

4400/6400 PROBLEM SET 1

0)(O) How do you know there is no largest integer n ?

- 1)a) Show that any integer a divides 0, but 0 divides only itself.
- b) Suppose $a|b$ and $b|c$. Show that $a|(b+c)$ and $a|(b-c)$.
- c) Suppose $a|b$ and a does not divide c . Show that a does not divide $b+c$.
- d) Suppose a does not divide b and a does not divide c . What can we conclude about whether a divides $b+c$?
- e) 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)

Is divisibility a partial ordering on the integers? What about on the natural numbers (recall $\mathbb{N} = \{0, 1, 2, \dots\}$); on the positive integers (recall $\mathbb{Z}^+ = \{1, 2, \dots\}$).

2) In class we gave the example of 5, 11, 17, 23, 29 as a 5-term arithmetic progression (AP) consisting of primes.

a) 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.)

b) Show that it is never the case that $10k+1$, $10(k+1)+1$, and $10(k+2)+1$ are all prime. (We explained this in class, but it doesn't hurt to go back and make sure.)

c) Let $a, a+d, \dots, a+(k-1)d$ be a k -term AP consisting entirely of primes, with common difference d . Show that for any prime $p \leq \frac{k}{2}$, $p|d$.

c')* In the situation of part c), 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 c'), you must do something else for divisibility by 5.) Now, whether you proved c') or not, assume it, and use it to give a lower bound on the last prime in a 25-term AP consisting of primes (in less jargony language, the question is: the last of 25 primes in an AP is at least...?) In fact, if you can find an AP this long,

you'll have beaten the record length, which is currently 23.¹

- 3) 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?
 c)(O) Prove: for every positive integer d , there exists a test for divisibility by d .

Comment: Exactly what is meant by a “divisibility by d ” test is part of what you have to figure out. For instance, of course we can use the division algorithm we learned in elementary school! Presumably a divisibility test is something that is faster and/or easier than this. That some divisibility tests are indeed faster and easier than actual division is pretty obvious: for instance, to test divisibility by 125 we only need to look and see if the last three digits are any of 125, 250, 375, 500, 625, 750, 875, or 000: much easier than that mathematics does not get (said Yoda). The test for divisibility by 7 is not as fast. Also, this is that rare problem where it is important that the number be given by its base 10 expansion – or at any rate, that it be expanded into powers of some fixed base a which does not depend on d . If we were allowed to rewrite a number n in base d notation, then the test is trivial: is the last digit 0? But this is cheating...

4) Formulate a conjecture about when a polynomial $p(x)$ with integer coefficients represents infinitely many primes. You will have to be more careful than I may have implied in class (I was vaguely hinting at the wrong answer): for instance $x^2 + x + 2$ does not represent infinitely many primes; why not? (You can consult wikipedia for the answer on this one if you like: the keywords are **Schinzel's Hypothesis**.)

5) 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: remember that Alex only suggested that $x^2 - 2$ might be prime for all odd n . 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 be prime for every odd number $1, 3, 5, 7, \dots$

6) The term “polynomial function on the integers” is ambiguous. On the one hand we could mean a polynomial

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

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**.

¹The Green-Tao theorem says there are infinitely many prime AP's which are as long as we want, but that doesn't mean that we can write them down explicitly, any more than the fact that there are infinitely many primes necessarily means we can write down a prime which has more than say, one million digits.

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.

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.

7) **Schuh's divisor game** is as follows: 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) 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:

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

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 . It is, in a certain sense we have not made precise, the “universal group” associated to M . This construction applied to the monoid $(\mathbb{N}, +)$ yields the infinite cyclic group \mathbb{Z} ; applied to the monoid $(\mathbb{Z}^+, *)$ it yields the multiplicative group of positive rational numbers. (The first example suggests that if we view $*$ as addition and also have a distinct multiplication operation, satisfying reasonable axioms, then $G(M)$ will in fact be a commutative ring. This is true.) This construction is awfully important in more advanced mathematics, for

instance in K-theory. (Please don't tell my colleagues that I mentioned K-theory on the first problem set – I don't have tenure yet!) One might wonder whether the same construction can be made to work for a noncommutative monoid, but forming quotients in the non-commutative case turns out to be quite a bit more intricate – and some further conditions are necessary. (Compare for instance, that not every non-commutative ring without zero divisors can be realized as a subring of a division ring: something called an “Ore condition” must be satisfied.)

G2) 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?

If you looked at these problems and thought, “Good god, those are the last graduate problems I'll ever look at,” look again next time anyway – this time around one of the graduate problem was very abstract. It won't always be like this.

Finally, a history problem (all history problems are optional):

H1) Read the wikipedia entry on Fermat. It is very nice, as usual, and it gives the right idea (i.e., mine!) about the stature of Fermat as a mathematician: one of the greatest of all time, probably on par with Newton and Gauss. (In fact it points out the extent to which Newton was able to lean on Fermat's work in his founding of the differential calculus, a point which the standard sound-bite level of treatment of the history of mathematics tends to skip over, although admittedly Fermat's principle appears in most calculus books.) They list Descartes and Fermat as the two leading mathematicians of the first half of the 17th century, but frankly it looks to me like Fermat blows Descartes out of the water. Think about what aspect of Fermat's life and/or work you might be interested in exploring in further depth, and come talk to me (or send email) about it.