

## 0 Prelims

### 0.1 Basics

#### 0.1.1

Direct computation or 0.1.4 gives YNYYN

#### 0.1.2

$$\begin{aligned}
 M(P+Q) &= MP + MQ \\
 &= PM + QM, & \text{since } P, Q \in \beta = (P+Q)M \\
 \implies P+Q &\in \beta
 \end{aligned}$$

#### 0.1.3

$$\begin{aligned}
 M(PQ) &= (MP)Q \\
 &= (PM)Q & P \in \beta \\
 &= P(MQ) \\
 &= P(QM) & Q \in \beta \\
 &= (PQ)M \\
 \implies PQ &\in \beta
 \end{aligned}$$

#### 0.1.4

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

yielding a system of equations

$$\begin{aligned}
 p+r &= p & \implies r &= 0 \\
 q+s &= p+q & \implies s &= p \\
 r &= r \\
 r+s &= s & \implies r &= 0
 \end{aligned}$$

So we need  $r = 0, s = p$

#### 0.1.5

1. (a) No, because

$$\begin{aligned}
 \frac{2}{4} &\mapsto 2 \\
 \frac{1}{2} &\mapsto 1
 \end{aligned}$$

- (b) Yes:

$$\begin{aligned}
 \frac{a}{b} &= \frac{c}{d} \\
 \implies \left(\frac{a}{b}\right)^2 &= \left(\frac{c}{d}\right)^2 \\
 \implies \frac{a^2}{b^2} &= \frac{c^2}{d^2}
 \end{aligned}$$

### 0.1.6

No: because there can be multiple decimal representations of numbers. e.g.  $1 = 0.99999 \dots$

### 0.1.7

- Reflexivity:  $f(a) = f(a)$ , hence  $a \sim a$
- Symmetry:

$$\begin{aligned}
 & a \sim b \\
 \implies & f(a) = f(b) \\
 \implies & f(b) = f(a) \\
 \implies & b \sim a
 \end{aligned}$$

- Likewise, transitivity follows from transitivity of equality

The equivalence classes are "clearly" the fibers of  $f$

## 0.2 Properties of the Integers

### 0.2.1

In my notebook not typing it out lol

### 0.2.2

$k|a, b$  means that  $\exists c, d \in \mathbb{Z}$  such that

$$\begin{aligned}
 kc &= a, \\
 kd &= b
 \end{aligned}$$

Then,

$$\begin{aligned}
 as + bt &= kcd + kdb \\
 &= k(cs + db)
 \end{aligned}$$

Hence,  $k|as + bt$

### 0.2.3

Let  $n = cd$ , with ints  $c, d > 1$ . Done.

### 0.2.4

$$\begin{aligned}
 ax + by &= a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) \\
 &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t \\
 &= ax_0 + by_0 \\
 &= N
 \end{aligned}$$

### 0.2.5

1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8

### 0.2.6

Let  $S$  be a nonempty subset of  $\mathbb{Z}^+$ .

Pick  $s_1 \in S$ . Then  $m_1 = s_1$  is the minimal element of  $S_1 = \{s_1\}$ .

Suppose now we have a chain of subsets of  $S$  going

$$S_1 \subset \cdots \subset S_n$$

with  $|S_i| = i$ , and minimal element  $m_n$ . If  $S_n = S$ , we're done. Otherwise, pick  $s_{n+1} \in S - S_n$ .

1. Case:  $s_{n+1} > m_n$   
Then keep  $m_{n+1} = m_n$  as the minimal element
2. Case:  $s_{n+1} < m_n$   
Then set  $m_{n+1} = s_{n+1}$  as the minimal element

In this way, we get that  $S_{n+1}$  has a minimal element  $m_{n+1}$ .

But Case 2 cannot occur inginitely many times, else that would make an infinite chain of positive integers with strict inequalities, which is impossible. I.e.

$$m_1 \geq m_2 \geq \cdots$$

can only have finitely many strict inequalities. Where the chain terminates is the (unique) minimal element

### 0.2.7 S

uppose  $a^2 = pb^2$ . Then  $p|a^2 \implies p|a$ , since  $p$  is prime. Hence  $\exists a_0 \in \mathbb{Z}$  such that  $pa_0 = a$  and  $|a_0| < |a|$  (otherwise we'd have  $p = \pm 1$  which is not prime). Then letting  $c = a_0$

$$a^2 = pb^2 \tag{1}$$

$$\implies (pc)^2 = pb^2 \tag{2}$$

$$\implies p^2c^2 = pb^2 \tag{3}$$

$$\implies pc^2 = b^2 \tag{4}$$

Analagously now, we have  $p|b^2 \implies p|b \implies \exists b_0 \in \mathbb{Z}$  where  $pb_0 = b$  and  $|b_0| < |b|$ . Letting  $d = b_0$  and leaving off from (4),

$$pc^2 = (pd)^2$$

$$\implies c^2 = pd^2$$

$$\implies a_0^2 = pb_0^2$$

which is the same situation we started with before. Hence, we can iterate the process, obtaining integers  $a_1, a_2, a_3, \dots$  and  $b_1, b_2, b_3, \dots$  such that

$$\begin{aligned} |a| &> |a_0| > |a_1| > |a_2| > |a_3| > \cdots, \\ |b| &> |b_0| > |b_1| > |b_2| > |b_3| > \cdots \end{aligned}$$

which is impossible

### 0.2.8

IDK

### 0.2.9

program

### 0.2.10

IDK

### 0.2.11

If  $d|n$ , then we can prime factorize each integer

$$d = p_0^{\alpha_0} \cdots p_k^{\alpha_k}$$

$$n = p_0^{\beta_0} \cdots p_k^{\beta_k}$$

such that  $\alpha_i < \beta_i$  for all  $i$ . Then

$$\phi(d) = p_0^{\alpha_0-1}(p_0-1) \cdots p_k^{\alpha_k-1}(p_k-1)$$

$$\phi(n) = p_0^{\beta_0-1}(p_0-1) \cdots p_k^{\beta_k-1}(p_k-1)$$

And so clearly  $\phi(d)|\phi(n)$

## 0.3 $\mathbb{Z}/n\mathbb{Z}$ : The Integers Modulo $n$

### 0.3.1

$\bar{r} = \{r + 18k | k \in \mathbb{Z}\}$  for  $r = 0, \dots, 17$ . Fuck you.

### 0.3.2

Suppose  $m \in \mathbb{Z}$ . By Euclidean Division,

$$m = kn + r$$

where  $|r| < n$  and we can take  $r \geq 0$  wlg, so  $r \in \{0, \dots, n-1\}$ , and  $m \equiv r \pmod{n}$ , hence falling into the equivalence class  $\bar{r}$ .

### 0.3.3

$$a - \sum_{i=0}^n a_i = \sum_{j=0}^n a_j 10^j - \sum_{i=0}^n a_i$$

$$= \sum_{i=0}^n a_i 10^i - a_i$$

$$= \sum_{i=0}^n a_i (10^i - 1)$$

$$= \sum_{i=0}^n a_i (9 \cdot 11 \dots 1) \quad \text{where the 1 appears } i \text{ times. E.g. } 10000 - 1 = 9999$$

$$= 9 \sum_{i=0}^n a_i (\cdot 11 \dots 1)$$

Which is a multiple of 9. Hence  $a \equiv \sum_{i=0}^n a_i \pmod{9}$

### 0.3.4

Awfully convoluted guess work that eventually got me there lol

### 0.3.5

Same as above

### 0.3.6

$$\begin{aligned}\bar{0}^2 &= \bar{0}^2 = \bar{0} \\ \bar{1}^2 &= \bar{1}^2 = \bar{1} \\ \bar{2}^2 &= \bar{2}^2 = \bar{4} = \bar{0} \\ \bar{3}^2 &= \bar{3}^2 = \bar{9} = \bar{1}\end{aligned}$$

### 0.3.7

Clearly from above the only residues are 0 and 1, so the remainder is at most  $1 + 1 = 2$

### 0.3.8

$a^2 + b^2 = 3c^2$  directly implies that

$$a^2 + b^2 \equiv 3c^2 \pmod{4} \quad (5)$$

from ??, we have that  $a^2, b^2, c^2$  are each congruent either to 1 or 0.

1. Case:  $a^2, b^2 \equiv 1$

Then (5) becomes

$$2 \equiv 3c^2 \pmod{4}$$

but  $c^2 \equiv 0$  or  $c^2 \equiv 1$ , resulting in a contradiction in either case.

2. Case: One of  $a^2, b^2$  is congruent to 1.

Assume wlg  $a^2 \equiv 1$ , so  $b^2 \equiv 0$ . Then we get

$$1 \equiv 3c^2 \pmod{4}$$

Again, setting  $c^2 \equiv 0$  or  $c^2 \equiv 1$  fails

3. Case:  $a^2, b^2 \equiv 0$  Clearly, this is the only possible case that works in (5), and it only works by likewise setting  $c^2 \equiv 0$ .

Hence, we must have  $a^2, b^2, c^2 \equiv 0 \pmod{4}$ . This implies that, for example,

$$a^2 = 0 + 4k \quad k \in \mathbb{Z} \quad (6)$$

$$\implies a^2 = 4k \quad (7)$$

$$\implies a = \pm 2\sqrt{k} \quad (8)$$

So  $a$  is even (and analogously, so is  $b$  and  $c$ ). Dividing (8) by 4, we obtain

$$\frac{a^2}{4} = k$$

implying that  $k$  itself must be even. So we can restrict our possible solution set to

$$a^2 = 4k, k \in 2\mathbb{Z}$$

So  $a^2 = 8k$ , and likewise,  $b^2 = 8l, c^2 = 8m$ . Returning to the original equation,

$$\begin{aligned}a^2 + b^2 &= 3c^2 \\ \implies (8k)^2 + (8l)^2 &= 3(8m)^2 \\ \implies 64k^2 + 64l^2 &= 3 \cdot 64m^2 \\ \implies k^2 + l^2 &= 3m^2\end{aligned}$$

But this is the same situation we started with. So iterating,  $k, l, m$  would themselves have to be multiples of 8, whose factors themselves would have to be multiples of 8, and so on...

**0.3.9**

Let  $s = 2n + 1$  be an odd int

1. Case:  $n = 2k$  is even  
Then

$$\begin{aligned} s^2 &= (2n + 1)^2 \\ &= (2(2k) + 1)^2 \\ &= (4k + 1)^2 \\ &= 16k^2 + 8k + 1 \\ &\equiv 1 \pmod{8} \end{aligned}$$

2. Case:  $n = 2k + 1$  is odd  
Then

$$\begin{aligned} s^2 &= (2n + 1)^2 \\ &= (2(2k + 1) + 1)^2 \\ &= (4k + 3)^2 \\ &= 16k^2 + 24k + 9 \\ &\equiv 1 \pmod{8} \end{aligned}$$

**0.3.10**

Follows from 0.3.14 LOL

**0.3.11**

NO SHIT

**0.3.12**

IDK

**0.3.13**

le  $\exists c, d \in \mathbb{Z}$  such that

$$\begin{aligned} ac + nd &= 1 \\ \implies nd &= 1 - ac \\ \implies ac &\equiv 1 \pmod{n} \end{aligned}$$

**0.3.14**

$$\bar{a} \in \mathbb{Z}/n\mathbb{Z}$$

$$\iff \exists c : \bar{a}\bar{c} = 1$$

$$\iff \exists c : ac \equiv 1 \pmod{n}$$

$$\iff a, n \text{ relatively prime from the last two exercises}$$

Not doing manual verification

**0.3.15**

Ew