November 2010

SOLUTIONS TO THE EXAM PROBLEMS

MATH 342

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 are on VITAL

BW = Book work
HW = Home work

Problem 1

(i) Suppose $\exists$ only finitely many primes in $\mathbb{Z}$, say

BW

$$p_1, \ldots, p_s$$

And let

$$N = p_1 \cdot \ldots \cdot p_s + 1 .$$

As any positive integer can be decomposed into primes, we have that

$$N = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$$

where $\alpha_i \geq 0$ for each index i, and some α_i is positive, say α_1.

Then $p_1 \mid N$ & $p_1 \mid (p_1 \cdot \ldots \cdot p_s) \Rightarrow$

$\Rightarrow p_1 \mid 1$ — contradiction.

(ii) Let

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

BW for any $a, b \in \mathbb{Z}$, $b \neq 0$.

HW Then S contains non-negative integers. Let r be the smallest

one. If we suppose that $r \geq |b|$ then

$$r = a - bq = |b| + s$$

for some

$$0 \leq s < r.$$

But $s \in S$, which contradicts to the choice of r, because r is the smallest ~~positive from~~ non-negative from S. Therefore,

$$r < |b|.$$

Then

$$a = bq + r \quad \& \quad 0 \leq r < |b|.$$

Suppose now that $\exists$ two pairs (q_1, r_1) and (q_2, r_2), such that

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|$$
$$a = bq_2 + r_2, \quad 0 \leq r_2 < |b|$$

Then

$$b(q_2 - q_1) = r_2 - r_1$$

and

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

(without loss of generality we assume that $r_2 > r_1$). On the other hand,

$$|b| \cdot |q_2 - q_1| = r_2 - r_1$$

$$\Rightarrow \quad r_2 - r_1 \geq |b|$$

– contradiction. Therefore, the pair (q, r) is unique.

(iii) $a, b \in \mathbb{Z}$, $b \neq 0$

BW HW

$$r_0 = a, \quad r_1 = b$$

$$r_0 = r_1 q_1 + r_2, \quad 0 \leq r_2 < |r_1|$$

$$r_1 = r_2 q_2 + r_3, \quad 0 \leq r_3 < |r_2|$$

$$\vdots$$

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

$$r_{n-1} = r_n q_n, \quad r_{n+1} = 0$$

Then

$$\gcd(r_{n-1}, r_n) = \ldots = \gcd(r_1, r_2) = \gcd(r_0, r_1)$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| \gcd(a, b)$$

$$r_n$$

whence $\gcd(a, b) = r_n$.

(iv)

HW

$$\left.\begin{aligned} &\gcd(105875, 105512) = \\ &= \gcd(105875, 3637) = \\ &= \gcd(402, 3637) = \\ &= \gcd(402, 19) = \\ &= \gcd(3, 19) = 1 \end{aligned}\right\} \text{EA}$$

Problem 2

(i) $37\,632 = 2^{8} \cdot 3^{0} \cdot 5^{0} \cdot 7^{2} \cdot 11^{0} \cdot 13^{0} \cdot \ldots \Rightarrow$

BW HW

$$\operatorname{ord}_2(37\,632) = 8$$

$$\operatorname{ord}_3(37\,632) = 1$$

$$\operatorname{ord}_5(37\,632) = 0$$

$$\operatorname{ord}_7(37\,632) = 2$$

(ii) Let $a = p^s a'$, $\gcd(p, a') = 1$

BW $\quad b = p^t b'$, $\gcd(p, b') = 1$

Then $ab = p^{s+t} a'b'$ and $\gcd(p, a'b') = 1$

$\Rightarrow \operatorname{ord}_p(ab) = s+t = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$.

(iii) Let $n \in \mathbb{Z}$, $n > 0$. If $n = 1$ BW then n can be factorized into primes by the trivial reason.

Suppose we know that all integers less than n can be factorize into integers. If n is a prime, then it is its own factorization into a single prime. If n is a composite, then $n = ab$, where $a < n$ & $b < n$. By the above induction hypothesis

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

and

$$b = q_1^{\beta_1} \cdots q_t^{\beta_t}$$

— prime-power factorizations for a and b. Then

$$n = ab = p_1^{\alpha_1} \cdots p_s^{\alpha_s} q_1^{\beta_1} \cdots q_t^{\beta_t}$$

is the prime-power factorization for n.

(iv) $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$

BW HW

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$$
$$b = q_1^{\beta_1} \cdot \ldots \cdot q_t^{\beta_t}$$

} prime-power factorizations

Without loss of generality, one can assume that

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$$
$$b = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$$

where all $\alpha_i, \beta_j \geq 0$.

For $\forall$ i let

$$\gamma_i = \max\{\alpha_i, \beta_i\}$$
$$\delta_i = \min\{\alpha_i, \beta_i\}$$

Then

$$\gcd(a,b) = \prod_{i=1}^{s} p_i^{\delta_i}$$

$$\operatorname{lcm}(a,b) = \prod_{i=1}^{s} p_i^{\gamma_i}$$

Now, for any two non-negative

α and β one has

$$\max\{\alpha,\beta\} = \alpha+\beta-\min\{\alpha,\beta\}.$$

In particular,

$$\gamma_i = \alpha_i+\beta_i-\delta_i$$

for all i. Then

$$\operatorname{lcm}(a,b) = \prod_{i=1}^{s} p_i^{\gamma_i} = \prod_{i=1}^{s} p_i^{\alpha_i+\beta_i-\delta_i} =$$

$$= \frac{\prod_{i=1}^{s} p_i^{\alpha_i}\ \prod_{i=1}^{s} p_i^{\beta_i}}{\prod_{i=1}^{s} p_i^{\delta_i}} = \frac{ab}{\gcd(a,b)} \Rightarrow$$

$$\Rightarrow ab = \gcd(a,b)\cdot\operatorname{lcm}(a,b).$$

Problem 3

(i) Since $\gcd(a,b)=1$

BW

$$r_0 = a\ ,\quad r_1 = b$$

$$r_0 = r_1 q_1 + r_2\ ,\quad 0 \le r_2 < |r_1|$$

$$r_1 = r_2 q_2 + r_3\ ,\quad 0 \le r_3 < |r_2|$$

$$\vdots$$

$$\vdots$$

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

$$r_{n-1} = r_n q_n$$

Since $\gcd(a,b) = 1 \Rightarrow r_n = 1$

Let's say $n = 3$, so that $r_3 = 1$

Then we have

$$a = bq_1 + r_2$$

$$b = r_2 q_2 + r_3 \quad , \quad r_3 = 1$$

$$b = r_2 q_2 + 1$$

Since $r_2 = a - bq_1$ we have:

$$1 = b - r_2 q_2 = b - q_2(a - bq_1) =$$

$$= b - q_2 a + b q_1 q_2 =$$

$$= -q_2 a + (1 + q_1 q_2) b$$

Thus, $s = -q_2$, $t = 1 + q_1 q_2$.

(ii) $a, b, m \in \mathbb{Z}$, $m > 0$

BW HW We need to solve the equation

$$ax \equiv b \pmod m$$

Let $d = \gcd(a, m)$

Then $d \mid a$ and $d \mid m$. If x is

a solution, then m divides $ax-b$. Then d divides $ax-b$. Since d also divides a $\Rightarrow$ d divides b.

Thus, if solutions exist, then $d \mid b$. Therefore, if $d \nmid b$ $\Rightarrow$ there are no solutions.

Suppose $d = \gcd(a,m)$ divides b. let

$$b = db'$$
$$a = da'$$
$$m = dm'$$

Then the congruence $ax \equiv b \pmod m$ is equivalent to the congruence

$$a'x \equiv b' \pmod{m'}$$

Now we see that a' is coprime to m', so that $\exists$ $s,t \in \mathbb{Z}$ with

$$sa' + tm' = 1,$$

whence

$$sa' \equiv 1 \pmod{m'}, \text{ i.e.}$$

$$s = (a')^{-1} \pmod{m'}.$$

Then, multiplying by s, we get

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