Cryptographic Protocol Exercise 3

Deadline: 30.12.2010

1 Recover a shared secret

A dealer used Shamir's secret sharing scheme (SSSS) to share a secret v among ten parties, such that any four of them could recover it. The secret value, as well as the shares of parties belong to the field $\mathbb{Z}_{911}$. At the recovery time, the parties reported the following shares:

p_1	p_2	p_3	p_4	p_5
389	834	291	527	329

p_6	p_7	p_8	p_9	p_{10}
404	168	779	621	144

The value reported by p_i is the value of the sharing polynomial at the point i. It is known that up to three parties may have lied when reporting the value of their share. Find v and which parties are corrupted.