

4400/6400 PROBLEM SET 3

Recommended instructions: For 4400, solve at least 7 problems, including (for an A grade) at least one starred part of a problem. For 6400, solve at least 9 problems, including at least two starred parts and at least one of the last three problems. A part of a problem labelled (O) is always optional.

The first four problems pertain to the Euclidean algorithm, which we will be applying to positive integers $a \geq b \geq 1$.

3.1(E): Explain how to use a handheld calculator to find the q and r such that $a = qb + r$.

3.2(E): Use the Euclidean algorithm to find the gcd of 12345 and 67890. (Suggestion: Get a calculator to do the divisions for you, using the previous exercise.)

3.3: Recall that the Euclidean algorithm generates a sequence of remainders: say $r_{-1} = a$, $r_0 = b$ and

$$r_{i-1} = q_{i+1}r_i + r_{i+1},$$

terminates when $r_{n+1} = 0$ and then r_n , the last nonzero remainder, is $\gcd(a, b)$.

- Show that for all $-1 \leq i \leq n$, $0 \leq r_{i+1} < r_i$.
- Explain why the result of part a) implies that the algorithm is an algorithm (i.e., that it terminates eventually for all inputs).
- Show that in fact $r_{i+2} < \frac{r_i}{2}$ for all $i \leq n+1$.
(Suggestion: consider separately the cases $r_{i+2} < \frac{r_{i+1}}{2}$ and $r_{i+2} \geq \frac{r_{i+1}}{2}$; apply part a) in the first case, and in the second case use $r_{i+1} = r_{i-1} - q_{i+1}r_i$.)
- Explain why the result of part b) implies that the Euclidean Algorithm terminates in at most $2 \log_2(b)$ steps, as advertised in class.
- (O) Let F_n be the n th Fibonacci number (as usual $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$). Deduce from part d) the remarkable inequality¹: for all $n \geq 0$, $F_{n+2} > 2F_n$. Note that this inequality is not best possible. How can it be improved, and what do these improvements suggest for the running time of the Euclidean algorithm?

3.4: Find all integer solutions to each of the following equations:

- $105x + 121y = 1$.
- $12345x + 67890y = \gcd(12345, 67890)$.
- $54321x + 9876y = \gcd(54321, 9876)$.

3.5: Let a, b, c, N be integers. Under what conditions does the linear equation

$$xa + yb + zc = N$$

¹I'm being sarcastic here, sorry: I'm not much of a Fibonacci fan.

have an integer solution (x, y, z) ?²

3.6(O): Find all integer solutions (x, y, z) to

$$3x + 4y + 5z = 1.$$

Suggestion: First find a particular solution (x_0, y_0, z_0) ; second find the general solution to $3x + 4y + 5z = 0$, and then add. It may help to think of this in terms of linear algebra (planes, scalar products).

3.7: Let a and b be relatively prime positive integers, and $N \in \mathbb{N}$.³ We are interested in solutions (x, y) to $xa + yb = N$ with $x, y \in \mathbb{N}$.

a)(E) Show that this is not always possible: e.g. show that the equation $3x + 7y = 11$ has no solution in non-negative integers x and y . Interpret the result in terms of (simplified) football.

b)* More generally, show that one cannot write $ab - a - b$ as $xa + yb$ with $x, y \in \mathbb{N}$.

c)* Show that if $N > ab - a - b$, one can write N as $xa + yb$ with $x, y \in \mathbb{N}$.

d)* Show that, in fact, exactly half of all integers N , $1 \leq N \leq ab - a - b + 1$ can be written as $xa + yb$ with $x, y \in \mathbb{N}$.

Comment: This is one case where adding more variables makes the problem harder: for the equation $xa + yb + zc = N$ there is no closed form solution for the largest value of N which cannot be written as a non-negative integral linear combination of three integers a, b, c with $\gcd(a, b, c) = 1$ (although one can show that such an N exists). Many people have written papers on this topic over the years, including me:

<http://www.cs.uwaterloo.ca/journals/JIS/VOL8/Clark/clark80.pdf>

You might try your hand at the following “real life” special case:

3.8: Chicken McNuggets are (or were, up until recently) sold in packs of 6, 9 and 20. What is the largest number of Chicken McNuggets you *cannot* buy?

3.9: Factor $123 + 456i$ into irreducibles in the Gaussian integers.

3.10(G):

a) Show that in any commutative ring R , if $x = uy$ for some unit $u \in R^\times$, then $(x) = (y)$.

b) If R is an integral domain, show the converse: if $(x) = (y)$, then $y = xu$ for some unit u .⁴

3.11(G): Let D be a squarefree integer – not 0 or 1 – and put

$$R_D = \mathbb{Z}[\sqrt{D}] = \mathbb{Z}[X]/(X^2 - D).$$

²Of course one could ask a similar question for integers a_1, \dots, a_n , but if you can do the case of $n = 3$ you can do the general case, which is only notationally more elaborate.

³Recall that, according to me, $\mathbb{N} = \{0, 1, 2, \dots\}$.

⁴In fact there are non-integral domains for which this fails; thanks to Ted Shifrin for showing me an example.

a) Show that R_D is an integral domain, with quotient field

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

Note that this field can be construed to be a subfield of \mathbb{C} ; if $D > 0$, it actually sits inside \mathbb{R} , albeit not in as geometrically pleasant a way:

b)* Suppose $D > 1$; show that $\mathbb{Z}[\sqrt{D}]$ is dense in \mathbb{R} : that is, every nonempty open interval (a, b) of \mathbb{R} contains a number of the form $a + b\sqrt{D}$ for some $a, b \in \mathbb{Z}$.

c) Define the norm map $N : \mathbb{Q}[\sqrt{D}] \rightarrow \mathbb{Q}$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

Show that N is multiplicative:

$$N((a + b\sqrt{D})(c + d\sqrt{D})) = N(a + b\sqrt{D})N(c + d\sqrt{D}).$$

d) For $z \in \mathbb{Q}[\sqrt{D}]$, show that $N(z) = 0 \iff z = 0$, and that $N(z) = \pm 1$ iff z is a unit in R_D . (Hint for the last part: $(a + b\sqrt{D})^{-1} = \frac{a - b\sqrt{D}}{a^2 - Db^2}$.)

d') Show that, for any $D < -1$, the units of $\mathbb{Z}[\sqrt{D}]$ are ± 1 .

e) Can you find a value of $D > 1$ for which $\mathbb{Z}[\sqrt{D}]$ has more units than just ± 1 ?

f) Suppose $z \in R_D$ is such that $N(z) = \pm p$, for p a prime number. Show that z is irreducible in $\mathbb{Z}[\sqrt{D}]$.

3.12(G)*: Which integers n are norms of irreducible elements z of $\mathbb{Z}[i]$?