Vergelijkingen oplossen modulo priemmachten (Ronald van Luijk)

De eenheidscirkel in $\mathbb{R}^2$ bestaat uit alle punten (x, y) waarvan de coördinaten voldoen aan de vergelijking

$$x^2 + y^2 = 1.$$

Van diezelfde vergelijking kunnen we ook de oplossingen bekijken over de complexe getallen, de rationale getallen of elk ander lichaam. Sterker nog, we kunnen de oplossingen bekijken over elke ring, zoals bijvoorbeeld de ring van gehele getallen modulo een priemmacht.

Zo is het bijvoorbeeld makkelijk in te zien dat de vergelijking

$$x^2 + y^2 = 0$$

over $\mathbb{Z}/3\mathbb{Z}$ alleen de oplossing $(x, y) = (0, 0)$ heeft en daarmee dat over $\mathbb{Z}/9\mathbb{Z}$ de oplossingen van de vergelijking

$$x^2 + y^2 = 3z^2$$

precies de drietallen $(x, y, z) \in (\mathbb{Z}/9\mathbb{Z})^3$ zijn waarvoor x, y en z alle veelvouden zijn van 3. Het leuke is dat je met deze observatie kunt bewijzen dat de enige oplossing van deze laatste vergelijking over $\mathbb{Q}$ het drietal $(0, 0, 0)$ is.

In dit project zullen we dit formaliseren door voor elk priemgetal p eerst het lichaam $\mathbb{Q}_p$ van p-adische getallen te construeren. Daarna zullen we nagaan hoe oplossingen over $\mathbb{Q}_p$ van een vergelijking of van een stelsel vergelijkingen overeenkomen met oplossingen over $(\mathbb{Z}/p^n\mathbb{Z})$ voor alle positieve gehele exponenten n.

Omdat het lichaam $\mathbb{Q}$ is bevat in $\mathbb{Q}_p$ voor elke p, volgt dat als er geen oplossingen zijn over $\mathbb{Q}_p$ voor een zekere p, dan ook (zeker) niet over $\mathbb{Q}$. Het omgekeerde is in sommige gevallen ook waar: als een kegelsnede over $\mathbb{Q}$ (dus een ellips, een parabool of een hyperbool) punten heeft over $\mathbb{Q}_p$ voor elk priemgetal p, dan heeft hij ook punten over $\mathbb{Q}$. Dit staat bekend als het Hasse principe dat we ook zullen proberen te doorgronden in dit project.