My (other) exercises in abstract algebra

Evgeny Markin

2023

Contents

Prefase

Started with another book on the subject, switched to Dummit and Foote, since I don't like this book very much. Left here those exercises, because why not

Chapter 1

Integers

1.1 Divisors

1.1.1

Let $m, n, r, s \in Z$. If $m^2 + n^2 = r^2 + s^2 = mr + ns$, prove that $m = r$ and $n = s$.

We can state that there are 3 possible cases: $m = r$ and $n = s$, one of the equation holds and none of the equations hold.

If one of the equations does not hold, suppose that $m \neq r$, then we follow that

$$ns = s^2 = n^2$$

, therefore

$$m^2 + n^2 = mr + ns$$

$$m^2 + n^2 = mr + n^2$$

$$m^2 = mr$$

$$m = r$$

which is a contradiction. Thus we follow that the case when only one of the equations does not hold is impossible.

Suppose now that $m \neq r$ and $n \neq s$. We follow that $(m - r) \neq 0$ and $(n - s) \neq 0$. Thus $(m - r)^2 \neq 0$ and $(n - s)^2 \neq 0$. moreover, since we've got squares we follow that

$$(m - r)^2 > 0$$

and

$$(n - s)^2 > 0$$

thus

$$(m - r)^2 + (n - s)^2 > 0$$

thus

$$(m-r)^2+(n-s)^2 \neq 0$$

therefore

$$(m-r)^2+(n-s)^2 = m^2-2mr+r^2+n^2-2ns+s^2 = (m^2+r^2)+(r^2+s^2)-2(mr+ns) \neq 0$$

Now if we use our identity $m^2+n^2 = r^2+s^2 = mr+ns$, we gonna get that

$$(m^2+r^2)+(r^2+s^2)-2(mr+ns) = (m^2+r^2)+(m^2+r^2)-2(m^2+r^2) = 0 \neq 0$$

which gives us a contradiction. Thus we follow that this case is impossible as well. Thus we conclude that $m=r$ and $n=s$, as desired.

We can prove that simular conclusion holds for reals as well, since we haven't used properties that are exclusive for Z.

1.1.2

For each number between 6 and the next perfect number, make a list containing the number, its proper divisors, and their sum

```
7: 1, sum:  1
8: 1, 2, 4, sum:  7
9: 1, 3, sum:  4
10: 1, 2, 5, sum:  8
11: 1, sum:  1
12: 1, 2, 3, 4, 6, sum:  16
13: 1, sum:  1
14: 1, 2, 7, sum:  10
15: 1, 3, 5, sum:  9
16: 1, 2, 4, 8, sum:  15
17: 1, sum:  1
18: 1, 2, 3, 6, 9, sum:  21
19: 1, sum:  1
20: 1, 2, 4, 5, 10, sum:  22
21: 1, 3, 7, sum:  11
22: 1, 2, 11, sum:  14
23: 1, sum:  1
24: 1, 2, 3, 4, 6, 8, 12, sum:  36
25: 1, 5, sum:  6
26: 1, 2, 13, sum:  16
27: 1, 3, 9, sum:  13
28: 1, 2, 4, 7, 14, sum:  28 PERFECT
```

1.1.3

Find the quotent and remainder when a is divided by b

$$99 = 17 * 5 + 14$$
$$-99 = 17 * (-6) + 3$$
$$17 = 99 * 0 + 17$$
$$-1017 = -11 * 99 + 72$$

1.1.4

Use the Eucledian algorithm to find the following greatest common divisors.

$$(35, 14) = (14, 7) = 7$$
$$(15, 11) = (11, 4) = (4, 3) = (3, 1) = 1$$
$$(252, 180) = (180, 72) = (72, 36) = 36$$
$$(513, 187) = (187, 139) = (139, 48) = (48, 43) = (43, 5) = (5, 3) = (3, 2) = (2, 1) = 1$$
$$(7655, 1001) = (1001, 648) = (648, 353) = (353, 295) =$$
$$= (295, 58) = (58, 5) = (5, 3) = (3, 2) = (2, 1) = 1$$

1.1.5

Use the Eucledian algorith to find the following greatest common divisors

$$(6643, 2873) = (2873, 897) = (897, 182) = (182, 169) = (169, 13) = 13$$
$$(7684, 4148) = (4148, 3536) = (3536, 612) = (612, 476) = (476, 136) = (136, 68) = 68$$
$$(26460, 12600) = (12600, 1260) = 1260$$
$$(6540, 1206) = (1206, 510) = (510, 186) = (186, 138) = (138, 48) = (48, 42) = (42, 6) = 6$$
$$(12081, 8439) = (8439, 3642) = (3642, 1155) =$$
$$= (1155, 177) = (177, 93) = (93, 84) = (84, 9) = (9, 3) = 3$$

1.1.6

1.1.7

Skipped

1.1.8

Let $a, b, c \in Z$. Give a proof for these facts about divisors:

(a) If $b|a$, then $b|ac$

Suppose that $b|a$. We follow that $a = qb$ for some $q \in Z$. Thus we follow that $ca = cqb$. Thus $b|ac$, as desired.

(b) If $b|a$ and $c|b$, then $c|a$

We follow that $a = qb$ and $b = wc$ for some $w, q \in Z$. Thus $a = wqc$, thus $c|a$.

(c) If $c|a$ and $c|b$, then $c|(ma + nb)$

We follow that since $c|a$ and $c|b$ that $c|(a, b)$. We follow that $(a, b)|(ma + nb)$, since $ma + nb$ is a linear combination of a, b. Thus by previous point we follow $c|(ma + nb)$.

1.1.9

Let $a, b, c \in Z$ are such that $a + b + c = 0$. Show that if $n \in Z$ and n is a divbvisor of two of the three integers, then it is also a divisot of the third.

Suppose that $n|a$ and $n|b$. Then we follow that $n|(a, b)$. Since $-a - b = c$ we follow that $(a, b)|c$, thus $n|c$, as desired.

1.1.10

Let $a, b, c \in Z$.

(a) Show that if $b|a$ and $b|(a + c)$, then $b|c$.

We follow that $\exists q, w \in Z$ such that

$$a = qb$$

$$a + c = wb$$

thus

$$qb + c = wb$$

$$c = wb - qb$$

$$c = b(w - q)$$

$$b|c$$

(b) Show that if $b|a$ and $b \not| c$ the $b \not| (a + c)$.

If $b \not| c$, then we follow that there exists $q, w, r \in Z$ such that $0 < r < b$ and

$$a = qb \wedge c = wb + r$$

thus

$$a + c = (q + w)b + r$$

thus $b \not| (a + c)$ as desired.

1.1.11

Let $a, b, c \in Z$ and $c \neq 0$. Show that $bc|ac$ iff $b|a$.

Suppose that $bc|ac$. This means

$$ac = qbc$$

and since $c \neq 0$ we follow that it is equivalent to

$$a = qb$$

i.e. $b|a$. Since every implication here is an equivalence, we follow that we've got a converse as well.

1.1.12

Show that if $a > 0$, then $(ab, ac) = a(b, c)$

We follow that there exist $m, n \in Z$ such that

$$(b, c) = mb + nc$$

thus

$$a(b, c) = a(mb + nc)$$

$$a(b, c) = m(ab) + n(ac)$$

therefore we follow that $a(b, c)$ is a multiple of (ac, bc), thus $(ac, bc)|a(b, c)$

$(b, c)|b$ and $(b, c)|c$, thus $a(b, c)|ab$ and $a(b, c)|ac$, thus $a(b, c)|(ab, ac)$. Thus we follow that $(ac, bc) = a(b, c)$, as desired.

1.1.13

Show that if n is any integer, then $(10n + 3, 5n + 2) = 1$

We know that gcd is a smallest positive linear combination of $10n+3$ and $5n+2$. Thus

$$-(10n + 3) + 2(5n + 2) = -10n - 3 + 10n + 4 = 1$$

Since gcd is a smallest positive linear combination of $10n + 3$ and $5n + 2$, and there is no smaller positive number then 1, we follow that $(10n + 3, 5n + 2) = 1$, as desired.

1.1.14

Show that if n is any integer then $(a + nb, b) = (a, b)$

We follow that (a, b) is the least positive linear combination of a, b. Also, $(a + nb, b)$ is the least linear combination of $a + nb$ and b. Since

$$q(a + nb) + wb = qa + qnb + wb = qa + (qn - w)b$$

we follow that $(a+nb,b)$ is also the linear combination of a and b (because $qn+w$ with fixed qn can be still any number). Since there is only one positive linear combination of a and b, we follow that $(a+bn,b)=(a,b)$, as desired.

1.1.15

For what positive integers n is it true that $(n,n+2)=2$? Prove your claim.

It appears that it is true for all even numbers. It is certainly true, that if n is even, then $n+2$ is also even, therefore both of them are divisible by 2.

We know that $(a,b)=(b,a)$, thus we follow that $(n,n+2)=(n+2,n)$.

Suppose that n is even By euclidean algoritm we've got that

$$(n+2)=1(n)+2$$

thus

$$(n+2,n)=(n,2)=2$$

Thus if n is even, then $(n,n+2)=2$.

If $n=1$, then $(n+2,n)=(3,1)=1$.

If $n>1$ and n is odd, then there exists $k\in N$ such that $k\geq 1$ and $n=2k+1$. THus we follow that $n+2=2k+1+2=2k+3$. Thus

$$(2k+3)=1*(2k+1)+2$$

since $k\geq 1$, we follow that $0\leq 2\leq 2k+1$. Thus we can conclude that

$$(n+2,n)=(2k+3,2k+1)=(2k+1,2)=1$$

Therefore we follow that the only positive numbers such that $(n,n+2)=2$ are the even numbers.

1.1.16

Show that the positive integer n is the difference of two squares if and only if n is odd or divisible by 4.

Let $n\in Z^+$ and $a,b\in Z$ be such that $a^2-b^2=n$.

We follow that since $n\geq 0$, than $a^2-b^2\geq 0$, therefore $a^2\geq b^2$. Since $a^2=(-a)^2$, let us assume that $a,b\geq 0$, because other cases will be trivial.

Since $a^2\geq b^2$, we follow that $a\geq b$, therefore there exists r such that $b+r=a$. Thus

$$n=a^2-b^2=(b+r)^2-b^2=b^2+2br+r^2-b^2=2br+r^2$$

We've got that r is either odd or even. If r is odd, then r^2 is odd as well. Thus the sum of the even number $2br$ and odd r^2 is odd. Therefore n is odd as well. If r is even, then there exists $k \in N$ such that $r = 2k$. Thus

$$n = 2br + r^2 = 2b2k + (2k)^2 = 4bk + 4k^2 = 4(bk + k^2)$$

thus we follow that n is divisible by 4. Therefore we follow that n is either odd or divisible by 4, as desired.

Conversely, suppose that $n \in Z^+$ is either odd or divisible by 4.

If $4|n$, then we follow that there exists $k \in N$ such that $n = 4k$. Thus we follow that

$$(k+1)^2 - (k-1)^2 = k^2 + 2k + 1 - k^2 + 2k - 1 = 4k = n$$

thus we follow that n is the difference of two squares.

If n is odd, then we follow that there exists $k \in N$ such that $n = 2k - 1$. Thus we follow that

$$k^2 - (k-1)^2 = k^2 - k^2 + 2k - 1 = 2k - 1 = n$$

Thus we follow that if n is divisible by 4 or is odd, then it is the difference of two squares, as desired.

1.1.17

Show that the positive integer k is the difference of two odd squares if and only if k is divisible by 8

Suppose that n is the difference between two odd squares. Thus we follow that

$$n = (2k+1)^2 - (2n+1)^2$$

if we expand and contract this expression, then we'll get

$$n = 4(k-n)(n+k+1)$$

We follow that if both n and k are odd or both of them are even, then $(n-k)$ is even. If one of them is odd while the other one is even, then $(n+k+1)$ is even. Thus we follow that $(k-n)(n+k+1)$ is even, therefore there exists q such that

$$2q = (k-n)(n+k+1)$$

thus

$$n = 4 * 2q = 8q$$

thus we follow that n is divisible by 8.

Suppose that n is divisible by 8. Then we follow that there exists k such that $n = 8k$. Thus

$$(2k+1)^2 - (2k-1)^2 = 8k = n$$

thus n is the difference between two odd squares.

1.1.18

Give a detailed proof of the statement in the text that if a and b are integers, then $b|a$ if and only if $aZ \subseteq bZ$.

Suppose that $b|a$. Then we follow that $a = qb$ for some $q \in Z$. Suppose that $n \in aZ$. Then we follow that $n = wa$ for some $w \in Z$. Thus $n = wqb$, therefore $n \in bZ$. Thus we follow that $aZ \subseteq bZ$.

Conversely, suppsoe that $aZ \subseteq bZ$. We follow that because $a = 1a$ we can state that $a \in aZ$. Thus $a \in bZ$, threfore by definition of bZ we follow that there exists $q \in Z$ such that $a = qb$. Thus $b|a$, as desired.

1.1.19

Let $a, b, c \in Z \wedge b > 0 \wedge c > 0 \wedge a = qb + r$.

$$a = qb + r \Leftrightarrow ca = c(qb + r) = cqb + cr = (cq)b + cr$$

Since $r < b$, we follow that $cr < cb$, thus everything holds. (Skipping (b) because I'm lazy)

1.1.20

Let $a, b, n \in Z \wedge n > 1$. Suppose that $a = nq_1 + r_1$ with $0 \leq r1 < n$ and $b = nq_2 + r_2$ with $0 \leq r_2 < n$. Prove that $n|(a - b)$ if and only if $r_1 = r_2$.

Suppose that $n|(a - b)$.

$$(a - b) = nq_1 + r_1 - (nq_2 + r_2) = n(q_1 - q_2) + (r_1 - r_2)$$

Since $0 \leq r_1, r_2 < n$, we follow that $-n < (r_1 - r_2) < n$, thus we follow that if $r_1 \neq r_2$, then we've got a contradiction. Converse case is trivial.

1.1.21

Show that any nonempty set of integers that is closed under substraction must also be closed under addition.

I personally like closure under additive inverse and closure under addition, but whatever.

Suppose that S is closed under substraction and let $a_1, a_2 \in S$. We follow that

$$a_2 \in S$$
$$a_2 - a_2 = 0 \in S$$
$$0 - a_2 = -a_2 \in S$$
$$a_1 - (-a_2) = a_1 + a_2 \in S$$

thus the set is closed under addition, as desired.

1.1.22

1.1.23

skip

1.1.24

Show that 3 divides the sum of the cubes of any three consecutive positive integers

Suppose that $n \in Z^+$. Then we follow that the sum of cubes of 3 consecutive numbers is equal to

$$n^3 + (n+1)^3 + (n+2)^3 = n^3 + n^3 + 3n^2 + 3n + 1 + n^3 + 6n^2 + 12n + 8 =$$

$$= 3n^3 + 9n^2 + 15n + 9 = 3(n^3 + 3n^2 + 5n + 3)$$

thus it is divisible by 3, as desired.

It's also divisible by $n + 1$, since

$$3(n^3 + 3n^2 + 5n + 3) = 3(n + 1)(n^2 + 2n + 3)$$

1.1.25

Find all integers x such that $3x + 7$ is divisible by 11

Suppose that

$$Y = \{y \in Z : (\exists x \in Z)(y = 11x + 5)\}$$

. Then we follow that

$$3(11x + 5) + 7 = 33x + 22 = 11(3x + 2)$$

thus $x \in Y \to 11|3x + 7$.

Can't find the other inclusion.

Rest of the exercises is left for better days.

1.2 Primes

1.2.4

Find all positive integers less than 60 and relatively prime to 60

```
( 1 , 60) =  1
( 7 , 60) =  1
( 11 , 60) =  1
( 13 , 60) =  1
```

```
( 17 , 60) = 1
( 19 , 60) = 1
( 23 , 60) = 1
( 29 , 60) = 1
( 31 , 60) = 1
( 37 , 60) = 1
( 41 , 60) = 1
( 43 , 60) = 1
( 47 , 60) = 1
( 49 , 60) = 1
( 53 , 60) = 1
( 59 , 60) = 1
```

1.2.5

Let $p_1, ...,$ be the sequence of primes and set $a_1 = p_1 + 1$, $a_2 = p_1 p_2 + 1$ and so on. What is the least n such that a_n is composite

$$2 * 3 * 5 * 7 * 11 * 13 + 1 = 30031 = 59 * 509$$

1.2.9

$$2, 1, 2, 2$$

1.2.10

Prove that $n^4 + 4$ is composite if $n > 1$

If n is even, then the sum is even, therefore it's composite. If n is odd, then there exists $k \in N$ such that $n = 2k + 1$. Thus

$$n^4 + 4 = (2k + 1)^4 + 4 = 16k^4 + 32k^3 + 24k^2 + 8k + 5 = (4k^2 + 1)(4k^2 + 8k + 5)$$

thus we follow that it's composite.

1.3 Congruences

1.3.[1, 3, 4, 5, 7, 15, 16]

```
4 x <eq> 1 (mod 7 ) = [2]
2 x <eq> 1 (mod 9 ) = [5]
5 x <eq> 1 (mod 32 ) = [13]
19 x <eq> 1 (mod 36 ) = [19]
```

```
10 x <eq>  5 (mod  21 ) =  [11]
10 x <eq>  5 (mod  15 ) =  [2, 5, 8, 11, 14]
10 x <eq>  4 (mod  15 ) =  []
10 x <eq>  4 (mod  14 ) =  [6, 13]
20 x <eq>  12 (mod  72 ) =  [15, 33, 51, 69]
25 x <eq>  45 (mod  60 ) =  [9, 21, 33, 45, 57]
8 x <eq>  0 (mod  12 ) =  [0, 3, 6, 9]
7 x <eq>  0 (mod  12 ) =  [0]
21 x <eq>  0 (mod  28 ) =  [0, 4, 8, 12, 16, 20, 24]
12 x <eq>  0 (mod  18 ) =  [0, 3, 6, 9, 12, 15]
lambda x: x ** 2, 1, 16] = [1, 7, 9, 15]
lambda x: x ** 3, 1, 16] = [1]
lambda x: x ** 4, 1, 16] = [1, 3, 5, 7, 9, 11, 13, 15]
lambda x: x ** 8, 1, 16] = [1, 3, 5, 7, 9, 11, 13, 15]
lambda x: x ** 3 + 2 * x + 2, 0, 5] = [1, 3]
lambda x: x ** 4 + x ** 3 + x**2 + x + 1, 0, 2] = []
lambda x: x ** 4 + x ** 3 + 2 * x**2 + 2 * x + 1, 0, 3] = []
```

1.3.6

Find all integers x such that $3x + 7$ is divisible by 11

We follow that this is equivalent to congruence

$$3x + 7 \equiv 0 \mod 11$$

$$3x \equiv 4 \mod 11$$

for which the solution is 5. Thus we follow that integers in form

$$3 * (11q + 5) + 7 : q \in Z$$

are the desired solution

1.3.8

Prove that if p is a prime number and a is any integer, such taht $p \not| a$, then the additive order of a modulo p is equal to p.

Suppose that it isn't then we follow that there exists $0 < p' < p$ such that

$$p'a \equiv 0 \mod p$$

$$pq = p'a$$

Thus we've got that $p|p'a$, which is a contradiction of unique prime representation.

1.4 Integers Modulo n

1.4.[1, 2]

modulo.py in progs folder produces answers, not gonna repeat them here

1.4.3

Find the multiplicative inverses of given elements (if possible)

$$[14]_{15} * [14]_{15} = [1]_{15}$$
$$[38]_{83} * [59]_{83} = [1]_{83}$$

351 is a zero divisor in Z_{6669}, to be precise we've got that

$$[351]_{6669} * [19]_{6669} = [0]_{6669}$$

$$[91]_{2565} * [451]_{2565} = [1]_{2565}$$

everyhting was followed from congr.py in progs folder (in essence it comes from usage of Euclidean algorithm)

1.4.4.

Let a and b be integers.

(a) Prove that $[a]_n = [b]_n$ iff $a \equiv b \mod n$.

$$[a]_n = [b]_n$$
$$[a]_n - [b]_n = [0]_n$$
$$[a - b]_n = [0]_n$$
$$n|(a - b)$$
$$a \equiv b \mod n$$

everything here is a equivalence, thus we've got converse case for free.

(b) Prove that either $[a]_n \cap [b]_n = \emptyset$ or $[a]_n = [b]_n$

GOTO set theory book, section on equivalence relations and partitions that they make.

1.4.5

Prove that each congruence class $[a]_n$ in Z_n has a unique representative r that satisfies $0 \le r \le n$

Given that $n > 0$, we follow that there exist unique q and $0 \le r < n$ such that

$$a = nq + r$$

from this we follow that $r \in [a]_n$, as desired.