Solutions to exam problems

M342 09/10

All the problems in the present exam paper are those or analogous to those appeared in the class/lecture notes or in handouts/homework and their solutions (all on VITAL) (1)

BW = Book work
HW = Homework

Problem 1

(BW) (i) For any two integers a, b $(b \neq 0)$ $\exists$ a unique pair of integers q, r, such that

$$a = bq + r,$$

where

$$0 \leq r < |b|.$$

□ The set

$$S = \{a - bq \mid q \in \mathbb{Z}\}$$

contains non-negative numbers. Take the smallest $r \in S$, $r > 0$. If we assume that $r \geq |b|$ then $r = a - bq = |b| + s$ for some q and s, where $0 \leq s < r$. This $s \neq r$ because $|b| \neq 0$. Then $s \in S$, $s \geq 0$ and $s < r$ - contradiction with the choice of r. Therefore, $0 \leq r < |b|$. Moreover $a = bq + r$.

Let (q_1, r_1) and (q_2, r_2) be two pairs satisfying the conditions of the lemma. Then

$$b(q_2 - q_1) = r_2 - r_1 \quad (*)$$

and

$$0 < r_2 - r_1 < |b|$$

If $r_2 \neq r_1$ - we get a contradiction because $(*) \Rightarrow r_2 - r_1 > |b|$. Hence $r_2 = r_1$. Then $bq_1 = bq_2 \Rightarrow q_1 = q_2$. (6) (7)

(BW) (ii) If $d \mid a$ & $d \mid b \Rightarrow d \mid a$ & $d \mid (b + at)$
If $d \mid a$ & $d \mid (b + at) \Rightarrow d \mid a$ & $d \mid b$
(in both cases we use 2-out-of-3 property for division). Hence, the

sets of divisors for a and b and for a and b+at coincide $\Rightarrow (a,b)=(a,b+at)$. [3]

(iii) Run EA for a and b:

$r_0 = a$, $r_1 = b$

$r_i = r_{i+1}q_{i+1} + r_{i+2}$, $0 \le r_{i+2} < |r_{i+1}|$

$\vdots$

$r_{n-2} = r_{n-1}q_{n-1} + r_n$, $0 \le r_n < |r_{n-1}|$

$r_{n-1} = r_n q_n$ [4]

By (ii): $(a,b) = (r_0,r_1) = (r_1,r_2) = \dots = (r_{n-1},r_n) = r_n$.

(iv) $(45675, 6854) = (6\cdot 6854 + 4551, 6854) =$

$= (4551, 6854) = (4551, 1\cdot 4551 + 2303) =$

$= (4551, 2303) = (1\cdot 2303 + 2248, 2303) =$

$= (2248, 2303) = (2248, 1\cdot 2248 + 55) =$

$= (2248, 55) = (2^3 \cdot 281, 5\cdot 11) = 1$ [3]

(v) Matrix method:

$$\left(\begin{array}{cc|c} 1 & 0 & 39 \\ 0 & 1 & 119 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 39 \\ -3 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 39 \\ -57 & 19 & 38 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|c} 58 & -19 & 1 \\ -57 & 19 & 38 \end{array}\right) \Rightarrow$$ [4]

$58 \cdot \underline{39} + 19 \cdot \underline{119} = 2262 - 2261 = 1$

Problem 2:

(i) $\mathrm{ord}_{71}(15123) = \mathrm{ord}_{71}(3\cdot 71^2) = 2$, while

$\mathrm{ord}_5(15123) = 0$

Also $\mathrm{ord}_{17}(30246) = \mathrm{ord}_{17}(2\cdot 3\cdot 71^2) = 0$

$\mathrm{ord}_2(151230) = \mathrm{ord}_2(2\cdot 3\cdot 5\cdot 71^2) = 1$

$\mathrm{ord}_{101}(61206) = \mathrm{ord}_{101}(2\cdot 3\cdot 101^2) = 2$ [2]

P.W

(ii) Let $a = p^s a'$ & $b = p^t b'$ where both a' and b' are coprime to p, so that $s = \mathrm{ord}_p(a)$ & $t = \mathrm{ord}_p(b)$. Then

$\mathrm{ord}_p(ab) = \mathrm{ord}_p(p^s a' p^t b') = \mathrm{ord}_p(p^{s+t} a' b')$

Since $p \nmid a'$ and $p \nmid b' \Rightarrow p \nmid (a'b')$ (otherwise p divides at least one of the integers a' or b')

Therefore, $\mathrm{ord}_p(ab) = s+t = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$ 3

(iii) Let n be an integer (without loss of generality one can assume $n > 0$).
Then $\exists$ a unique (up to the order of factors) decomposition

$$n = \prod_p p^{\alpha(p)}$$

where p runs primes (and, obviously, only for a finite collection of primes p $\alpha(p) \neq 0$).

□ If ~~$p=2$~~ $n = p$ – prime, then nothing to prove. Assume that any number $a < n$ is a product of primes. If n is a prime nothing to prove. If n is a composite, then $n = ab$, $a < n$, $b < n$. By inductive hypothesis, both a and b have decompositions into primes. Therefore, $n = ab$ can be decomposed into primes.

So, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$.

Apply ord_p:

$$\mathrm{ord}_p(n) = \mathrm{ord}_p(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}) \overset{\text{by (ii)}}{=\!=}$$

$$= \mathrm{ord}_p(p_1^{\alpha_1}) + \mathrm{ord}_p(p_2^{\alpha_2}) + \cdots + \mathrm{ord}_p(p_s^{\alpha_s}) =$$

$$= \begin{cases} \alpha_i, & \text{if } p = p_i \\ 0, & \text{otherwise} \end{cases} \Rightarrow \alpha_i = \mathrm{ord}_{p_i}(n)$$ ■

6

(iv) Let $a = p_1^{n_1} \cdot \ldots \cdot p_s^{n_s}$

$b = p_1^{m_1} \cdot \ldots \cdot p_s^{m_s}$

(assuming $m_i = 0$ or $n_j = 0$ when necessary),

let $k_i = \max\{n_i, m_i\}$ and $l_i = \min\{n_i, m_i\}$ for each index $i = \overline{1,s}$. Then

$(a,b) = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s}$ and $[a,b] = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$.

All we need to show is that

$$n_i + m_i = \min\{n_i, m_i\} + \max\{n_i, m_i\}.$$

Without loss of generality, if n and m are two integers and $n \geq m$, then

$$n + m = \underbrace{\min\{n,m\}}_{m} + \underbrace{\max\{n,m\}}_{n}$$

- obviously true. [5]

(v) Use the formula $\operatorname{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots$

to compute

$\operatorname{ord}_2(1000!) = 994$ & $\operatorname{ord}_5(1000!) = 249$

Hence there are 249 zero at the end [4]

Problem 3

(i) Let $(a,b) = 1$. Run up EA:

$a = q_1 b + r_1$, $0 \leq r_1 < b$ (without loss of generality assume $a, b > 0$)

$b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$, $0 \leq r_n < r_{n-1}$

$r_n = d = 1$ - g.c.d. for a & b.

Induction: If $n = 1$ then $1 = a - q_1 b$, so that $s = 1$, $t = -q_1$.

Assuming the assertion holds true for $1, 2, \dots, n-1$ let's prove it when n steps in EA. By inductive hypothesis $\exists\, t'$ and s, such that $t'b + sr_1 = 1$, whence

$1 = t'b + s(a - bq_1) = b(t' - q_1) + sa = $

$= sa + tb$, when $t = t' - q_1$. 5

(ii) $ax \equiv b \pmod m$

Let $d = (a, m)$ - g.c.d. for a and m.

If a solution $\exists$ then $m \mid (ax - b) \Rightarrow$ (RW)

$\Rightarrow d \mid (ax - b)$. Since $d \mid a \Rightarrow d \mid (ax) \Rightarrow$ (HW)

$\Rightarrow d \mid b$. Therefore, if $d \nmid b \Rightarrow$ no solutions. If $d \mid b$, let $a = da'$, $m = m'd$, $b = b'd$, so that we have an equivalent congruence $a'x \equiv b' \pmod{m'}$, but now $(a', m') = 1$, i.e. a' and m' are coprime. By (i) $\exists\, s, t$, such that $sa' + tm' = 1$, i.e. $sa' \equiv 1 \pmod{m'}$, i.e. s is invertible mod m'. Multiplying by s:

$$\underbrace{sa'}_{1} x \equiv sb' \pmod{m'}$$

$$x \equiv sb' \pmod{m'}$$

$x = sb' + m'l$, $l \in \mathbb{Z}$. 3

(iii) $469x \equiv 143 \pmod{29}$ (HW)

$469 = 7 \cdot 67$ - coprime to 29

Matrix method:

$$\left(\begin{array}{cc|c} 1 & 0 & 469 \\ 0 & 1 & 29 \end{array}\right) \sim \dots \sim \left(\begin{array}{cc|c} 6 & -97 & 1 \\ 0 & 1 & 29 \end{array}\right)$$

So $6 \cdot 469 - 97 \cdot 29 = 1 \Rightarrow 6$ is the inverse

to 469 mod 29:

$$\underbrace{6\cdot 469}_{=1}\, x \equiv \underbrace{6\cdot 143}_{858} \pmod{29}$$

$$x \equiv 858 \equiv 17 \pmod{29}$$

$$x = 17 + 29t,\ t \in \mathbb{Z}.$$

$$707x \equiv 118 \pmod{1313}$$

$707 = 7\cdot 101$, $1313 = 13\cdot 101$

$(707, 1313) = 101 \nmid 118 \Rightarrow$ no solutions at all. ☐

(ii) Chinese Thm: for any positive integers

$$m_1, \dots, m_s$$

such that $(m_i, m_j) = 1$ for ∀ two indeces i, j, and for any integers

$$a_1, \dots, a_s$$

the system of equations

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_s \pmod{m_s} \end{cases}$$

has a solution, and this solution is unique modulo $m_1 \cdot \dots \cdot m_s$.

□ for ∀ i set

$$k_i = m_1 \cdot \dots \cdot m_{i-1} m_{i+1} \cdot \dots \cdot m_s$$

By FTA: $(k_i, m_i) = 1 \Rightarrow \exists\, s_i, t_i$, such that $s_i k_i + t_i m_i = 1 \Rightarrow s_i k_i \equiv 1 \pmod{m_i}$

Then

$$b = a_1 k_1 s_1 + \dots + a_s k_s s_s \equiv \begin{cases} a_i \pmod{m_i} \\ 0 \pmod{m_j},\ j \neq i \end{cases}$$

– so b is a solution.

If b' is another one solution then

$$b' \equiv a_i \equiv b \pmod{m_i}.$$

As m_i's are pair-wise coprime $\Rightarrow$

$$b' \equiv b \pmod{m_1 \cdot \ldots \cdot m_s}.$$

(HW) $\begin{cases} 3x \equiv 3 \pmod 9 \\ 7x \equiv 4 \pmod 5 \\ 5x \equiv 3 \pmod{14} \end{cases}$

HW BW

$$\left(3x \equiv 3 \pmod 9\right) \Leftrightarrow \left(x \equiv \cancel{1}\ 1 \pmod 3\right)$$

$(-2)\cdot 7 + 3\cdot 5 = -14 + 15 = 1 \Rightarrow$

$$(-2)\cdot 7\, x \equiv -8 \equiv 2 \pmod 5$$

$$\text{III}$$

$$x$$

$$3\cdot 5 + (-1)\cdot 14 = 15 - 14 = 1$$

$$3\cdot 5\, x \equiv 9 \pmod{14}$$

$$\text{II}$$

$$x$$

$$\begin{cases} x \equiv \cancel{1}\ 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 9 \pmod{2\cdot 7} \end{cases}$$

Apply Chinese Theorem:

$k_1 = 70$
$k_2 = 42$
$k_3 = 15$

Matrix Method: $s_1 = 1$, $s_2 = -2$, $s_3 = 1$

And:

$m_1 = 3$
$m_2 = 5$
$m_3 = 14$

Thus, $b = 1\cdot 70\cdot 1 + 2\cdot 42\cdot(-2) + 9\cdot 15\cdot 1 = 37$

$b \equiv 37 \pmod{210}$ — the solution.

[4]

Problem 4:

(i) Let $\mathbb{N} = \{ n \in \mathbb{Z} \mid n > 0 \}$ – set of natural numbers. Euler's function

$$\phi : \mathbb{N} \longrightarrow \mathbb{N}$$

(B,W)

$$\phi(m) = \#\{ a \in \mathbb{Z} \mid 1 \le a \le m \ \& \ (a,m) = 1 \}$$

If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ then

$$\phi(m) = \prod_{i=1}^{s} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right)$$

For example, $\phi(p) = p - 1$ for $\forall$ prime p. [3]

(B,W)

(ii) For any $m \ge 1$

$$m = \sum_{d \mid m}' \phi(d)$$ where d runs all the divisors of m. Indeed, for any divisor d of m let

$$C_d = \{ a \in \mathbb{Z} \mid 1 \le a \le m \ \& \ (a,m) = d \}$$

Then $C_d \cap C_{d'} = \emptyset$ if $d \neq d'$ and $\bigcup_d C_d = \{1, 2, \ldots, m\}$. Therefore,

$$m = \sum_{d \mid m} \# C_d$$

Furthermore,

$$a \in C_d \Leftrightarrow \left(1 \le a \le m \ \& \ (a,m) = d \right) \Leftrightarrow$$

$$\Leftrightarrow \left(1 \le \frac{a}{d} \le \frac{m}{d} \ \& \ \left(\frac{a}{d}, \frac{m}{d} \right) = 1 \right)$$

so that there are exactly $\phi\left(\frac{m}{d}\right)$ such

integers. Hence

$$m = \sum_{d|m} \#C_d = \sum_{d|m} \phi\left(\frac{m}{d}\right)$$

It is clear that when d runs the set of divisors for m, $\frac{m}{d}$ runs the same set. Hence

$$m = \sum_{d|m} \phi(d).$$

[5]

(iii) Euler's theorem: $a^{\phi(m)} \equiv 1 \pmod m$ for $\forall (a, m) = 1$.

(P.W)

□ Let $k = \phi(m)$ and set

$T = \{r_1, \ldots, r_k\}$ be the set of all numbers among $\{1, 2, \ldots, m\}$ coprime to m. Let $(a, m) = 1$ and consider another set

$$S = \{ar_1, \ldots, ar_k\}.$$

Since $(a, m) = 1$, if $ar_i \equiv ar_j \pmod m$ then it would follow that $r_i \equiv r_j \pmod m$ — contradiction since $0 < r_i, r_j < m$. Therefore, the numbers in S are pair-wise distinct mod m.

Moreover $(ar_i, m) = 1$ because $(a, m) = 1$ and $(r_i, m) = 1$. Therefore, S coincides with T mod m. In particular,

$$ar_1 \cdot \ldots \cdot ar_k \equiv r_1 \cdot \ldots \cdot r_k \pmod m.$$

i.e. $a^k r_1 \cdot \ldots \cdot r_k \equiv r_1 \cdot \ldots \cdot r_k \pmod m$

Since $(r_1 \cdot \ldots \cdot r_k, m) = 1 \Rightarrow$

$$a^k \equiv 1 \pmod m .$$

Since $k = \phi(m)$ we get:

$$a^{\phi(m)} \equiv 1 \pmod m .$$

6

BW

HW

(iv) $7^{864} = (7^3)^{288} = (7^3)^{\phi(864)} \equiv 1 \pmod{864}$

because $864 = 2^5 \cdot 3^3$, so that

$\phi(864) = 2^4(2-1)3^2(3-1) =$

$= 2^5 \cdot 3^2 = 288$

$7^{100} = 7^{96+4} = 7^{96}7^4 \equiv 7^{\phi(360)}7^4 \equiv 7^4 \pmod{36}$

$7^4 = (49)^2 = 2401$

2

(v) $162 = 2 \cdot 3^4 = 3^4(3-1) = \phi(3^5) = \phi(243)$

$18 = 2 \cdot 3^2 = 3^2(3-1) = \phi(3^3) = \phi(27)$

$2 = \phi(3)$

HW

$\Rightarrow a^{162} \equiv 1 \pmod{243}$

$a^{18} \equiv 1 \pmod{27}$ for $\forall (a,3) = 1$

$a^2 \equiv 1 \pmod 3$

If $a = 5$ then we have:

$5^{162} + 5^{18} + 5^2 \equiv 1+1+1 = 3 \pmod 3$ because 3 divides 243, 27 and 3.

$\Rightarrow 5^{162} + 5^{18} + 5^2 \equiv 0 \pmod 3$

4