

Miscellaneous mathematical concepts

1. “For all” and “there exists”

In mathematics, many assertions involve the idea of “for all”. Others involve the idea of “there exists”. Still others have both as ingredients.

“For all x ” has the shorthand form $(\forall x)$.

“There exists x ” has the shorthand form $(\exists x)$.

There are many ways to express these two concepts in English but you can learn to recognize them.

Here are some examples of statements that can be re-expressed in a shorter form using these ideas. They all apply to real numbers, which we won't mention explicitly.

Example (i): “For any $y \geq 0$ there is an x whose square is y ” becomes $(\forall y \geq 0)(\exists x)(y = x^2)$.

Example (ii): “Any nonnegative real number is in the range of the squaring function $y = x^2$.” becomes the same as (i).

Example (iii): “Given any y with $|y| \leq 1$ there is an x so that (x, y) lies on the circle $x^2 + y^2 = 1$ ” becomes $(\forall y)(|y| \leq 1 \Rightarrow (\exists x)(x^2 + y^2 = 1))$.

The ingredients in these mathematical “sentences” (assertions) are \forall , \exists , variable letters, “and”, “or”, “not”, $=$, inequalities, \Rightarrow , and parentheses. If we were talking about sets we would use \in also. Some of these ingredients can be re-expressed using others, but it's easier just to use them all. For “not =” you can use \neq , etc.

Problem Q-1. Write each of these in shorter form as in the examples above.

- The range of the function $y = x^3 - x$ is all numbers.
- The real numbers obey the law $x + y = y + x$.
- If a number is positive so is its square.
- There is a solution to the equation $1 - 8x + x^2 = 5$.
- It is possible to find x and y so that $17x + 25y = 6$ and $101x - 37y = 13$.
- For at least one a , the equation $ax = x + 1$ has no solution. (For “has no” you can use $\nexists x$.)
- Re-do (f) using the idea that “there does not exist x with property P ” is the same as “for all x we have not- P ”. (So it isn't ever really necessary to use \nexists .)

(You are not asked to prove any statements or solve for any answers; just restate them.)

2. Partitions

A *partition* of a set S is a list of subsets A_1, \dots, A_n (for some n) so that

- (i) $A_1 \cup A_2 \cup \dots \cup A_n$ is all of S .
- (ii) The A_i are pairwise disjoint, i.e., $A_i \cap A_j = \emptyset$ for $i \neq j$.

The subsets are called “blocks” or “classes” (an older term).

More generally, it is OK to have infinitely many blocks, in which case (i) can be expressed as $\bigcup_i A_i = S$.

Problem Q-2. In each of the following examples, say whether the subsets form a partition, and if they are not, say why not. (If they are a partition, no proof is needed.)

(a) S is the set of seven plants in Problem G-9 and the blocks are the ones the problem asks for.

(b) S is \mathbb{R}^3 and the blocks are a 2-dimensional subspace and all the planes parallel to it.

(c) S is \mathbb{R}^3 and the blocks are a 1-dimensional subspace and all the lines parallel to it.

(d) S is \mathbb{R}^3 and the blocks are all the 1-dimensional subspaces.

(e) S is \mathbb{Z} and there are two blocks, one consisting of all even integers and the other consisting of all odd integers.

(f) S is \mathbb{Z} and there are ten blocks, each consisting of integers that are congruent to each other modulo 10. For example, one of the blocks is $\{\dots, -13, -3, 7, 17, 27, \dots\}$.

(g) S is any set and the blocks are all the singleton subsets (1-element subsets).

(h) $f : S \rightarrow T$ is a function between sets, and the blocks are the inverse images of elements in the image [range] of f , in other words, the subsets $f^{-1}(t)$ for $t \in \text{image } f$.

(i) S is $\text{Pols}(\mathbb{R})$ (polynomials of all degrees) and for each $r \in \mathbb{R}$ there is a block $A_r = \{f \in \text{Pols}(\mathbb{R}) \mid f(r) = 0\}$.

(j) $S = \mathbb{R}^2$ and for each $m, n \in \mathbb{Z}$ there is a block $A_{m,n} = \{(x, y) \mid m \leq x < m + 1, n \leq y < n + 1\}$.

Problem Q-3. (a) Show that in a vector space V , the nonzero part $V \setminus \{0\}$ (meaning V with $\{0\}$ omitted) is partitioned by the nonzero parts of the 1-dimensional subspaces of V .

(b) If V is a 3-dimensional vector space over $GF(q)$, find a formula for the number of 1-dimensional subspaces of V .

(Method: Use (a). How large are the 1-dimensional subspaces? Your answer will be a polynomial in q . Does it check with the solution to Problem J-5? As mentioned before, q will be a power of a prime, but that fact isn't needed for this problem.)

3. The Euclidean algorithm

Problem Q-4. The *Euclidean algorithm* is an efficient way of finding the greatest common divisor of two integers: Given two positive integers such as 30 and 56, replace the larger one by its remainder after division by the smaller one, and keep repeating this process until one of them is 0. Then the gcd is the other number left. For example, 30 and 56 become 30 and 26, which become 4 and 26, which become 4 and 2, which become 0 and 2, so the gcd is 2.

(a) Explain why this works. (Method: If the integers are a and b with $0 < a < b$, if you divide b by a and get quotient q and remainder r , then $b = qa + r$. Show that the set of positive integers that divide both a and b is exactly the same as the set of positive integers that divide both a and r . How about the gcd of 0 and d , once you have reached that stage? If you wish, you may use the notation common in number theory: $d|a$ means “ d divides a ”. Note: It is OK to divide *into* 0 but not *by* 0.)

(b) Find the gcd of 91 and 221 this way.

Problem Q-5. Decide which two numbers a, b between 30 and 60 with $a < b$ will take the most steps of the Euclidean algorithm to get their gcd. (Give your reasoning.)

Problem Q-6. Solving for the gcd as a linear combination.

It is a theorem about integers that if $d = \gcd(a, b)$ then there exist integers r and s with $d = ar + bs$. For example, there should be r and s so $2 = 30r + 56s$.

Here is a method to find r and s by getting more information out of the Euclidean algorithm. First, put the two numbers as a column of a matrix augmented by the identity matrix: $\begin{bmatrix} 56 & 1 & 0 \\ 30 & 0 & 1 \end{bmatrix}$. Then row-reduce as best you can using integer operations only, as follows. At each step, subtract off an integer multiple of one row from the other row so that the left columns

follow the Euclidean algorithm. Do not scale rows. You don't need to swap rows either.

$$\begin{bmatrix} 56 & 1 & 0 \\ 30 & 0 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 26 & 1 & -1 \\ 30 & 0 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 26 & 1 & -1 \\ 4 & -1 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 7 & -13 \\ 4 & -1 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 7 & -13 \\ 0 & -15 & 28 \end{bmatrix}.$$

Now in the last matrix look at the row that has the gcd. This row is in the row space of the original matrix. With what coefficients? Easy—from the identity matrix part, we see that this row with 2 is 7 times the first row of the original matrix minus 13 times the second row. But this says $7 \cdot 56 + (-13) \cdot 30 = 2$.

As a check on arithmetic, since these row operations do not affect determinants, along the way the determinant of the right-hand 2×2 submatrix should always be 1.

Do this procedure to express the gcd of 91 and 221 as an integer linear combination of these two integers.

(You are not asked to prove the theorem, but this procedure itself really amounts to the proof. Be careful about which coefficient goes with 91 and which with 221, and check your answer.)

Problem Q-7. $p = 101$ is a prime. Find the multiplicative inverse of 97 in the field \mathbb{Z}_{101} .

(Method: This sounds difficult but it's not. The gcd of a prime p and a number not divisible by p is 1, so you can find r and s with $1 = 101r + 97s$. In \mathbb{Z}_{101} , 101 is the same as 0 so this expression says $1 = 0r + 97s$, so s is the multiplicative inverse. If s is among 0 to $p - 1$, you'll need to change it by \pm a multiple of p .)