

4400/6400 PROBLEM SET 2

A sufficient number of problems: 6 for 4400 students, 8 for 6400 students.

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

2.1) Explain how to use a nonprogrammable handheld calculator to find the q and the r such that $a = qb + r$.

2.2) Use the Euclidean Algorithm to find the gcd of 12345 and 67890.

2.3) Let us analyze the Euclidean algorithm applied to integers $a \geq b \geq 1$. It is helpful to give a precise labelling to the sequence of remainders: $r_{-1} = a$, $r_0 = b$,

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

The algorithm terminates as soon as it reaches an n such that $r_{n+1} = 0$.

a) Explain why we have that for all i , $-1 \leq i \leq n$, $0 \leq r_{i+1} < r_i$, and why this implies that the algorithm is guaranteed to terminate (i.e., it really is an algorithm).

b) Show that r_n , the last nonzero remainder, is equal to $\gcd(a, b)$.

c) Show that for all $i \leq n + 1$, $r_{i+2} < \frac{r_i}{2}$.

d) Deduce that the Euclidean Algorithm applied to $a \geq b \geq 1$ will terminate in at most $2 \log_2(b) + 1$ steps. (That's fast!)

2.4) Find all integer solutions to each of the following equations:

a) $105x + 121y = 1$.

b) $12345x + 67890y = \gcd(12345, 67890)$.

c) $54321x + 9876y = \gcd(54321, 9876)$.

2.5) Prove the **Generalized Euclid's Lemma**: if $a, b, c \in \mathbb{Z}$ are such that $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

2.6) Find all integer solutions (x, y, z) to

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

2.7) Let a and b be relatively prime positive integers and $N \in \mathbb{N}$. We are interested in solutions (x, y) to $xa + yb = N$ with $x, y \in \mathbb{N}$, i.e., non-negative integral solutions.

a) Give an example of a, b, N as above for which $xa + yb = N$ has no non-negative integral solution. Extra points¹ if your example comes from real life, like the football example $a = 2$, $b = 3$, $N = 1$.

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

c)* Show that every $N > ab - a - b$ can be written as $xa + yb$ for some $x, y \in \mathbb{N}$.

Thanks to Kelly Edenfield for pointing out typos.

¹So to speak.

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

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

2.9) Suppose that a_1, \dots, a_d are positive integers with $\gcd(a_1, \dots, a_d) = 1$.

a)* Show that for all sufficiently large N , there exist $x_1, \dots, x_d \in \mathbb{N}$ such that

$$(1) \quad x_1 a_1 + \dots + x_d a_d = N.$$

b)* For fixed a_1, \dots, a_d as above and $N \in \mathbb{Z}^+$, define

$$r(N) = \#\{(x_1, \dots, x_d) \in \mathbb{N}^d \mid x_1 a_1 + \dots + x_d a_d = N\},$$

i.e., $r(N)$ counts the number of representations of the non-negative integer N as a non-negative integral combination of a_1, \dots, a_d . Show that

$$r(N) \sim \frac{N^{d-1}}{(d-1)! (a_1 \cdots a_d)}.$$

(Here by $f(N) \sim g(N)$ we mean $\lim_{N \rightarrow \infty} \frac{f(N)}{g(N)} = 1$.)

c)(U) Define the **Frobenius number** $f(a_1, \dots, a_d)$ to be the largest positive integer N such that (1) has no solution in non-negative integers x_1, \dots, x_d . (For example, 2.7b) and c) give $f(a_1, a_2) = a_1 a_2 - a_1 - a_2$.) Can you find a similarly simple exact formula for f in the general case? Or even for $d = 3$?²

2.10) In any primitive Pythagorean triple (x, y, z) , show that exactly one of x, y, z is divisible by 5.

2.11) Consider the Diophantine equation $3X^2 + 7Y^2 = 3Z^2$.

a) Find all \mathbb{Q} -rational points on the curve $x^2 + \frac{7}{3}y^2 = 1$.

b) Use part a) to find all integral solutions to $3X^2 + 7Y^2 = 3Z^2$ up to scaling.

c)* Find all primitive integral solutions to $3X^2 + 7Y^2 = 3Z^2$, i.e., all solutions with $\gcd(X, Y, Z) = 1$.

2.12) For $a, b, c \in \mathbb{Z} \setminus \{0\}$, consider the Diophantine equation $aX^2 + bY^2 = cZ^2$.

a) Suppose that $a, b > 0$ and $c < 0$. Show that there are no nontrivial \mathbb{R} -solutions, so certainly no nontrivial \mathbb{Z} -solutions.

b) Show that $3X^2 + 5Y^2 = Z^2$ has no nontrivial \mathbb{Z} -solutions, even though it has nontrivial \mathbb{R} -solutions.

²Warning: you can't (there are theorems to this effect!). But it's fun to think about anyway.