Opgelet: er is een apart multiple-choice gedeelte op de laatste bladzijde (vraag 4). Schrijf op dat blad je naam en lever het mee in met je overige tentamenkopij!

1. Project Gehele Getallen.

Herinner de axioma's voor optelling en vermenigvuldiging in $\mathbb{Z}$:

- **(A1)** Optelling is associatief: $(x+y)+z=x+(y+z)$
- **(A2)** Neutraal element 0: $x+0=0+x=x$
- **(A3)** Tegengestelde: Bij iedere x bestaat een tegengesteld element x' zo dat $x+x'=x'+x=0$
- **(A4)** Optelling is commutatief: $x+y=y+x$
- **(A5)** Distributieve wet: $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
- **(A6)** Vermenigvuldiging is associatief: $(x\cdot y)\cdot z=x\cdot(y\cdot z)$
- **(A7)** Neutraal element 1: $x\cdot 1=1\cdot x=x$
- **(A8)** Vermenigvuldiging is commutatief: $x\cdot y=y\cdot x$
- **(A9)** Wet van nuldelers: Als $x\cdot y=0$ dan is $x=0$ of $y=0$

(a) Algemene kennis.

(i) Wat zegt de "gelijkheidsregel" (ook wel "vervangingsregel" genoemd)?

In een formule mag men een deelformule door een gelijke deelformule vervangen.

(ii) Geef een voorbeeld van deze regel.

Gegeven $x=y$ volgt $x+z=y+z$ wanneer je in de (ware) formule $x+z=x+z$ de rechter 'x' vervangt vervangt door de gelijke y.

(b) Formuleer en bewijs een van de "schrapwetten". Geef daarbij aan welke van de axioma's gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.

Linker Schrapwet: $x+y=x+z\rightarrow y=z$.

Neem aan dat $x+y=x+z$. Volgens A3 bestaat bij x een x' met $x'+x=0$. Dan geldt:

$y=0+y$ A2

$=(x'+x)+y$ gelijkheidsregel: $x'+x=0$ gegeven via A3

$=x'+(x+y)$ A1

$=x'+(x+z)$ gelijkheidsregel: $x+y=x+z$ gegeven

$=(x'+x)+z$ A1

$=0+z$ gelijkheidsregel: $x'+x=0$ gegeven via A3

$=z.$ A2

(c) Leid af uit (b) dat bij iedere $z\in\mathbb{Z}$ een unieke tegengestelde bestaat ("$-z$" genoteerd).

Het bestaan van tegengestelden wordt in axioma A3 verzekerd. We tonen de uniciteit aan: als $z+y_1=0$ en $z+y_2=0$ dan is $y_1=y_2$. Neem aan dat $z+y_1=0$ en $z+y_2=0$. Dan is $z+y_1=z+y_2$ (gelijkheidsregel). Uit de schrapwet (cf. onderdeel (a)) volgt nu $y_1=y_2$.

(d) Toon aan dat $z\cdot 0 = 0$. Geef daarbij aan welke van de axioma's gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.

We berekenen met A2, A2, A5:

$$0 + z\cdot 0 = z\cdot 0 = z\cdot(0+0) = z\cdot 0 + z\cdot 0.$$

De tweede gelijkheid is een toepassing van de gelijkheidsregel met $0 = 0+0$ Uit de schrapwet volgt nu dat $0 = z\cdot 0$.

2. Rekenen modulo $m \geq 2$

(a) Algemene kennis.

(i) Wat bedoelt men met: "reductie van een getal modulo m"?

Het omrekenen van een getal naar zijn rest modulo m (bijvoorbeeld, via het delingsalgoritme). Bij een rest $r > m/2$ gebruikt men soms het negatieve getal $r - m$ omdat het dichter bij 0 ligt.

(ii) Reduceer modulo 34: $38 + 15\cdot 103$ (*mod* 34).

Vervang elk getal door de standaard representant van zijn klasse (reductie modulo 34). Het resultaat modulo 34 moet hetzelfde zijn.

$$38 + 15\cdot 103 \equiv 4 + 15\cdot 1 \equiv 19.$$

(b) Los het volgende stelsel vergelijkingen op. $\bar{6}\cdot x + y = \bar{1}$ en $\bar{2}\cdot x + \bar{2}\cdot y = -\bar{2}$ (modulus 8).

Eliminatiemethode: (2)-(1): $-\bar{4}x + y = -\bar{3}$ en dus $y = -\bar{3} + \bar{4}x$ (3). Gelijkheid (3) in (1): $\bar{6}x - \bar{3} + \bar{4}x = \bar{1}$. Dit geeft $\bar{2}x = \bar{4}$. Nu heeft $\bar{2}$ geen inverse modulo 8. Handmatig oplossen:

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}x$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$

Dit geeft twee mogelijkheden:
$x = \bar{2}$: dan is $y = -\bar{3} + \bar{8} = \bar{5}$.
$x = \bar{6}$: dan is $y = -\bar{3} + \overline{24} = \bar{5}$.
Invullen in het gegeven stelsel: beide paren voldoen.

N.B.: De matrixmethode werkt niet, want de determinant van het stelsel is $\bar{2}$. Dit element heeft geen inverse restklasse.

(c) Gegeven is dat $ggd(a, m) = d$. In dit onderdeel bekijken we de volgende congruentievergelijking in de onbekende $x \in \mathbb{Z}$:

$$a\cdot x \equiv b \,(mod\, m).$$

Toon aan dat de vergelijking een oplossing heeft als $d \mid b$.

Neem aan dat d|b. Een oplossing x moet voldoen aan m|ax-b. Dat betekent dat een gehele k bestaat met mk=ax-b. Dit geeft (m/d)k=(a/d)x-(b/d), anders gezegd: (m/d) deelt het verschil (a/d)x-(b/d), en dus (a/d)x≡(b/d) (mod (m/d)). Maar ggd(a/d,m/d)=1 (opgave 4.9(b)) en dus is de vorige vergelijking oplosbaar in x via de inverse restklasse van a/d. Deze bestaat op grond van stelling 4.§7.

3. Diversen.

(a) Algemene kennis.

(i) Wat is een priemrestklasse modulo m?

Een priemrestklasse modulo m is een restklasse modulo m die een representant heeft welke relatief priem is met m. Equivalent: het is een restklasse die een inverse restklasse heeft modulo m.

(ii) Wat is de Euler ϕ-functie?

Het is een functie van type $\mathbb{N}\to\mathbb{N}$ die bij gegeven $m\in\mathbb{N}$ als waarde geeft: het aantal getallen x met $1\le x\le m$ die relatief priem zijn met m (voor $m:=1$ geeft dit 1). Anders gezegd: $\phi(m)$ is het aantal priemrestklassen modulo m.

(iii) Wat zegt de Stelling van Euler over machten van een geheel getal?

Gegeven een modulus $m\ge 2$ en een geheel getal a met $ggd(a,m)=1$, is $a^{\phi(m)}\equiv 1\,(mod\,m)$.

(b) Geef (zonder bewijs) twee belangrijke formules waarmee je in principe $\phi(z)$ kan berekenen voor elke $z\in\mathbb{N}$. Bereken hiermee $\phi(360)$ en $\phi(6!)$ (zes faculteit).

1. Als $ggd(m,n)=1$, dan is $\phi(m\cdot n)=\phi(m)\cdot\phi(n)$.

2. Als p een priemgetal is en $e\ge 1$ geheel, dan is $\phi(p^e)=p^e-p^{e-1}=p^e(1-1/p)$.

Hiermee berekenen we:

$360=2^3\cdot 3^2\cdot 5$, dus $\phi(360)=\phi(8)\cdot\phi(9)\cdot\phi(5)=(8-4)\cdot(9-3)\cdot 4=96$.

$\phi(6!)=\phi(2^4\cdot 3^2\cdot 5)=\phi(2^4)\cdot\phi(3^2)\cdot\phi(5)=(16-8)\cdot(9-3)\cdot 4=192$.

(c) Bereken, met toelichting, $16^{213}\,(mod\,21)$. (Eventuele resultaten mogen worden gebruikt zonder bewijs.)

Merk eerst op dat $ggd(16,21)=1$ en $\phi(21)=12$, dus de Euler stelling kan worden gebruikt: $16^{12}\equiv 1\,(mod\,21)$. Verder is $213=12\cdot 17+9$, dus

$16^{213}=(16^{12})^{17}\cdot 16^9\equiv 16^9$.

Daarbij is $9=(1001)_2$ met instructiecode 1001 -> 1s0s0s1 -> xs0s0sx -> xsssx.
Dat geeft:

	x	s	s	s	x
1	16	25	16	25	64
	≡-5	≡4	≡-5	≡4	≡1

Resultaat: $16^{213}\equiv 1\,(mod\,21)$.

Normering:

1a	4	2a	4	3a	6	4	24
1b	6	2b	9	3b	8		
1c	6	2c	9	3c	8		
1d	6						
	22		22		22		24

Cijfer = Totaal/10 + 1

Multiple choice gedeelte: -5 ptn per foute keuze.

4. Multiple-choice gedeelte

- Bij iedere vraag is precies één van de onderdelen juist én (meest) volledig.
- Het antwoord (aangekruist of zwartgemaakt bolletje) hoeft niet te worden toegelicht.

4.1. De Zeef van Eratosthenes is een algoritme om
- **o** alle positieve getallen < m te vinden die relatief priem zijn met m (waar $m \geq 2$).
- **o** alle positieve delers van een getal m te vinden.
- **o** alle priemgetallen < m te vinden. ☞ JA
- **o** de grootste gemene deler van twee getallen $a, b \neq 0$ te vinden.

4.2. Gegeven zijn twee vergelijkingen $x \equiv a_1 \,(mod\, m_1)$ en $x \equiv a_2 \,(mod\, m_2)$ met gehele getallen a_1, a_2 en moduli m_1, $m_2 \geq 2$. De Chinese reststelling zegt dan dat
- **o** er een unieke oplossing bestaat als $ggd(m_1, m_2) = 1$.
- **o** er een oplossing bestaat als $ggd(a_1, a_2) = 1$ en elke twee oplossingen zijn dan congruent modulo $kgv(m_1, m_2)$.
- **o** de oplossingsverzameling precies een congruentieklasse is modulo $m_1 \cdot m_2$ indien $ggd(m_1, m_2) = 1$. ☞ JA
- **o** het stelsel oplosbaar is enkel en alleen als de determinant niet nul is.

4.3. Het RSA Lemma (dat aan de basis ligt van de gelijknamige cryptografische methode) stelt dat
- **o** voor een modulus m en een geheel getal a geldt: $a^e \equiv 1$ modulo m indien $e \equiv 1$ modulo $\phi(m)$.
- **o** voor een modulus m en een geheel getal a met $ggd(a, m) = 1$ geldt: $a^e \equiv 1$ modulo m indien $e \equiv 1$ modulo $\phi(m)$.
- **o** voor een kwadraatvrije modulus m en een geheel getal a geldt: $a^{\phi(m)} \equiv 1$ modulo m.
- **o** voor een kwadraatvrije modulus m en een geheel getal a geldt: $a^e \equiv a$ modulo m indien $e \equiv 1$ modulo $\phi(m)$. ☞ JA

4.4. De orde van een element g in een eindige groep G met neutraal element e is:
- **o** het kleinste getal $k > 0$ waarvoor $g^k = e$, indien zo'n getal bestaat. ☞ JA
- **o** het grootste getal $k > 0$ waarvoor $g^k = e$, indien zo'n getal bestaat.
- **o** het rangnummer van g in de opsomming van alle elementen uit G.
- **o** het aantal elementen in G met dezelfde inverse als g.

4.5. In een groep geldt:
- **o** het neutraal element en de inverse bij een gegeven element zijn uniek. ☞ JA
- **o** het neutraal element is uniek maar de inverse bij een gegeven element is niet noodzakelijk uniek.
- **o** het neutraal element is niet noodzakelijk uniek maar de inverse bij een gegeven element is uniek.
- **o** noch het neutraal element noch de inverse bij een gegeven element zijn noodzakelijk uniek.

4.6. Een semigroep voldoet niet aan alle voorwaarden (axioma's)van een groep. Wat valt er precies weg uit de axioma's:
- **o** Het bestaan van inversen.
- **o** Het bestaan van een neutraal element en van inversen. ☞ JA
- **o** De associativiteit van de bewerking.
- **o** De stabiliteit onder de bewerking.