ELEMENTARY NUMBER THEORY II, FINAL EXAMINATION SOLUTIONS

Problem 1. *Find the positive rational-integer solutions to $x^2 - 22y^2 = 3$.*

Solution. First find the expansion of $\sqrt{22}$:

$$\begin{aligned}
& & a_0 &= 4; & \xi_0 &= \sqrt{22}-4;\\
\frac{1}{\sqrt{22}-4} &= \frac{\sqrt{22}+4}{6}, & a_1 &= 1, & \xi_1 &= \frac{\sqrt{22}-2}{6};\\
\frac{6}{\sqrt{22}-2} &= \frac{\sqrt{22}+2}{3}, & a_2 &= 2, & \xi_2 &= \frac{\sqrt{22}-4}{3};\\
\frac{3}{\sqrt{22}-4} &= \frac{\sqrt{22}+4}{2}, & a_3 &= 4, & \xi_3 &= \frac{\sqrt{22}-4}{2};\\
\frac{2}{\sqrt{22}-4} &= \frac{\sqrt{22}+4}{3}, & a_4 &= 2, & \xi_4 &= \frac{\sqrt{22}-2}{3};\\
\frac{3}{\sqrt{22}-2} &= \frac{\sqrt{22}+2}{6}, & a_5 &= 1, & \xi_5 &= \frac{\sqrt{22}-4}{6};\\
\frac{6}{\sqrt{22}-4} &= \sqrt{22}+4, & a_6 &= 8, & \xi_6 &= \xi_0.
\end{aligned}$$

So $\sqrt{22} = [4; \overline{1,2,4,2,1,8}]$. If 3 is the denominator of ξ_{n+1}, then

$$p_n{}^2 - 22q_n{}^2 = (-1)^{n+1}3.$$

Hence the positive solutions of $x^2-22y^2 = 3$ that come from convergents are (p_{6k+1}, q_{6k+1}) and (p_{6k+3}, q_{6k+3}). To verify that these are all of the (positive) solutions, we assume that (a, b) is a solution and show

$$\left|\frac{a}{b} - \sqrt{22}\right| < \frac{1}{2b^2},$$

that is,

$$|a - b\sqrt{22}| < \frac{1}{2b},$$

that is,

$$3 < \frac{a+b\sqrt{22}}{2b} = \frac{1}{2}\left(\frac{a}{b} + \sqrt{22}\right).$$

Since $a/b > \sqrt{22} > 3$, we do have this. To be more explicit about the solutions, we compute the first convergents:

$$\frac{4}{1},\quad \frac{5}{1},\quad \frac{14}{3},\quad \frac{61}{13},\quad \frac{136}{29},\quad \frac{197}{42}.$$

So $(5, 1)$ and $(61, 13)$ are solutions; the others are (a, b), where

$$a + b\sqrt{22} = (5+\sqrt{22})(197+42\sqrt{22})^k \text{ or } (61+13\sqrt{22})(197+42\sqrt{22})^k.$$

Date: June 2, 2008; revised, June 12, 2008.

Remark. In an alternative approach, we can rewrite the equation to be solved as

$$\mathrm{N}(x + y\sqrt{22}) = 3,$$

where the norm is taken in $\mathbb{Q}(\sqrt{22})$. Let K be this field, and $\omega = \sqrt{22}$. We want to solve $\mathrm{N}(\xi) = 3$, where $\xi \in \langle 1, \omega\rangle$, which is $\mathfrak{O}_K$. We first find the fundamental unit ε of $\mathfrak{O}_K$. Then there will be a certain finite set of solutions α of $\mathrm{N}(\xi) = 3$ such that every solution is uniquely of the form $\pm\alpha \cdot \varepsilon^n$.

From the work in the solution above, $\varepsilon = 197 + 42\sqrt{22}$. (We have $\mathrm{N}(197 + 42\sqrt{22}) = 1$ and not -1 because the period of $\sqrt{22}$ has even length. It would take a while to find ε by testing all $a + b\sqrt{22}$ such that a is the closest integer to $b\sqrt{22}$; however one student did try this approach.)

Now the α will satisfy $1 \leqslant \xi < \varepsilon$. One of these α, namely $5+\sqrt{22}$, can be found by trial; but perhaps not the other one, $61+13\sqrt{22}$. Finding it from the convergents of $\sqrt{22}$ seems most efficient. Alternatively, one might find it within the appropriate parallelogram, by the method worked out in class (and in the notes). We are looking for integers x and y such that

$$x^2 - 22y^2 = 3, \qquad 1 \leqslant x + y\sqrt{22} < 197 + 42\sqrt{22}.$$

The two inequalities determine two sides of the parallelogram, given by $1 = x+y\sqrt{22}$ and $x+y\sqrt{22} = 197+42\sqrt{22}$. The original equation defines a hyperbola with asymptotes given together by $x^2 - 22y^2 = 0$, or individually by $x \pm y\sqrt{22} = 0$; the equation $x - y\sqrt{22} = 0$ defines a third side of the parallelogram. Using $1 = x + y\sqrt{22}$ in the equation of the hyperbola gives the fourth side, $x - y\sqrt{22} = 3$. Written in slope-intercept form, the sides are:

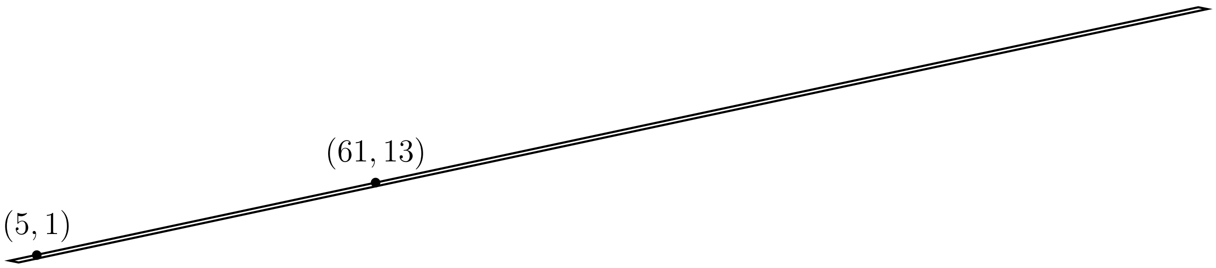
$$y = \frac{x}{\sqrt{22}} \qquad\qquad y = -\frac{x}{\sqrt{22}} + \frac{197 + 42\sqrt{22}}{\sqrt{22}},$$

$$y = \frac{x}{\sqrt{22}} - \frac{3}{\sqrt{22}}, \qquad\qquad y = -\frac{x}{\sqrt{22}} + \frac{1}{\sqrt{22}}.$$

The vertices then are:

$$\Bigl(\frac{197 + 42\sqrt{22}}{2}, \frac{197 + 42\sqrt{22}}{2\sqrt{22}}\Bigr),\ \Bigl(\frac{1}{2}, \frac{1}{2\sqrt{22}}\Bigr),\ \Bigl(100 + 21\sqrt{22}, \frac{97 + 21\sqrt{22}}{\sqrt{22}}\Bigr),\ \Bigl(2, \frac{-1}{\sqrt{22}}\Bigr).$$

These are approximately $(197, 42.0)$, $(0.5, 0.1)$, $(198.5, 41.7)$, $(2, -0.2)$. In particular, the parallelogram contains at least 41 integer points, rather a lot to find and test by hand.



Problem 2. *The curve E defined by the cubic equation*

$$y^2 = x^3 - 2$$

has the rational point $(3, 5)$. This problem is about obtaining other rational points. (a) *Find an equation for the tangent line to E at $(3, 5)$. (You may use implicit differentiation.)* (b) *This tangent line meets E twice at $(3, 5)$. Find the third point of intersection.*

(You may use that the sum of the roots of $x^3 - Ax^2 + Bx - C$ is A.) (c) *Now generalize: Suppose (a, b) is on E, and let λ be the slope of the tangent line to E at (a, b). Find λ (assuming $b \neq 0$).* (d) *Derive the conclusion that this tangent line meets E also at*

$$\Bigl(\frac{a^4 + 16a}{4b^2}, \frac{-a^6 + 40a^3 + 32}{8b^3}\Bigr).$$

Solution. (a) $2yy' = 3x^2$, $y' = 3x^2/2y = 27/10$; the tangent line is given by

$$y = \frac{27}{10}(x - 3) + 5 = \frac{27}{10}x - \frac{31}{10}.$$

(b) Substitute:

$$\begin{aligned}\Bigl(\frac{27}{10}x - \frac{31}{10}\Bigr)^2 &= x^3 - 2,\\ 0 &= x^3 - ax^2 + bx - c,\end{aligned}$$

where $a = (27/10)^2$; we compute

$$\begin{aligned}\Bigl(\frac{27}{10}\Bigr)^2 - 2 \cdot 3 = \frac{729}{100} - 6 = \frac{129}{100};\\ \frac{27}{10} \cdot \frac{129}{100} - \frac{31}{10} = \frac{3483}{1000} - \frac{31}{10} = \frac{383}{1000};\end{aligned}$$

the point is

$$\Bigl(\frac{129}{100}, \frac{383}{1000}\Bigr).$$

(c) As in (a), $\lambda = 3a^2/2b$.

(d) The tangent line is $y = \lambda(x - a) + b$, so $(\lambda x - a\lambda + b)^2 = x^3 - 2$, the sum of the roots is λ^2, the third root is $\lambda^2 - 2a$, that is,

$$\frac{9a^4}{4b^2} - 2a = \frac{9a^4 - 8a(a^3 - 2)}{4b^2} = \frac{a^4 + 16a}{4b^2}.$$

For the corresponding y-coordinate, use the tangent line:

$$\begin{aligned}\frac{3a^2}{2b}\Bigl(\frac{a^4 + 16a}{4b^2} - a\Bigr) + b &= \frac{3a^6 + 48a^3}{8b^3} - \frac{3a^3}{2b} + b\\ &= \frac{3a^6 + 48a^3 - 12a^3b^2 + 8b^4}{8b^3}\\ &= \frac{3a^6 + 48a^3 - 12a^3(a^3 - 2) + 8(a^3 - 2)^2}{8b^3}\\ &= \frac{3a^6 + 48a^3 - 12a^6 + 24a^3 + 8a^6 - 32a^2 + 32}{8b^3}\\ &= \frac{-a^6 + 40a^3 + 32}{8b^3}.\end{aligned}$$

Remark. Problem 1, and much of our class, concerned integer points on a curve defined by a quadratic equation. For 'most' curves given by equations of higher degree, there are only finitely many integer points; but for cubic equations, there may be infinitely many *rational* points, as Problem 2 suggests.

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