

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

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

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

Here $\mathbf{N}(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. 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

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

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

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} ?

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 the conjectured square patterns discussed in class to decide if $t^2 + t + 1$ 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 .)