4400/6400 PROBLEM SET 0

0) **Proof of Fermat's Last Theorem, Step 0**: For a positive integer n, let $FLT(n)$ denote the following statement: for $x, y, z \in \mathbb{Z}$ such that $x^n + y^n = z^n$, $xyz = 0$. Show that if FLT(4) holds and FLT(p) holds for each odd prime p, then FLT(n) holds for all $n \geq 3$.

1) **Divisibility in Commutative Rings**: For elements x, y of a commutative ring R, we define $x \mid y$ (read as "x divides y") to mean: there exists $z \in R$ such that $zx = y$. This is binary relation on R.
a) Give a complete description of the divisibility relation on the field of rational numbers $\mathbb{Q}$. (Note: the point is that this is trivial.)
For the remainder of this problem, let a, b, c be integers.
b) Show that any integer a divides 0, but 0 divides only itself.
c) Suppose $a|b$ and $a|c$. Show that $a|(b + c)$ and $a|(b - c)$.
d) Suppose $a|b$ and a does not divide c. Show that a does not divide $b + c$.
e) Suppose a does not divide b and a does not divide c. What can we conclude about whether a divides $b + c$?

2) **Divisibility Tests**
a) Show that 7 divides a positive integer $10a + b$ if and only if 7 divides $a - 2b$. Explain why this gives a test for divisibility by 7.
b) Can you find a similar divisibility test for, say, 13?

3) **Divisbility as a partial ordering**: A relation R on a set is a *partial ordering* if it satisfies the following axioms:

(PO1) xRx for all x (reflexivity)
(PO2) If xRy and yRx then $x = y$ (anti-symmetry)
(PO3) If xRy and yRz then xRz (transitivity)

A partial ordering is **total** or **linear** if for any pair of elements x, y, either xRy or yRx holds ("**comparability**").

a) Note that the usual $\leq$ relation on the real numbers is a total ordering, hence endows every subset of the real numbers with a total ordering. In particular, the natural numbers $\mathbb{N}$ are totally ordered under $\leq$.[1]
b) For each of the following subsets of $\mathbb{R}$, determine whether the divisibility relation is a partial ordering and/or a total ordering:
(i) The set $\mathbb{Z}^+$ of positive integers.
(ii) The set $\mathbb{N}$ of non-negative integers.
(iii) The set $\mathbb{Z}$ of all integers.

[1] I'm not sure that there is anything to show here, but write a sentence or two to indicate that you understand the statement.

4) **Irrationality of $\sqrt{3}$**: Adapt the proof given in class of the irrationality of $\sqrt{2}$ to show the irrationality of $\sqrt{3}$. (You can either phrase the argument in terms of infinite descent, or start by reducing to lowest terms, according to your taste.) Make sure you give a complete proof of the fact that $3 \mid x^2$ implies $3 \mid x$ and that your proof **does not** assume the uniqueness of factorization into primes.

4.5) **Irrationality of $\sqrt{p}$**: It is in fact true that for any prime number p, $\sqrt{p}$ is irrational.[2] Explain instead how this can be proved for a particular prime p by brute force. (Suggestion/hint: again, the key implication is that $p \mid x^2 \implies p \mid x$. This is very closely related to Theorem 2 in Algebra Handout 1, but notice that the proof of this uses **Euclid's Lemma**, a result of number theory that we have not yet discussed. But for a given prime p, the theorem can be verified by direct calculation.)

5) **Irrationality of $\sqrt{n}$**: Explain how Theorem 2 from Algebra Handout 1 implies that for any squarefree integer $n > 1$, $\sqrt{n}$ is irrational.
b) Obviously it is not always the case that $\sqrt{n}$ is irrational, e.g. $\sqrt{4} = 2$. Can you figure out (i.e., successfully guess) for which integers $n > 1$ $\sqrt{n}$ is irrational?[3]

6) **Euclid sequences**: Let $p_1 < \ldots < p_n$ be distinct prime numbers. Euclid's proof of the infinitude of primes showed that if we put $N_n := p_1 \cdots p_n + 1$, then (i) (since $N_n > 1$) N_n has at least one prime divisor and (ii) every prime divisor of N_n is different from $p_1, \ldots, p_n$. Therefore if we define p_{n+1} to be the least prime divisor of N_n, we have given a canonical procedure for passing from a set $\{p_1, \ldots, p_n\}$ of n primes to a set $\{p_1, \ldots, p_n, p_{n+1}\}$ of $n+1$ primes and thus an infinite sequence $p_1, \ldots, p_n, p_{n+1}, \ldots$ of distinct primes. Let us call this sequence the **Euclid sequence** with **seed** $\{p_1, \ldots, p_n\}$. Also define $N_{n+1} = p_1 \cdots p_{n+1} + 1$, and so forth. In the literature, the Euclidean sequence with seed $\{2\}$ is known as the **Euclid-Mullin sequence**.
a) Computing Euclid sequences takes time because it involves factoring very large integers. How many terms of the Euclid-Mullin sequence are known?
b) Is it always the case that N_n is itself prime? (Hint: no. Try it with the Euclid-Mullin sequence.)
c) Suppose that $p_1 > 2$, so that all the "seed primes" $p_1, \ldots, p_n$ are odd. Show that $p_{n+1} = 2$. Note in particular that a Euclid sequence need not be monotonically increasing.
d) Is the Euclid-Mullin sequence monotonically increasing?
e) (U) Is there any seed $\{p_1, \ldots, p_n\}$ whose Euclid sequence contains every prime number? Does in fact every prime number occur at some point of the Euclid-Mullin sequence?
f) (U) Is there any seed $\{p_1, \ldots, p_n\}$ such that for all $k \geq 0$, N_{n+k} is prime?
g) (U) Is there any seed $\{p_1, \ldots, p_n\}$ such that the Euclid sequence is monotonically increasing?
h)(U) In part c) we showed that 2 occurs in every Euclid sequence. Does 3 occur

[2] The ancient Greeks proved this for some particular small primes p by geometric methods.

[3] We will state and prove this theorem in due course. If you like, you can try to find the answer in the notes online – I never mind if you want to read ahead.

in every Euclid sequence?

Remark: (U) denotes a problem that is, so far as I know, unsolved. In part h), I don't know the difficulty, because I haven't (yet!) thought much about the question.

7) **On arithmetic progressions**: In class we gave the example of 5, 11, 17, 23, 29 as a 5-term arithmetic progresssion (AP) consisting entirely of primes.

a) It is a recent and spectacular theorem of B. Green and T. Tao that for any positive integer k, there exist positive integers a_0 and d such that $a_0,\ a_1 = a_0 + d, a_2 = a_1 + d = a_0 + 2d, \ldots, a_N = a_{N-1} + d = a_0 + (k-1)d$ are all prime numbers. This is a theoretical result. What is the largest value of k for which anyone has found an explicit a_0 and d? (Suggestion: the way to solve this problem is to search on the internet.)

b) Find a 6-term AP consisting of primes. (Suggestion: start with a prime p and a common difference d such that $p + d$ is also prime. Then just check and see whether $p + 2d$, $p + 3d$, $p + 4d$ and $p + 5d$ are also prime. Usually not, of course. As far as I can see, you might as well pick p randomly, but you will find that some values of d are more promising than others.)

c) Show that it is never the case that $10k + 1$, $10(k + 1) + 1$, and $10(k + 2) + 1$ are all prime.

8) **More on Arithmetic Progressions**
a) Let a, $a + d$,...,$a + (k - 1)d$ be a k-term AP consisting entirely of primes, with common difference d. Show that for any prime $p \leq \frac{k}{2}$, $p \mid d$.
b) Show that there is no infinite arithmetic progression consisting entirely of primes.
c) In the situation of part a), show that in fact every prime $p < k$ must divide d.
d) Show that if we want a 6 term AP consisting of primes, then d must be divisible by $2 \cdot 3 \cdot 5 = 30$. (You can use part c) to get divisibility by 2 and 3; unless you did b)), you must do something else for divisibility by 5.) Now use part b) to give a lower bound on the last prime in a 25-term AP consisting of primes.

9) **Schinzel's Hypothesis** Formulate a conjecture about when a polynomial $p(x)$ with integer coefficients represents infinitely many primes. (Hint: look up Schinzel on Wikipedia.)

10) **No Prime-producing Polynomials**
a)* Let $p(x)$ be a nonconstant polynomial with integer coefficients. Show that there are infinitely many positive integers n such that $p(n)$ is not prime.
(Suggestion: if the constant term is anything other than 1 or -1, this should be relatively easy. The real question is what to do in the other case, e.g. $x^2 + 1$. Try perhaps a change of variables...)
b)* Strengthen part a) by showing that a nonconstant polynomial cannot take on exclusively prime values on any infinite arithmetic progression: for instance, we could have predicted that $x^2 - 2$ would not prime for every odd number $1, 3, 5, 7, \ldots$

11) **Polynomial Functions**: The term "polynomial function on the integers" is a ambiguous. On the one hand we could mean a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0,$$

where the a_i's are integers. On the other hand, we could mean merely that the coefficients a_i's are real numbers, but that nevertheless when we plug in any integer n, $p(n)$ is an integer. Let us call this latter-condition **integer-valued**.
a) Show that the polynomial $p_2(x) = \frac{1}{2}x^2 + \frac{1}{2}x$ is integer-valued, despite the fact that its coefficients are not integers.
b)* Show that an integer-valued polynomial at least has rational coefficients. (Hint: Look up the Lagrangne interpolation formula.)
c)* Find an explicit description of all integer-valued polynomials. For instance, any quadratic integer-valued polynomial is of the form $ap_2(x) + bx + c$, where a,b, and c are integers.

12) **Schuh's divisor game**: We begin with a positive integer N and all of its positive divisors d. Two players play, alternating turns. On a given turn, a player chooses a positive divisor d of N, and takes that divisor and also all positive integers e dividing d. The game ends when there are no divisors of N left to take.
a) I haven't told you who wins the game. Should the player who makes the last move win, or lose? (One way makes an uninteresting game.)
b) For any given N, there must be a winning strategy for either the first player or the second player: why?
c) Analyze the game for small values of N. You will find that the game does not depend so much on the numerical values themselves, but rather on the shape of the prime factorization of N. Find an explicit winning strategy for $N = p^a$ (a prime power), for $N = pq$ (a product of two primes), for $N = pqr$ (a product of three distinct primes).
d)* Show that, in fact, no matter what N is (except $N = 1$), the first player has a winning strategy, even though for general N – and even for N of the form $p^a q^b$ – no explicit winning strategy is known! (Hint: suppose for the sake of argument that the second player has a winning strategy. Figure out how to "steal" it, as the first player.)
e)* Despite the fact that I hadn't heard of it until a few days ago, this is a rather famous game. There ought to be some online applet where you can play the game against a computer, who will, for a sufficiently complicated choice of N, beat you consistently whether you are the first or the second player. Can you find such an applet on the internet? Can you build one? (I confess that the programming involved in getting the computer to play reasonably well is beyond me, but a computer science student might enjoy doing it.)

The next two problems are for graduate credit.

G1) **Group completion of a monoid**: A monoid is a set M equipped with a single binary operation $*$, which is associative, and has a two-sided identity e: $e * a = a * e = a$ for all a in M. Monoids do not have to be commutative, but let's work with commutative monoids in this problem.
a) Show that the natural numbers under addition form a commutative monoid, as do the positive integers under multiplication.

b) In the above two examples, we considered an auxiliary relation, $a \leq b$ iff there exists c in M such that $a * c = b$. Show that this relation is reflexive and transitive always (definitions above), but not in general anti-symmetric: we could have $a \leq b$ and $b \leq a$ without $a = b$. (Hint: try a nontrivial group.)
c) The two monoids from above have further nice properties:

(P1) Cancellation: if $a * b = a * c$, then $b = c$.
(P2) Minimality of e: if $a * b = e$, then $a = b = e$.

Show that in any commutative monoid satisfying these properties, the relation $\leq$ forms a partial ordering.
d) Define a direct sum operation on monoids M and N: $M \oplus N$ is, as a set, the set of all ordered pairs (m, n) for m in M, n in N, and is endowed with the "componentwise" operation:

$$(m_1, n_1) * (m_2, n_2) = (m_1 * m_2, n_1 * n_2).$$

Assume that M and N both satisfy (P1) and (P2), and show that $M \oplus N$ does as well.
d′) Still assuming that M and N satisfy (P1) and (P2), show that the resulting partial ordering is also "componentwise." In particular, if M and N each have more than one element, the $\leq$ on $M + N$ is not a total ordering: there exist two elements neither of which is less than or equal to the other.
e) Show that $(\mathbb{N}, +) \oplus (\mathbb{N}, +)$ is isomorphic to the submonoid of $(\mathbb{Z}^+, *)$ of all positive integers of the form $p^a q^b$ for (any) two distinct primes p and q.
f) Formulate a notion of an infinite direct sum (note: this is different from an infinite direct product: you want every entry to be the identity in all but finitely many coordinates), and show that the direct sum of a countably infinite number of copies of $(\mathbb{N}, +)$ with itself is isomorphic to the multiplicative monoid $(\mathbb{Z}+, *)$.
g)* The process of forming the integers from the natural numbers can be directly generalized to get a group out of a commutative monoid. Namely, for a commutative monoid M, let $G'(M)$ be the set of all ordered pairs (m, n) in $M \times M$, and consider the following equivalence relation on $G'(M)$: $(m, n) \sim (m', n')$ iff there exists $s \in M$ such that $s * m * n' = s * m' * n$. Show that the operation * on $M \times M$ is well-defined on equivalence classes and forms a group: indeed the inverse of (m, n) is (n, m). The group is denoted $G(M)$. The mysterious "s" can be dispensed with if M satisfies cancellation (P1).

Comment: The group $G(M)$ is called the Grothendieck group (or "group completion") of the monoid M.

G2) **Poset Game**: Let $(S, \leq)$ be a finite partially ordered set with a unique minimal element e – i.e., an element e with $e \leq s$ for all $s \in S$. We can play the "poset game" on S: players alternate choosing an element $s \in S$; they remove the element s they chose and also all elements $t \leq s$

a) Explain how the poset game generalizes the divisor game.
b) Either prove that the first player always has a win, or give a counterexample. (I mean, apart from the case in which $S = \{e\}$.)
c)(O) Lest you think that I made all this up, the poset game is the subject of an

award-winning high school science project of Steven Byrnes. What is Byrnes' Poset Game Periodicity Theorem?