Een cryptokromme voor Jan Karel

Het Mathematisch Instituut in Leiden, dat volgens sommigen gaarne voor een dubbeltje op de eerste rang zit, kent een lange traditie in het aanbieden van exquisiete immateriële geschenken. Bij je afscheid van het CWI wil ik je dan ook, geheel in stijl, een gepersonaliseerde *elliptische kromme* meegeven.

Deze kromme, $\mathcal{E}$ geheten, heeft Weierstrass-gedaante

$$Y^2 = X^3 + 26266794886933499972341(X - 1).$$

Precies zoals de politiek dat dezer dagen graag ziet, is $\mathcal{E}$ een toonbeeld van *valorisatie*, dat laat zien dat ook de zuiverste wiskunde heel toepasbaar kan zijn. Immers, neem je je kromme modulo het priemgetal $10^{60} + 38187$, dan krijg je een puntengroep waarvan de orde een *priemgetal* van zestig cijfers is. De discrete logaritme in zo'n puntengroep zal nog wel tot na mijn afscheid in Leiden ondoenlijk blijven, dus $\mathcal{E}$ is uitermate geschikt voor alle huis-, tuin- en keukencryptografische toepassingen die je de komende jaren nog zult hebben. Met zo'n kromme kun je bij vrouw en kinders thuiskomen.

Neem je $\mathcal{E}$ echter modulo $p = 194712192003938259582209$, een veel kleiner priemgetal, dan blijkt $\mathcal{E} \bmod p$ je persoonlijke CWI-kromme te zijn, met puntenaantal

$$19471219\ 20031001\ 20111104.$$

Met dank voor vele jaren van prettige samenwerking,

Peter Stevenhagen