Elementaire Getaltheorie (WISB321)

Tentamen, 4 november 2015, 9:00 -12:00 uur

Bij dit tentamen is gebruik van boeken, dictaat of aantekeningen niet toegestaan. Als rekenhulp kun je een eenvoudige calculator gebruiken (dus geen GR of smartphone). Als je een onderdeel mist mag je wel het resultaat ervan in de volgende onderdelen gebruiken.
Motiveer je antwoorden!
Veel succes!

1. We beschouwen de vergelijking $x^7 \equiv x (\text{mod } 312)$ in $\mathbb{Z}/312\mathbb{Z}$.
   (a) (1/2 pt) Bepaal $\phi(312)$.
   (b) (1/2 pt) Geef een oplossing x met $x \neq 0, 1 (\text{mod } 312)$.
   (c) (1 pt) Hoeveel restklassen heeft de vergelijking als oplossing?

2. Zij $x \in \mathbb{N}$ oneven en p een priemdeler van $x^2 + 4$.
   (a) (1/2 pt) Bewijs dat $p \equiv 1 (\text{mod } 4)$.
   (b) (1/2 pt) Stel bovendien dat x niet deelbaar is door 3. Bewijs dat $x^2 + 4$ deelbaar is door een priemgetal p van de vorm $3k - 1$.
   (c) (1 pt) Bewijs dat er oneindig veel priemgetallen bestaan van de vorm $12k + 5$.

3. (a) (1 pt) Bewijs dat er oneindig veel paren opeenvolgende kwadraten zijn waarvan de som weer een kwadraat is (hint: maak van de vergelijking $x^2 + (x+1)^2 = y^2$ een Pell-vergelijking).
   (b) (1 pt) Bewijs dat er geen drie opeenvolgende kwadraten zijn waarvan de som weer een kwadraat is.

4. (2 pt) Met $P(n)$ geven we de grootste priemdeler aan van een getal $n \geq 2$. Zij $F(x) = x(x-u)$ met $u \in \mathbb{N}$. Bewijs dat de correctheid van het abc-vermoeden impliceert dat $P(F(n)) \to \infty$ als $n \to \infty$.

5. (1 pt) Bewijs dat bij elke $\epsilon > 0$ een $n_0(\epsilon)$ bestaat zó dat
$$\prod_{\substack{p \leq n \\ p \ priem}} p < e^{(1+\epsilon)n} \quad \text{voor alle } n > n_0(\epsilon).$$
   Je mag hierbij de priemgetalstelling gebruiken.

6. (1 pt) Zij $h(n)$ het aantal priemgetallen $\leq n$ van de vorm $4k + 1$. Bewijs dat
$$h(n) \leq \frac{2}{15} n + 2 \quad \text{voor alle } n \in \mathbb{N}.$$

UITWERKINGEN VANAF VOLGENDE PAGINA

1. We beschouwen de vergelijking $x^7 \equiv x (\mathrm{mod}\ 312)$ in $\mathbb{Z}/312\mathbb{Z}$.

   (a) Bepaal $\phi(312)$.
   Antwoord: priemiontbinding van 312, $312 = 3\times 2^3 \times 13$ Dus $\phi(312) = \phi(3)\phi(2^3)\phi(13) = 2 \times 4 \times 12 = 96$.

   (b) Geef een oplossing x met $x \neq 0, 1 (\mathrm{mod}\ 312)$.
   Antwoord: De congruentie is equivalent met het stelsel congruenties

   $$x^7 \equiv x (\mathrm{mod}\ 3), \quad x^7 \equiv x (\mathrm{mod}\ 8), \quad x^7 \equiv x (\mathrm{mod}\ 13).$$

   Kies bijvoorbeeld de oplossing met $x \equiv 1 (\mathrm{mod}\ 3), x \equiv 0 (\mathrm{mod}\ 8), x \equiv 0 (\mathrm{mod}\ 13)$ Dus x is een veelvoud van $8 \times 13 = 104$ en $1 (\mathrm{mod}\ 3)$. Je kunt de congruenties oplossen, maar je kunt ook opmerken dat $208 \equiv 1 (\mathrm{mod}\ 3)$. Dus bijvoorbeeld $x = 208$.

   Nog simpeler (had ik eerst niet opgemerkt): $x = -1$.

   (c) Hoeveel restklassen heeft de vergelijking als oplossing?
   Antwoord: We bekijken de aantallen oplossingen van elk der drie congruentievergelijkingen in voorgaand onderdeel en nemen het product daarvan. Met de hand checken we dat $x^7 \equiv x (\mathrm{mod}\ 3)$ voor elke $x (\mathrm{mod}\ 3)$. Dus drie oplossingen modulo 3. De vergelijking $x^7 \equiv x (\mathrm{mod}\ 8)$ kunnen we ook met de hand doen. Dat geeft 5 oplossingen. Je kunt ook opmerken dat $8|x^7 - x$ impliceert $8|x(x^6 - 1)$, en dat impliceert weer $x \equiv 0 (\mathrm{mod}\ 8)$ of $x^6 \equiv 1 (\mathrm{mod}\ 8)$. De laatste heeft vier oplossingen, namelijk alle oneven x. Modulo 13 kunnen we ook met de hand doen, maar is meer werk. Je kunt ook opmerken dat ofwel $x \equiv 0 (\mathrm{mod}\ 13)$, ofwel $x^6 \equiv 1 (\mathrm{mod}\ 13)$. En dit geldt precies dan als x een kwadraatrest modulo 13 is. Er zijn 6 kwadraatresten. Samen met 0 zijn er dus 7 oplossingen. Gevolg, het aantal oplossingen is $3 \times 5 \times 7 = 105$ oplossingen.

2. Zij $x \in \mathbb{N}$ oneven en p een priemdeler van $x^2 + 4$.

   (a) Bewijs dat $p \equiv 1 (\mathrm{mod}\ 4)$.
   Antwoord: Omdat x^2+4 oneven is, is p dat ook. Uit $p|x^2+4$ volgt $x^2 \equiv -4 (\mathrm{mod}\ p)$. Dus -4 (en daarmee ook -1) is kwadraatrest modulo p, dus $p \equiv -1 (\mathrm{mod}\ 4)$.

   (b) Stel bovendien dat x niet deelbaar is door 3. Bewijs dat $x^2 + 4$ deelbaar is door een priemgetal p van de vorm $3k - 1$.
   Antwoord: x niet deelbaar door 3 impliceert dat $x^2 + 4 \equiv 1 + 4 \equiv -1 (\mathrm{mod}\ 3)$. Priemgetallen $\neq 3$ zijn 1 of -1 modulo 3. Als de ontbinding van $x^2 + 4$ alleen priemgetallen $1 (\mathrm{mod}\ 3)$ zou bevatten, dan zou $x^2 + 4 \equiv 1 (\mathrm{mod}\ 3)$ moeten gelden, in tegenspraak met $x^2 + 4 \equiv -1 (\mathrm{mod}\ 3)$. Dus concluderen we dat $x^2 + 4$ minstens één priemfactor $-1 (\mathrm{mod}\ p)$ bevat.

   (c) (1 pt) Bewijs dat er oneindig veel priemgetallen bestaan van de vorm $12k + 5$.
   Antwoord: Uit het voorgaande volgt dat een getal van de vorm $x^2 + 4$ met x

oneven en niet deelbaar door 3 een priemfactor $-1 (\mathrm{mod}\ 3)$ bevat die tegelijkertijd $1 (\mathrm{mod}\ 4)$ is. Dus we hebben een prienfactor van de vorm $5 (\mathrm{mod}\ 12)$.

Stel er zijn eindig veel van zulke priemgetallen. Neem hun product en noem dat P. Bekijk P^2+4. Uit voorgaande volgt dat P^2+4 een priemfactor $q \equiv 5 (\mathrm{mod}\ 12)$ heeft. Dus $q|P$. Maar ook $q|P^2+4$. Combinatie van die twee geeft dat $q|4$, waarmee een tegenspraak hebben. Er moeten dus oneindig veel priemgetallen $5 (\mathrm{mod}\ 12)$ zijn.

3. (a) Bewijs dat er oneindig veel paren opeenvolgende kwadraten zijn waarvan de som weer een kwadraat is (hint: maak van de vergelijking $x^2 + (x+1)^2 = y^2$ een Pell-vergelijking).
Antwoord: De vergelijking wordt $2x^2 + 2x + 1 = y^2$. Maal twee geeft $2y^2 = 4x^2 + 4x + 2 = (2x+1)^2 + 1$. Anders geschreven: $(2x+1)^2 - 2y^2 = -1$. We weten dat $X^2 - 2Y^2 = -1$ oneindig veel oplossingen heeft. Neem bijvoorbeeld $X + Y\sqrt{2} = (1+\sqrt{2})^k$ met willekeurige oneven k. Met kettingbreuken gaat het ook. Voor elke oplossing geldt dat X oneven is, dus is er x zó dat $X = 2x+1$.

   (b) Bewijs dat er geen drie opeenvolgende kwadraten zijn waarvan de som weer een kwadraat is.
Antwoord: Neem voor de drie opeenvolgende kwadraten $(x-1)^2, x^2, (x+1)^2$. Hun som is $3x^2+2$. Stel dat dit een kwadraat y^2 is. Dan $3x^2+2 = y^2$. Modulo 3 geeft dit $2 \equiv y^2 (\mathrm{mod}\ 3)$ en dat kan niet.

4. Met $P(n)$ geven we de grootste priemdeler aan van een getal $n \geq 2$. Zij $F(x) = x(x-u)$ met $u \in \mathbb{N}$. Bewijs dat de correctheid van het abc-vermoeden impliceert dat $P(F(n)) \to \infty$ als $n \to \infty$.
Antwoord: Zij P_n het product van alle verschillende priemdelers van $F(n)$. Pas het abc-vermoeden toe met $a = u, b = n-u, c = n$. Neem even aan dat $\mathrm{ggd}(x,u) = 1$. Dan volgt uit 'abc' dat als $n > c_0(\epsilon)$ dan

$$n < \mathrm{Rad}(n(n-u)u)^{1+\epsilon} \leq (P(n)u)^{1+\epsilon}.$$

Kies $\epsilon = 1$. Dan volgt dat $P(n) > n^{1/2}/u$. We zien dat $P_n \to \infty$ als $n \to \infty$. Maar dat impliceert dat ook de grootste priemfactor in P_n naar oneindig gaat als $n \to \infty$.

Nu het algemene geval. Stel $d = \mathrm{ggd}(x,u)$. Pas 'abc' toe op $a = u/d, b = (n-u)/d, c = n/d$,

$$n/d < \mathrm{Rad}(n(n-u)u/d^3)^{1+\epsilon} \leq (P(n)u)^{1+\epsilon}.$$

De rest gaat op dezelfde manier.

5. Bewijs dat bij elke $\epsilon > 0$ een $n_0(\epsilon)$ bestaat zó dat

$$\prod_{\substack{p \leq n \\ p\ priem}} p < e^{(1+\epsilon)n} \quad \text{voor alle } n > n_0(\epsilon).$$

Je mag hierbij de priemgetalstelling gebruiken.
Antwoord: De priemgetalstelling zegt dat $\frac{\pi(n)}{n/\log n} = \frac{\pi(n)\log n}{n}$ naar 1 gaat als $n \to \infty$. Dus is er bij elke $\epsilon > 0$ een $n_0(\epsilon)$ zó dat $\frac{\pi(n)\log n}{n} < 1 + \epsilon$ als $n > n_0(\epsilon)$. Merk nu op,

$$\prod_{p \le n} p < \prod_{p \le n} n = n^{\pi(n)} = \exp(\pi(n)\log n) < \exp((1+\epsilon)n)$$

als $n > n_0(\epsilon)$.

6. Zij $h(n)$ het aantal priemgetallen $\le n$ van de vorm $4k+1$. Bewijs dat

$$h(n) \le \frac{2}{15}n + 2 \quad \text{voor alle } n \in \mathbb{N}.$$

Antwoord: We tellen het aantal getallen $\le n$ van de vorm $4k+1$ dat niet deelbaar is door 3 of door 5.

We tellen het aantal gehele getallen $x \le n$ die $1 (\mathrm{mod}\ 4)$ zijn en niet deelbaar door $3, 5$.

Het aantal getallen van de vorm $4k+1$ kleiner dan n is $\lfloor (n+3)/4 \rfloor$. Een getal $4k+1$ dat deelbaar is door 3 moet van de vorm $12m+9$ zijn. Aantal van dergelijke getallen $\le n$ is $\lfloor (n+3)/12 \rfloor$. Een getal deelbaar door 5 en van de vorm $4k+1$ is van de vorm $20m+5$. Aantal van dergelijke getallen $\le n$ is $\lfloor (n+15)/20 \rfloor$. Een getal van de vorm $4k+1$ dat deelbaar is door 15 is van de vorm $60m+45$. Het aantal getallen van deze vorm en $\le n$ is $\lfloor (n+15)/60 \rfloor$. Hieruit volgt

$$\begin{aligned} h(n) &\le \lfloor (n+3)/4 \rfloor - \lfloor (n+3)/12 \rfloor - \lfloor (n+15)/20 \rfloor + \lfloor (n+15)/60 \rfloor \\ &\le (n+3)/4 - (n+3)/12 + 1 - (n+15)/20 + 1 + (n+15)/60 = 2n/15 + 2. \end{aligned}$$

Een tweede manier is, we tellen het aantal x met $x \equiv 1 (\mathrm{mod}\ 4)$ en $x \equiv 1, 2 (\mathrm{mod}\ 3)$ en $x \equiv 1, 2, 3, 4 (\mathrm{mod}\ 5)$. Modulo 60 zijn er 8 oplossingen. Dat betekent dat elk blok van lengte 60 precies 8 van deze getallen bevat. Dus $h(n+60) - h(n) \le 8 = (2/15) \times 8$. Check de ongelijkheid voor $n \le 60$ en pas vervolgens inductie toe.