Homework 2 - Math 580, Frank Thorne (thornef@mailbox.sc.edu)

Due Wednesday, September 16

(1) Dudley, p. 19, 11, 14, 15; p. 26, 1, 3, 6, 9.

(2) (a) Determine a complete list of reduced residue classes $c \pmod 7$ for which the equation $x^2 \equiv c \pmod 7$ has an integer solution.

(b) Repeat the same when 7 is replaced with: 5, 11, 13.

(c) Look at your four lists of c. What do you notice? How many are there for each modulus? Do you see any patterns? Can you prove anything? Make some guesses? Ask questions?

Either post your observations, guesses, and (if you have any!) proofs to Piazza, or respond to what others post there. Can you build off of each other's guesses? Can you identify any patterns together?

(3) **Bonus problem:** This problem considers the ring of **Gaussian integers** $\mathbb{Z}[i]$, consisting of all numbers $a + bi$, where a and b are integers and $i = \sqrt{-1}$.

(a) A Gaussian integer x is a *unit* if there is another Gaussian integer y with $xy = 1$.

Prove that the units of $\mathbb{Z}[i]$ are precisely $\{1, -1, i, -i\}$.

(b) A Gaussian integer x is **prime** if its only divisors are: the units, and the Gaussian integers ux where u is a unit.

Find some prime Gaussian integers.

(c) An ordinary prime number p is **inert** if it is also prime when regarded as the Gaussian integer $p + 0i$. Which of the primes $p \leq 15$ are inert? Describe any patterns you see. (If you are feeling extremely ambitious, try to prove whatever conjectures you make.)

(d) A version of the unique factorization theorem holds for the Gaussian integers, "up to units". Can you guess what this means precisely?