OPGAVEN en UITWERKINGEN

1. (a) (1 pt) Los $x^2 \equiv 2(\text{mod } 161)$ op in $x \in \mathbb{Z}$. (Let op: 161 is geen priemgetal).
*Oplossing*: De vergelijking is equivalent met het stelsel $x^2 \equiv 2(\text{mod } 7)$ en $x^2 \equiv 2(\text{mod } 23)$. Oplossingen van de eerste twee zijn: $x \equiv \pm 3(\text{mod } 7)$ en $x \equiv \pm 5(\text{mod } 23)$ (door 'proberen'). Dit geeft via de Chinese reststelling aanleiding tot vier oplossingen:
   - $x \equiv 3(\text{mod } 7), x \equiv 5(\text{mod } 23) \Rightarrow x \equiv 143(\text{mod } 161)$
   - $x \equiv -3(\text{mod } 7), x \equiv -5(\text{mod } 23) \Rightarrow x \equiv -143 \equiv 18(\text{mod } 161)$
   - $x \equiv 3(\text{mod } 7), x \equiv -5(\text{mod } 23) \Rightarrow x \equiv 87(\text{mod } 161)$
   - $x \equiv -2(\text{mod } 7), x \equiv 3(\text{mod } 23) \Rightarrow x \equiv -87 \equiv 74(\text{mod } 161)$

   (b) (1 pt) Stel $N$ is een product van $t$ verschillende oneven priemgetallen. Stel dat de vergelijking $x^2 \equiv 2(\text{mod } N)$ een oplossing $x \in \mathbb{Z}$ heeft.
Bewijs dat deze vergelijking $2^t$ restklassen modulo $N$ als oplossingsverzameling heeft.
*Oplossing*: Stel $N = p_1 p_2 \cdots p_t$ met $p_1, \ldots, p_t$ priem. De vergelijking $x^2 \equiv 2(\text{mod } N)$ is equivalent met het stelsel $x^2 \equiv 2(\text{mod } p_1), \ldots, x^2 \equiv 2(\text{mod } p_t)$. We weten dat er een oplossing is voor de vergelijking modulo $N$. Noem deze $x_0$. Dan heeft het stelsel de als volledige oplossingsverzameling $x \equiv \pm x_0(\text{mod } p_1), \ldots, x \equiv \pm x_0(\text{mod } p_t)$. Elk van deze vergelijkingen heeft twee verschillende oplossingen omdat $p_i$ oneven is voor elke $i$. Lopen we alle keuzemogelijkheden voor de $\pm$-tekens af, dan zien we dat het stelsel $2^t$ oplossingen heeft. Via de Chinese reststelling geldt dat ook het oorspronkelijke stelsel $2^t$ oplossingen heeft.

2. (a) (1 pt) Voor welke oneven priemgetallen $p$ is 3 een kwadraatrest modulo $p$? (geef een afleiding met behulp van kwadratische wederkerigheid).
*Oplossing*: We nemen aan dat $p > 3$. $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. Er geldt $\left(\frac{p}{3}\right) = 1$ als $p \equiv 1(\text{mod } 3)$ en $\left(\frac{p}{3}\right) = -1$ als $p \equiv -1(\text{mod } 3)$. Blijkbaar hangt $\left(\frac{3}{p}\right)$ af van $p(\text{mod } 12)$. We gaan de gevallen na:
   - $p \equiv 1(\text{mod } 12) \Rightarrow \left(\frac{3}{p}\right) = 1 \cdot 1 = 1$
   - $p \equiv 5(\text{mod } 12) \Rightarrow \left(\frac{3}{p}\right) = 1 \cdot (-1) = -1$
   - $p \equiv -5(\text{mod } 12) \Rightarrow \left(\frac{3}{p}\right) = -1 \cdot 1 = -1$
   - $p \equiv -1(\text{mod } 12) \Rightarrow \left(\frac{3}{p}\right) = (-1) \cdot (-1) = 1$

   Dus 3 is een kwadraatrest modulo $p$ precies dan als $p \equiv \pm 1(\text{mod } 12)$.

Zij $p > 3$ een priemgetal zó dat $q = 4p + 1$ ook priem is.

(b) (1/2 pt) Bewijs dat 3 geen kwadraatrest modulo $q$ is.
*Oplossing*: Als $p = 1 + 3k$ geldt $q = 12k + 5 \equiv 5 (\text{mod } 12)$ en als $k = 2 + 3k$ geldt $q = 12k + 9$. In het laatste geval kan $q$ niet priem zijn, in het eerste geval is 3 geen kwadraatrest modulo $q$ (want $q \equiv 5 (\text{mod } 12)$).

(c) (1/2 pt) Bewijs dat 3 een primitieve wortel modulo $q$ is.
*Oplossing*: De orde van 3 deelt $\phi(q) = q - 1 = 4p$. De mogelijke ordes zijn dus $1, 2, 4, p, 2p, 4p$. Voor de eerste drie gevallen geldt $3^4 \equiv 1 (\text{mod } q)$. Dus $q|81 - 1$ en dus $q = 2$ of 5. Beiden zijn niet van de vorm $4p + 1$ met $p$ priem. Orde $p$ of $2p$ impliceert $3^{2p} \equiv 1 (\text{mod } q)$. Dit kan herschreven worden als $3^{(q-1)/2} \equiv 1 (\text{mod } q)$. Volghens de stelling van Euler volgt hieruit dat 3 een kwadraatrest modulo $q$. Dit is in tegenspraak met het voorgaande onderdeel. De enige orde die overblijft is $4p$ en dus is 3 primitieve wortel modulo $q$.

3. Beschouw de vergelijking $x^2 + y^2 = z^3$ in $x, y, z \in \mathbb{Z}$.

(a) (1 pt) Laat zien dat er oneindig veel oplossingen zijn met $x, y, z > 0$.
*Oplossing*: Hiervoor zijn diverse mogelijkheden:

$$x = a(a^2 + b^2),\ y = b(a^2 + b^2),\ z = a^2 + b^2$$

met $a, b \in \mathbb{Z}_{>0}$ willekeurig. Of speciale gevallen daarvan, zoals

$$x = 2^{3k+1},\ y = 2^{3k+1},\ z = 2^{2k+1}$$

waarin $a = b = 2^k$ genomen is.

(b) (1 pt) Laat zien dat er oneindig veel oplossingen zijn met $x, y, z > 0$ en $\text{ggd}(x, y) = 1$.
*Oplossing*: Een derde mogelijkheid begint met de identiteit $(a+bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i$ waarvan we de norm kunnen nemen:

$$(a^2 + b^2)^3 = (a^3 - 3ab^2)^2 + (3a^2b - b^3)^2.$$

We moeten nu $a, b$ geschikt kiezen. In ieder geval kiezen we $a, b$ Er zijn hier vele mogelijkheden voor. Laten we voor het gemak $b = 1$ nemen. Stel $p$ is een deler van $a^3 - 3a$ en $3a^2 - 1$. Dus $3a^2 \equiv 1 (\text{mod } p)$. Vullen we dit in $3a^3 - 9a \equiv 3(a^3 - 3a) \equiv 0 (\text{mod } p)$ in, $a - 9a \equiv 0 (\text{mod } p)$. En dus $p|8a$. Hieruit volgt $p = 2$ of $p|a$. Dat laatste kan niet, want $p|(3a^2 - 1)$. Dus $p = 2$ is de enig mogelijke gemeenschappelijke deler. Kiezen we nu $a$ even dan zien we dat $a^3 - 3a$ even is en $3a^2 - 1$ oneven is. Dus de ggd is 1 in dit geval. Er zijn oneindig veel keuzen voor $a$.

4. (a) (1 pt) Bepaal de kettingbreuk van $\sqrt{19}$.
*Oplossing*: Het blijkt: $\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$ (rekenwerk).

(b) (1/2 pt) Bepaal een niet-triviale oplossing (dwz $y > 0$) van $x^2 - 19y^2 = 1$ in $x, y \in \mathbb{N}$.
*Oplossing*: We bepalen $[4, 2, 1, 3, 1, 2] = 170/39$. Dus $170^2 - 19 \cdot 39^2 = \pm 1$. Narekenen (of modulo 10 kijken) levert dat we $170^2 - 19 \cdot 39^2 = 1$ hebben.

(c) (1/2 pt) Bepaal $\alpha \in \mathbb{R}$ zó dat $\alpha$ de zuiver periodieke kettingbreuk $[\overline{1, 2, 1}]$ heeft.
*Oplossing*: Uit het gegeven volgt dat

$$\alpha = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\alpha}}}.$$

De rechterkant uitwerken:

$$\alpha = \frac{4\alpha + 3}{3\alpha + 2}.$$

Dit geeft $\alpha(3\alpha + 2) - (4\alpha + 3) = 3\alpha^2 - 2\alpha - 3 = 0$. Oplossing: $\alpha = \frac{2 \pm \sqrt{40}}{6} = \frac{1 \pm \sqrt{10}}{3}$. Omdat $\alpha > 0$ moeten we het plusteken kiezen.

5. Een machtrijk getal is een natuurlijk getal $n > 1$ zó dat alle priemfactoren van $n$ tot de macht 3 of hoger in de ontbinding voorkomen.

Laat zien dat het abc-vermoeden het bestaan van een constante $c > 0$ impliceert zó dat voor elk opeenvolgend tweetal machtrijke getallen $x > y$ geldt:

$$x - y > cx^{1/6}.$$

Geef eerst de afleiding voor die gevallen waarin $\text{ggd}(x, y) = 1$ (3/2 pt), bewijs daarna de ongelijkheid in het algemeen (1/2 pt).
*Oplossing*: We doen eerst het geval $\text{ggd}(x, y) = 1$. Stel $k = x - y$. Het abc-vermoeden toegepast op $a = k, b = y, c = x$ geeft $x < c(\epsilon)N(xyk)^{1+\epsilon}$. Omdat $x, y$ machtrijk zijn, geldt $N(xy) \leq (xy)^{1/3}$. Dus we vinden:

$$x < c(\epsilon)(xy)^{(1+\epsilon)/3}k^{1+\epsilon} \leq c(\epsilon)x^{2(1+\epsilon)/3}k^{1+\epsilon}$$

Omdat $y < x$. Kies nu $\epsilon = 1/5$ en stel $\gamma = c(1/5)$. We vinden, $x < \gamma x^{12/15}k^{6/5}$, waaruit volgt $x^{1/5} < \gamma k^{6/5}$ en na het nemen van de (5/6)-de macht, $\gamma^{-5/6}x^{1/6} < k$.

Stel nu, dat $d = \text{ggd}(x, y)$. Pas abc toe op $a = k/d, b = y/d$ en $c = x/d$. We krijgen $x/d < c(\epsilon)N(xyk/d^3)^{1+\epsilon}$. Merk op dat $N(xyk/d^3) \leq N(xy(k/d)) \leq (xy)^{1/3}k/d$. Dus, $x/d < c(\epsilon)x^{2(1+\epsilon)/3}(k/d)^{1+\epsilon}$. Vermenigvuldigen met $d^{1+\epsilon}$ levert $x \leq xd^{\epsilon} < c(\epsilon)x^{2(1+\epsilon)/3}k^{1+\epsilon}$. De rest gaat hetzelfde als boven.