2003 - Number Theory Solutions

[[Comments are written like this.
Please send me (dave@wildd.freeserve.co.uk) details of any errors you find or suggestions for improvements.]]

Question 1

(ii) (4 marks)

219 = 2 * 93 + 33
93 = 2 * 33 + 27
33 = 1 * 27 + 6
27 = 4 * 6 + 3
6 = 2 * 3 + 0

Therefore gcd(93, 219) = 3.

3 = 27 - 4 * 6 = 27 - 4 * (33 - 27) = 5 * 27 - 4 * 33
= 5 * (93 – 2 * 33) - 4 * 33 = 5 * 93 - 14 * 33
= 5 * 93 – 14 * (219 - 2 * 93) = 93 * 33 + 219 * (-14).

Therefore solutions of $93x + 219y = \gcd(93, 219)$ are of the form

$$x = 33 + \frac{219}{\gcd(93, 219)}t = 33 + 73t \text{ , and } y = -14 - \frac{93}{\gcd(93, 219)}t = -14 - 31t \text{ ,}$$

where t is an integer.

[[You could try the following method which uses negative remainders. I do not know whether it is acceptable to the examiners but it is valid and shorter in some cases.
*219 = 2 * 93 + 33*
*93 = 3 * 33 - 6*
*33 = 5 * 6 + 3*
*6 = 2 * 3 + 0*

Therefore gcd(93, 219) = 3.

*3 = 33 - 5 * 6 = 33 + 5 * (93 - 3 * 33) = 5 * 93 - 14 * 33*
*= 5 * 93 - 14 * (219 - 2 * 93) = 93 * 33 + 219 * (-14).*
]]

(ii) (3 marks)

Since n has remainder 3 when divided by 6 then n is odd.

As m = 5n + 4 then	gcd(m, n) = gcd(n, 4)	Euclidean Algorithm
	= 1	Since n is odd.

(iii) (4 marks)

For any positive integer n let P(n) be the proposition that $10^{n+1} - 4$ is divisible by 12.

P(1) is $10^2 - 4 = 96$ is divisible by 12. As P(1) is true then we have the basis for induction.

Assume P(k) is true for some positive integer k so $10^{k+1} - 4$ is divisible by 12.

$10^{(k+1)+1} - 4 = 10(10^{k+1} - 4) + 36.$

Since, by assumption, $12 \mid 10^{k+1} - 4$, and $12 \mid 36$ then $12 \mid 10^{(k+1)+1} - 4$.

Therefore if P(k) is true then P(k + 1) is true. This completes the induction step.

The result then follows from the Principle of Mathematical Induction.

Question 2 (11 marks)

Assume there are a finite number of primes of the form 3k + 2, where k is a non-negative integer. Let these primes be $p_1, p_2, \ldots, p_r$.

Let $N = (p_1 p_2 \ldots p_r)^2 + 1$.

If p is of the form 3k + 2 then $p \equiv 2 \pmod 3$ and $p^2 \equiv 1 \pmod 3$.
Therefore $N \equiv 1^r + 1 \equiv 2 \pmod 3$. Therefore N is of the form 3k + 2, where k is a non-negative integer.

As N is greater than any of the primes of the form 3k + 2 then it cannot be a prime.

As N is not divisible by 3 then all of its prime factors must be of the form 3k + 1 or 3k+2.

Dividing N by a prime of the form 3k + 2 leaves a remainder of 1 so none of the prime factors can be of this form. Therefore all of the prime factors must be of the form 3k + 1.

If all the prime factors of the form 3k + 1 equal 1 (mod 3) then multiplying them together results in a number equal to 1 (mod 3). Since $N \equiv 2 \pmod 3$ then all the factors cannot be of the form 3k + 1.

Since the assumption there are a finite number of primes of the form 3k + 2 has lead to a contradiction then the assumption is incorrect. Therefore there are an infinite number of primes of the form 3k + 2.

Question 3

(i) (2 marks)

Since $n \equiv 3 \pmod{10}$ then $n = 10k + 3$ for some integer k.
Therefore $6n + 1 = 6(10k + 3) + 1 = 60k + 19$.

(i)(a) $6n + 1 = 60k + 19 \equiv 7 \pmod{12}$

(i)(b) $6n + 1 = 60k + 19 \equiv 4 \pmod{15}$

(ii) (3 marks)

$r\,a \equiv r\,b \pmod{r\,n} \Leftrightarrow r\,a = r\,b + \alpha\, r\,n$, for some integer α
$\Leftrightarrow a = b + \alpha\, n$
$\Leftrightarrow a \equiv b \pmod{n}$, since $n > 0$.

[[I am not sure why they have added the condition n > 1 rather than n > 0. If n = 1 then we have $r\,a \equiv r\,b \pmod{r} \Leftrightarrow a \equiv b \pmod{1}$. Both sides are always true.]]

(iii) (6 marks)

Since $5x \equiv 7 \pmod{19}$ then $4 * 5x = 20x \equiv x \equiv 4 * 7 \equiv 9 \pmod{19}$

By the Chinese remainder theorem the congruences
$x \equiv 1 \pmod{2}$ $x \equiv 6 \pmod{7}$ $x \equiv 9 \pmod{19}$
have a unique solution modulo $2 * 7 * 19 = 266$.

Integers which satisfy the congruence $x \equiv 9 \pmod{19}$ are 9, 28, 47, 66, 85, 104, ...
Integers which also satisfy the congruence $x \equiv 6 \pmod{7}$ are 104, 237, ...
237 also satisfies the congruence $x \equiv 1 \pmod{2}$.

Hence 237 is the unique solution modulo 266.
Therefore the least positive integer which satisfies the congruences is 237.

Question 4

(i) (3 marks)

By FLT, $7^{16} \equiv 3^{16} \equiv 1 \pmod{17}$.

Therefore $7^{20} + 3^{20} \equiv 7^4 + 3^4 \equiv 49^2 + 81 \equiv (-2)^2 - 4 \equiv 0 \pmod{17}$.

Hence $7^{20} + 3^{20}$ is divisible by 17.

(ii) (3 marks)

If p is a prime less than 19 then p divides 18!. Therefore p does not divide 18! + 1 since there is a remainder of 1.

Since 19 is a prime then by Wilson's Theorem $(19 - 1)! = 18! \equiv -1 \pmod{19}$.
As $18! + 1 \equiv -1 + 1 \equiv 0 \pmod{19}$ then $18! + 1$ is divisible by 19.

Therefore 19 is the smallest prime divisor of $18! + 1$.

(iii) (5 marks)

(ii)(a)

As 23 is a prime, then by Theorem 2.2 the length of the cycle in decimal of 1/23 is equal to the order of 10 (modulo 23). Therefore $10^{22} \equiv 1 \pmod{23}$.

As $10^{22} \equiv (10^{11})^2 \equiv 1 \pmod{23}$. Therefore $10^{11} \equiv \pm 1 \pmod{23}$. If $10^{11} \equiv 1 \pmod{23}$ then the order of 10 would be 11. Since the order of 10 is 22 then we must have $10^{11} \equiv -1 \pmod{23}$.

(ii)(b)

As 10 has order 22 then it is a primitive root of of 23. Therefore 5/23 has the same cycle starting at a different point.

As 5 * 043 = 215 then the cycle starts at 21. Therefore the recurring decimal of 5/23 is
0.<217391304347826086956 5>.

Question 5

(i) (4 marks)

If p is a prime and a is a positive integer then $\phi(p^a)$ in the number of integers not exceeding p^a which are relatively prime to p^a.

The p, 2p, 3p, …, (p^{a-1}) p are the only integers not relatively prime to p^a. As there as p^{a-1} of these then $\phi(p^a) = p^a - p^{a-1} = p^a\left(1-\frac{1}{p}\right)$.

Any integer $n > 1$ can be written as a product of primes.

Let $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, where the primes $p_1, \ldots, p_r$ are distinct, and the a_i (i = 1 to r) are positive integers.

As ϕ is a multiplicative function then

$$\phi(n) = \phi\left(p_1^{a_1}\right)\phi\left(p_2^{a_2}\right)\ldots\phi\left(p_r^{a_r}\right) = p^{a_1}\left(1-\frac{1}{p_1}\right)p^{a_2}\left(1-\frac{1}{p_2}\right)\ldots p^{a_r}\left(1-\frac{1}{p_r}\right)$$

$$= n\prod_{p|n}\left(1-\frac{1}{p}\right).$$

(ii)(a) (2 marks)

If $n = p^2$, where p is a prime, then $\sigma(n) = 1 + p + p^2$.

So $2n + \sigma(n) = 1 + p + 3p^2$. As this is divisible by 3 then $1 + p \equiv 0 \pmod 3$.

Hence $p \equiv 2 \pmod 3$.

(ii)(b) (2 marks)

If $n = p^3$, where p is a prime, then $\sigma(n) = 1 + p + p^2 + p^3$.

So $2n + \sigma(n) = 1 + p + p^2 + 3p^3$. As this is divisible by 3 then $1 + p + p^2 \equiv 0 \pmod 3$.

Therefore $p \equiv 1 \pmod 3$ and hence $p \equiv 1 \pmod 6$ or $p \equiv 4 \pmod 6$.

If $p \equiv 4 \pmod 6$ then p is divisible by 2 and hence not prime.

Therefore $p \equiv 1 \pmod 6$.

[[I found this tricky. I originally thought there was a misprint on the exam paper.]]

(ii)(c) **(3 marks)**

We have to consider the prime p = 2 separately from all the others.

If p = 2 then $n = 2^4$ and $\sigma(n) = 2^5 - 1$. Therefore $2n + \sigma(n) = 32 + 31 = 63$. Therefore p = 2 is possible.

If $p \neq 2$ then $\sigma(n) = \sigma(2) * \sigma(p^3) = 3\ \sigma(p^3)$. Therefore if $2n + \sigma(n) = 4p^3 + 3\ \sigma(p^3)$ is divisible by 3 then $3 \mid 4p^3$. Therefore p = 3.

Therefore p = 2 or 3 are the only possible primes.

2002 Question 6

(i) (4 marks)

The quadratic congruence has solutions if $(-5)^2 - 4 * 2 * 4 = 25 - 32 = -7$ is a quadratic residue of 19.

$(-7/19) = (12/19)$	Th. 2.1(a), $-7 \equiv 12 \pmod{19}$
$= (2^2/19)(3/19)$	Th. 2.1(c).
$= 1 * (-1) = -1$	Th. 2.1(b), and Th. 4.4.

Therefore the congruence does not have solutions.

(ii) (4 marks)

$(86/127) = (2/127)\,(43/127)$	Th. 2.1(c).
$= 1 * \{-(127/43)\}$	Th. 3.2, LQR. $127 \equiv 43 \equiv 3 \pmod{4}$.
$= -(-2/43)$	Th. 2.1(a). $127 \equiv -2 \pmod{43}$.
$= -(-1/43)\,(2/43)$	Th. 2.1(c).
$= -\{-1 * (-1)\} = -1$	Th. 2.1(e). Th. 3.2.

(iii) (4 marks)

If $p = 2$ or $p = 3$ then $(6/p)$ is not defined (Definition 2.1)..

If $p \geq 5$ then

$(6/p) = (2/p)\,(3/p)$ Th. 2.1(c).

If $(6/p) = 1$ then either $(2/p) = (3/p) = 1$, or $(2/p) = (3/p) = -1$.

Case 1. $(2/p) = (3/p) = 1$

If $(2/p) = 1$ then $p \equiv \pm 1 \pmod{8}$. If $(3/p) \equiv 1$ then $p \equiv \pm 1 \pmod{12}$.
As lcm(8, 12) = 24 then we consider values of p modulo 24.
The values which satisfy both equations are 1 and 23 (mod 24).

Case 2. $(2/p) = (3/p) = -1$

If $(2/p) = -1$ then $p \equiv 3$ or 5 (mod 8). If $(3/p) \equiv 1$ then $p \equiv 5$ or 7(mod 12).
As lcm(8, 12) = 24 then we consider values of p modulo 24.
The values which satisfy both equations are 5 and 19 (mod 24).

Therefore $(6/p) = 1$ when $p \equiv \pm 1 \pmod{24}$ or $p \equiv \pm 5 \pmod{24}$.

Question 7

(i) (2 marks)

113 = 2 * 48 + 17
48 = 2 * 17 + 14
17 = 1 * 14 + 3
14 = 4 * 3 + 2
3 = 1 * 2 + 1
2 = 2 * 1 + 0

Therefore 113/48 = [2, 2, 1, 4, 1, 2] = [2, 2, 1, 4, 1, 1, 1].

(ii) (3 marks)

Using Theorem 1.2 and Corollary 1.2 we have

$p_1 = 1$; $q_1 = 1$;
$p_2 = 1 * 2 + 1 = 3$; $q_2 = 2$;
$p_3 = 3 * 3 + 1 = 10$; $q_3 = 3 * 2 + 1 = 7$;
$p_4 = 4 * 10 + 3 = 43$; $q_4 = 4 * 7 + 2 = 30$,

and so the first 4 convergents are $C_1 = 1/1 = 1$; $C_2 = 3/2$; $C_3 = 10/7$; and $C_4 = 43/30$.

$q_5 = 5 * 30 + 7 = 157$. Therefore, using Theorem 2.1, we have

$$| x - C_4 | < 1/ (q_4 q_5) = 1 / (30 * 157) = 1/ 4710.$$

(iii) (6 marks)

Corrections by Peter Monk (8/10/05)

Let y = [2, 2, x] where x = [<3>] = [3, x].

The convergents of [3, x] are 3/1, (3x + 1)/x = x.

So $x^2 - 3x - 1 = 0$ and the positive solution is $x = \frac{3+\sqrt{9+4}}{2} = \frac{3+\sqrt{13}}{2}$.

The convergents of [2, 2, x] are 2/1, 5/2, (5x + 2)/(2x + 1) = (10x + 4)/(4x + 2) = y.

[2, 2, <3>] = y

$$= \frac{19+5\sqrt{13}}{8+2\sqrt{13}} = \frac{\left(19+5\sqrt{13}\right)\left(8-2\sqrt{13}\right)}{64-52} = \frac{(152-130)+\sqrt{13}(40-38)}{12} = \frac{11+\sqrt{13}}{6}.$$

Question 8

(i) (7 marks)

(i)(a)

$490 = 2 * 5 * 7^2$. Since no factor of the form $4k + 3$ occurs to an odd power then 490 can be expressed as the sum of 2 squares (Th. 4.3) or 3 squares (add 0^2).

$492 = 4 * 123 = 2^2 * 3 * 41$. Since a factor of the form $4k + 3$ occurs to an odd power then 492 cannot be expressed as the sum of 2 squares (Th. 4.3).

Since 492 is not of the form $4^n (8m + 7)$ for some integers $m,n \geq 0$ then 492 can be expressed as a sum of 3 squares (Theorem 4.4).

$496 = 16 * 31 = 4^2 * 31 = 4^2 * (8 * 3 + 7)$. Therefore, by Theorem 4.4, 496 cannot be expressed as a sum of 3 squares. It follows that it cannot be expressed as a sum of 2 squares.

(i)(b)

$490 = 10 * 49 = (3^2 + 1^2) * 7^2 = 21^2 + 7^2$.

(ii) (4 marks)

Assume there is a solution $x = x_1$, $y = y_1$, and $z = z_1$.

Therefore $4x_1^3 - 2y_1^3 = z_1^3$. As the two of the terms in the equation are divisible by 2 then the 3rd term must also be divisible by 2. Since $2 \mid z_1^3$ then $2 \mid z_1$. Therefore $z_1 = 2 z_2$ where z_2 is an integer.

Hence $2x_1^3 - y_1^3 = 4 z_2^3$. Similarly $2 \mid y_1$ and so $y_1 = 2 y_2$ where y_2 is an integer.

Hence $x_1^3 - 4y_2^3 = 2 z_2^3$. Similarly $2 \mid x_1$ and so $x_1 = 2 x_2$ where x_2 is an integer.

Hence $4x_2^3 - 2y_2^3 = z_2^3$. As we have found another solution with $x_2 < x_1$, $y_2 < y_1$, and $z_2 < z_1$ then the descent step is complete. Hence the method of infinite descent shows can be no solutions in the positive integers.

END OF NUMBER THEORY SOLUTIONS