

# Mathematics 170: Ideas in Mathematics

## Midterm exam solutions

Here are solutions to the exam.

**1.** Consider an equilateral triangle with side length 1. Let there be 10 points inside the triangle. Is it possible that no two of these points are within distance  $1/3$  of each other? Justify your answer.

*Solution.* No, it is not possible. Use the pigeonhole principle. The triangle can be divided into nine equilateral triangles, each with side length  $1/3$ . There must be two of these points in the same triangle. The distance between any two points in the same equilateral triangle is at most the side length, so the two points in the same triangle must be within distance  $1/3$  of each other.

**2.** Prove (by induction, or otherwise) that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for all positive integers  $n$ .

*Solution.* We prove this by induction. The base case, for  $n = 1$ , is just  $1 = 1(1+1)/2$ , which is obvious.

For the inductive step, we assume that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for some positive integer  $n$ , and show that

$$1 + 2 + 3 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}.$$

This is algebra.  $1 + 2 + 3 + \cdots + n = n(n+1)/2$  by the inductive hypothesis. So the left-hand-side of the above equation is

$$\frac{n(n+1)}{2} + (n+1) = \frac{n^2 + n}{2} + (n+1) = \frac{n^2 + n + 2n + 2}{2} = \frac{(n+1)(n+2)}{2}$$

which is what we wanted.

**3.** Imitate Cantor's proof of the uncountability of the real numbers to find a real number not on the list

$$\begin{aligned} r_1 &= 3.14159\dots \\ r_2 &= 1.41421\dots \\ r_3 &= 2.71828\dots \\ r_4 &= 0.57721\dots \\ r_5 &= 4.66920\dots \\ &\vdots \end{aligned}$$

*Solution.* Go down the diagonal of the array. The  $n$ th digit after the decimal point in your number should *not* be the  $n$ th digit of  $r_n$ , which is indicated in boldface. (These were not in boldface on the original exam.) Also make sure not to use 9.

**4.** Show that the cardinality of the set of all pairs of natural numbers is the same as the cardinality of the set of all natural numbers.

*Solution.* This is Cantor's other diagonal proof. We write the pairs of natural numbers in a grid

$$\begin{array}{ccccccc} (1, 1) & (1, 2) & (1, 3) & (1, 4) & \cdots & & \\ (2, 1) & (2, 2) & (2, 3) & (2, 4) & \cdots & & \\ (3, 1) & (3, 2) & (3, 3) & (3, 4) & \cdots & & \\ (4, 1) & (4, 2) & (4, 3) & (4, 4) & \cdots & & \\ \vdots & \vdots & \vdots & \vdots & \ddots & & \end{array}$$

and proceed down the "anti-diagonals" (which run from northeast to southwest) in turn, giving the list

$$(1, 1), (1, 2), (2, 1), (1, 3), (2, 2), (3, 1), (1, 4), (2, 3), (3, 2), (4, 1) \dots$$

**5(a).** Compute  $3^{43} \pmod{8}$  using Euler's theorem.

*Solution.* First,  $\phi(8) = 4$ . (This is the number of numbers less than 4 and having no factor in common with it, which are 1, 3, 5, 7.) Euler's theorem states that  $a^{\phi(n)} \equiv 1 \pmod{n}$  whenever  $a$  and  $n$  have no common factor. Since 3 and 8 have no common factor, this gives us  $3^4 \equiv 1 \pmod{8}$ . (You could check this explicitly, since  $3^4 = 81$ .) Thus

$$3^{43} = (3^4)^{10}(3^3) \equiv 3^3 \pmod{8}$$

and  $3^3 = 27$ ; the answer is the remainder when 27 is divided by 8, which is 3.

**5(b).** Why can Fermat's little theorem not be used in part (a)?

*Solution.* Fermat's little theorem only applies when the modulus is prime. 8 is not prime.

**6.** Bank identification numbers consist of nine digits  $n_1, n_2, \dots, n_9$ , such that

$$7n_1 + 3n_2 + 9n_3 + 7n_4 + 3n_5 + 9n_6 + 7n_7 + 3n_8 + 9n_9 \equiv 0 \pmod{10}.$$

Consider the bank identification number

$$211X72946$$

where  $X$  is a missing digit. What is  $X$ ?

*Solution.* Putting the claimed bank identification number into the formula, we get

$$7 \cdot 2 + 3 \cdot 1 + 9 \cdot 1 + 7 \cdot x + 3 \cdot 7 + 9 \cdot 2 + 7 \cdot 9 + 3 \cdot 4 + 9 \cdot 6 \equiv 0 \pmod{10}.$$

Doing the arithmetic gives  $194 + 7x \equiv 0 \pmod{10}$ . So  $7x \equiv 6 \pmod{10}$ ; that is,  $7x$  is six more than a multiple of 10. A multiple of 7 which is six more than a multiple of 7 is  $56 = 7 \cdot 8$ , which can be found by trial and error; the answer is  $x = 8$ .

7. Explain in a few sentences the major steps of the proof that positive integers have unique prime factorizations.

*Solution.* There are many ways to answer this, but what I had in mind was something like the following. Assume there are positive integers that do not have unique prime factorizations. Then there is a smallest integer with two or more prime factorizations; call it  $n$ . Let  $n = p_1 \dots p_r = q_1 \dots q_s$ , where none of the  $p_i$  equal any of the  $q_j$  and  $p_1$  is the smallest among all the primes. Then using the division algorithm to divide  $q_1$  by  $p_1$ , we can find a smaller number  $k$  which also has two prime factorizations, which is a contradiction. This works because we know that the remainder in this division is less than  $p_1$ ; in number systems where remainders don't work this way we don't have unique factorization.

8. We have seen that an infinite decimal corresponds to a rational number if and only if it is eventually repeating. If instead we consider real numbers expressed in some other base, is this still true? Explain why or why not.

*Solution.* On the one hand, if we have an infinite "decimal" in another base, we can sum a geometric series to find the rational number it represents. On the other hand, if we have two integers and we divide them to find the "decimal" expansion, there are only a finite number of remainders which are possible, so the remainders must eventually repeat, and the expansion is eventually repeating. The answer is yes.

9. Recall the RSA algorithm for cryptography, here reproduced as it appeared on Homework 3:

1. Choose two distinct primes  $p$  and  $q$ . (These are usually of similar size, and large; in our examples they will be small.)

2. Compute  $n = pq$ ; this will be the modulus.

3. Compute  $\phi(n) = (p-1)(q-1)$ , the *totient* of  $n$ . This is the number of numbers among  $1, 2, \dots, n-1$  which have no factor in common with  $n$ .

4. Choose an exponent  $e$  such that  $1 < e < \phi(n)$ , where  $e$  and  $\phi(n)$  are relatively prime.  $e$  is the *encoding exponent*.

5. Find  $d$  such that  $de \equiv 1 \pmod{\phi(n)}$ , by either trial and error or the Euclidean algorithm.  $d$  is called the *decoding exponent*.

Then the *public key* (which is used to encode messages to be sent to you) is the pair of numbers  $(n, e)$ ; the *private key* is the single number  $d$ . To encrypt the message  $W$ , compute  $C = W^e \pmod{n}$ , and send that. To decode the ciphertext  $C$ , compute  $C^d \pmod{n}$ . This will be  $W$ .

**Question:** Why do we choose a decoding exponent  $d$  such that  $de \equiv 1 \pmod{\phi(n)}$ ? In particular, what theorem must we use to prove that this is the correct decoding exponent, and why?

*Solution.* The reason for this choice of decoding exponent is that decoding should reverse encoding: that is, after encoding and then decoding we should get back the original message. Encoding and then decoding corresponds to raising the original message  $W$  to the  $de$  power and reducing  $\pmod{n}$ . Euler's theorem allows us to ignore multiples of  $\phi(n)$  in the exponent;  $de$  is one more than a multiple of  $\phi(n)$ , and so  $W^{de} \equiv W \pmod{n}$ .

10. We saw two proofs that  $\sqrt{2}$  is irrational. Explain why *one of these proofs* fails to

show that  $\sqrt{4}$  is irrational. (The answer should be specific to one of the proofs we saw in class; the observation that  $\sqrt{4}$  is rational, by itself, does not suffice.)

*Solution.* In one proof that we gave, we wrote  $\sqrt{2} = c/d$ , which we rearranged to get  $c^2 = 2d^2$ . We then observed that  $c^2$  is divisible by 2 and so  $c$  must be divisible by 2, which is why the proof worked. But if  $c^2$  is divisible by 4, then  $c$  is not necessarily divisible by 4.

In the other proof we gave, we considered the prime factorizations of  $c$  and  $d$  in  $c^2 = 2d^2$ . On the left-hand side, there must be an even number of twos in the prime factorization; on the right-hand side there must be an odd number of twos. But this does not work when 2 is replaced with 4 because now both sides have an even number of twos.

**END OF EXAM**