UBC MATH 312 - ASSIGNMENT 3

6 OCT 2012

(1)

$$44350 = 2 \cdot (20785) + (2780)$$
$$20785 = 7 \cdot (2780) + (1325)$$
$$2780 = 2 \cdot (1325) + (130)$$
$$1325 = 10 \cdot (130) + (25)$$
$$130 = 5 \cdot (25) + (5)$$
$$25 = 5 \cdot \underline{\underline{(5)}} + 0$$

$$\Longrightarrow \gcd(20785, 44350) = 5.$$

Total: 5 marks

---

(2)

$$100313 = 2 \cdot (34709) + (30895)$$
$$34709 = 1 \cdot (30895) + (3814)$$
$$30895 = 8 \cdot (3814) + (383)$$
$$3814 = 9 \cdot (383) + (367)$$
$$383 = 1 \cdot (367) + (16)$$
$$367 = 22 \cdot (16) + (15)$$
$$16 = 1 \cdot (15) + (1)$$
$$15 = 15 \cdot \underline{\underline{(1)}} + 0$$

$$\Longrightarrow \gcd(34709, 100313) = 1$$

5 marks

(2) (cont'd)

$$\gcd(34709, 100313) = 1$$

$$= 16 - 1(15) = 16 - 1(367 - 22(16))$$

$$= 23(16) - 1(367) = 23(383 - 1(367)) - 1(367)$$

$$= 23(383) - 24(367) = 23(383) - 24(3814 - 9(383))$$

$$= 239(383) - 24(3814) = 239(30895 - 8(3814)) - 24(3814)$$

5 marks

$$= 239(30895) - 1936(3814) = 239(30895) - 1936(34709 - 1(30895))$$

$$= 2175(30895) - 1936(34709) = 2175(100313 - 2(34709)) - 1936(34709)$$

$$= 2175(100313) - 6286(34709)$$

[Total: 10 marks]

(3) Noting that $(3k+2)$ and $(5k+3)$ are both positive integers, we use the Euclidean division algorithm to see that:

$$5k+3 = 1\cdot(3k+2) + (2k+1)$$

$$3k+2 = 1\cdot(2k+1) + (k+1)$$

$$2k+1 = 1\cdot(k+1) + (k)$$

$$k+1 = 1\cdot(k) + (1)$$

$$k = k\cdot\underline{\underline{(1)}} + 0$$

$$\Longrightarrow \gcd(5k+3, 3k+2) = 1$$

Total: 5 marks

(4) Starting with positive integers $x \geq y$, a player can subtract positive multiples of y from x until s/he gets an integer x_1 such that $0 \leqslant x_1 < y$. If $x_1 = 0$, then the game is over, with $\{0, y\}$ and $\gcd(x, y) = y$.

If $x_1 > 0$, then now the player subtracts positive multiples of x_1 from y until s/he gets an integer x_2 such that $0 \leqslant x_2 < x_1$. Again, if $x_2 = 0$, then the game is over, with $\{0, x_1\}$ and $\gcd(x, y) = \gcd(x_1, y) = x_1$.

If $x_2 > 0$, then the process continues.
But if we write out the steps as equations, we realise that the player is simply applying the Euclidean division algorithm to $\{x, y\}$:

$$x = t_1 y + x_1 \qquad 0 \leqslant x_1 < y$$
$$y = t_2 x_1 + x_2 \qquad 0 \leqslant x_2 < x_1$$
$$\vdots$$

and we know that the process ultimately terminates with $\{0, \gcd(x, y)\}$ Total: 10 marks
[where $\gcd(x,y)$ will be the last nonzero remainder].

(5) For $\alpha = a + b\sqrt{-5}$, $a, b \in \mathbb{Z}$, notice

$$N(\alpha) = \alpha\bar{\alpha} = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2.$$

Now for $\alpha = a+b\sqrt{-5}$, $a,b,c,d \in \mathbb{Z}$,

$\beta = c + d\sqrt{-5}$

$$N(\alpha)N(\beta) = (a^2+5b^2)(c^2+5d^2)$$
$$= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$$

$$N(\alpha\beta) = N((a+b\sqrt{-5})(c+d\sqrt{-5}))$$
$$= N((ac-5bd)+(ad+bc)\sqrt{-5})$$
$$= (ac-5bd)^2 + 5(ad+bc)^2$$
$$= a^2c^2 \cancel{-10abcd} + 25b^2d^2 + 5a^2d^2 \cancel{+10abcd} + 5b^2c^2$$
$$= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$$
$$= N(\alpha)\cdot N(\beta)$$

Total: ~~8~~ marks 10

(6) If we write 2 as a product of two numbers:

$$2 = uv, \quad u, v \in S,$$

then from Question 5, we see that

$$N(2) = N(uv) = N(u)N(v)$$

Now $N(2) = N(2+0\sqrt{-5}) = 2^2+5(0)^2 = 4.$

So as $4 = N(u)N(v)$ (and u, v, cannot be 0),

we have 3 cases: i) $N(u) = N(v) = 2$

ii) $N(u) = 1$, $N(v) = 4$

iii) $N(u) = 4$, $N(v) = 1$.

(6) (cont'd)

<u>Case 1</u> $N(u) = N(v) = 2$.

If we write $u = a + b\sqrt{-5}$, this means that

$$N(u) = a^2 + 5b^2 = 2.$$

As $a, b \in \mathbb{Z}$, b must be 0. But $a^2 = 2$ does not have integer solutions either. ※ Impossible.

<u>Case 2</u> $N(u) = 1$, $N(v) = 4$.

$$N(u) = a^2 + 5b^2 = 1 \Rightarrow b = 0, \ a = \pm 1.$$

So $u = \pm 1$.

<u>Case 3</u> $N(u) = 4$, $N(u) = 1$

Same reasoning as Case 2. $v = \pm 1$.

In summary, 2 cannot be written as a product uv without either u or v being ± 1.

$\Rightarrow$ 2 is a prime number in S. 10 marks

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

To show that these 2 factorisations of 21 in S are distinct prime factorisations, we need to check that the numbers $3, 7, 1 + 2\sqrt{-5}$ and $1 - 2\sqrt{-5}$ are primes in S.

The process is identical to that above, where we show that 2 is a prime.

⑥ (cont'd)

I will do the working for $1+2\sqrt{-5}$.

$N(1+2\sqrt{-5}) = 1^2 + 5(2)^2 = 21$.

So if $\exists\ u, v \in S$ s.t. $uv = 1+2\sqrt{-5}$, then

$$N(u)N(v) = N(uv) = N(1+2\sqrt{-5}) = 21.$$

If either $N(u) = 1$ or $N(v) = 1$, then either u or v would be ± 1.

So we are left with the case that $N(u) = 3$ and $N(v) = 7$ [or $N(u) = 7$ and $N(u) = 3$].

But this is impossible, because there are no integers a or b s.t. $a + 5b^2 = 3$ or 7.

$\Longrightarrow$ $1+2\sqrt{-5}$ cannot be written as a product uv without either u or v being ± 1.

$\Longrightarrow$ $1+2\sqrt{-5}$ is a prime number in S. 10 marks

Do similarly for $1-2\sqrt{-5}$, 3 and 7.

Finally, we note that as $N(3) = 9$, $N(7) = 49$

but $N(1+2\sqrt{-5}) = N(1-2\sqrt{-5}) = 21$,

3 and 7 are not simply $1 \pm 2\sqrt{-5}$ multiplied by ± 1. [Total: 20 marks]

$\Longrightarrow$ 21 indeed has 2 distinct prime factorisations in S

[Remark: We say that S is NOT a unique factorisation domain]

(7) By the Fundamental Theorem of Arithmetic, we have unique prime factorisations (up to re-ordering)

$$343 = 7^3$$
$$999 = 3^3 \times 37$$

As the two numbers have no common prime divisors, $\gcd(343, 999) = \underline{1}$ and $\operatorname{lcm}(343, 999)$
$$= 3^3 \times 7^3 \times 37 = \underline{342657}$$

If $a = 1$, then $a^n = 1$ for every $n \in \mathbb{N}$, and
$$(a^n, b^n) = (1, b^n) = 1.$$
A similar reasoning applies if $b = 1$.

Now suppose $a, b \geq 2$. Then by the fundamental theorem of arithmetic, we can write out their unique prime factorisations:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} \quad \text{and} \quad b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$$

where p_i, q_j are primes, $\alpha_i, \beta_j \in \mathbb{N}$.

Now as $(a, b) = 1$, $p_i \neq q_j$ for every $\begin{matrix} 1 \leq i \leq \ell \\ 1 \leq j \leq m \end{matrix}$.

So then for any $n \in \mathbb{N}$,

$$a^n = p_1^{n\alpha_1} p_2^{n\alpha_2} \cdots p_\ell^{n\alpha_\ell} \quad \text{and} \quad b^n = q_1^{n\beta_1} q_2^{n\beta_2} \cdots q_m^{n\beta_m}$$

But again, $p_i \neq q_j$ for every $\begin{matrix} 1 \leq i \leq \ell \\ 1 \leq j \leq m. \end{matrix}$

So a^n & b^n share no common prime divisors.

$\Longrightarrow (a^n, b^n) = 1.$

Total: 10 marks

(8) Suppose $\sqrt{2}+\sqrt{3}$ is rational, i.e. $\sqrt{2}+\sqrt{3} = \frac{a}{b}$ for some nonzero $a, b \in \mathbb{Z}$. WLOG, we can assume $a, b \geq 1$ and $\gcd(a, b) = 1$.

Squaring both sides of $\sqrt{2}+\sqrt{3} = \frac{a}{b}$ gives

$$2 + 2\sqrt{2}\sqrt{3} + 3 = \frac{a^2}{b^2}$$

$$2\sqrt{6} = \frac{a^2}{b^2} - 5$$

$$2b^2\sqrt{6} = a^2 - 5b^2$$

Squaring again, $24b^4 = a^4 - 10a^2b^2 + 25b^4$

$$0 = a^4 - 10a^2b^2 + b^4$$

$$8a^2b^2 = a^4 - 2a^2b^2 + b^4$$

$$8a^2b^2 = (a^2 - b^2)^2$$

Noting that $a \neq 0 \neq b$, we see that the LHS is not zero, so the RHS cannot be zero.
But then the RHS is a perfect square, whilst the LHS is not (8 is not the square of an integer). $\times\!\!\!\times$.

$\Rightarrow \sqrt{2}+\sqrt{3}$ is irrational.

Total: 10 marks

(9) Suppose $\log_2 3$ is rational, i.e. $\log_2 3 = \frac{a}{b}$ for some nonzero $a, b \in \mathbb{Z}$. As $3 > 2 > 0$, $\log_2 3$ is positive. So we can assume $a, b \geq 1$ and $\gcd(a, b) = 1$.

$$\log_2 3 = \frac{a}{b} \implies 2^{a/b} = 3$$

$$\sqrt[b]{2^a} = 3$$

$$2^a = 3^b$$

As $a, b \geq 1$, LHS is even; RHS is odd. $\times\!\!\!\times$.

$\Longrightarrow \log_2 3$ is irrational.

Total 10 marks

(10) For a, b positive integers, suppose
$$\gcd(a,b) = d = \operatorname{lcm}[a,b].$$

As d is the gcd of a & b, it is a common <u>divisor</u> of a & b, i.e. $\begin{cases} d \mid a \\ d \mid b. \end{cases}$

As d is the lcm of a & b, it is a common <u>multiple</u> of a & b, i.e. $\begin{cases} a \mid d \\ b \mid d. \end{cases}$

This means that $\begin{cases} d = |a| \\ d = |b| \end{cases}$

But as a, b + d are all positive, $\begin{cases} d = a \\ d = b \end{cases}$ Total: 10 marks

$\Longrightarrow a = b.$