STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

ZW 1966-003

Over de congruentie $u^{p-1} \equiv 1$ modulo p^2

door

D. Kruyswijk

maart 1966

The Mathematical Centre at Amsterdam, founded the 11th of February, 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

Over de congruentie $u^{p-1} \equiv 1$ modulo p^2

Samenvatting van een voordracht,
gehouden in maart 1966.

In 1828 stelde ABEL de vraag, welke paren (u,p) met $1 < u < p$, p priem, aan bovengenoemde congruentie voldoen. Er is een uitgebreide literatuur over ontstaan; hoofdstuk IV van Dickson's "History of the theory of numbers" is daar volledig aan gewijd.

Niettemin heeft men tot dusver slechts een beperkt aantal van dergelijke paren gevonden. De bekendste zijn (3,11), (2,1093) en (2,3511). Tussen 1900 en 1940 vonden WIEFERICH en anderen het opzienbarende resultaat, dat bij een gegeven p alle u met $1 \leq u \leq 46$ aan Abels congruentie moeten voldoen, willen er getallen a, b, c kunnen bestaan met

$$a^p + b^p = c^p, \quad abc \not\equiv 0 \bmod p.$$

D.H. Lehmer en Emma Lehmer leidden hieruit af dat dan $p > 253747900$ moet zijn. Opgemerkt zij, dat ook a, b en c zelf (wanneer men ze paarsgewijs onderling ondeelbaar onderstelt) aan Abels congruentie moeten voldoen en dat dit zeer elementair aangetoond kan worden.

Buiten de sfeer van het beruchte Fermatprobleem blijken nog tal van (meer centrale) vraagstellingen verband te houden met Abels probleem en met de algemenere congruentie

$$u^{p-1} \equiv 1 \text{ modulo } p^{\alpha} \quad (\alpha \geq 2).$$

We besteden er de volgende opmerkingen aan.

§1.

Stelling 1. Gegeven een priemmacht p^{α} met $p \geq 3$, $\alpha \geq 2$.
Het aantal oplossingen van het stelsel

$$\begin{cases} u^{p-1} \equiv 1 \text{ modulo } p^{\alpha} \\ 0 < u < p \end{cases}$$

is dan $< p^{\frac{1}{\alpha} + \frac{\alpha\theta}{\log\log p}}$,

waarbij θ een absolute constante is.

We bewijzen deze stelling met behulp van het volgende lemma.

Lemma 1.1 Zij H een multiplicatieve halfgroep van natuurlijke getallen en zij voor reële $x > 1$ een telfunctie gedefinieerd door:

$$A_H(x) = ||H \cap [1,x]||.$$

Dan geldt:

$$A_H(x) \cdot A_H(y) \leq z^{\frac{\theta}{\log\log z}} \cdot A_H(z)$$

voor alle x, y, z met $xy = z \geq 2{,}7183$. Hierin is θ een absolute constante.

Bewijs. Gegeven H, x en y. Beschouw een willekeurige $n \geq 1$ en definieer $t(n)$ als het aantal oplossingen (a,b) van het stelsel

$$\begin{cases} ab = n \\ a \in H \cap [1,x] \\ b \in H \cap [1,y]. \end{cases}$$

Zeker is dan

$$A_H(x) \cdot A_H(y) = t(1) + t(2) + \ldots + t([xy]).$$

Van de termen in het rechterlid zijn er hoogstens $A_H(xy)$ ongelijk aan 0. Hieruit volgt:

$$A_H(x) \cdot A_H(y) \leq \{\operatorname{Max}_n t(n)\} \cdot A_H(xy);\ (n \leq xy).$$

Schrijven we nu verder $xy = z$, dan is de accolade-vorm hoogstens gelijk aan

$$\operatorname{Max}_{n \leq z} \tau(n),$$

waarbij $\tau(n)$ het aantal delers van n beduidt. Een bekende schatting, geldig voor alle $n \geq 3$, luidt:

$$\tau(n) < n^{\frac{\theta_1}{\log \log n}},$$

waarbij θ_1 een absolute constante is. Na enig overleg kan men hieruit besluiten tot:

$$\operatorname*{Max}_{n \leq z} \tau(n) < z^{\frac{\theta_2}{\log \log z}} \quad \text{voor } z \geq 2{,}7183$$

en daarmee is lemma 1.1 bewezen.

Een iteratieve procedure, toegepast op lemma 1.1, voert nu tot de ongelijkheid

$$\{A_H(x)\}^\alpha \leq x^{\frac{\alpha^2\theta_3}{\log \log x}} \cdot A_H(x^\alpha),$$

geldig voor iedere H, iedere $x \geq 2{,}7183$ en $\alpha = 2, 3, 4, \ldots$. Daaruit volgt gemakkelijk Stelling 1, in verband met het feit dat de positieve wortels van $u^{p-1} \equiv 1 \bmod p^\alpha$ een multiplicatieve halfgroep H vormen met

$$||H \cap [1, p^\alpha]|| = p - 1.$$

Deze laatste formule berust op het cyclisch karakter van de wortelklassen-groep; zie daarvoor het aanhangsel (§4).

§2.

We geven een toepassing van stelling 1, betreffende de distributie van primitieve wortels. Zij $p \geq 3$ en zij W_α de verzameling van alle gehele getallen die primitieve wortel van p^α zijn. Uit het cyclisch karakter van de Eulerse groep $\Phi(p^\alpha)$ kan men zeer eenvoudig de volgende bekende relaties afleiden:

(i) $W_1 \supset W_2 = W_3 = W_4 = \ldots$;

(ii) $W_1 \setminus W_2 = \{u \in W_1 \mid u^{p-1} \equiv 1 \text{ modulo } p^2\}$.

Een primitief wortelgetal w van p heet <u>sterk</u> (of <u>generaal</u>) als het tevens primitieve wortel is van p^2, p^3,... ; dus als $w \in W_2$. Anders heet het <u>zwak</u> ($w \in W_1 \setminus W_2$).

Men bewijst gemakkelijk dat er op ieder half-open interval van lengte p^2 precies $(p-1)\phi(p-1)$ sterke en precies $\phi(p-1)$ zwakke primitieve wortels van p liggen; maar over het distributiepatroon van de zwakke tussen de sterke geven (i) en (ii) geen enkele inlichting. Met behulp van stelling 1 kunnen we een begin van informatie krijgen:

Stelling 2. Zij $\phi_z(p-1)$ het aantal zwakke primitieve wortels van p op het vak $[0,p]$, dus

$$\phi_z(p-1) = ||(W_1 \setminus W_2) \cap [0,p]||.$$

Dan is $\dfrac{\phi_z(p-1)}{\phi(p-1)} < p^{-\frac{1}{2}+\varepsilon}$

voor iedere $\varepsilon > 0$ en bijna alle p.
Het percentage zwakken op $[0,p]$ nadert dus sterk naar 0 voor $p \to \infty$.

<u>Aanvulling</u>. Met behulp van tabulaties van Beeger, Haussner en Kraitchik hebben we de functie $\phi_z(p-1)$ berekend voor alle $p < 300$. Het resultaat is aldus:

$\phi_z(p-1) = 1$ voor $p = 29, 37, 43, 71, 103, 109, 113, 131, 181, 191, 211, 223, 257, 269, 283$.

$\phi_z(p-1) = 0$ voor alle andere $p < 300$.

Bewijs van stelling 2. Wegens (ii) en stelling 1 is $\phi_z(p-1) < p^{\frac{1}{2}+\frac{1}{2}\varepsilon}$ voor bijna alle p bij de gekozen ε. Volgens een bekende schatting is tevens $\phi(p-1) > p^{1-\frac{1}{2}\varepsilon}$ voor bijna alle p. Daaruit volgt het gestelde.

§3.

Heeft iedere $p \geq 3$ minstens één sterke primitieve wortel tussen 0 en p? De vorige paragraaf suggereert dit, maar we willen het toch ook bewijzen.

Stelling 3. Voor iedere $p \geq 3$ is $\phi_z(p-1) \leq \frac{1}{2}\phi(p-1)$. Met andere woorden: minstens de helft der primitieve wortels op $[0,p]$ is sterk.

Bewijs.

Geval I: p is een 4-voud + 1.

Zij in dit geval u een getal van W_1 dan is ook $p^2 - u \in W_1$, want

$$p^2 - u \equiv -u \equiv u^{\frac{p-1}{2}} \cdot u \equiv u^{\frac{p+1}{2}} \text{ modulo } p,$$

waarbij de exponent $\frac{p+1}{2}$ onderling ondeelbaar is met $p-1$. Geldt bovendien: $u \in W_1 \setminus W_2$, dan is ook $p^2 - u \in W_1 \setminus W_2$, hetgeen blijkt door substitutie in Abels congruentie. Bij iedere zwak-primitieve u tussen 0 en p behoort dus een zwak-primitieve $u^* = p^2 - u$ tussen p en p^2; waarbij $u_1 \neq u_2$ impliceert $u_1^* \neq u_2^*$.
Uit $||(W_1 \setminus W_2) \cap [0,p^2]|| = \phi(p-1)$ volgt nu het gestelde.

Geval II: p is een 4-voud - 1.

Uit $u \in W_1$ volgt nu $p^2 - u^2 \in W_1$, want

$$p^2 - u^2 \equiv -u^2 \equiv u^{\frac{p+3}{2}} \text{ modulo } p$$

en $\frac{p+3}{2}$ is in dit geval onderling ondeelbaar met $p-1$. De rest van het bewijs verloopt analoog aan het voorgaande, met $u^* = p^2 - u^2 = (p+u)(p-u) \geq p+u > p$, voor $0 < u < p$.

§4. Aanhangsel.

De structuur van de Eulerse groep $\Phi(p^\alpha)$ wordt niet in alle handboeken volledig besproken. De volgende afleiding doet het verband met Abels

congruentie naar voren komen en vereist weinig rekenwerk. We onderstellen steeds $p \geq 2$, $\alpha \geq 1$ (p priem).

Lemma 1. Zij K een klasse van de ring $R(p^\alpha)$. Verheft men alle getallen van K tot de p-de macht dan liggen de uitkomsten in één en dezelfde klasse van $R(p^{\alpha+1})$.

Definitie: Deze klasse van $R(p^{\alpha+1})$ wordt aangeduid met K^p. Bij iedere $K \in R(p^\alpha)$ is nu ook de betekenis van

$$K^{p^\beta} \quad (\beta \geq 0),$$

als klasse van $R(p^{\alpha+\beta})$, welgedefinieerd.

[Opmerking: Voor gegeven $K \in R(p^\alpha)$ zullen nu, als men $\beta \to \infty$ laat gaan, alle getallen van K^{p^β} tot één en hetzelfde p-adische gehele getal naderen].

Lemma 2. Zij $\{K_1, K_2, \ldots, K_n\}$ een subgroep van $\Phi(p^\alpha)$.
Dan is $\{K_1^p, K_2^p, \ldots, K_n^p\}$ een subgroep van $\Phi(p^{\alpha+1})$.

In het geval dat $p = 2$, $\alpha \geq 2$ en minstens één der $K_i \equiv -1 \bmod 4$, zijn deze groepen niet isomorf. In alle overige gevallen zijn ze rechtstreeks isomorf, volgens $K_i \leftrightarrow K_i^p$. In het bijzonder geldt deze isomorfie voor $p \geq 3$ en iedere α.

[Opmerking: Wanneer het uitzonderingsgeval zich niet voordoet, kan men nu door iteratie een eindige multiplicatieve groep van p-adische gehele getallen verkrijgen, welke nog steeds rechtstreeks isomorf is met $\{K_1, K_2, \ldots, K_n\}$].

Lemma 3. Voor $p \geq 3$, $\alpha \geq 2$ geldt:

$$\Phi(p^\alpha) = \{1^{p^{\alpha-1}}, 2^{p^{\alpha-1}}, \ldots, (p-1)^{p^{\alpha-1}}\} \times \{1, 1+p, \ldots, 1+Kp, \ldots\}.$$

Daarbij is $\{1, 2, \ldots, (p-1)\} = \Phi(p)$, terwijl K alle klassen van $R(p^{\alpha-1})$ doorloopt.

Beide faktoren zijn cyclisch, $\Phi(p^\alpha)$ zelf ook.

De generatoren van de linkerfaktor zijn de klassen $G^{p^{\alpha-1}}$, waarbij G de generatoren van $\Phi(p)$ doorloopt.

De generatoren van de rechterfaktor zijn de klassen $1 + Kp$ met $K \in \Phi(p^{\alpha-1})$.

De linkerfaktor is de oplossingengroep van $U^{p-1} \equiv 1 \bmod p^{\alpha}$.

De rechterfaktor is de oplossingengroep van $U^{p^{\alpha-1}} \equiv 1 \bmod p^{\alpha}$.

[Opmerking: Afhankelijk van de manier waarop men de p-adische getallen wenst in te voeren, kan men met behulp van bovenstaand lemma de stelling van Hensel bewijzen dat

$$\Phi(p^{\infty}) = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{p-1}\} \times \{1 + p\zeta \mid \zeta \in R(p^{\infty})\}$$

waarbij $\{\varepsilon_i\}$ de p-adische wortelgroep van $u^{p-1} = 1$ is, $R(p^{\infty})$ de ring der p-adische gehelen en $\Phi(p^{\infty})$ de multiplicatieve groep der eenheden van $R(p^{\infty})$. Omgekeerd kan men ook lemma 3 uit Hensels stelling afleiden].

Lemma 4. Voor $\alpha \geq 3$ geldt:

$$\Phi(2^{\alpha}) = \{1, -1\} \times \{1, 5, 9, \ldots, 2^{\alpha} - 3\}$$

Beide faktoren zijn cyclisch, $\Phi(2^{\alpha})$ zelf niet. De generatoren van de rechterfaktor zijn die klassen die $\equiv 5$ modulo 8 zijn.