My abstract algebra exercises

Evgeny Markin

2023

Contents

0.1 Basics 2
- 0.1.1 2
- 0.1.2 2
- 0.1.3 3
- 0.1.4 3
- 0.1.5 3
- 0.1.6 4
- 0.1.7 4

0.2 Properties of the Integers 4
- 0.2.1 4
- 0.2.2 5
- 0.2.3 5
- 0.2.4 5
- 0.2.5 6
- 0.2.6 6
- 0.2.7 6
- 0.2.8 7

0.3 Z/nZ: The Integers Modulo n 7
- 0.3.1 7
- 0.3.2 7
- 0.3.3 7
- 0.3.4 8
- 0.3.5 8
- 0.3.6 8
- 0.3.7 9
- 0.3.8 9
- 0.3.9 9
- 0.3.10 9

Prelinimaries

0.1 Basics

0.1.1

Determine which of the following elements of A lie in B

M is defined to be

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$B = \{x \in A : MX = XM\}$$

thus all of the following are in B.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

0.1.2

Prove that $P, Q \in B \Rightarrow P + Q \in B$

Suppose that $P, Q \in B$. Then we follow that

$$(P + Q)M = PM + QM = QM + PM = (Q + P)M$$

where we've used distributive and commutativity under addition for matrices

0.1.3

Prove that $P, Q \in B \Rightarrow PQ \in B$

Suppose that $P, Q \in B$. Thus we follow that $PM = MP$ and $QM = MQ$. Thus

$$(PQ)M = PQM = P(QM) = P(MQ) = PMQ = (PM)Q = (MP)Q = M(PQ)$$

as desired.

0.1.4

Find conditions on p, q, r, s, *which determine precisely when*

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in B$$

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$$

thus we follow that we need to have

$$\begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}$$

thus we follow that the matrix is in B if and only if $r = 0$ and $p = s$. (ocave seems to support this point).

0.1.5

Determine whether the following functions f *are well-defined:*

(a)

$$f : Q \to Z : f(a/b) = a$$

If we assume that a/b is in form, where $b > 0$ and a/b in their lower terms, then the function is well-defined. Otherwise, we've got that

$$2/4 = 1/2$$

but

$$f(2/4) = 2 \neq 1 = f(1/2)$$

(b)

$$f : Q \to Q : f(a/b) = a^2/b^2$$

is indeed well-defined, since for every $a \in Q$ there is only one square.

0.1.6

Determine whether the function $f : R^+ \to Z$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well-defined.

This is a somewhat trick question, since we've got that

$$1 = 0.99999999...$$

which in this case gives us that f is not well-defined.

0.1.7

Let $f : A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \Leftrightarrow f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f.

$$f(a) = f(a) \Rightarrow a \sim a$$
$$(f(a) = f(b) \wedge f(b) = f(c) \Rightarrow f(a) = f(c)) \Rightarrow (a \sim b \wedge b \sim c \Rightarrow a \sim c)$$
$$a \sim b \Rightarrow f(a) = f(b) \Rightarrow f(b) = f(a) \Rightarrow b \sim a$$

which gives us reflexive, transitive and symmetric properties, thus $\sim$ is an equivalence relation.

We follow that if $x \in B$ and $a, b \in f^{-1}(\{x\})$, then $a \sim b$ by definition. Suppose that $a \sim b$. Then we follow that $f(a) = f(b)$, therefore $a \in f^{-1}(\{f(a)\}) \wedge b \in f^{-1}(\{f(a)\})$. Thus we follow that if $a \sim b$, then they are fibers for the same value. Thus we follow that $a \sim b$ if and only if $(\exists x \in B)(a, b \in f^{-1}(\{x\})$. Thus we follow that fibers of f are indeed the equivalence classes for $\sim$.

0.2 Properties of the Integers

0.2.1

Find GCD and LCM for following numbers and find integers x and y such that $ax + by = gcd(a, b)$

```
gcd:   1; lcm:        260, 2 * 20 + -3 * 13 = 1
gcd:   3; lcm:       8556, 27 * 69 + -5 * 372 = 3
gcd:  11; lcm:      19800, 8 * 792 + -23 * 275 = 11
gcd:   3; lcm:   21540381, -126 * 11391 + 253 * 5673 = 3
gcd:   1; lcm:    2759487, -105 * 1761 + 118 * 1567 = 1
gcd: 691; lcm:   44693880, -17 * 507885 + 142 * 60808 = 691
```

0.2.2

Prove that if the integer k divides the integers a and b, then k divides $as+bt$ for every pair of integers s and t

We follow that because k divides both a and b it also divides (a, b). Since (a, b) divides both a and b we follow that there exist $q, w \in Z$ such that $a = q(a, b), b = w(a, b)$. Thus

$$as + bt = q(a, b) + w(a, b) = (q + w)(a, b)$$

thus we follow that (a, b) divides $as + bt$. Since $|$ is transitive, we follow that $k|(a, b)$ and $(a, b)|as + bt$ implies that $k|as + bt$, as desired.

(We could've actually skip this part, don't know why I've used it)

0.2.3

Let a, b, N be fixed integers with $a, b \neq 0$ and let $d = (a, b)$. Suppose that $x_0, y_0 \in Z$ are such that $ax_0 + by_0 = N$. Prove that

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = N$$

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + a\frac{b}{d}t + by_0 - b\frac{a}{d}t = ax_0 + by_0 + t(\frac{ab}{d} - \frac{ab}{d}) =$$

$$= ax_0 + by_0 + t(0) = N + 0 = N$$

0.2.4

Determine the value $\phi(n)$ for each integer $n \leq 30$ where ϕ denotes the Euler ϕ-function

```
phi(1) = 1
phi(2) = 1
phi(3) = 2
phi(4) = 2
phi(5) = 4
phi(6) = 2
phi(7) = 6
phi(8) = 4
phi(9) = 6
phi(10) = 4
phi(11) = 10
phi(12) = 4
phi(13) = 12
```

```
phi(14) = 6
phi(15) = 8
phi(16) = 8
phi(17) = 16
phi(18) = 6
phi(19) = 18
phi(20) = 8
phi(21) = 12
phi(22) = 10
phi(23) = 22
phi(24) = 8
phi(25) = 20
phi(26) = 12
phi(27) = 18
phi(28) = 12
phi(29) = 28
phi(30) = 8
```

0.2.5

Prove the WOP of Z by induction and prove the minimal element is and prove the minimal element is unique.

GOTO set theory book

0.2.6

If f is a prime prove that there do noe exist nonzero integers a and b such that $a^2 = pb^2$

We follow that a and b can be represented as multiples of primes. Therefore the powers of primes, that represent a^2 and b^2 are even. Since the power of p in pb^2 is not even, we follow that such numebers do not exist, as desired

0.2.7

Let p be a prime, $n \in Z^+$. Find a formula for the largest power of p which divides n!

We follow that every p'th number is a multiple of p. Thus the amount of of multiples of p in the list $1, 2, ..., n$ is $\lfloor n/p \rfloor$. To those we need to add the number of multiples of p^2, of which there will be $\lfloor n/p^2 \rfloor$, and thus we follow that the number of multiples of p in n is

$$\sum_{i=1}^{n} \lfloor n/p^i \rfloor$$

Since for every prime number we've got that $p^n > n$, we can follow that this formula will do.

0.2.8

Write a computer program to determine ....

Way ahead of you, check congr.py in progs.

Rest is left for later

0.3 Z/nZ: The Integers Modulo n

0.3.1

Write down explicitly all the elements in the residue classes $Z/18Z$.

$$\overline{1}, \overline{2}, ..., \overline{17}$$

0.3.2

Prove that the distinct equivalence classes in Z/nZ are precisely $\overline{0}, ..., \overline{n-1}$.

Suppose that $q \in N$. We follow that $q = an + r$, where $0 \leq r < n$, thus we follow that $q \in \overline{r}$. Therefore every integer is in one of those sets. Since r is unique, we follow that q is only in one of those sets.

0.3.3

Prove that of $a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0$ is any positive integer then $a \equiv \sum a_n \mod 9$.

We follow that $10 \equiv 1 \mod 9$, and therefore $10^n \equiv 1 \mod 9$ for any $n \in Z$. Thus we can follow that

$$10a_n \equiv a_n \mod 9$$

and in general

$$10^n a_n \equiv a_n \mod 9$$

therefore

$$\overline{a_n 10^n} = \overline{a_n}$$

and since

$$\sum \overline{a_n} = \overline{\sum a_n}$$

we follow the desired result.

0.3.4

Compute the remainder when 37^{100} *is divided by* 29

We follow that

$$37^{100} \equiv 8^{100} \mod 29$$

thus

$$8^1 \equiv 8 \mod 29$$

$$8^2 \equiv 6 \mod 29$$

$$8^4 \equiv 36 \equiv 7 \mod 29$$

$$8^8 \equiv 49 \equiv 20 \mod 29$$

$$8^{10} \equiv 120 \equiv 4 \mod 29$$

$$8^{20} \equiv 16 \mod 29$$

$$8^{40} \equiv 256 \equiv 24 \mod 29$$

$$8^{50} \equiv 96 \equiv 9 \mod 29$$

$$8^{100} \equiv 81 \equiv 23 \mod 29$$

thus we follow that 37^{100} divided by 29 gives us the answer 23.

0.3.5

$$9^{1500} = ...01$$

0.3.6

Prove that the squares of the elements in $Z/4Z$ *are jsut* 0 *and* 1

We follow that

$$0^2 = 0$$

$$1^2 = 1$$

$$2^2 = 4 \equiv 0 \mod 4$$

$$3^2 = 9 \equiv 1 \mod 4$$

so yeah

0.3.7

Prove for any integers a and b that $a^2 = b^2$ never leaves a remainder of 3 *when divided by 4*

From previous exercise we follow that

$$a^2 \equiv [0,1] \mod 4$$

$$b^2 \equiv [0,1] \mod 4$$

thus

$$a^2 + b^2 \equiv [0,1,2] \mod 4$$

0.3.8

Prove that the equation $a^2 + b^2 = 3c^2$ has no nonzero integer solutions

We follow from previous exercise that $a^2 + b^2 \equiv [0,1,2] \mod 4$, and $c^2 \equiv [0,1] \mod 4$, therefore $3c^2 \equiv [0,3] \mod 4$. Thus we follow that the only possible case is when $a^2 + b^2 \equiv 3c^2 \equiv 0 \mod 4$. Thus we follow all of the a^2, b^2 and c^4 have the factor of 4. Thus there exist a_0, b_0, c_0 such that $a^2 = 4^n a_0^2$, $b^2 = 4^n b_0^2$ $c^2 = 4^n c_0^{@}$ and a_0^2, b_0^2, c_0^2 are not divisible by 4 (otherwise we get a contradiction). Thus we follow that

$$a_0^2 + b_0^2 = 3c_0^2$$

all of which are not divisible by 4, which gets us a contradiction, as desired.

0.3.9

Prove that the square of any odd integer always leaves a remainder of 1 *when divided by* 8

We follow that remainders of squares of congruent classes of 8 are

$$01410141$$

thus we follow the desired conclusion.

0.3.10