ELEMENTARY NUMBER THEORY II, EXAMINATION I SOLUTIONS

DAVID PIERCE

Solution 1. (i) Apply the Euclidean algorithm:

$$\frac{\alpha}{\beta}=\frac{40+5\mathrm{i}}{39\mathrm{i}}=\frac{5-40\mathrm{i}}{39}=-\mathrm{i}+\frac{5-\mathrm{i}}{39}, \qquad 40+5\mathrm{i}=(39\mathrm{i})(-\mathrm{i})+1+5\mathrm{i};$$
$$\frac{39\mathrm{i}}{1+5\mathrm{i}}=\frac{195+39\mathrm{i}}{26}=7+\mathrm{i}+\frac{1+\mathrm{i}}{2}, \qquad 39\mathrm{i}=(1+5\mathrm{i})(7+\mathrm{i})-2+3\mathrm{i};$$
$$\frac{1+5\mathrm{i}}{-2+3\mathrm{i}}=\frac{(1+5\mathrm{i})(-2-3\mathrm{i})}{13}=1-\mathrm{i}, \qquad 1+5\mathrm{i}=(-2+3\mathrm{i})(1-\mathrm{i}).$$

Therefore $-2+3\mathrm{i}$ is a greatest common divisor of α and β.

(ii) By the computations above,

$$\alpha=\beta\cdot(-\mathrm{i})+1+5\mathrm{i}, \qquad 1+5\mathrm{i}=\alpha+\beta\cdot\mathrm{i};$$
$$\beta=(\alpha+\beta\cdot\mathrm{i})(7+\mathrm{i})-2+3\mathrm{i}, \qquad -2+3\mathrm{i}=\alpha\cdot(-7-\mathrm{i})+\beta\cdot(2-7\mathrm{i}).$$

Remark. In (i), each step of the computation should lower the norm of the remainder. Indeed, $\mathrm{N}(39\mathrm{i})>\mathrm{N}(1+5\mathrm{i})>\mathrm{N}(-2+3\mathrm{i})$. But the way to achieve this is not unique. For example, from the second line, the computation could have been

$$\frac{39\mathrm{i}}{1+5\mathrm{i}}=\frac{195+39\mathrm{i}}{26}=8+\mathrm{i}+\frac{-1+\mathrm{i}}{2}, \qquad 39\mathrm{i}=(1+5\mathrm{i})(8+\mathrm{i})-3-2\mathrm{i};$$
$$\frac{1+5\mathrm{i}}{-3-2\mathrm{i}}=\frac{(1+5\mathrm{i})(-3+2\mathrm{i})}{13}=-1-\mathrm{i}, \qquad 1+5\mathrm{i}=(-3-2\mathrm{i})(-1-\mathrm{i}).$$

So $-3-2\mathrm{i}$ could also be found as a greatest common divisor of α and β. (Also $2-3\mathrm{i}$ and $3+2\mathrm{i}$ are gcd's.)

In an alternative approach to (i), one might observe that

$$\alpha=5\cdot(8+\mathrm{i})=(2+\mathrm{i})(2-\mathrm{i})(8+\mathrm{i}), \qquad \mathrm{N}(\alpha)=5^2\cdot 65=5^3\cdot 13;$$
$$\beta=3\cdot 13\mathrm{i}, \qquad \mathrm{N}(\beta)=3^2\cdot 13^2.$$

The factors $2\pm\mathrm{i}$ of α are prime, and their norm is 5, and $5\nmid\mathrm{N}(\beta)$. Also, 3 is prime, and $3\nmid\mathrm{N}(\alpha)$. One can therefore take γ as a gcd of $8+\mathrm{i}$ and $13\mathrm{i}$. To find this, one could apply the Euclidean algorithm to the latter pair. Alternatively, since $\gcd(\mathrm{N}(\alpha),\mathrm{N}(\beta))=13$, we must have $\mathrm{N}(\gamma)\mid 13$. Since 13 has the prime factorization $(3+2\mathrm{i})(3-2\mathrm{i})$, each factor having norm 13, one could test whether one of these factors divides α and β: if one does, then it is γ; if neither does, then α and β are co-prime. However, these alternative approaches are not much help in solving (ii).

Once one *does* have an answer to (ii), it is easy to check.

Date: March 25, 2008.

Solution 2. (i) Let $x = \sqrt{3/2} = \sqrt{6}/2$. Applying our algorithm to x, we have

$$\begin{array}{lll} & a_0 = [x] = 1, & \xi_0 = \dfrac{\sqrt{6}}{2} - 1 = \dfrac{\sqrt{6}-2}{2}; \\ \dfrac{2}{\sqrt{6}-2} = \sqrt{6}+2, & a_1 = 4, & \xi_2 = \sqrt{6}-2; \\ \dfrac{1}{\sqrt{6}-2} = \dfrac{\sqrt{6}+2}{2}, & a_2 = 2, & \xi_2 = \dfrac{\sqrt{6}-2}{2} = \xi_0; \end{array}$$

therefore $\sqrt{3/2} = [1; \overline{4,2}]$.

(ii) The equation $(*)$ can be written as $x^2 - (3/2)y^2 = 1$. Assuming it is like a Pell equation, we expect solutions to $(*)$ to come from convergents of x. These are:

$$\frac{1}{1}, \quad \frac{5}{4}, \quad \frac{11}{9}, \quad \frac{49}{40}, \quad \frac{109}{89}, \quad \frac{485}{396}, \quad \dots$$

In particular, we expect the solutions to come from $[1;4]$, $[1;4,2,4]$, $[1;4,2,4,2]$, and so on. Indeed, $(5,4)$ is a solution.

(iii) Also $(49,40)$.

(iv) Also $(485,396)$.

Remark. Since we have not *yet* proved that our procedure for solving a Pell equation works in general; and since $(*)$ is not literally a Pell equation anyway, one should check one's answers to (ii), (iii), and (iv) here.

Solution 3. (i) The solutions are $\left(\dfrac{1-3t^2}{1+3t^2}, \dfrac{2t}{1+3t^2}\right)$, where $t \in \mathbb{Q}$; and $(-1,0)$.

(ii) Letting $t = 2$ in the given formula yields $(-3+4\mathrm{i})/5$, not a Gaussian integer.

(iii) Letting $t = 2$ in (i) yields $(-11+4\mathrm{i}\sqrt{3})/13$, which is not in $\mathbb{Z}[(1+\mathrm{i}\sqrt{3})/2]$.

Remark. One may solve (i) just by thinking about why the given point is on the circle. Alternatively, one may just use the same method for deriving it: find the other intersection, besides $(-1,0)$ of the line $y = tx + t$ and the ellipse $x^2 + 3y^2 = 1$.

Solution 4. (i) $221 = 13 \cdot 17$. In the Gaussian integers, $\mathrm{N}(\xi) = 13$ is solved by $3 \pm 2\mathrm{i}$ and their associates; $\mathrm{N}(\eta) = 17$, by $4 \pm \mathrm{i}$ and their associates. We have

$$(3 \pm 2\mathrm{i})(4 \pm \mathrm{i}) = 10 \pm 11\mathrm{i}, \qquad (3 \pm 2\mathrm{i})(4 \mp \mathrm{i}) = 14 \pm 5\mathrm{i}.$$

Hence the 16 desired solutions are

$$(10, \pm 11), (-10, \mp 11), (\mp 11, 10), (\pm 11, -10), (14, \pm 5), (-14, \mp 5), (\mp 5, 14), (\pm 5, -14).$$

(ii) $27 - 57\mathrm{i} = 3 \cdot (9 - 19\mathrm{i})$, where 3 is prime; and $\mathrm{N}(9 - 19\mathrm{i}) = 81 + 361 = 442 = 2 \cdot 221$. But 2 has associated prime factors $1 \pm \mathrm{i}$, and

$$\frac{9-19\mathrm{i}}{1+\mathrm{i}} = \frac{(9-19\mathrm{i})(1-\mathrm{i})}{2} = -5 - 14\mathrm{i} = -\mathrm{i} \cdot (14 - 5\mathrm{i}) = -\mathrm{i} \cdot (3 - 2\mathrm{i})(4 + \mathrm{i})$$

by (i). Since $(1 + \mathrm{i}) \cdot (-\mathrm{i}) = 1 - \mathrm{i}$, we conclude

$$27 - 57\mathrm{i} = 3 \cdot (1 - \mathrm{i})(3 - 2\mathrm{i})(4 + \mathrm{i}).$$

Mathematics Dept, Middle East Technical University, Ankara 06531, Turkey
E-mail address: dpierce@metu.edu.tr
URL: http://www.math.metu.edu.tr/~dpierce/