Math 3240 (Roby) **HW #2** **Due in MSB 212**
24 Sept. 2010, 3 PM

The purpose of computing is insight, not numbers. — Richard Hamming

- *Required Reading*: Text Chapter 5, 7; handouts on "Modular Arithmetic," and "Decimal Data."
- At least two students in each homework group should work out numerical results *separately* and then compare, as a check on each other's work.

1. **Exploration:** Try to generate data and make interesting conjectures based on them.

   (a) The sequence $(1, 2, 3, 4)$ has 4 different *cyclic shifts*: $(1, 2, 3, 4)$, $(2, 3, 4, 1)$, $(3, 4, 1, 2)$, and $(4, 1, 2, 3)$. But the sequence $(1, 2, 1, 2)$ has the same length and only two cyclic shifts: $(1, 2, 1, 2)$ and $(2, 1, 2, 1)$. The sequence $(1, 1, 1, 1)$ has the same length and only one cyclic shift.

   How many different cyclic shifts can a sequence of length 3 have? Of length 5? Of length 6? Of length 9? Of length 10? Give explicit examples to illustrate what you find and formulate a general conjecture for any length.

   (b) Look at the handout "Decimal Data" and make some interesting conjectures. Some themes to consider are: which unit fractions $1/b$ are purely periodic, relations between the period length of the decimal expansion for $1/b$ and the value of b (particularly for $1/p$ when p is prime), and the shifting of digit sequences in the periods of different reduced fractions with the same denominator (particularly prime denominators).

   (c) For each prime $p = 2, 3, 5, \dots, 29$, compute all the nonzero squares modulo p and arrange your answers in a table with the squares for each modulus in numerical order. (For example, by squaring every number modulo 7 and reducing the answer, the nonzero squares modulo 7 are 1, 2, 4.) What do you notice about the *number* of nonzero squares modulo p as p varies?

2. Use mathematical induction in the proofs below.

   (a) When a is odd, $\frac{a-1}{2}$ is an integer. Prove by induction on $n \geq 2$ that for all *odd* numbers $a_1, a_2, \dots, a_n$,

$$\frac{a_1 a_2 \cdots a_n - 1}{2} \equiv \frac{a_1 - 1}{2} + \frac{a_2 - 1}{2} + \cdots + \frac{a_n - 1}{2} \bmod 2.$$

   So the expression $\frac{a-1}{2}$, when thought of modulo 2, behaves like a logarithm: products go to sums! (Hint for the case $n = 2$: write $a_1 = 2k_1 + 1$ and $a_2 = 2k_2 + 1$ for integers k_1 and k_2.)

   Note. There are n terms in the product and sum, not 3; the $\cdots$ on both sides represents intermediate terms. And if you are going to clear the denominator (which is not strictly necessary), be sure to change the modulus too and prove the congruence for the new modulus, not for modulus 2.

(b) When a is odd, show $\frac{a^2-1}{8}$ is an integer. Then prove by induction on $n \geq 2$ that for all *odd* numbers $a_1, a_2, \ldots, a_n$,

$$\frac{(a_1 a_2 \cdots a_n)^2 - 1}{8} \equiv \frac{a_1^2 - 1}{8} + \frac{a_2^2 - 1}{8} + \cdots + \frac{a_n^2 - 1}{8} \bmod 2.$$

3. Prove or Disprove and Salvage if Possible. (For each statement below give either a careful proof or a specific numerical counterexample; in the latter case, try to create a similar statement, perhaps by adding a hypothesis, that would be true.)

   (a) If $n \geq 1$ and $\{a_1, a_2, \ldots, a_n\}$ is a complete set of representatives mod n, then for any nonzero $b \in \mathbf{Z}/n$ the set $\{ba_1, ba_2, \ldots, ba_n\}$ is also a complete set of representatives.

   (b) If $a^j \equiv b^j \pmod{n}$ and $j \equiv k \pmod{n}$, then $a^k \equiv b^k \pmod{n}$, for all $j, k, n \in \mathbf{Z}$, $n > 1$.

   (c) If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, then $b \equiv c \pmod{(n_1, n_2)}$, for all $a, b, c \in \mathbf{Z}$ and $n_1, n_2 \in \mathbf{Z}^+$.

   (d) If $a \equiv b \pmod{n}$, then $(a, n) = (b, n)$ for all $a, b, n \in \mathbf{Z}$.

4. Numerical Problems (Some Food for Thought)

   (a) Make multiplication tables for $\mathbf{Z}/10$ and $\mathbf{Z}/11$. Do you notice any patterns? Can you explain any of them from basic properties of modular arithmetic? (Good explanations or proofs will earn extra credit!)

   (b) Find the remainder when 13^{12345} is divided by 17 and when 4444^{4444} is divided by 9.

   (c) Without performing the divisions, determine whether the integer 1,010,908,899 is divisible by 7, by 11, and by 13.

   (d) Describe the solution set for each of the following linear congruences:

      i. $5x \equiv 2 \pmod{26}$.

      ii. $36x \equiv 8 \pmod{102}$.

      iii. $140x \equiv 133 \pmod{301}$.

5. The *Gaussian integers* are complex numbers with integral coordinates and is denoted

$$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}.$$

Examples include $3+i$ and $2-7i$, but *not* $\frac{1}{2}+i$. We will see later in the course how properties of $\mathbf{Z}[i]$ give insight into properties of $\mathbf{Z}$.

We measure the size of a Gaussian integer $\alpha = a + bi$ by its *norm*, which is defined to be

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2.$$

In particular, $\mathrm{N}(\alpha) \in \mathbf{Z}$ and $\mathrm{N}(\overline{\alpha}) = \mathrm{N}(\alpha)$. For example, $\mathrm{N}(3 + i) = 10$. Notice $3 - i$ and $-3 + i$ also have norm 10. For $a \in \mathbf{Z}$, $\mathrm{N}(a) = a^2$.

   (a) Show, from its definition, that $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ for all $\alpha, \beta \in \mathbf{Z}[i]$.

   (b) The Gaussian integers with norm 1 are ± 1 and $\pm i$. Each of them has a multiplicative inverse in $\mathbf{Z}[i]$ by an explicit check: $1 \cdot 1 = 1$, $(-1)(-1) = 1$ and $i(-i) = 1$. Use norms to prove ± 1 and $\pm i$ are the only Gaussian integers with multiplicative inverses in $\mathbf{Z}[i]$. (Hint: if α has a multiplicative inverse in $\mathbf{Z}[i]$, *i.e.*, $\alpha\beta = 1$ for some $\beta \in \mathbf{Z}[i]$, use part a to show $\mathrm{N}(\alpha) = 1$.)

(c) In $\mathbf{Z}[i]$, say α is a *factor* of β (or α *divides* β) if $\beta = \alpha\gamma$ for some $\gamma \in \mathbf{Z}[i]$. For example $1 + 2i$ is a factor of $3 + i$ since $3 + i = (1 + 2i)(1 - i)$. But $1 - 2i$ is not a factor of $3 + i$ since the ratio $\frac{3+i}{1-2i} = \frac{1}{5} + \frac{7}{5}i$ is not in $\mathbf{Z}[i]$.

Just as a nonzero integer a with $|a| > 1$ has four trivial factors ± 1 and $\pm a$, a nonzero Gaussian integer α with $\mathrm{N}(\alpha) > 1$ has eight trivial factors: $\pm 1, \pm i, \pm\alpha, \pm i\alpha$. (For instance, $i\alpha$ is a factor of α because $\alpha = (i\alpha)(-i)$.) Call a Gaussian integer α *prime* if $\mathrm{N}(\alpha) > 1$ and the only factors of α are the eight trivial ones listed already. Call α *composite* if $\mathrm{N}(\alpha) > 1$ and α is not prime. For instance $3 + i$ is composite in $\mathbf{Z}[i]$ because it has the nontrivial factor $1 + 2i$.

If $\mathrm{N}(\alpha) > 1$, prove α is composite in $\mathbf{Z}[i]$ if and only if it has a factorization $\alpha = \beta\gamma$ where $\mathrm{N}(\beta) < \mathrm{N}(\alpha)$ and $\mathrm{N}(\gamma) < \mathrm{N}(\alpha)$. Then use induction on the value of the norm to prove every Gaussian integer with norm greater than 1 can be written as a product of prime Gaussian integers. Don't worry about uniqueness of the prime factorization; just prove prime factorization in $\mathbf{Z}[i]$ exists. (Hint: Extend the proof from class that every positive integer > 1 is a product of prime numbers.)

(d) Prepare a table of Gaussian primes with norm up to 15 by running through the Gaussian integers with norm from 2 to 15 and discarding any Gaussian integer divisible by a Gaussian integer (other than ± 1 and $\pm i$) with smaller norm.