# NUMBER THEORY 1999

## Question 1

(i) $156 = 91 + 65$

$95 = 65 + 26$

$65 = 2.26 + 13$

$26 = 2.13$

Thus $\gcd(91, 156) = 13 = 65 - 2.26$

$= 65 - 2(91 - 65)$

$= 3(156 - 91) - 2.91$

$= 3.156 - 5.91$.

Thus a particular solution is $x = -5$, $y = 3$ and the general solution is

$$x = -5 + \frac{156}{13}t = -5 + 12t,$$

$$y = 3 - \frac{91}{13}t = 3 - 7t, \quad t \in \mathbb{Z}.$$

(ii) Let $d = \gcd(6n-1, 6n+3)$. As

$$(6n+3) - (6n-1) = 4,$$

$d|4$ and so $d$ is 1, 2 or 4. But $6n-1$ is odd so we must have $d = 1$.

(iii) When $n = 1$, $3^{3n} = 3^3 = 27$, so the statement is true for $n = 1$.

Suppose that the statement is true for $n = k$ where $k$ is a positive integer. Then

$$3^{3k} = 13a + 1$$

for some integer $a$. Now

$$3^{3(k+1)} = 27.3^{3k} = 27.13a + 27$$

$$= 13(27a + 2) + 1.$$

Thus the statement is true for $n = k+1$.
Therefore the statement is true for all positive integers $n$ by the Principle of Induction.

## Question 2

(i) TRUE.

Proof by contradiction. Suppose there are only finitely many primes $p_1, p_2, \ldots, p_n$ and put

$$N = (p_1 p_2 \cdots p_n) + 1.$$

Then $N > 1$ so $N$ has a prime divisor which by hypothesis must be $p_j$ for some $j = 1, \ldots, n$. But then $p_j \mid N$ and $p_j \mid (p_1 p_2 \cdots p_n)$ so that $p_j \mid 1$ which is a contradiction.

(ii) FALSE

A counterexample is 87:

$$17.5 + 2 = 87 = 3.29$$

and neither 3 nor 29 is of the asserted form.

(iii) TRUE

Suppose that none of $a, b$ and $c$ is divisible by 5. If $x \not\equiv 0 \pmod 5$ then $x^2 \equiv 1 \pmod 5$ or $x^2 \equiv 4 \pmod 5$. Hence $a^2 + b^2 + c^2$ is congruent to 3, 6, 9 or 12 (that is, 1, 2, 3 or 4) modulo 5 and so is not divisible by 5. Thus if $a^2 + b^2 + c^2$ is divisible by 5 then at least one of $a, b, c$ is divisible by 5.

## Question 3

(i) Since $n = 8k + 5$ for some integer $k$, it follows that

$$6n + 3 = 48k + 33$$

so that: (a) the least positive residue of $6n+3$ modulo 8 is 1; (b) the least positive residue of $6n+3$ modulo 12 is 9.

(ii) Suppose first that $a \equiv b \pmod{n}$. Then $a - b = kn$ so that $ra - rb = rkn$ and so $ra \equiv rb \pmod{rn}$. Conversely if $ra \equiv rb \pmod{rn}$ then $ra - rb = krn$ and so $a - b = kn$; that is, $a \equiv b \pmod{n}$.

(iii) The congruences are

$$x \equiv 2 \pmod{3}, \quad x \equiv 4 \pmod{7}, \quad x \equiv 5 \pmod{11}.$$

Note that $x \equiv 5 \pmod{11}$ and $x \equiv 2 \pmod{3}$ if and only if $x \equiv 5 \pmod{33}$. Also

$$x \equiv 5 \pmod{33} \Rightarrow x = 5, 38, 71, 104, 137, \ldots$$

and $137 \equiv 4 \pmod{7}$. The smallest positive integer which satisfies the congruences simultaneously is <u>137</u>.

## Question 4

(i) The cases $p = 2, 3$ are evident so we suppose that $p > 3$. Let $a$ be an integer such that $1 \leq a \leq p - 1$. Then $\gcd(a, p) = 1$ so that the congruence

$$ax \equiv 1 \pmod{p}$$

has a unique solution modulo $p$. Thus for each $a$ there is a unique integer $a'$ such

that $1 \leqslant a' \leqslant p-1$ and $aa' \equiv 1 \pmod{p}$. If $a^2 \equiv 1 \pmod{p}$ then $(a-1)(a+1) \equiv 0 \pmod{p}$ so that $a=1$ or $a=p-1$. Hence if $a \neq 1, p-1$ then $a \neq a'$. It follows that the set $\{2,3,\ldots,p-2\}$ is partitioned into subsets $\{a,a'\}$ such that $aa' \equiv 1 \pmod{p}$. Thus

$$2.3.\ldots.(p-2) \equiv 1 \pmod{p}$$

so that

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

(ii)(a) By FLT, $7^{16} \equiv 1 \pmod{17}$ so

$$7^{100} = (7^{16})^6 7^4 \equiv 49.49 \equiv (-2)(-2) \equiv 4 \pmod{17}.$$

(b) Note that $105 = 3.5.7$. By the Corollary to FLT:

$$a^{13} \equiv (a^3)^4 a \equiv a^4 a \equiv a^3 a^2 \equiv a a^2 \equiv a^3 \equiv a \pmod{3}$$
$$a^{13} \equiv (a^5)^2 a^3 \equiv a^2 a^3 \equiv a^5 \equiv a \pmod{5}$$
$$a^{13} \equiv a^7 a^6 \equiv a a^6 \equiv a^7 \equiv a \pmod{7}.$$

Since 3, 5 and 7 are primes, $a^{13} \equiv a \pmod{105}$.

## Question 5

(i) As

$$\sigma(m) = \sigma(2^{p-1})\,\sigma(2^p-1) = (2^p-1)\sigma(2^p-1)$$

and $2m = 2^p(2^p-1)$, $\sigma(m) = 2m$ if and only if $\sigma(2^p-1) = 2^p$ and this is the case if and only if $2^p-1$ is prime.

(ii)(a) Suppose $n$ is prime. Then

$$n + 2\sigma(n) = n + 2(n+1) = 3n+2$$

so that $n+2\sigma(n)$ is not divisible by 3.

(b) Suppose $n = p^2$ where $p$ is a prime. Then

$$n + 2\sigma(n) = p^2 + 2(p^2 + p + 1)$$
$$= 3p^2 + 2p + 2.$$

Thus $n + 2\sigma(n)$ is divisible by 3 if and only if $2p + 2 \equiv 0 \pmod 3$; that is, if and only if $p \equiv 2 \pmod 3$.

(c) Suppose $n = 2p$ where $p$ is an odd prime. Then

$$n + 2\sigma(n) = 2p + 2\sigma(2p) = 2p + 2.3.(p+1)$$
$$= 8p + 6.$$

So $3 \mid n + 2\sigma(n)$ if and only if $3 \mid p$ and this is the case if and only if $p = 3$.
Also $p = 2$ satisfies the condition by part (b).

Question 6.

(i) The discriminant is $16 - 4.3.5 = -44$, so we evaluate the Legendre symbol

$$(-44/17) = (-1/17)(44/17)$$
$$= (44/17) = (11/17)$$
$$= (17/11)$$
$$= (2/11)(3/11) = -1.$$

Thus the congruence has no solutions.

(ii) $(127/167) = -(167/127)$
$$= -(40/127) = -(2/127)(5/127)$$
$$= -(5/127) = -(127/5)$$
$$= -(2/5) = -(-1) = 1.$$

(iii) Let $p = 8k+7$ and consider the set

$$S = \{2, 4, .., 8k+6\}.$$

We must count the number of elements of S that exceed $\frac{8k+7}{2}$. These are $4k+4$, $4k+6, .., 8k+6$; that is, $4k+2+2j$ for $j = 1, 2, .., 2k+2$ and so the number is $2k+2$. By the Gauss Lemma

$$(2 \mid 8k+7) = (-1)^{2k+2} = 1.$$

## Question 7

(i) By the Euclidean algorithm

$$55 = \underline{1} \cdot 42 + 13$$
$$42 = \underline{3} \cdot 13 + 3$$
$$13 = \underline{4} \cdot 3 + 1$$
$$3 = \underline{3} \cdot 1 .$$

Thus $\frac{55}{42} = [1, 3, 4, 3]$.

The convergents can be found from the table

| | | | |
|---|---|---|---|
| 1 | 4 | 17 | 55 |
| 1 | 3 | 4 | 3 |
| 1 | 3 | 13 | 42. |

Thus $13 \cdot 55 - 17 \cdot 42 = 1$ so a particular solution is $x = -17$, $y = -13$. The general solution is

$$x = -17 + 55t, \quad y = -13 + 42t, \quad t \in \mathbb{Z},$$

so the required solution is $x = 38$, $y = 29$.

(ii) Put $x = [\langle 1, 2\rangle]$. Then

$$x = [1, 2, x] = 1 + \frac{1}{2 + \frac{1}{x}} = 1 + \frac{x}{2x+1}$$

$$= \frac{3x+1}{2x+1}.$$

Hence

$$2x^2 - 2x - 1 = 0$$

and so, since $x > 0$,

$$x = \frac{2 + \sqrt{12}}{4} = \frac{1+\sqrt{3}}{2}.$$

Now $x = [1, 2, \langle 1, 2\rangle]$ so

$$[2, 2, \langle 1, 2\rangle] = 1 + x = \frac{3+\sqrt{3}}{2}.$$

Question 8

(i) Since the cycle length is, even convergents give solutions to the equation. The convergents can be found from the table

| | | | | | |
|---|---|---|---|---|---|
| 2 | 3 | 14 | 17 | 82 | 99 |
| 2 | 1 | 4 | 1 | 4 | 1 |
| 1 | 1 | 5 | 6 | 29 | 35. |

The solutions are (3, 1), (17, 6) and (99, 35).

(ii) As $11 \mid 990$ and $11^2 \nmid 990$, it is not possible to write 990 as a sum of two squares.

$$980 = 7^2(4^2 + 2^2) = 28^2 + 14^2.$$

(iii) Suppose the equation has a solution $(x, y, z)$ where $x$, $y$ and $z$ are positive integers.

Then $x^3$ must be divisible by 3 and so $x$ is divisible by 3, say $x = 3x_1$. Then

$$27x_1^3 + 3y^3 = 9z^3,$$
$$9x_1^3 + y^3 = 3z^3.$$

Hence $y$ is divisible by 3, say $y = 3y_1$. Then

$$9x_1^3 + 27y_1^3 = 3z^3,$$
$$3x_1^3 + 9y_1^3 = z^3.$$

Hence $z$ is divisible by 3, say $z = 3z_1$. Then

$$3x_1^3 + 9y_1^3 = 27z_1^3,$$
$$x_1^3 + 3y_1^3 = 9z_1^3.$$

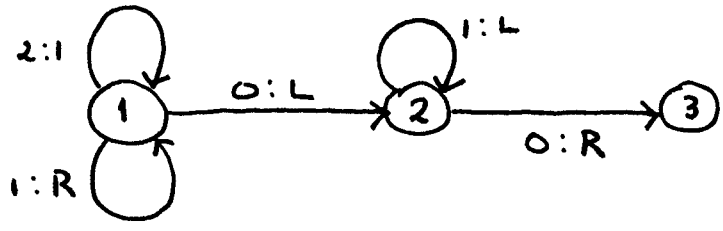
Thus if $(x, y, z)$ is a solution in positive integers then $\left(\frac{x}{3}, \frac{y}{3}, \frac{z}{3}\right)$ is a solution in positive integers. Since infinite descent through positive integers is impossible, the equation has no solution in positive integers.

# MATHEMATICAL LOGIC 1999

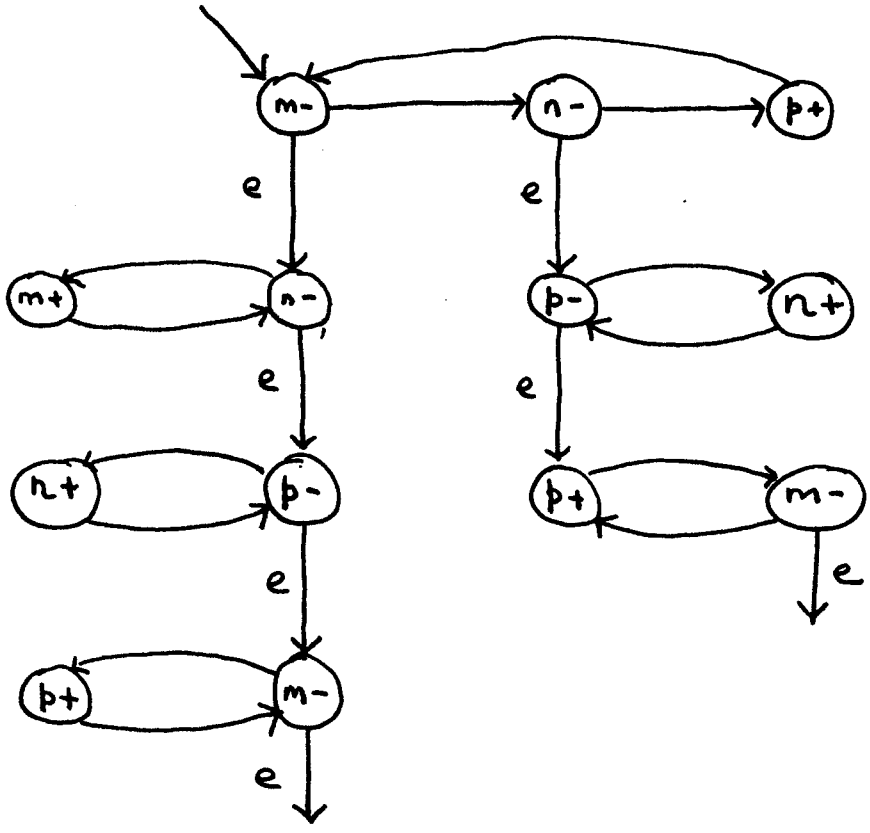
## Question 9

(i) (a) Machine (1) does not halt (prints 1s moving left forever).
Machine (2) halts in the wrong position (scanning rightmost 1).

(b) Adapt machine (2):




(ii)



## Question 10

(i) $h = Pr[f, g]$ where

$$f(x) = s(s(x)) = x+2$$

$$g(x_1, x_2, x_3) = dif(x_3, s(x_2)) = dif(x_3, x_2+1).$$

Thus

$$h(x, 0) = f(x) = x+2$$

$$h(x, s(y)) = g(x, y, h(x,y)) = dif(h(x,y), y+1)$$

So

$$h(3,0) = 5$$

$$h(3,1) = h(3, s(0)) = dif(5, 0+1) = 4$$

$$h(3,2) = h(3, s(1)) = dif(4, 1+1) = 2.$$

(ii)(a) As

$$prod(x, 0) = 0$$

$$prod(x, y+1) = x(y+1) = x + prod(x,y),$$

$$prod = Pr[z, Cn[sum, id_1^3, id_3^3]].$$

As

$$sum(x, 0) = x$$

$$sum(x, y+1) = x+y+1 = s(sum(x,y)),$$

$$sum = Pr[id, Cn[s, id_3^3]].$$

So $$prod = Pr[z, Cn[Pr[id, Cn[s, id_3^3]], id_1^3, id_3^3]].$$

(b) Informal definition:

$$f(x_1, x_2, 0) = 1 = s(z(x_1))$$

$$f(x_1, x_2, s(x_3)) = (x_1 + x_2)^{x_3+1}$$

$$= (x_1 + x_2) f(x_1, x_2, x_3)$$

$$= prod(sum(x_1, x_2), f(x_1, x_2, x_3)).$$

(iii) $Mn[f](x_1, x_2)$ is defined for those pairs $(x_1, x_2)$ with the property that there exists $y$ such that $f(x_1, x_2, y) = 0$. Now

$$f(x_1, x_2, y) = 0 \iff x_2^{y+1} = 0 \text{ or } (x_1 + y) \dot{-} x_2 = 0,$$

$$x_2^{y+1} = 0 \iff x_2 = 0,$$

$$(x_1 + y) \dot{-} x_2 = 0 \iff x_1 \leq x_2.$$

Thus $Mn[f](x_1, x_2)$ is defined for all pairs $(x_1, x_2)$ with $x_2 = 0$ and all pairs $(x_1, x_2)$ with $x_1 \leq x_2$.

Question 11

(i) As $25 = 2^4 + 2^3 + 2^0$ and

$54 = 2^5 + 2^4 + 2^2 + 2^1$,

the original configuration is

$$\cdots 0\,1\,1\,0\,0\,1\,\underset{\triangle}{0}\,1\,1\,0\,1\,1\,0 \cdots$$

The new configuration is

$$\cdots 0\,1\,1\,0\,0\,1\,\underset{\triangle}{0}\,1\,1\,0\,1\,1\,0 \cdots$$

so the new left number is $2^2 + 2^3 = 12$ and the new right number is $2^0 + 2^2 + 2^3 + 2^5 + 2^6$ $= 109$.

(ii) (a) Let $c_1, c_2$ be the characteristic functions of $C_1$ and $C_2$ respectively and define $c_3$ by

$$c_3(x, y) = \overline{sg}\,(c_1(x, y) + c_2(x, y)).$$

Then $c_1, c_2, c_3, g_1, g_2$ and $g_3$ are primitive recursive functions and

$$f(x, y) = \sum_{j=1}^{3} c_j(x, y)\, g_j(x, y)$$

so $f$ is a primitive recursive function.

(b) Let $c_1, c_2$ be the characteristic functions of $C_1, C_2$ respectively and define $c$ by

$$c(x,y) = c_1(x,y)c_2(x,y).$$

Then $c$ is primitive recursive and is the characteristic function of '$C_1 \& C_2$'.

(c) This function is of the form considered in (a) where

$$g_1(x,y) = 3^{xy} = \text{prod}(3, \text{prod}(x,y)),$$

$$g_2(x,y) = y^4 = \text{exp}(y,4),$$

$$g_3(x,y) = 5,$$

$C_1$ is the condition "$5x+7y$ is even" and $C_2$ is the condition "$x$ is odd and $2x=y$".

Note first that the conditions $C_1$ and $C_2$ are mutually exclusive, for if $C_2$ holds then $5x+7y = 19x$ where $x$ is odd, so $5x+7y$ is odd.

The characteristic function $c_1$ of $C_1$ is given by

$$c_1(x,y) = \overline{sg}\left(e\left(\text{sum}\left(\text{prod}(5,x), \text{prod}(7,y)\right)\right)\right)$$

so $C_1$ is a primitive recursive condition.

The characteristic function of the condition '$x$ is odd' is $(x,y) \mapsto e(x)$ and the characteristic function of the condition '$y=2x$' is $(x,y) \mapsto Eq(y, \text{prod}(2,x))$. As both of these functions are primitive recursive, $C_2$ is a primitive recursive condition by (b).

Finally, $g_1, g_2$ and $g_3$ are primitive recursive functions. Thus $f$ is a primitive recursive function.

## Question 12.

(i) As

$$c(x,y,z) = \overline{sg}\,(dif\,(prod(y,z),x))$$

it is a primitive recursive function.

(ii)(a) As $c(x,y,z) = 1$ for $z = 1, \ldots, quot(x,y)$ and $c(x,y,z) = 0$ for $z > quot(x,y)$,

$$quot(x,y) = \sum_{z=1}^{x} c(x,y,z)$$

$$= \left(\sum_{z=0}^{x} c(x,y,z)\right) \dot{-} 1.$$

Thus the function quot is primitive recursive.

(b) As

$$rem(x,y) = x \dot{-} prod(y, quot(x,y)),$$

the function rem is primitive recursive.

## Question 13

(i) Let $\varphi$ be the subformula $\forall y\ y = x$,
let $\psi$ " " " $-y = x$, and
" $\theta$ " " " $\forall y\,(y = x \vee \forall y\ y = x)$.

Then the given formula is

$$((-\varphi \to (\psi \,\&\, \theta)) \to (\psi \vee \varphi)).$$

This is shown to be a tautology by writing down an 8-line truth table.

(ii) (a) 1 on line (1); 1 on line (2); 3 on line (3); 4 on line (4); 1, 3 on line (5); 1 on line (6); 1, 3 on line (7); 1, 4 on line (8); 1 on line (9).

(b) The tautology used on line (5) is

$$(((\theta \,\&\, -\varphi) \,\&\, (\varphi \to \psi)) \to (\varphi \to \psi)).$$

(c) (A) YES (B) NO.

(iii) Let X be a set with at least two members. Then $\forall x \exists y\ -x = y$ is true when interpreted in X, but $\exists y\ -y = y$ is not true.

Question 14

(i) (a) NO (b) NO (c) YES.

(ii) (a)

| | | | |
|---|---|---|---|
| 1 | (1) | $\exists x \forall y\ (x+y) = x$ | Ass |
| 2 | (2) | $\forall y\ (x+y) = x$ | Ass |
| 2 | (3) | $(x+y) = x$ | UE, (2) |
| 2 | (4) | $\exists x\ (x+y) = x$ | EI, (3) |
| 2 | (5) | $\exists y \exists x\ (x+y) = x$ | EI, (4) |
| 1 | (6) | $\exists y \exists x\ (x+y) = x$ | EH, (5). |

(b)

| | | | |
|---|---|---|---|
| 1 | (1) | $\forall x\ (\varphi \to \theta)$ | Ass |
| 2 | (2) | $\exists x\ (\psi \vee -\varphi)$ | Ass |
| 3 | (3) | $\varphi$ | Ass |
| 4 | (4) | $\forall x\ -(\psi \,\&\, \theta)$ | Ass |
| 5 | (5) | $(\psi \vee -\varphi)$ | Ass |
| 1 | (6) | $(\varphi \to \theta)$ | UE, (1) |
| 4 | (7) | $-(\psi \,\&\, \theta)$ | UE, (4) |
| 1,4,5 | (8) | $-\varphi$ | Taut (5), (6), (7) |
| 1,3,4,5 | (9) | $(\varphi \,\&\, -\varphi)$ | Taut (3), (8) |

/ continued

| | | |
|---|---|---|
| 1,3,5 (10) | $(\forall x\,\neg(\psi \,\&\, \theta) \rightarrow (\varphi \,\&\, \neg\varphi))$ | CP, (9) |
| 1,3,5 (11) | $\neg\forall x\,\neg(\psi \,\&\, \theta)$ | Taut. (10) |
| 1,5 (12) | $(\varphi \rightarrow \neg\forall x\,\neg(\psi \,\&\, \theta))$ | CP, (11) |
| 1,2 (13) | $(\varphi \rightarrow \neg\forall x\,\neg(\psi \,\&\, \theta))$ | EH, (12) |

The condition on $\varphi$ is needed to justify the use of EH to obtain line (13).

Question 15

(i) This is a theorem of Q.

| | | |
|---|---|---|
| 1 (1) | $\forall x\,(x+0) = x$ | Ass |
| 2 (2) | $\forall x\,(x.0) = 0$ | Ass |
| (3) | $\theta(0.(x+0)) = (0.(x+0))$ | II |
| 1 (4) | $(x+0) = x$ | UE, (1) |
| 1 (5) | $(0.(x+0)) = (0.x)$ | SR, (3), (4) |
| (6) | $((0.x)+(0.0)) = ((0.x)+(0.0))$ | II |
| 2 (7) | $(0.0) = 0$ | UE, (2) |
| 2 (8) | $((0.x)+0) = ((0.x)+(0.0))$ | SR, (6), (7) |
| 1 (9) | $((0.x)+0) = (0.x)$ | UE, (1) |
| 1,2 (10) | $(0.x) = ((0.x)+(0.0))$ | SR, (8), (9) |
| 1,2 (11) | $(0.(x+0)) = ((0.x)+(0.0))$ | SR, (5), (10) |
| 1,2 (12) | $\forall x\,(0.(x+0)) = ((0.x)+(0.0))$ | UI, (11) |

As assumptions 1, 2 are axioms of Q

$$\vdash_Q \forall x\,(0.(x+0)) = ((0.x)+(0.0)).$$

(ii) For all $y$ in $N^{**}$, $y + \alpha' = y + \alpha = \beta \neq \alpha'$. So there is no $y$ such that $y + \alpha' = \alpha'$. Since all the axioms of Q hold in $N^{**}$ and the sentence is false in $N^{**}$, the sentence

is not a theorem of Q by the Correctness Theorem.

(iii) This is a theorem of Q.

| | | |
|---|---|---|
| 1 (1) | $\forall x\,(x+0) = x$ | Ass |
| 1 (2) | $(y'+0) = y'$ | UE, (1) |
| 1 (3) | $\forall y\,(y'+0) = y'$ | UI, (2) |
| 1 (4) | $\exists x \forall y\,(y'+x) = y'$ | EI, (3) |

As assumption 1 is an axiom of Q,

$$\vdash_Q \exists x \forall y\,(y'+x) = y'.$$

Question 16

(i)(a) A theory T is said to be complete if $T \vdash \theta$ or $T \vdash -\theta$ for all sentences $\theta$.

(b) A theory T is said to be consistent if there is no sentence $\theta$ such that $T \vdash \theta$ and $T \vdash -\theta$.

(c) A theory T is said to be axiomatizable if it has a recursively enumerable set of axioms.

(ii) NO, because $Z \vdash -\underline{0} = \underline{1}$ and Z is consistent.

(iii) $\forall x \forall y\,(x+y) = (y+x)$.

(iv) (a) NO (b) YES.

(v) Gödel's First Incompleteness Theorem: arithmetic is a complete and consistent extension of Q as so is not axiomatizable.