Introduction to mathematical cryptography
Homework problems
Week 11

21. Consider the real projective plane

$$\mathbf{P}^2(\mathbf{R}) = \left(\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : x, y, z \in \mathbf{R} \right\} \setminus \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} \right) / \sim,$$

where $\sim$ is the equivalence relation identifying constant multiples (this is just the space we covered in class). In notation, we write $\left[\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right]$ for points of the projective plane, note that for example,

$$\begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix} = \begin{bmatrix} -4 \\ -6 \\ -2 \end{bmatrix}$$

(because of the identified constant multiples).

Consider then the projective lines determined by the equations

$$L_1 = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbf{P}^2(\mathbf{R}) : x + y = 3z \right\};$$

$$L_2 = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbf{P}^2(\mathbf{R}) : x + y = 6z \right\}.$$

(Observe that these defining equations are independent of the chosen representatives.) Compute the intersection point of L_1 and L_2.

22. Let $A, B \in \mathbf{R}$ be fixed numbers. Prove that the equation $x^3 + Ax + B = 0$ has no multiple roots if and only if $4A^3 + 27B^2 \neq 0$.

Explanation: prove that if $A, B \in \mathbf{R}$ satisfy $4A^3 + 27B^2 = 0$, then there exist (not necessarily distinct) $r, s \in \mathbf{R}$ such that $x^3 + Ax + B = (x - r)^2(x - s)$; while on the other hand, if $4A^3 + 27B^2 \neq 0$, then $x^3 + Ax + B$ cannot be written in the form $(x-r)^2(x-s)$ with (not necessarily distinct) $r, s \in \mathbf{R}$.

Example: $A = -3$, $B = 2$. Then $x^3 + Ax + B = x^3 - 3x + 2$, and you may easily check that this is the same as $(x-1)^2(x+2)$ (that is, $r = 1, s = -2$ in the notation of the explanation). Also, $4A^3 + 27B^2 = 4\cdot(-3)^3 + 27\cdot 2^2 = -108 + 108 = 0$.

Example: $A = -1$, $B = 0$. Then $x^3 + Ax + B = x^3 - x$, and you may easily check that this is the same as $(x-1)x(x+1)$. Also, $4A^3 + 27B^2 = 4 \cdot (-1)^3 + 27 \cdot 0^2 = -4 \neq 0$.

Note: Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.