Math 3240 - Introduction to Number Theory | Due by email
Problem Set 1 | 2/1/20 at noon

A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and at least ten times as entertaining as the same amount of "calculus for engineers." G. H. Hardy

- Required Reading: "Pell's Equation I," "Division Theorem in **Z** and $F[T]$," "Divisibility and Greatest Common Divisors" and "Modular Arithmetic".
- Optional: "Induction Examples".
- 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. (Induction practice)

   a) (**10 pts**) When a is odd, $(a-1)/2$ is an integer. Prove by induction on $r \geq 2$ that for all *odd* numbers $a_1, a_2, \ldots, a_r$,

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

   This says the expression $(a-1)/2$, when thought of modulo 2, behaves like logarithms: products go to sums! (Hint when $r = 2$: write $a_1 = 2k_1 + 1$ and $a_2 = 2k_2 + 1$ for integers k_1 and k_2.)

   Note. 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.

   Note. There are r terms in the product and in the sum, not 3 terms; the $\cdots$ on both sides represents intermediate terms. It is insufficient to check only that the case $r = 3$ implies the case $r = 4$. Theorem 4.2 of the induction handout is an example of induction on the number of terms.

   b) (**10 pts**) When a is odd, show $(a^2 - 1)/8$ is an integer. Then prove by induction on $r \geq 2$ that for all *odd* numbers $a_1, a_2, \ldots, a_r$,

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

2. (Exploration)

   a) (**8 pts**) 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 different 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 could 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 *all* lengths. (Don't treat only the cases of length 3 and 5.)

   b) (**5 pts**) Look at the handout "Decimal Data" on the course website and make conjectures based on patterns you find. Some themes to consider are: for which b is the decimal expansion of $1/b$ purely periodic, how is the period length of the decimal expansion for $1/b$ related to b (particularly for $1/p$ when p is prime), and the different digit sequences in the periods of all the reduced fractions with the same denominator (particularly prime denominators).

   c) (**5 pts**) For each prime $p = 2, 3, 5, \ldots, 29$ (that's 10 primes), 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? Use a calculator or computer algebra system to assist you.

3. a) (**5 pts**) Use Euclid's algorithm to compute the greatest common divisor of 5082 and 19943, writing out *every* equation of the algorithm as in class and then *explaining* how the calculations justify that the last nonzero remainder really is a greatest common divisor: why every common divisor of 5082 and 19943 is a factor of the last nonzero remainder and, conversely, why the last nonzero remainder is a common factor of 5082 and 19943.

   b) (**5 pts**) Using part a and back-substitution, express $(5082, 19943)$ in the form $5082x+19943y$ for some integers x and y, (Wolfram Alpha will tell you an answer, as a check, but it won't carry out the back-substitution steps.)

   c) (**5 pts**) Carry out Euclid's algorithm for $T^5 + T^4 + 1$ and $T^5 - 2T^2 - T - 1$ in $\mathbf{Q}[T]$ **and** factor the greatest common divisor from each polynomial. (Remember the convention that the gcd of two polynomials is always scaled to be monic, so it may not be the last nonzero remainder in Euclid's algorithm.)

4. Provide counterexamples to the following false statements about $\mathbf{Z}$. (Don't give examples, only counterexamples!)

   a) (**3 pts**) If a, b, and c are integers such that $ax+by = c$ for some x and y in $\mathbf{Z}$, then $(a, b) = c$.

   b) (**3 pts**) When d is the greatest common divisor of a and b, a/d and b are relatively prime. (Give 3 counterexamples.)

   c) (**3 pts**) If $a \equiv b \bmod m$ then $a \equiv b \bmod 2m$.

   d) (**3 pts**) If ab is a perfect square in $\mathbf{Z}$ and a and b are relatively prime integers then a and b are both perfect squares.

5. (Some gcd properties) Solve the following problems **without** using fractions, *e.g.*, use Bezout's identity or that if $a \mid bc$ in $\mathbf{Z}$ and $(a, b) = 1$ then $a \mid c$.

   a) (**5 pts**) Using only the definition of greatest common divisor, prove that if $a \mid b$ and $(b, c) = 1$ then $(a, c) = 1$.

   b) (**5 pts**) If $(a, b) = 1$, show $(a, bc) = (a, c)$ using Bezout's identity. (Hint: show (a, bc) and (a, c) divide each other.)

   c) (**5 pts**) If $a \mid bc$, $a \mid bd$, and $(c, d) = 1$, show $a \mid b$ using Bezout's identity. (**Warning**. If $ax + by = c$ in $\mathbf{Z}$, you can't say right away that $(a, b) = c$.)

   d) (**5 pts**) If $ad = bc$, $(a, b) = 1$, $(c, d) = 1$, and a, b, c, and d are all positive, show $a = c$ and $b = d$.

6. (Pell's equation)

   a) (**5 pts**) In class, simultaneous triangular and square numbers were related to positive integer solutions of the equation $x^2 - 2y^2 = 1$. Adapt this method to show that a positive integer that is both square and pentagonal leads to a positive integer solution of $x^2 - 6y^2 = 1$ where x is odd and y is even.

   b) (**5 pts**) Show every integral solution of $x^2 - 6y^2 = 1$ must have x odd and y even.

   c) (**5 pts**) The first three positive integer solutions of $x^2 - 6y^2 = 1$ are $(x, y) = (5, 2), (49, 20)$, and $(485, 198)$. Which of these lead to a simultaneous square and pentagonal number (not all do!), and what numbers are they? (In your work, don't confuse indices m and n with the numbers S_m and P_n.)