Uitwerking Tentamen Toegepaste Algebra, TW2560, vrijdag 21 april 2017.

K1. (a) Het aantal kolommen in de parity-check matrix van een Ham(q,r) code is $n=\frac{q^r-1}{q-1}=\frac{3^r-1}{3-1}$ (hier is q immers drie). De dimensie is $n-r$ dus $\frac{3^r-1}{3-1}-r=10$. Dat is het geval als $r=3$. Dus $n=13$, $|C|=q^k=3^{10}$ en $d=3$.

(b) Bijvoorbeeld $H=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\\1&1&0&1\\1&0&1&1\\0&1&1&1\\1&1&1&1\\0&0&0&1\end{bmatrix}$.

K2. (a) Dan moet q een macht van een priemgetal zijn waarbij 9 een deler is van $q-1$. Uit het laatste volg dat $q=10$ of $q=19$, of .... Merk op dat $q=19$ al voldoet, dat is immers een priemgetal en dus zeker een macht van een priemgetal (en 10 is geen macht van een priemgetal).

(b) Dan moet $q=2^r$ en 9 een deler van 2^r-1. Ga na dat de eerste r met deze eigenschap gelijk is aan 6 en dus dat $q=2^6=64$.

K3. (a) Dat is 5 want $125=5^3$ en dus is F_5 het kleinste deellichaam van F_{125}.

(b) 124.

(c) 3.

(d) De nulpunten zijn β^{12}, $\left(\beta^{12}\right)^5=\beta^{60}$ en $\left(\beta^{60}\right)^5=\beta^{300}=\beta^{52}$. Merk op dat $(\beta^{52})^5=\beta^{260}=\beta^{12}$ en die hadden we al. Blijkbaar zijn er drie nulpunten en is de graad van het minimaalpolynoom van β^{12} over F_5 dus gelijk aan 3.
Andere manier: bepaal de cyclotomische coset van 12 voor 5 en $5^3-1=124$: $\{12,60,300=52\}$. Deze bevat drie elementen waaruit volgt dat de graad van het minimaalpolynoom van β^{12} gelijk is aan 3.

K4. (a) Een Reed-Solomon code met parameters $q=256$ en $\delta=13$ heeft een lengte $n=256-1=255$ en een minimale afstand $d=\delta=13$. Verder is de code MDS dus $k=n-d+1=255-13+1=243$.

(b) Omdat $d=13$ is $t=6$. Een burst mag dus maximaal over zes aaneensluitende symbolen heen liggen. Een symbool bestaat uit 8 bits, dus een burst van lengte $5\cdot 8+1=41$ wordt gegarandeerd goed verbeterd.

1. (a) Nee als gevolg van de Hamming-bound.

(b) Omdat $d=2$ geldt dat twee verschiilende woorden na verwijdering van het laatst bit nog steeds verschillend zijn. Dat betekent dat $M'=M$ en dus ook $k'=k=3$. Verder is duidelijk dat $n'=6$. Als twee codewoorden op afstand 2 in het laatste bit verschillen, dan is $d'=1$, anders $d'=2$. De code C_1 met generatormatrix

$$G_1=\begin{bmatrix}1&0&0&1&0&0&0\\0&1&0&0&1&0&0\\0&0&1&0&0&1&0\end{bmatrix}$$

is een $[7,3,2]$ code waarbij verwijdering van het laatste bit een $[6,3,2]$ code oplevert (alle laatste bits van woorden uit de oorspronkelijke code zijn nul).
De code C_2 met generatormatrix

$$G_1=\begin{bmatrix}1&0&0&1&0&0&0\\0&1&0&0&1&0&0\\0&0&1&0&0&0&1\end{bmatrix}$$

is een $[7,3,2]$ code waarbij verwijdering van het laatste bit een $[6,3,1]$ code oplevert.

2. 4^5 want $x^{24}-1 = (x^8-1)^3 = (x^4-1)^3(x^4+1)^3 = (x-1)^3(x+1)^3(x^2+1)^3(x^2+x+2)^3(x^2+2x+2)^3$. Om een deler van $x^{24}-1$ te maken moet je bij elke factor besluiten of je deze 0, 1 , 2 of drie keer opneemt in de delter. Dat betekent dat er 4^5 delers zijn.
Als je de ontbinding niet ziet dan kun je ook een primitieve 3^{e} eenheidswortel α nemen (die leeft in F_{3^2} en de cyclotomische cosets maken ten opzicht van 3 en modulo 8. Dat zijn dan $\{0\}$, $\{1,3\}$, $\{2,6\}$, $\{4\}$, $\{5,7\}$. Blijkbaar bestaat de ontbinding van x^8-1 uit vijf irreducibele polynomen. Omdat $x^{24}-1 = (x^8-1)^3$ zijn er $4^5 = 1024$ cyclische codes van lengte 24 over F_3.

3. (a) C is de binaire lineaire cyclische code van lengte 9 met $g(X) = m0(X)m1(X)$ als generatorpolynoom. De dimensie van de code is dus $k = n-r$ waarbij r de graad is van g. We gaan die graad bepalen. Merk daartoe eerst op dat $m_1(x)$ het minimaalpolynoom is van 1 en dat is natuurlijk $x-1$. Voor de exponent i van de nulpunten α^i van het polynoom m_α geldt dat $i \in \{1,2,4,8,16=7,14=5\}$ (de cyclotomische coset van 1). Dat betekent dat m_α graad 6 heeft. Maar dan heeft g graad 7 zodat $r=7$. Daarmee is de dimensie van de code gelijk aan $n-r = 9-7 = 2$.

(b) De nulpunten van g zijn α^0, α^1, α^2, α^4, α^5, α^7 en α^8. Deze bevat dus het rijtje α^7, α^8, α^9, α^{10}, α^{11} (want $\alpha^9 = \alpha^0$, $\alpha^{10} = \alpha^1$, $\alpha^{11} = \alpha^2$. Het is dus de (niet narrow sense) BCH-code met parameters $n=9$, $\delta = 6$ en $b=7$ over F_2 waarbij het generatorpolynoom het kleinste gemene veelvoud is van de minimaalpolynomen van α^7, α^8, α^9, α^{10}, α^{11}.

4. (a) Omdat het databestand M in principe oncontroleerbaar is (de sleutel van bijvoorbeeld AES kan van alles zijn) zorgt toevoegen van persoonsgegevens ervoor dat het bericht, na ontsleuteling, nog een herkenbaar deel bevat. Als er onderweg met het bericht geknoeid zou zijn, dan is die herkenbare informatie niet meer leesbaar. Met andere woorden, de integriteit wordt op deze manier gewaarborgd. Verder: Alice heeft het bericht versleuteld met haar eigen geheime sleutel. Dat kan zij alleen. Dus als Bob de publieke sleutel van Alice toepast bij het ontcijferen en de leesbare persoonlijke informatie tevoorschijn komt, dan moet het bericht wel van Alice komen.

(b) Het systeem is dan onbetrouwbaar. Bob en Alice merken namelijk dat hun publieke modulus gelijk is en omdat de priemfactorontbinding uniek is, weten ze dat ze dan dezelfde priemgetallen gekozen hebben. Daarmee kunnen ze elkaars geheime sleutel bepalen en in elkaars naam berichten gaan versturen en de berichten van de ander oncijferen. Omdat Alice en Bob elkaar in principe niet hoeven te kennen, is hun veiligheid niet meer gewaarborgd.

(c) Bob: $n = pq = 5 \cdot 13 = 65$ en $\varphi(n) = 48$. Dan $e = d^{-1} = 29^{-1} \pmod{\varphi(n)}$. Euclides leert dat $-3 \cdot 48 + 5 \cdot 29 = 1$ en dat betekent dat $e = 5$.
Alice: $n = pq = 2 \cdot 11 = 22$ en $\varphi(n) = 10$. Dan $d = e^{-1} = 7^{-1} \pmod{\varphi(n)}$. Euclides of inspectie leert dat $-2 \cdot 10 + 3 \cdot 7 = 1$ en dat betekent dat $d = 3$.

(d) Stap 1: Bereken $D_{K_{privA}}(M||A) = 17^3 \pmod{22}$.
Merk op dat modulo 22 geldt dat $17 = -5$ en dus $17^3 = -5 \cdot 25 = -5 \cdot 3 = -15 = 7$.
Stap 2: Bereken $E_{K_{publB}}(17) = 7^5 \pmod{65}$.
Merk op dat modulo 65 geldt dat $7^2 = 49 = -16$ en dat $7^4 = (-16)^2 = 256 = -4$. Dus $7^5 = -28 = 37$.
Conclusie: $C_1 = 37$.

(e) Bob berekent eerst $C = C_1^{29} \pmod{65}$ en daarna $M||A = C^7 \pmod{22}$. Vervolgens checkt hij of het leesbare deel aanwezig is (in dit voorbeeld moet dat het tweede cijfer van het bericht zijn).

5. (a) Omdat n anders een Carmichael getal is.

(b) Neem $a \in A$ zo dat $a = a_0 s \pmod{n}$.Dan $a^{n-1} = (a_0 s)^{n-1} = a_0^{n-1} s^{n-1} = a_0^{n-1} \neq 1 \pmod{n}$. Dus $a \notin S$

(c) Definieer $f : S \to A \setminus S$ door $f(s) = a_0 s \pmod{n}$. Volgens onderdeel (b) is f goed gedefinieerd. Verder is f injectief. Immers: als $f(s_1) = f(s_2)$ dan $a_0 s_1 = a_0 s_2 \pmod{n}$. Omdat $a_0 \in \mathbb{Z}/n\mathbb{Z}^*$ heeft a_0 een inverse modulo n. Vermenigvuldigen met deze inverse levert dat $s_1 = s_2 \pmod{n}$.
Omdat f een injectie is, geldt dat $|S| \leq |A \setminus S|$.