which means that

$$A' = (A - \alpha I)(A - \beta I) = \frac{1}{n(k-\alpha)(k-\beta)} J.$$

In particular then A^2 is a linear combination of A, I and J, hence of A, I and $J - I - A$. This means that A^2 has the same entry in every position on the diagonal, the same entry in all positions corresponding to edges of G, and the same entry in all positions corresponding to non-edges of G. Since A is a $(0,1)$-matrix, these entries are all non-negative integers and it follows that G is strongly regular. □

4.3 Two classes of strongly regular graphs

Let G is a strongly regular graph with parameters (n, k, λ, μ), and assume that $k \leqslant \frac{n-1}{2}$; there is no real loss of generality in this assumption since either G or its complement has this property. We have seen that the eigenvalues of G occur with multiplicities

$$1, m_1 = \frac{1}{2}\left[(n-1) - \frac{2k + (n-1)(\lambda-\mu)}{\sqrt{\Delta}}\right],\ m_2 = \frac{1}{2}\left[(n-1) + \frac{2k + (n-1)(\lambda-\mu)}{\sqrt{\Delta}}\right].$$

The condition that m_1 and m_2 are integers means that one of the following two cases occurs:

1. $2k + (n-1)(\lambda-\mu) \neq 0$ and Δ is an integer square; $m_1 \neq m_2$ in this case.
2. $2k+(n-1)(\lambda-\mu) \neq 0$, and $m_1 = m_2 = \frac{1}{2}(n-1)$ (this is referred to as the "half case" for this reason). In this case n must be odd obviously. Furthermore, since $2k \leqslant n-1$, the condition that

   $$2k = (n-1)(\mu-\lambda)$$

   can be satisfied only if $2k = n-1$ and $\mu - \lambda = 1$, so $\lambda = \mu - 1$ Moreover we know from Theorem **??** that $k(k-\lambda-1) = (n-1-k)\mu$. Since $n-1-k = k$ and $\lambda + 1 = \mu$, this means that $k - \mu = \mu$ or $k = 2\mu$. Finally $n = 2k+1 = 4\mu+1$ and G has parameters

   $$(4\mu+1, 2\mu, \mu-1, \mu)$$

   for some positive integer μ. A strongly regular graph of this type is called a *conference graph*.

We look briefly at some examples of both types. The Kneser graph $Kn(n,2)$ (the complement of the line graph of K_n) is an example of the first type. In the case $n = 5$, this is the Petersen graph which has parameters $(10,3,0,1)$, with

$$\Delta = 1^2 + 4(3-1) = 9, \theta_1 = \frac{-1+3}{2} = 1, \theta_2 = \frac{-1-3}{2} = -2.$$

$$m_1 = \frac{1}{2}\left[9 - \frac{6+9(-1)}{3}\right] = 5,\ m_2 = \frac{1}{2}\left[9 + \frac{6+9(-1)}{3}\right] = 4.$$

In general the Kneser graph $Kn(n,2)$ has parameters

$$\left(\binom{n}{2}, \binom{n-2}{2}, \binom{n-4}{2}, \binom{n-3}{2}\right).$$

Recall that for any integer m, $\binom{m+1}{2} - \binom{m}{2} = m$ (easily verified by a calculation or by a counting exercise). Thus $\lambda - \mu = 4 - n$ for the $Kn(n,2)$, and $k - \mu = n - 3$. Then

$$\Delta = (4-n)^2 + 4(n-3) = n^2 - 8n + 16 + 4n - 12 = n^2 - 4n + 4 = (n-2)^2,$$

so Δ is a square. The eigenvalues are

$$\theta_1 = \frac{(4-n) + (n-2)}{2} = 1,\ \ \theta_2 = \frac{(4-n) - (n-2)}{2} = 3 - n.$$

The multiplicities are given by

$$\begin{aligned} m_1 + m_2 &= \binom{n}{2} - 1 \\ m_1(1) + m_2(3-n) &= -\binom{n-2}{2} \\ \implies m_2(n-2) &= \binom{n}{2} + \binom{n-2}{2} - 1 \\ &= \frac{n(n-1) + (n-2)(n-3) - 2}{2} \\ &= \frac{2n^2 - 6n + 4}{2} \\ &= n^2 - 3n + 2 \\ &= (n-2)(n-1) \implies m_2 = n-1. \end{aligned}$$

Then $m_1 = \binom{n}{2} - n$.

Families of examples of the second type are a bit harder to construct, although one example is the cycle C_5, which has parameters $(5, 2, 0, 1)$. In this graph $\Delta = 1 + 4(2-1) = 5$ is not a square, and

$$2k + (n-1)(\lambda - \mu) = 4 + 4(-1) = 0.$$

The eigenvalues are $\frac{-1 \pm \sqrt{5}}{2}$, which are irrational, both appearing with multiplicity 2.

The graph C_5 does belong to an infinite family of strongly regular graphs known as the *Paley* graphs, which are constructed from finite fields. A Paley graph on p vertices exists for every p with the property that p is a power of some prime and $p \equiv 1 \mod 4$. We will only consider the case where p is prime, examples of primes of the form $4t+1$ are $5, 13, 17$ etc.

For such a prime p, let $\mathbb{F}_p$ denote the finite field $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p. The elements of $\mathbb{F}_p$ are $0, 1, \ldots, p-1$, with addition and multiplication modulo p. The non-zero elements form a group under multiplication, and this group is cyclic of order $p - 1 = 4\mu$, because all finite subgroups of multiplicative groups of fields are cyclic. This means that there is an element x of $\mathbb{F}_p$, with the property that $x^{p-1} = 1$ and the powers $x, x^2, \ldots, x^{p-1}$ are the distinct non-zero elements of $\mathbb{F}_p$ in some order. Note that

$$(x^{\frac{p-1}{2}})^2 = 1,$$

which means that $x^{\frac{p-1}{2}}$ is a square root of 1 in $\mathbb{F}_p$ that is different from 1, so it is -1. Then (since $p-1$ is a multiple of 4), we have that $x^{\frac{p-1}{4}}$ is an element of $\mathbb{F}_p$ whose square is -1. Thus -1 is a square in $\mathbb{F}_p$ if (and only if) $p \equiv 1 \mod 4$. The squares in $\mathbb{F}_p$ are the even powers of x (and 0), they account for $\frac{p+1}{2}$ of the p elements. Note also that the set of squares in $\mathbb{F}_p$ is closed under multiplication, since the product of two squares is a square.

Example 4.3.1. *If $p = 13$, the squares in $\mathbb{F}_{13}$ are $-4, -3, -1, 0, 1, 3, 4$:*

$$0^2, 1^2 = 1, 2^2 = 4, 3^2 = -4, 4^2 = 3, 5^2 = -1, 6^2 = -3, 7^2 = -3, 8^2 = -1, 9^2 = 3, 10^2 = -4, 11^2 = 4, 12^2 = 1$$

Definition 4.3.2. *For $p = 4\mu + 1$, the Paley graph $P(p)$ is defined to be the graph whose vertices are labelled by the elements of $\mathbb{F}_p$ and in which two vertices are adjacent if the difference of the corresponding elements of $\mathbb{F}_p$ is a square.*

The fact that -1 is a square means that an element is a square if and only if its negative is, so this adjacency condition does not depend on which element is subtracted from the other to form the difference. The degree of each vertex of $P(p)$ is $\frac{p-1}{2}$, and $P(p)$ is a strongly regular graph with

parameters $(4\mu+1, 2\mu, \mu-1, \mu)$. For example $P(13)$ has parameters $(13, 6, 6, 3)$. The adjacency matrix of $P(13)$ (with rows and columns labelled 0 through 12) is

$$\begin{pmatrix}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0
\end{pmatrix}$$

This is a *circulant* matrix (every row is obtained from the previous one by shifting the entries one step to the right and then wrapping the last entry to the front).
Note: it is not true that conference graphs exist of all orders n with $n \equiv 1 \mod 4$. For example there is no conference graph on 21 vertices.