EXAM SOLUTIONS 2011 by Linda Brown

Question 1

(i) Using the **Euclidean Algorithm**: [4 Marks]

156 = 1 x 91 + 65
91 = 1 x 65 + 26
65 = 2 x 26 + 13
26 = 2 x 13 + 0
Hence gcd (156, 91) = 13

Reversing the above equations:
13 = 65 – 2 x 26 = 65 – 2(91 – 65) = 3 x 65 – 2 x 91 = 3(156 – 91) – 2 x 91
So 13 = 3 x156 – 5 x 91 = 91(– 5) + 156 (3)
One solution $x_0 = -5$, $y_0 = 3$

Hence the general solution to $91x + 156y = 13$ (Theorem 5.1 Unit 1), dividing through by 13 to obtain $7x + 12y = 1$, is

$x = -5 + 12k$, $y = 3 - 7k$, $k \in \mathbb{Z}$

(ii) **Divisibility & gcds** [3 Marks]

Using the Result in NT1, p10 Handbook:

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

So gcd $(6n + 3, 6n - 1)$ = gcd $(6n - 1, 4) = 1$ because $4 = 2^2$ and $6n - 1$ is odd

(iii) **Mathematical Induction** [4 Marks]

Let $P(n)$ be the stated formula

$P(1)$ is true because $1 = 1/6 \times 1 \times 2 \times 3$, giving the basis for induction

Assume $P(k)$ is true for some integer $k \geq 1$, i.e.

$1 + 7 + 18 + \ldots + \frac{1}{2} k(5k - 3) = 1/6\ k(k + 1)(5k - 2)$ [Induction Hypothesis]

Then $1 + 7 + 18 + \ldots + \frac{1}{2} k(5k - 3) + \frac{1}{2}(k + 1)[5(k + 1) - 3]$

$= 1/6\ k(k + 1)(5k - 2) + \frac{1}{2}(k + 1)(5k + 2)$ using the Induction Hypothesis

$= 1/6\ (k + 1)[5k^2 + 13k + 6] = 1/6\ (k + 1)(k + 2)(5k + 3)$

$= 1/6\ (k + 1)((k + 1) + 1)(5(k + 1) - 2)$ Completing the induction step

Hence $P(k)$ true $\Rightarrow P(k + 1)$ true
Therefore by the Principle of Mathematical Induction, $P(n)$ is true for all integers $n \geq 1$

Question 2 – TRUE/FALSE, Divisibility & Primes [11 Marks]

(i) FALSE: 25 has the form $6k + 1$ ($k = 4$); its only prime divisor is 5, which is not of the same form. This counterexample shows that the given statement is false.

(ii) TRUE: Using the Division Algorithm, all prime divisors must take one of the forms $6m + r$, with $0 \leq r \leq 5$ (proof by exhaustion)
$6m$, $6m + 2$, $6m + 3$, $6m + 4$ are all composite (so not prime) except for primes 2 and 3, but neither 2 nor 3 divides a number of the form $6k + 5$, leaving $6m + 1$ & $6m + 5$.
$(6r + 1)(6s + 1) = 6(6rs + r + s) + 1$ means that a number with all its prime divisors of the form $6m + 1$ will itself be of this form, which it is not.
Hence a number of the form 6k + 5 must have a prime divisor of the same form.
[Note that this is needed for proof of part (iv)]

EXAM SOLUTIONS 2011 by Linda Brown

Question 2 – Divisibility & Primes

(iii) FALSE: Let $m = 1$ and $n = 1$, then gcd $(m, n) = 1$
but this gives gcd $(6m + 1, 6n + 1)$ = gcd $(7, 7) = 7 \neq 1$
This counterexample shows that the given statement is false.

(iv) TRUE: Assume that there are a finite number of primes of the form $6k + 5$ which are $p_1, p_2, \ldots, p_n$
Consider the number $N = 6(p_1p_2 \ \ldots \ p_n) - 1$ which is of the form $6k + 5$
Hence N must have a prime divisor, p say, of the same form by part (ii).
Therefore $p = p_i$ for some $i : 1 \leq i \leq n$
Hence $p \mid 6(p_1p_2 \ \ldots \ p_n) - 1 = N$ and $p \mid p_1p_2 \ \ldots \ p_n \Rightarrow p \mid 1$
which is a contradiction because p is prime
Hence there are infinitely many primes of the form $6k + 5$

Question 3 – Congruences

(i) As $n \equiv 3 \pmod{10} \Rightarrow n = 10k + 3$ then $6n + 1 = 60k + 19$, $k \in \mathbb{Z}$

(a) $6n + 1 \equiv 19 \equiv 7 \pmod{12}$ so the least positive residue mod 12 is 7

(b) $6n + 1 \equiv 19 \equiv 4 \pmod{15}$ so the least positive residue mod 15 is 4

[2 Marks]

(ii) By definition $a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$
If $a \equiv b \pmod{n}$, let $a - b = kn$, $k \in \mathbb{Z} \Rightarrow ra - rb = rkn \Rightarrow r\,n \mid (ra - rb) \Rightarrow ra \equiv rb \pmod{rn}$
Similarly if $ra \equiv rb \pmod{r\,n}$, let $ra - rb = rkn \Rightarrow a - b = kn \Rightarrow n \mid (a - b) \Rightarrow a \equiv b \pmod{n}$
Hence $ra \equiv rb \pmod{r\,n} \Leftrightarrow a \equiv b \pmod{n}$ as required [3 Marks]

(iii) $5x \equiv 7 \equiv 45 \pmod{19} \Leftrightarrow x \equiv 9 \pmod{19}$
The Chinese Remainder Theorem guarantees a unique solution satisfying all three congruences simultaneously mod 2 x 7 x 19 = 266
$x \equiv 9 \pmod{19} \Rightarrow x = 9 \equiv 1 \pmod{2}$
and
$x \equiv 9 \pmod{2 \times 19} \Rightarrow x = 9, 47, 85, 123, 161, 199, 237 \equiv 6 \pmod{7}$
Hence $x \equiv 237 \pmod{266}$ satisfies all three congruences [6 Marks]

Question 4 – Fermat's Little Theorem (FLT)

(i) Note that 13 is prime so by FLT $a^{12} \equiv 1 \pmod{13}$ for gcd $(a, 13) = 1$
As gcd $(5, 13)$ = gcd $(3, 13) = 1$
$5^{50} + 3^{30} \equiv (5^{12})^4 \times 5^2 + (3^{12})^2 \times 3^6 \equiv 1^4 \times 25 + 1^2 \times 27^2 \equiv 1 \times (-1) + 1 \times 1 \equiv 0 \pmod{13}$
Therefore $5^{50} + 3^{30}$ is exactly divisible by 13 (no remainder) [4 Marks]

(ii) [7 Marks]

(a) Using Theorem 2.2 of NT4 with 19 being prime and cycle length 18,
the order of 10 (mod 19) is 18.

(b) Using part (a), $10^{18} \equiv 1 \pmod{19}$; 18 is the smallest power of 10 for which this is true*.
$10^{18} = (10^9)^2 \equiv 1 \pmod{19}$ giving $10^9 \equiv \pm 1 \pmod{19}$ – Lagrange's Theorem, with 19 being prime, confirms that there are only these two possibilities
But $10^9 \not\equiv 1$ see * above
Hence $10^9 \equiv -1 \pmod{19}$

(c) Using long division (p11 Unit NT4)
$12 = \mathbf{0} \times 19 + 12$
$120 = \mathbf{6} \times 19 + 6$
$60 = \mathbf{3} \times 19 + 3$
$30 = \mathbf{1} \times 19 + 11$
Hence the first few digits of 12/19 are 0.<631…….
Therefore, using the cycle for 1/19 and taking a different starting position –

EXAM SOLUTIONS 2011 by Linda Brown

12/19 = 0.<631578947368421052>

[Alternatively calculate the first few numbers of 12 x 0.<0526315……>]

Question 5 – Multiplicative Functions

(i) Using the multiplicative property of σ [7 Marks]

(a) $\sigma(74) = \sigma(2)\,\sigma(37) = 3 \times 38 = 114 < 148 = 2 \times 74$, hence 74 is not abundant.

(b) $\sigma(174) = \sigma(2)\,\sigma(3)\,\sigma(29) = 3 \times 4 \times 30 = 360 > 348 = 2 \times 174$, hence 174 is abundant.

(c) Need $\sigma(10p) > 20p$ for $10p$ to be abundant, using the multiplicative property of σ,
If $p = 2$ then $\sigma(10p) = \sigma(4)\,\sigma(5) = (1 + 2 + 2^2) \times 6 = 42 > 40$, so $10p$ abundant
If $p = 5$ then $\sigma(10p) = \sigma(2)\,\sigma(25) = 3 \times (1 + 5 + 5^2) = 93 < 100$, so $10p$ not abundant
If p is a prime other than 2 or 5 then $\sigma(10p) = \sigma(2)\,\sigma(5)\,\sigma(p) = 3 \times 6 \times (1 + p) > 20p$
So $18 + 18p > 20p \Rightarrow p < 9$, i.e. $p = 3$ or 7
Hence the only primes for which $10p$ are $p = 2, 3, 7$

(ii) If p is an odd prime then gcd $(4, p) = 1$ and using the multiplicative property of ϕ:
$\phi(4p) = \phi(4)\,\phi(p) = 2(2 - 1) \times (p - 1) = 2(p - 1)$
If $2p - 1$ is an odd prime then gcd $(2, 2p - 1) = 1$ & using the multiplicative property of ϕ:
$\phi(4p - 2) = \phi(2(2p - 1)) = \phi(2)\,\phi(2p - 1) = (2 - 1) \times ((2p - 1) - 1) = 2(p - 1) = \phi(4p)$
[4 Marks]

Question 6 – Quadratic Reciprocity: Legendre Symbol & LQR

(i) The discriminant of the quadratic congruence is $25 - 4 \times 4 \times 2 = -7$
So evaluate $(-7/19) = (12/19) = (4/19)(3/19) = (1) \times (-1) = -1$, using Theorem 2.1(a),(b),(c) & 4.4 Unit 6
Hence the congruence has no solutions, because – 7 is a quadratic non-residue of 19.
[4 Marks]

(ii)

$(86/127) = (2/127)\,(43/127)$	Theorem 2.1(b)
$= (1)\,(-1)\,(127/43)$	LQR, Theorem 3.2
$= (-1)\,(41/127)$	Theorem 2.1(a)
$= (-1)\,(127/41)$	LQR
$= (-1)\,(4/41)$	Theorem 2.1(a)
$= (-1)\,(1) = -1$	Thm 2.1(b) [3 Marks]

(iii) $(6/p) = (3/p)(2/p) = 1$ so either $(3/p) = (2/p) = 1$ or $(3/p) = (2/p) = -1$, with $p \neq 2, 3$ (because by definition gcd $(6, p) = 1$), using Theorems 4.4 and 3.2

$(3/p) = 1 \Rightarrow p \equiv \pm 1 \pmod{12}$ and $(2/p) = 1 \Rightarrow p \equiv \pm 1 \pmod 8$
This gives $p \equiv \pm 1 \pmod{\text{lcm } (8, 12)}$, i.e. $p \equiv 1, 23 \pmod{24}$

$(3/p) = -1 \Rightarrow p \equiv \pm 5 \pmod{12}$ and $(2/p) = -1 \Rightarrow p \equiv \pm 5 \pmod 8$
This gives $p \equiv \pm 5 \pmod{\text{lcm } (8, 12)}$, i.e. $p \equiv 5, 19 \pmod{24}$

Primes for which $(6/p) = 1$: $p \geq 5$, $p \equiv 1, 5, 19, 23 \pmod{24}$ [4 Marks]

Question 7 – Continued Fractions

(i) Using the Euclidean Algorithm: [4 Marks]
$82 = \mathbf{1} \times 69 + 13$
$69 = \mathbf{5} \times 13 + 4$
$13 = \mathbf{3} \times 4 + 1$
$4 = \mathbf{4} \times 1 + 0$ or $4 = \mathbf{3} \times 1 + 1$
$1 = \mathbf{1} \times 1 + 0$
Hence $82/69 = [1, 5, 3, 4] = [1, 5, 3, 3, 1]$

(ii) Let $x = [<2, 1>] = [2, 1, x]$, which has convergents 2/1, 3/1, $\frac{3x + 2}{x + 1} = x$ [7 Marks]
$\Rightarrow 3x + 2 = x^2 + x$
$\Rightarrow x^2 - 2x - 2 = 0$

$\Rightarrow x = \frac{2 + \sqrt{12}}{2} = 1 + \sqrt{3}$ using the quadratic formula and taking the positive root

Question 7 – Continued Fractions

Hence $\alpha = [0, 2, x]$ with convergents $0/1, 1/2, x/(2x + 1)$

Therefore $\alpha = \frac{x}{x+1} = \frac{1 + \sqrt{3}}{3 + 2\sqrt{3}} = \frac{(1 + \sqrt{3})(3 - 2\sqrt{3})}{(3 + 2\sqrt{3})(3 - 2\sqrt{3})} = \frac{3 - \sqrt{3}}{3} = [0, 2, <2, 1>]$

Convergents: $C_1 = 0/1$, $C_2 = 1/2$, $C_3 = 2/5$, $C_4 = 3/7$, $C_5 = 8/19$, $C_6 = 11/26$, $C_7 = 30/71$, ...
Corollary to Theorem 4.1 Unit 7 gives:
$|\alpha - C_5| < 1/(19 \times 26) < 1/(20 \times 25) = 1/500 < 1/400$, but
$|\alpha - C_4| > 1/(2 \times 7 \times 19) > 1/(2 \times 7 \times 20) = 1/280 > 1/400$
Hence the first convergent to have the required accuracy is C_5

Question 8

(i) **Pythagorean Triples** [4 Marks]

For primitive triples (x, y, z) only $x = 2mn$ is even, with m & n being opposite parity, $m > n$

(a) Hence let $x = 20 \Rightarrow mn = 10$, the only possibilities are:
$m = 10$, $n = 1$, giving $(20, 99, 101)$
$m = 5$, $n = 2$, giving $(20, 21, 29)$ (Theorem 2.1 Unit 8)

(b) Let $x = 22 \Rightarrow mn = 11$, so the only possibility is $m = 11$, $n = 1$ but m and n are both odd
Hence there are no primitive triples with side 22

(ii) **Sums of Squares** [3 Marks]

$360 = 2^3 \times 3^2 \times 5 = (6^2 + 0^2)(3^2 + 1^2) = 18^2 + 6^2$,
using the Identity in Unit 8. Hence 360 can be expressed as the sum of two squares.

$365 = 2^2 \times 7 \times 13$
By Theorem 4.3 Unit 8, 365 cannot be expressed as a sum of two squares because 7, the only prime divisor of 365 with form $4k + 3$, occurs to an odd power.

(iii) **Method of Infinite Descent** [4 Marks]

Assuming $\sqrt{8}$ is rational, let $\sqrt{8} = m / n \Rightarrow \sqrt{8}\, n = m$

Hence $\frac{8n - 2m}{m - 2n} = \frac{8n - 2\sqrt{8}\, n}{\sqrt{8}\, n - 2n} = \frac{(8 - 2\sqrt{8})(\sqrt{8} + 2)}{(\sqrt{8} - 2)(\sqrt{8} + 2)} = \frac{4\sqrt{8}}{4} = \sqrt{8}$

Note that $2 < \sqrt{8} < 3$ so that $0 < m - 2n = (\sqrt{8} - 3)n < n$ and we have found a further rational expression for $\sqrt{8}$ with smaller positive integer denominator than the first.

Therefore we could continue this process ad infinitum, finding rational expressions for $\sqrt{8}$ with smaller and smaller positive integer denominators.
This is a contradiction because we can't descend forever through the positive integers.
Hence using the method of infinite descent $\sqrt{8}$ must be irrational.

EXAM SOLUTIONS 2011 by Linda Brown

Question 9 – URMs

(i)(a) [2 Marks]

R_1	R_2	R_3	Next Instruction
2	3	0	1
2	3	1	2
2	3	1	3
2	3	1	4
2	3	1	1
2	3	2	2
2	3	2	5
3	3	2	STOP

(i)(b) If m = n = 0 the machine doesn't halt so the given URM does not compute max (0, 0)
Also, if either of m or n is zero then URM will compute max (n, m) giving an output of 0

$f^1{}_P$: $\mathbb{N} \to \mathbb{N}$ [6 Marks]

$$f^1{}_P(n) = \begin{cases} 0, & \text{if } n > 0 \\ \text{undefined}, & \text{otherwise (if n = 0)} \end{cases}$$

$f^2{}_P$: $\mathbb{N}^2 \to \mathbb{N}$

$$f^2{}_P(n) = \begin{cases} 0, & \text{if either m = 0 or n = 0} \\ \max(n, m), & \text{if m > 0 and n > 0} \\ \text{undefined}, & \text{otherwise (if n = m = 0)} \end{cases}$$

(ii) [3 Marks]

1 J (1, 3, 5)
2 J (2, 3, 6)
3 S (3)
4 J (1, 1, 1)
5 C (2, 1)

Question 10 – Primitive recursive relations and definition by cases

(i) The characteristic function of the relation *eq* is: [2½ Marks]

$$X_{eq}(n, m) = \overline{\text{sg}}(\text{adf}(n, m)) = \begin{cases} 1, & \text{if } |n - m| = 0, \text{ i.e. if } n = m \\ 0, & \text{if } |n - m| > 0, \text{ i.e. if } n \neq m \end{cases}$$

Hence the characteristic function of the relation X_{eq}, and therefore the relation *eq*, is primitive recursive because it can be expressed in terms of primitive recursive functions signum bar and adf using substitution (Handbook p20).

(ii) $X_{A\cup B}(n) = \text{sg}(X_A(n) + X_B(n)) = \text{sg}(\text{add}(X_A(n), X_B(n)))$ [2½ Marks]

$$= \begin{cases} 1, & \text{if } X_A(n) + X_B(n) > 1, \Rightarrow \text{if either or both } n \in A \text{ and } n \in B, \quad \text{i.e. if } n \in A \cup B \\ 0, & \text{if } X_A(n) + X_B(n) = 0, \Rightarrow \text{if } n \notin A \text{ and } n \notin B, \quad \text{i.e. if } n \notin A \cup B \end{cases}$$

Hence the characteristic function of the set $X_{A\cup B}$, and therefore the set $A \cup B$, is primitive recursive because it is obtained from primitive recursive functions sg, add X_A, X_B, using substitution. Sets A and B are primitive recursive, so X_A and X_B are primitive recursive.

EXAM SOLUTIONS 2011 by Linda Brown

NB Only the characteristic function in terms of other p.r. functions, plus the words at the end, are required for full marks on (i) & (ii) … rest is included to demonstrate that I have the correct c. f.

Question 10 – Primitive recursive relations and definition by cases

(iii) Using definition by cases [6 Marks]

Define $g_1(n, m) = mn$ = mult (n, m), $g_2(n, m) = m^7$ = exp$(m, 7)$, and $g_3(n, m) = 11$
These functions are all primitive recursive because they are obtained from primitive recursive functions mult and exp, constant and projection functions using substitution.

Define R_1 as the relation min $(2n, 3m) > 600$. The characteristic function of R_1 is

$$X_{R1}(n, m) = X_{>}(\text{min (mult } (2, n), \text{ mult } (3, m)), 600)$$

Define R_2 as the relation $5n + 4m = 2000$. The characteristic function of R_2 is

$$X_{R2}(n, m) = X_{\leq}(\text{add (mult } (5, n), \text{ mult } (4, m)), 2000)$$

The functions X_{R1} and X_{R2} and therefore the relations R_1 and R_2 are primitive recursive because they are obtained from primitive recursive functions $X_{>}$, $X_{\leq}$, min, add and mult, plus constant and projection functions, using substitution (Handbook p20).

Define $R_3(n, m) \Leftrightarrow$ 'not $R_1(n, m)$' and 'not $R_2(n, m)$'
The relation R_3 is primitive recursive as a result of Problem 1.10.

If R_1 holds then $2n > 600$ and $3m > 600$, so $n > 300$ and $m > 200$, hence $5n + 4m > 2300$ and therefore cannot equal 2000, so R_2 is not satisfied.
R_3 holds when neither R_1 nor R_2 holds.
Therefore R_1, R_2 and R_3 are mutually exclusive and exhaustive conditions.

Hence by Theorem 1.5 (Handbook p22) the function f is primitive recursive.

Question 11 – Primitive recursive functions including bounded minimization

(i)(a) Define $g(n_1, n_2) = f(\text{succ } (U_2^2(n_1, n_2)), \text{zero } (U_1^2(n_1, n_2)), U_1^2(n_1, n_2))$
The function g is obtained from the basic primitive recursive functions zero, succ and U_k^m, and the function f, which is primitive recursive, using substitution.
Hence g is primitive recursive. [2 Marks]

(i)(b) mult $(n, 0) = n \times 0 = 0 = f(n) \quad \Rightarrow f(n) = \text{zero}(n)$
mult $(n, m + 1) = n(m + 1) = nm + n = g(n, m, \text{mult}(n, m))$
$\Rightarrow g(n_1, n_2, n_3) = n_1 + n_3 = \text{add}(U_3^3(n_1, n_2, n_3), U_1^3(n_1, n_2, n_3))$
Hence mult is primitive recursive as it is obtained from the basic primitive recursive functions U_1^3, U_3^3, zero and succ, and the primitive recursive function add, using primitive recursion. [4 Marks]

(ii) Define the relation $R(n, y) \Leftrightarrow n < 2^y$;
its characteristic function is $X_R(n, y) = X_{<}(n, \exp(2, y))$
Hence relation R is primitive recursive because its characteristic function is obtained from primitive recursive functions $X_{<}$ and exp, plus constant and projection functions, using substitution (Handbook p20/1).
Therefore by Theorem 3.5, $g: \mathbb{N}^2 \to \mathbb{N}$, $g(n, z) = \mu y \leq z R(n, y)$ is primitive recursive.
Choose the bound z for y to be n.
Hence $f(n) = g(n, n)$
Therefore f is primitive recursive because it is obtained from the primitive recursive function g. (Problem 1.4 ML2) [5 Marks]

EXAM SOLUTIONS 2011 by Linda Brown

Question 12 – Algorithmic procedure/set of programs not recursive

(i) Consider the following URM programs for $a \in \mathbb{N}$, $a > 0$:

1 C (1, a)
2 S (1)
3 S (1)

With input n these URMs all compute h as they don't alter the contents of register R_1 after the first instruction, then add 2 to R_1 always halting with output $n + 2$.
There are infinitely many values of a, hence there are infinitely many URM programs that compute the function h for all $n \in \mathbb{N}$. [2 Marks]

(ii) A suggested algorithmic procedure is as follows.

- Recover the instructions for program P by decoding its code number e
- Let Q be the URM that computes h 1 S (1)
  2 S (1)
- $\rho(Q) = 1$, so let $u = \max(\rho(P), 1) + 1$, a register not required by P or Q and store the input in there for use when running the program to compute h; run P, zero register 1 to be used by Q, copy the input back into R_1 (this will in effect erase contents in R_1) then concatenate instructions for Q and stop.
- Program P^* is as follows:
  C (1, u)
  P
  C (u, 1)
  Q

Hence if input is n, P halts so that the next part of P^* can operate, i.e. Q, and therefore P^* halts with output $h(n) = n + 2$, precisely when $f^1{}_P(n)$ is defined
Therefore P^* computes the function h exactly when $f^1{}_P$ is total
[5 Marks]

(iii) Assume that X is recursive
Hence there is an algorithm for testing whether a code number is in X
So construct an algorithm* for testing whether a code number e is in Tot:

- If e does not code a URM program then $e \notin Tot$
- If e codes a URM program then use the algorithmic procedure in (i) to construct P^*
- Test whether $\gamma(P^*)$ is in X (by the algorithm*)
- $\gamma(P^*) \in X \Leftrightarrow f^1{}_P(n)$ is total $\Leftrightarrow e \in Tot$ [4 Marks]

Hence we have an algorithmic procedure for deciding whether $e \in Tot$, so Tot is recursive, but this contradicts Theorem 3.2. Therefore X is not recursive.

Question 13 – Formal proof: truth tables and rules

(i) Let ϕ be the subformula $\exists x\ x = y$ ' [3 Marks]
Let χ be the subformula $x = y$ '
Let ψ be the subformula $\forall y\ (x = y\text{ '} \leftrightarrow \exists x\ x = y\text{ '})$

Hence the revised formula and truth table are as detailed below

(((φ	v	ψ)	→	χ)	→	(¬	χ	→	¬	φ))
1	1	1	1	1	**1**	0	1	1	0	1
1	1	1	0	0	**1**	1	0	0	0	1
1	1	0	1	1	**1**	0	1	1	0	1
1	1	0	0	0	**1**	1	0	0	0	1
0	1	1	1	1	**1**	0	1	1	1	0
0	1	1	0	0	**1**	1	0	1	1	0
0	0	0	1	1	**1**	0	1	1	1	0
0	0	0	1	0	**1**	1	0	1	1	0

Hence the given formula is a tautology

Question 13 – Formal proof: truth tables and rules

(ii)(a)

Line	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Ass No	1	2	1	4	1, 2	1, 2	1, 4	1	1,4

[2½ Marks]

(ii)(b) $(((\phi \vee \theta) \& (\theta \rightarrow \psi)) \rightarrow (\phi \vee \theta))$

[½ Mark]

(ii)(c) (A) YES
(B) NO [2 Marks]

(iii) Use of EI on line (2) is not valid. Term x is not freely substitutable for variable y in $\forall x\,(y + \mathbf{0}) = x$ as it becomes bound.

Consider the standard interpretation N, $(x + \mathbf{0}) = x$ is true in N for all $x \in \mathbb{N}$
However $\exists y\,\forall x\,(y + \mathbf{0}) = x$ is false in N: ["There exists a single y such that for all x…."]
For instance, if x is 1 then y can only be interpreted as 1 so that $y + 0 = 1 + 0 = 1 = x$
but if x is interpreted as 2, with y as 1, then $y + 0 = 1 + 0 = 1 \neq 2 = x$
Therefore, by definition, $\exists y\,\forall x\,(y + \mathbf{0}) = x$ is not a logical consequence of $\forall x\,(x + \mathbf{0}) = x$
[3 Marks]

Question 14 – Free & bound variables, & Formal Proof

(i)(a) NO
(i)(b) YES
(i)(c) NO [2 Marks]

(ii)(a)	1	(1)	$\forall x\,\forall y\,(y'.\,x) = (z + y')$	Ass
	1	(2)	$\forall y\,(y'.\,x') = (z + y')$	UE, 1
	1	(3)	$(\mathbf{0}'.\,x') = (z + \mathbf{0}')$	UE, 2
	1	(4)	$\exists y\,(y.\,x') = (z + y)$	EI, 3
	1	(5)	$\forall x\,\exists y\,(y.\,x') = (z + y)$	UI, 4

[3 Marks]

(ii)(b)	1	(1)	ψ	Ass
	2	(2)	$\forall x\,(\phi \rightarrow (\neg\,\theta \vee \neg\psi))$	Ass
	2	(3)	$(\phi \rightarrow (\neg\,\theta \vee \neg\psi))$	UE, 2
	4	(4)	$\exists x \neg\,(\phi \rightarrow \neg\,\theta)$	Ass
	5	(5)	$\neg\,(\phi \rightarrow \neg\,\theta)$	Ass
	2, 5	(6)	$\neg\,\psi$	Taut, 3, 5**
	1, 2, 5	(7)	$(\psi \& \neg\,\psi)$	Taut 1, 6
	1, 2, 4	(8)	$(\psi \& \neg\,\psi)$	EH, 7*
	1, 2	(9)	$(\exists x \neg\,(\phi \rightarrow \neg\,\theta) \rightarrow (\psi \& \neg\,\psi))$	CP, 8
	1, 2	(10)	$\neg\,\exists x \neg\,(\phi \rightarrow \neg\,\theta)$	Taut, 9
	1	(11)	$(\forall x\,(\phi \rightarrow (\neg\,\theta \vee \neg\psi)) \rightarrow \neg\,\exists x \neg\,(\phi \rightarrow \neg\,\theta))$	CP, 10

*Line (8) requires x not occurring free in ψ [6 Marks]
[** tautology is $(((\phi \rightarrow (\neg\,\theta \vee \neg\psi)) \& \neg\,(\phi \rightarrow \neg\,\theta)) \rightarrow \neg\,\psi)$]

EXAM SOLUTIONS 2011 by Linda Brown

Question 15 – Formal Proof in Q [11 Marks]

(i)

1	(1)	$\forall x\,(x + \mathbf{0}) = x$	Ass
1	(2)	$((\mathbf{0} + x) + \mathbf{0}) = (\mathbf{0} + x)$	UE, 1
1	(3)	$(x + \mathbf{0}) = x$	UE, 1
	(4)	$(\mathbf{0} + (x + \mathbf{0})) = (\mathbf{0} + (x + \mathbf{0}))$	II
1	(5)	$(\mathbf{0} + x) = (\mathbf{0} + (x + \mathbf{0}))$	Sub, 3, 4
1	(6)	$((\mathbf{0} + x) + \mathbf{0}) = (\mathbf{0} + (x + \mathbf{0}))$	Sub, 2, 5
1	(7)	$\forall x\,(\mathbf{0} + x) + \mathbf{0}) = (\mathbf{0} + (x + \mathbf{0}))$	UI, 6

Hence as assumption 1 is axiom Q4 of Q, $\vdash_Q \forall x\,(\mathbf{0} + x) + \mathbf{0}) = (\mathbf{0} + (x + \mathbf{0}))$
Therefore the sentence is a theorem of Q.

(ii) In interpretation $\mathcal{N}^{**}$ let x be α then we need to find a y such that y '$+ \alpha = \alpha$ ' $= \alpha$.
However, no such y exists so the sentence is not true in $\mathcal{N}^{**}$
Therefore, as the axioms of Q are true in $\mathcal{N}^{**}$, by the Correctness Theorem the sentence is not a theorem of Q.

(iii) Note that $y = 0$ seems to make the sentence true for all x, so derive $(x + \mathbf{0'}) = x$ '

	(1)	$(x + \mathbf{0'}) = (x + \mathbf{0'})$	II
2	(2)	$\forall x\,\forall y\,(x + y\text{ '}) = (x + y\,)\text{'}$	Ass
2	(3)	$\forall y\,(x + y\text{ '}) = (x + y\,)\text{'}$	UE, 2
2	(4)	$(x + \mathbf{0}\text{ '}) = (x + \mathbf{0}\,)\text{'}$	UE, 3
5	(5)	$\forall x\,(x + \mathbf{0}) = x$	Ass
5	(6)	$(x + \mathbf{0}) = x$	UE, 5
2, 5	(7)	$(x + \mathbf{0'}) = x\text{ '}$	Sub, 4, 6
2, 5	(8)	$\forall x\,(x + \mathbf{0'}) = x\text{ '}$	UI, 7
2, 5	(9)	$\exists y\,\forall x\,(x + y\text{ '}) = x\text{ '}$	EI, 8

Hence as assumptions 2 and 5 are axioms Q4 & Q5 of Q, $\vdash_Q \exists y\,\forall x\,(x + y\text{ '}) = x\text{ '}$
Therefore the sentence is a theorem of Q.

Question 16 – Gödel's Incompleteness Theorem

(i) Theory T is not consistent if there is a sentence of T, Φ say, such that $\vdash_T \Phi$ and $\vdash_T \neg\,\Phi$

Suppose T has an interpretation but is not consistent.
Then by the Correctness Theorem both Φ and $\neg\,\Phi$ are true in this interpretation
However a sentence cannot be both true and false in the same interpretation and this contradicts our original supposition (See ML6 p29)
Hence if theory T has an interpretation then it is consistent. [3 Marks]

(ii)(a) $Q \cup \{\mathbf{0} = 1\}$ is not consistent, because $\neg\,\mathbf{0} = 1$ is true in Q:

1	(1)	$\forall x \neg\,\mathbf{0} = x\text{ '}$	
2	(2)	$\neg\,\mathbf{0} = \mathbf{0'}$	

(ii)(b) $Q \cup \{\exists x\; x = x\text{ '}\}$ is consistent
Assume that $Q \cup \{\exists x\; x = x\text{ '}\}$ is not consistent. Then $\neg\,\exists x\; x = x\text{ '}$ is a theorem of Q.
However, in $\mathcal{N}^{**}$, if we interpret x as α then $\alpha = \alpha$ ', hence $\neg\,\exists x\; x = x\text{ '}$ is not true in $\mathcal{N}^{**}$.
As the axioms of Q are true in $\mathcal{N}^{**}$, by the Correctness Theorem $\neg\,\exists x\; x = x\text{ '}$ is not a theorem of Q $\exists x\; x = x\text{ '}$ is a theorem of Q. This contradicts our assumption.
Therefore, because Q has an interpretation and is consistent by part (i), $Q \cup \{\exists x\; x = x\text{ '}\}$ is consistent. [6 Marks]

(iii) CA has an interpretation $\mathcal{N}$ hence is a consistent (by part (i)) and complete extension of Q. By Gödel's First Incompleteness Theorem CA is not recursively axiomatizable (or could appeal direct to Theorem 2.4). Hence, by definition, CA does not have a set of axioms whose Gödel numbers form a recursive set. [2 Marks]