MOE H3 Math

Numbers and Proofs

Lecture 5

- Well Ordering Principle
- More on Number Theory
- Miscellaneous

PMI with Domain $\mathbb{Q}^+$

$(\forall\ q \in \mathbb{Q}^+)\ P(q)$ $\quad q = \dfrac{m}{n}$ where $m, n \in \mathbf{Z}^+$

1. $P(1)$ is true
2. For all $k \in \mathbb{Z}^+$, if $P(k)$ is true, then $P(k+1)$ is true

Then $P(n)$ is true for all $n \in \mathbb{Z}^+$

Fix $m \in \mathbb{Z}^+$

3. $P(m/1)$ is true (from 1 and 2 above)
4. For all $k \in \mathbb{Z}^+$, if $P(m/k)$ is true, then $P(m/(k+1))$ is true

Then $P(m/n)$ is true for all $m/n \in \mathbb{Q}^+$

PMI with Domain $\mathbb{Q}^+$

$(\forall\ q \in \mathbb{Q}^+)\ P(q)$ $\quad q = \dfrac{m}{n}$ where m, n $\in \mathbf{Z}^+$

By (1) and (2)

By (3) and (4)

P(m/1) is true

P(m/k)
→ P(m/(k+1))

$$
\begin{array}{ccccccc}
P(1) \rightarrow & P(2) \rightarrow & P(3) \rightarrow & \ldots & \rightarrow P(m) & \ldots \\
\downarrow & \downarrow & \downarrow & & \downarrow & \\
P(\frac{1}{2}) & P(\frac{2}{2}) & P(\frac{3}{2}) & & P(\frac{m}{2}) & \\
\downarrow & \downarrow & \downarrow & & \downarrow & \\
P(\frac{1}{3}) & P(\frac{2}{3}) & P(\frac{3}{3}) & & P(\frac{m}{3}) & \\
\downarrow & \downarrow & \downarrow & & \downarrow & \\
\downarrow & \downarrow & \downarrow & & \downarrow & \\
P(\frac{1}{n}) & P(\frac{2}{n}) & P(\frac{3}{n}) & & P(\frac{m}{n}) & \\
\downarrow & \downarrow & \downarrow & & \downarrow &
\end{array}
$$

Well Ordering Principle

Well-Ordering Principle for integers

If S is a non-empty subset of Z such that all its elements are greater than some fixed number, then S has a smallest element.

Well-ordering principle does not hold for rational numbers and real numbers

Example

The set Q^+ of positive rational numbers.

All the elements in Q^+ are greater than 0, but Q^+ does not have a smallest element.

Well Ordering Principle

Well-Ordering Principle for integers

If S is a non-empty subset of Z such that all its elements are greater than some fixed number, then S has a smallest element.

Example

$T = \{x \in Z \mid x = 15 - 12k \text{ for some } k \in \mathbb{Z}\}$

$= \{ \ldots, -21, -9, 3, 15, 27, \ldots\}$

$S = \{x \in Z \mid x \geq 0 \text{ and } x = 15 - 12k \text{ for some } k \in \mathbb{Z}\}$

$= \{3, 15, 27, \ldots\}$

Quotient Remainder Theorem

Theorem

For all integers n and d with $d > 0$,
there exist unique integers q and r such that

$$n = dq + r \qquad 0 \le r < d$$

Idea of proof (Existence part)

Consider

$S = \{x \in Z \mid x \geq 0 \text{ and } x = n - dk \text{ for some } k \in \mathbb{Z}\}$

Show that S is non-empty.

By well-ordering principle, S has a smallest element r.

Then $r \geq 0$, and is of the form $n - dk$ for some k, say $k = q$.

i.e. $r = n - dq$ which gives $n = dq + r$.

Quotient Remainder Theorem

Theorem

For all integers n and d with $d > 0$,
there exist unique integers q and r such that

$$n = dq + r \qquad 0 \le r < d$$

Idea of proof (Existence part)

It remains to prove $r < d$ (by contradiction):

Suppose $r \ge d$.

Then $r = d + r'$ for some $0 < r' < r$.

$r' = r - d \;\; = (n - dq) - d \;\; = n - d(q+1)$.

So there is a smaller element $r' \in S$ than r.

This contradicts that r is the smallest element in S.

Linear combination

Theorem (from lecture 1)

Let a and b be integers, not both 0.

(i) $\gcd(a, b) = ax_0+by_0$ for some integers x_0 and y_0.

(ii) If a and b are relatively prime,
then $1 = ax_0+by_0$ for some integers x_0 and y_0.

Proof of (ii) follow from (i)
Proof of (i) – Well Ordering Principle

Inverse modulo n

Theorem

For all integers a and n such that $\gcd(a, n) = 1$,

there exists an integer b such that $ab \equiv 1 \mod n$.

The integer b is called the inverse of a modulo n.

Proof

Since $\gcd(a, n) = 1$

we have $ab + nm = 1$ for some $b, m \in \mathbb{Z}$

So $ab + nm \equiv 1 \mod n$

Since $nm \equiv 0 \mod n$,

we get $ab \equiv 1 \mod n$. $\square$

Reversing Euclidean Algorithm

Example $a = 42$ and $b = 234$ $\gcd(234, 42) = 6$

Find integers x, y such that $6 = 234x + 42y$

Euclidean Algorithm

$234 = 42 \times 5 + 24$ (i)

$42 = 24 \times 1 + 18$ (ii)

$24 = 18 \times 1 + 6$ (iii)

$18 = 6 \times 3 + 0$

From (iii):

$6 = 24 + 18 \times (-1)$

From (ii):

$18 = 42 + 24 \times (-1)$

$6 = 24 + (42 + 24 \times (-1)) \times (-1)$

$6 = 42 \times (-1) + 24 \times (2)$

From (i):

$24 = 234 + 42 \times (-5)$

$6 = 42 \times (-1) + (234 + 42 \times (-5)) \times (2)$

$6 = 234 \times (2) + 42 \times (-11)$

Finding inverse modulo n

Example

Since $\gcd(17, 11) = 1$

we have $17b + 11m = 1$ for some $b, m \in \mathbb{Z}$

By reversing Euclidean Algorithm, we get

$17(2) + 11(-3) = 1$

Taking modulo 11, we get

$17(2) \equiv 1 \mod 11$

So 2 is the inverse of 17 modulo 11

Taking modulo 17, we get

$11(-3) \equiv 1 \mod 17$

So -3 (or 14) is the inverse of 11 modulo 17

Cancellation Theorem

Theorem

Let a, b, c, n be any integers with $n > 1$.

If $\gcd(c, n) = 1$ and $ac \equiv bc \bmod n$,

then $a \equiv b \bmod n$.

Proof

$$
\begin{aligned}
ac \equiv bc \bmod n \quad &\Rightarrow n \mid (ac - bc) \\
&\Rightarrow n \mid c(a - b) \\
\gcd(c, n) = 1 \quad &\Rightarrow n \mid (a - b) \quad \text{by Euclid's Lemma} \\
&\Rightarrow a \equiv b \bmod n
\end{aligned}
$$

□

Fermat's Little Theorem

Theorem

Let p be a prime and
a any integer not divisible by p.
Then $a^{p-1} \equiv 1 \mod p$.

Example $p = 23, a = 6$

So $6^{22} \equiv 1 \mod 23$

The converse of FLT is not true

Example $p = 341, a = 2$

$2^{340} \equiv 1 \mod 341$ but 341 is not a prime

Fermat's Little Theorem

Example

Find the remainder when 7^{62} is divided by 31.

Observe that 31 is a prime and $31 \nmid 7$

So $7^{30} \equiv 1 \mod 31$

$$7^{62} = 7^{(30x2)+2}$$

Fermat's Little Theorem

Idea of Proof

$$\{0,\ 1,\ 2,\ 3,\ \ldots,\ p-1\} \overset{\text{mod } p}{=} \{0a,\ 1a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\}$$

rearrangement

We just need to show the elements in the right hand side are all different mod p:

For $k_1 \equiv k_2$ mod p (from the left hand side)

we shall show: $k_1 a \not\equiv k_2 a$ mod p

Suppose $k_1 a \equiv k_2 a$ mod p

Since $\gcd(a, p) = 1$

$k_1 \equiv k_2$ mod p

Cancellation Theorem

Fermat's Little Theorem

Idea of Proof

$$\{0,\ 1,\ 2,\ 3,\ \ldots,\ p-1\} \overset{\text{mod } p}{=} \{0a,\ 1a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\}$$

$$1\times2\times3\times\ldots\times(p-1) \equiv 1a\times2a\times3a\times\ldots\times(p-1)a \text{ mod } p$$

$$(p-1)! \equiv a^{p-1}(p-1)! \quad \text{mod } p$$

Since $\gcd(p, (p-1)!) = 1$

Cancellation Theorem $\quad a^{p-1} \equiv 1 \text{ mod } p$

$\square$

2017 paper Q8

Fibonacci sequence: $F_1, F_2, F_3, \ldots, F_n, \ldots$

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Modulo 2: $\underbrace{1, 1, 0}, \underbrace{1, 1, 0}, 1, 1, \ldots$ Periodic with period 3

i. Find the periods of Fibonacci sequences modulo 3 and 4

ii. For any positive integer m, show that we can find two pairs (F_j, F_{j+1}) and (F_k, F_{k+1}) which are the same modulo m with $1 \leq j < k \leq m^2 + 1$

iii. For m, j and k as in (ii), explain why the Fibonacci sequence modulo m is periodic with period dividing $k - j$.

2017 paper Q8

i. Find the periods of Fibonacci sequences modulo 3 and 4

Modulo 3: 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, …

Modulo 4: 1, 1, 2, 3, 1, 0, 1, 1, …

2017 paper Q8

ii. For any positive integer m, show that we can find two pairs (F_j, F_{j+1}) and (F_k, F_{k+1}) which are the same modulo m with $1 \le j < k \le m^2 + 1$

Use Pigeonhole principle

Modulo m, there are m possible values 0, 1, 2, …, m-1. So there are exactly m^2 possible distinct pairs (a, b).

If we consider $m^2 + 1$ pairs of (F_i, F_{i+1}) modulo m where $1 \le i \le m^2 + 1$,
we can find two pairs (F_j, F_{j+1}) and (F_k, F_{k+1}) which are the same modulo m.

2017 paper Q8

iii. For m, j and k as in (ii), explain why the Fibonacci sequence modulo m is periodic with period dividing k – j.

This is the same as to show there exists $j < k$ such that $F_{j+n} \equiv F_{k+n} \bmod m$ for all non negative integer n.

Use PMI

Basis step: P(0) and P(1)

$F_j \equiv F_k \bmod m$ $\qquad$ $F_{j+1} \equiv F_{k+1} \bmod m$

Inductive step:

$[P(q-1) \text{ and } P(q)] \rightarrow P(q+1)$ for all $q \geq 1$

Given $F_{j+q-1} \equiv F_{k+q-1} \bmod m$ and $F_{j+q} \equiv F_{k+q} \bmod m$

Then $F_{j+q+1} = F_{j+q-1} + F_{j+q} \equiv F_{k+q-1} + F_{k+q} = F_{k+q+1} \bmod m$

So the sequence repeats itself after $k - j$ terms

2017 paper Q8

iv. For any positive integer m, prove that there is a Fibonacci number which is a multiple of m.

For any positive m, by part (iii), the Fibonacci sequence modulo m is periodic.
So there is a pair (F_i, F_{i+1}) with $i > 1$ such that

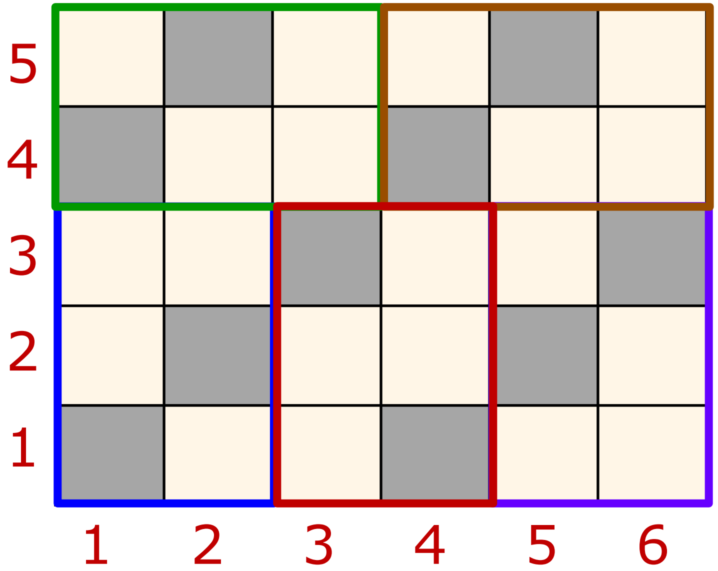
$$F_i \equiv F_1 \equiv 1 \bmod m \qquad F_{i+1} \equiv F_2 \equiv 1 \bmod m$$

Then $F_{i-1} = F_{i+1} - F_i \equiv 1 - 1 \equiv 0 \bmod m$

This means $m \mid F_{i-1}$

We have proven that there is a Finonacci number which is a multiple of m.

2018 paper Q5



5×6 chessboard
a unit square (x, y) is shaded if and only if $x \equiv y \pmod 3$

A tessellation of the chessboard by 3×2 tiles

A 5×6 chessboard can be tessellated with 3×2 tiles

To consider whether a $p \times q$ chessboard can be tessellated with $a \times b$ tiles.
A unit square (x, y) is shaded if and only if $x \equiv y$ $\pmod a$

2018 paper Q5

i. Explain why the following are necessary conditions for such a tessellation
   a) ab is a factor of pq
   b) p and q can be written in the form $ma + nb$ where m and n are non-negative integers
   c) The $p \times q$ chessboard has $\frac{pq}{a}$ shaded squares

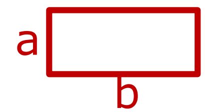
a) ab is a factor of pq

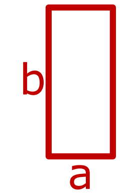
- A $p \times q$ chessboard has pq squares
- A $a \times b$ tile has ab squares
- Suppose k tiles are used to tessellate the board
- Then $pq = kab$.
- So $ab \mid pq$.

2018 paper Q5

i. Explain why the following are necessary conditions for such a tessellation

   b) p and q can be written in the form $ma + nb$ where m and n are non-negative integers

- p and q are the height and base of the $p \times q$ chessboard.
- a and b are the height and base of each $a \times b$ tile.
- Each tile can be places horizontally 

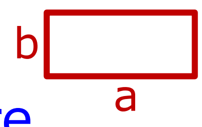
 or vertically 

 in the tessellation.
- If we tessellate the board at the bottom from left to right with m vertical and n horizontal tiles, there will be $ma + nb$ squares at the bottom row of the board.
- Each row of the board is made up of q squares.
  So we get $q = ma + nb$.
- Similarly, if we tessellate the board on the left from bottom to top, we will get $p = sa + tb$ (with s horizontal and t vertical tiles).

2018 paper Q5

i. Explain why the following are necessary conditions for such a tessellation

c) The $p \times q$ rectangle has $\frac{pq}{a}$ shaded squares

- In each $a \times b$ tile 

, along each row there is only one shaded square.
- Since there are b rows, there are exactly b shaded squares in each tile.
- If we use k tiles in the tessellation, there will be kb shaded squares in the board.
- Since $pq = kab$ (from part (a)),

  $\frac{pq}{a} = kb$ = number of shaded squares in the board.

2018 paper Q5

ii. Let t be the smaller of r and s such that

$$p \equiv r \pmod{a} \qquad 0 \le r < a$$
$$q \equiv s \pmod{a} \qquad 0 \le s < a$$

a) Explain why the number of shaded squares in the $p \times q$ chessboard is $\dfrac{pq - rs}{a} + t$.

b) Hence prove that for a tessellation, either $a \mid p$ or $a \mid q$.

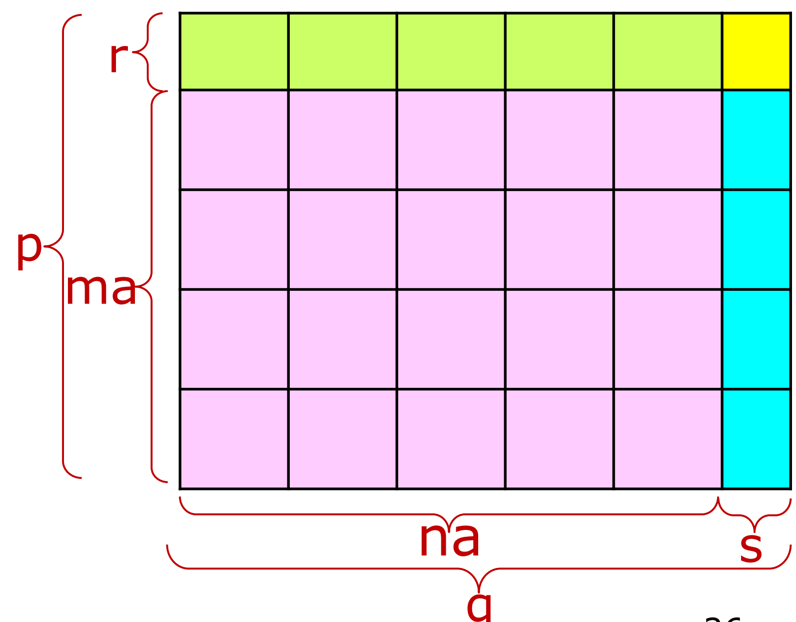
$p = ma + r$
$q = na + s$

$a \times a$ — a shaded squares

$a \times s$ — s shaded squares

$r \times a$ — r shaded squares

$r \times s$ — t shaded square



total number: $mna + ms + nr + t$

2018 paper Q5

ii. Let t be the smaller of r and s such that

$$p \equiv r \pmod{a} \qquad 0 \le r < a$$
$$q \equiv s \pmod{a} \qquad 0 \le s < a$$

b) Hence prove that for a tessellation, either $a \mid p$ or $a \mid q$.

From (a): # shaded squares in $p \times q$ board is $\dfrac{pq - rs}{a} + t$.

From i(c): # shaded squares in tessellated $p \times q$ board is $\dfrac{pq}{a}$.

$$\frac{pq - rs}{a} + t = \frac{pq}{a} \quad \Rightarrow t = \frac{rs}{a} \quad \Rightarrow at = rs$$

Two cases:

(i) $t = r$ $\Rightarrow ar = rs$ If $r \neq 0$, then $a = s$ contradiction

So $r = 0$, and $p \equiv 0 \pmod{a}$ $\Rightarrow a \mid p$

(ii) $t = s$ $\Rightarrow a \mid q$