

Er zijn in totaal 11 vragen c.q. onderdelen van vragen. Maak er 10 van.

1

Bepaal de kleinste oplossing x in $\mathbb{Z}$ van het stelsel congruentievergelijkingen $x \equiv 2 \pmod{5}$ (1), $x \equiv 3 \pmod{6}$ (2), $x \equiv 4 \pmod{7}$ (3), die voldoet aan $x \geq 500$. Leg uit waarom x geen priemgetal kan zijn. Als er een oplossing x is, dan moet x de vorm hebben $x = 2 + 5k$, (4) voor zekere $k \in \mathbb{Z}$. (4) in (2) geeft $2 + 5k \equiv 3 \pmod{6} \Rightarrow 5k \equiv 1 \pmod{6} \Rightarrow k \equiv 5 \pmod{6}$. Dus k heeft de vorm $k = 5 + 6m$ voor zekere $m \in \mathbb{Z}$ (5). In (4) geeft dit $x = 2 + 5(5 + 6m) = 27 + 30m$ (6). Nu (6) in (3) geeft: $27 + 30m \equiv 4 \pmod{7} \Rightarrow -1 + 2m \equiv 4 \pmod{7} \Rightarrow 2m \equiv 5 \pmod{7}$. vermenigvuldig beide kanten met 4 om te zien, dat $m \equiv 6 \pmod{7}$. Dit in (6) geeft $x = 27 + 30(6 + 7n) = 207 + 210n$ voor zekere $n \in \mathbb{Z}$ (8). Omgekeerd zien we, dat elke x van de vorm (8) een oplossing geeft, dus we hebben alle oplossingen gevonden. De kleinste oplossing ≥ 500 is $207 + 2 \cdot 210 = 627$. Daar 207 en 210 beide deelbaar zijn door 3, is elke oplossing een drievoud, en kan dus geen priemgetal zijn. (Dit zien we natuurlijk ook direct: een oplossing x voldoet aan $x \equiv 3 \pmod{6}$, dus is deelbaar door 3.)

2

In $(\mathbb{Z}/5\mathbb{Z})[X]$ zijn de veeltermen $F = X^4 + \bar{3}X^3 - \bar{12}X^2 - \bar{6}X + \bar{20}$ en $G = \bar{2}X^2 + \bar{3}X - \bar{4}$ gegeven. Bepaal de grootste gemene deler D van F en G en schrijf deze in de vorm $D = AF + BG$ met $A, B \in (\mathbb{Z}/5\mathbb{Z})[X]$. Deel G op F en constateer, dat $F = (\bar{3}X^2 + \bar{2}X + \bar{2})G + X + \bar{3}$. Deel nu weer de rest $X + \bar{3}$ op G en constateer, dat $G = (X + \bar{3})(\bar{2}X + \bar{2})$. We krijgen dan

$$\begin{array}{l|l|l} F & 1 & 0 \\ G & 0 & 1 \\ X + \bar{3} & 1 & \bar{2}X^2 + \bar{3}X + \bar{3} \\ 0 & ? & ? \end{array} \quad \begin{array}{l} - \\ \bar{3}X^2 + \bar{2}X + \bar{2} \\ \end{array} \quad \text{Er volgt, dat de grootste gemene}$$

deler gegeven wordt als

$$D = X + \bar{3} = F + (\bar{2}X^2 + \bar{3}X + \bar{3})G = AF + BG.$$

3

a. Geef de definitie van de volgende begrippen:

- De deelverzameling H is een *deelgroep* van de groep G . H is een *deelgroep* van G als H , met de operatie van G zelf een groep is.

- De groep G is een *cyclische groep*. G is een *cyclische groep*, als er een element $x \in G$ is, zodat - in multiplicatieve notatie - elk element van G te schrijven is in de vorm x^m , met $m \in \mathbb{Z}$.
 - Hoe luidt het *criterium voor een ondergroep*? Een niet lege deelverzameling H van een groep G is een ondergroep van G , als en alleen als met $a \in H$ en $b \in H$ ook $ab^{-1} \in H$.
 - De deelgroep N is een *normaaldeler* in de groep G . N is een *normaaldeler* in de groep G als N een ondergroep van G is en voor elke $a \in G$ geldt $aN \subset Na$, equivalent $Na \subset aN$, equivalent $aN = Na$, equivalent, als voor elke $n \in N$ $ana^{-1} \in N$. (Daar de genoemde eigenschappen equivalent zijn, is het goed, als U er een ervan als definitie kiest).
 - De *orde* van een element in een groep. De orde van het element g in een groep G is het kleinste positieve getal N , waarvoor - in de multiplicatieve notatie geldt, dat $g^N = e$, het neutrale element. Is een dergelijke N er niet, dan zeggen we, dat g *oneindige orde* heeft.
 - *Isomorfisme* van unitaire ringen. Zijn R en S unitaire ringen, dan is $f : R \rightarrow S$ een *isomorfisme van unitaire ringen*, als 1) f een *homomorfisme van unitaire ringen* is, waarbij tevens een homomorfisme $g : S \rightarrow R$ van unitaire ringen bestaat, zodat $f \circ g = 1_S$ en $g \circ f = 1_R$ beide de identieke afbeelding op S , respectievelijk R zijn.
 - Zij $X := \{1, 2, 3, 4, 5, 6, 7, 8\}$. Wat is een permutatie van X ? Een *permutatie van* X is een bijectieve afbeelding van X in zich zelf. X ?
- b. Laat zien, dat in een eindige groep elk element ook werkelijk een eindige orde heeft. Zij g een element in een eindige groep G , zeg met N elementen. Bekijk de verzameling $M = \{g^m | m \in \mathbb{N}\}$. $M \subset G$, dus vanwege de eindigheid van G zijn er twee verschillende natuurlijke getallen a en b , zodat $g^a = g^b$. Zonder beperking: $a > b$. Dan $g^{a-b} = e$, het neutrale element, dus er is een minimale $n > 0$ in $\mathbb{N}$ met $g^n = e$, dus g heeft (eindige) orde n .
- c. Schrijf de permutatie

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 8 & 6 & 5 & 3 & 4 & 2 \end{pmatrix}$$

als een product van disjuncte cykels. Schrijf deze tevens als een product van tweecykels. Geef in beide notaties de inverse van deze permutatie. $(1\ 7\ 4\ 6\ 3\ 8\ 2) = (2\ 1)(8\ 1)(3\ 1)(6\ 1)(4\ 1)(7\ 1)$. De inverse is te schrijven als $(2\ 8\ 3\ 6\ 4\ 7\ 1) = (7\ 1)(4\ 1)(6\ 1)(3\ 1)(8\ 1)(2\ 1)$.

4

Zij G een groep en $S \subset G$ een niet lege deelverzameling van G . Definieer

$$\langle S \rangle := \cap_H \{H \text{ is ondergroep van } G \text{ en } S \subset H\}.$$

- a. Bewijs, dat $\langle S \rangle$ een ondergroep van G is. We doen dit met het ondergroupecriterium: zeker is $\langle S \rangle$ niet leeg, daar S in de doorsnede zit. Zijn verder a en b in deze doorsnede, dan behoren a en b tot elke ondergroep H , die S bevat. Daar deze H een ondergroep is, behoort ook ab^{-1} tot een dergelijke H , dus ook tot de doorsnede van al dergelijke H , dus $ab^{-1} \in \langle S \rangle$.
- b. Laat zien, dat $\langle \langle S \rangle \rangle = \langle S \rangle$. Merk eerst op dat triviaalwijze $S \subset \langle S \rangle$, want elke H bevat S , dus ook de doorsnede van al dergelijke H . Dit geeft direct, dat $\langle S \rangle \subset \langle \langle S \rangle \rangle$. Zij omgekeerd K een ondergroep, die S bevat. Dan bevat K ook $\langle S \rangle$, immers K bevat dan de doorsnede van alle ondergroepen, die S bevatten, en $\langle S \rangle$ is ook zo een ondergroep, die S bevat. Nemen we nu de doorsnede van al dergelijke K , dan krijgen we - enerzijds - $\langle S \rangle$, anderzijds zien we, dat deze doorsnede ook $\langle S \rangle$ bevat, ergo: $\langle S \rangle \supset \langle \langle S \rangle \rangle$.
- c. Als $S = \{g\}$ uit èèn element bestaat, schrijven we $\langle S \rangle$ als $\langle g \rangle$. Laat zien, dat

$$\langle g \rangle = \{g^m | m \in \mathbb{Z}\}.$$

We weten, dat $g \in \langle g \rangle$. Daar $\langle g \rangle$ een groep is, moeta met $g \in \langle g \rangle$ ook $g^m \in \langle g \rangle$, dus we zien: $\langle g \rangle \supset \{g^m | m \in \mathbb{Z}\}$. Met het ondergroupecriterium is duidelijk, dat het rechterlid een ondergroep is, die g bevat, dus het rechterlid omvat $\langle g \rangle$ (!).

- d. Bedenk een voorbeeld, dat $\langle g \rangle$ uit 23577 verschillende elementen bestaat. Neem het element $\bar{1}$ in de abelse groep $\mathbb{Z}/23577\mathbb{Z}$.

5

Zij B het rechthoekige blok, gevormd door twee vierkanten V_1 en V_2 met zijden van lengte 1. De overige zijden hebben lengte 2. Nummer de hoekpunten van V_1 resp V_2 met 1, 2, 3 en 4, resp. 5, 6, 7 en 8, zodat er twee zijanten ontstaan met hoeknummers 1, 5, 8 en 4, resp. 2, 6, 7 en 3.

- a. Hoeveel elementen heeft de symmetriegroep G van B ? We gebruiken de formule voor een transitieve werking:

$$\#G_v \cdot \#Gv = \#G.$$

G werkt transitief op de 8 hoekpunten, dus $G1$ is de verzameling van alle 8 hoekpunten. De stabilisator G_1 van hoekpunt 1 is de identieke permutatie (1) en de spiegeling om het vlak door de punten 1,3 7 en 8. Dus G_1 heeft orde 2, en daarmee heeft G de orde 16.

- b. Geef een S aan met een minimaal aantal elementen, zodat $G = \langle S \rangle$. Motiveer Uw antwoord. Zij $r = (1234)(5678)$ de rotatie en $s = (12)(34)(56)(78)$ de spiegeling om het middenloodvlak van de ribbe die 1 en 2 verbindt. Daar $\# \langle r \rangle = 4$ en $s \notin \langle r \rangle$, is de ondergroep $\langle r, s \rangle$ de symmetriegroep van het vierkant met hoekpunten 1,2,3 en 4.

Honorering: Voor elk van de 10 gemaakte onderdelen kunt U 5 punten behalen. In totaal kunt U dus 50 punten behalen.

Het eindcijfer E wordt berekend naar:

$$E = \frac{\text{totaal behaald}}{5}.$$

gevolgd door afronden.