

4400/6400 PROBLEM SET 2

Here is an explanation of the strange letters and symbols which follow many of the problems:

(E) This denotes an **easier** problem. Students who find these problems *too* easy can write “OK” as the solution to the problem; but students with more modest backgrounds might appreciate having a supply of more straightforward problems.

(*) This denotes a **harder** problem. Harder problems are almost optional: in 4400 one can get up to an A^- grade without doing any star problems; in 6400 one can get up to a B grade without doing any star problems and up to an A^- by doing only a few starred problems. It should be said that the difficulty varies more widely in these problems than in any other. If I were to be honest about things, there may be a few problems which could be labelled:

(**) It may not be possible to solve this problem without more advanced knowledge (and/or I might not quite remember how to solve it!), or indeed

(***) This problem is to the best of my knowledge unsolved, and it is not at all clear to me how to solve it.

But I am not above leaving out the second and third stars to try to get you to think about problems you might otherwise skip over: welcome to the deep end of the pool.

(O) This problem is **open-ended**, meaning exactly what is being asked may not be quite clear, and several solutions (or in some cases, no solution) may be equally acceptable. These problems are all optional, and can be omitted by all students without penalty.

(G) This means graduate-level. In many cases it would have deserved a (*), but in addition to being challenging it may also be more abstract and may call upon more background: in particular more abstract algebra. All (G) problems are optional at the 4400 level and if solved have the same benefits as (*) problems. Not every 6400 student is expected to be able to solve every 6400 problem.

(H) This means a **historical** problem. Historical problems are also optional; however, students at the 4400 level may do (H) problems instead of (*) problems and still get an A in the course.

“Can you...?” In multi-part problems, one of the parts might ask for a sharpening of the previous parts in an interrogative way. These are also optional, and in some cases they are quite unreasonable, e.g., can you write a computer program which plays Schuh’s divisor game better than humans do? Clearly this is not required.

1. PROBLEM SET 2

Remark: This problem set is probably too long. However, almost every problem either follows up on something said in class or in the notes in an important way, is very basic and important, or both. On average, this problem set is considerably easier (and less interesting) than the previous one, so don't lose heart, study on Saturday, or do anything else rash. Sometimes I put stars next to parts of problems that are not especially hard; I did this to cut down the number of required problems. If sheer fatigue sets in before you can do all the problems, let me know.

2.1)(E) Prove the Division Theorem (Proposition 1). Hint: It suffices to take q to be the largest non-negative integer such that $n - qd \geq 0$.

2.2)(E) Show that $d|n \iff$ we have $r = 0$ in the Division Theorem.

2.3) Prove the converse of Euclid's Lemma: suppose d is a positive integer such that whenever $d|ab$, $d|a$ or $d|b$. Then d is prime.

Remark: Among other things, this allows us to generalize the notion of primes to not-necessarily principal ideals.

2.4) "To contain is to divide": for integers a and b , we have $a|b \iff (a) \supset (b)$.

2.5) Show that if $a = b = 0$, there is no integer d such that $e|a$ & $e|b \implies e|d$.

The next exercise concerns the rng \mathbb{E} .

2.6) Give a necessary and sufficient condition on a positive element $x \in \mathbb{E}$ to have two different factorizations into positive \mathbb{E} -primes. Hint: pay attention to $\text{ord}_2(x)$ and also to the number of odd primes dividing x .

2.7) Prove Proposition 12 (from Handout 1).

2.8) Complete the proof that $S_n = 1 + \frac{1}{2} + \dots + \frac{1}{n}$ is never an integer by showing that for all $n \geq 1$, $\text{ord}_2(S_n) \neq \text{ord}_2(\frac{1}{n+1})$.

2.9)** Show that except for $n = 1, 2, 6$, the decimal expansion of S_n is non-terminating. (I.e., show that except for these values, $\text{ord}_p(S_n) < 0$ for some prime $p \neq 2, 5$.)¹

2.10) For any nonzero integers a and b , show that

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

2.11) For integers a and b , show that the intersection of the two ideals $(a) \cap (b)$ is an ideal of \mathbb{Z} . In fact, if you know the definition of an ideal in a commutative ring, show that the intersection of any two (or more...) ideals is always an ideal.²

¹Note the double-star: this is quite difficult.

²It is a metatheorem of algebra that if H_1 and H_2 are some substructures of a structure G , then $H_1 \cap H_2$ is also a substructure. Unions do not work nearly as nicely.

Because \mathbb{Z} is a PID, we must have $(a) \cap (b) = (c)$ for some $c \in \mathbb{Z}$, well-determined up to a sign. What is c in terms of a and b ?

2.12) a) Let a_1, \dots, a_n be a (finite) set of integers, not all zero. Define the *greatest common divisor* $\gcd(a_1, \dots, a_n)$ of the set, and show that it exists and is unique up to a sign. In fact, show that the set

$$(a_1, \dots, a_n) = \{x_1 a_1 + \dots + x_n a_n \mid x_i \in \mathbb{Z}\}$$

is an ideal of \mathbb{Z} , and that the positive generator of this (necessarily principal!) ideal is the gcd we are looking for.

b)* Define $\text{lcm}(a_1, \dots, a_n)$, show it exists, and explain how to get it from the ideals $(a_1), \dots, (a_n)$.

2.13) Show that $\gcd(a_1, a_2, a_3) = \gcd(\gcd(a_1, a_2), a_3)$.

2.14)* Find an identity relating $\gcd(a_1, a_2, a_3)$, $\text{lcm}(a_1, a_2, a_3)$ and $a_1 a_2 a_3$. Can you extend this to more than three numbers? (Hint: inclusion/exclusion.)

2.15) One says that a set of integers a_1, \dots, a_n is **relatively prime in pairs** if for all $i \neq j$, $\gcd(a_i, a_j) = 1$.

a) Show that if a_1, \dots, a_n are relatively prime in pairs, then $\gcd(a_1, \dots, a_n) = 1$.

b) Show that the converse does not hold when $n \geq 3$: indeed, find the smallest example of three integers which are not simultaneously divisible by any $d > 1$ but for which any two have a nontrivial common divisor.³

Remark: The phrase “let a_1, \dots, a_n be relatively prime integers” is therefore ambiguous when $n \geq 3$. Probably it ought to mean the weaker condition that $\gcd(a_1, \dots, a_n) = 1$ but careful authors rephrase to avoid the ambiguity. If you hear someone say it, stop and ask them which one they mean!

2.16) Prove the rational roots theorem: if

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

is a polynomial with integer coefficients, the only possible rational roots are of the form $\pm \frac{c}{d}$ where $c|a_n$ and $d|a_0$. Explain how this gives yet another proof of, e.g., the irrationality of $\sqrt{2}$.

2.17) a) Show that $\log_2 10$ is irrational.

b)* Let $a, b \in \mathbb{Z}^+$. Give a criterion for the irrationality of $\log_a b$.

G2) Let F be a field and let $v : F^\times \rightarrow \mathbb{Z}$ be a surjective map satisfying properties a) and b) of Proposition 12; v is said to be a **discrete valuation** of F .

a) Let $R_v := \{x \in F^\times \mid v(x) \geq 0\} \cup \{0\}$. Show that R_v is a subring of F , the **valuation ring**. (It is common to formally set $v(0) = \infty$ to avoid having to keep “manually inserting 0.”)

³This is reminiscent of the fact that a set of vectors can be linearly dependent even when any two of them are linearly independent from each other, a fact that gives linear algebra students no end of trouble.

c) Since v is surjective, there is an element $\pi \in R_v$ with $v(\pi) = 1$.⁴ Show that for any $n \geq 1$,

$$\{x \in F^\times \mid v(x) \geq n\} \cup \{0\} = (\pi^n),$$

the principal ideal of R_v generated by π^n (of course $\pi^0 = 1$).

d) Show that every ideal of R_v is of the form (π^n) for a suitable $n \in \mathbb{N}$. In particular, every ideal of R_v is principal, and there is a unique maximal ideal, (π) .

e) When $F = \mathbb{Q}$, $v = \text{ord}_p$, what is the valuation ring R_v ?

f) Suppose k is a field, and consider $F = k(t)$, the quotient field of the ring of polynomials $k[t]$ with coefficients in k . Show that the map v which takes a rational function $\frac{p(x)}{q(x)}$ to $\deg(q(x)) - \deg(p(x))$ is a discrete valuation of $k(t)$. Note that this is consistent with our previous convention that the degree of the zero polynomial is $-\infty$!

⁴Denoting this element by π is traditional. Needless to say (?) it has nothing to do with 3.1415926535897...