Van onderstaande lijst opgaven verwacht ik, dat je er twee selecteert; één over codering en één over de overige onderwerpen. Maak deze twee opgaven, en lever uiterlijk 6 november aanstaande je werk bij mij in (Bernoulliborg kamer 396, of per email, of in mijn postvak op de vierde verdieping). We maken dan een afspraak voor een korte bespreking van je werk, en daarvoor krijg je een eindcijfer. Behalve dit, dien je ook bij Ena Tiesinga een evaluatieformulier over deze cursus te halen en ingevuld aan haar terug te geven.

(1) (De binaire Golay code.) Zie

`http://en.wikipedia.org/wiki/Binary_Golay_code`

Deze code werd onder andere rond 1980 door NASA gebruikt. Het is een cyclische $[23, 12, 7]$ code. Bewijs dat inderdaad de minimale afstand 7 is. Laat ook zien, dat dit een 'perfecte code' (zoek de definitie op bijvoorbeeld internet) is. Er bestaat nog een tweede cyclische code van lengte 23. Beschrijf ook deze.

(2) (Reed-Muller codes) Zie

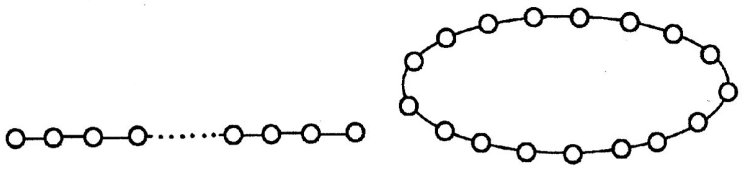
`http://en.wikipedia.org/wiki/Reed-Muller`

Het wikipedia artikel over de Reed-Muller codes is vrij compleet, inclusief de belangrijkste bewijzen. Werk het nog iets verder uit, met name de beweringen over de minimale afstand.

(3) (een rekenklus) Beschrijf zoveel mogelijk binaire cyclische codes van lengte hoogstens 12. Probeer in alle gevallen de minimale afstand te vinden. Dit is wat werk, maar met behulp van Magma is het niet moeilijk.

(4) Bereken alle gewichten die voorkomen in de codes $H(4)$ en $H(5)$.

(5) Probeer voor het spel FlipIt in de speciale gevallen van een rij punten en ook voor een kring van punten, na te gaan voor welke aantallen punten de oplossing uniek is.



Zie bijvoorbeeld

`http://www.math.rug.nl/~top/perio.pdf`

voor informatie over dit spel.

(6) Beschrijf en implementeer de Miller-Rabin priemtest, zie wikipedia en

`http://www.mat.uniroma2.it/~schoof/millerrabinpom.pdf`

(probeer met name Theorem 1.1 en het bewijs daarvan uit dit artikel te begrijpen).

(7) (Nog een priemtest: Lucas-Lehmer). De Lucas-Lehmer test is een spectaculair snelle test waarmee voor getallen van de vorm $2^n - 1$ kan worden nagegaan of het priemgetallen zijn. Alle recente records op het gebied van grote priemgetallen zijn met deze test gevonden; zie ook

`http://en.wikipedia.org/wiki/GIMPS`

Een bewijs van de Lucas-Lehmer test staat in §4.3 van het dictaat

`http://www.math.rug.nl/~top/compalg/CompAlgA.pdf`

Schrijf een verslag (incl. bewijs) over deze test en toepassingen ervan.

(8) Beschrijf en implementeer Rijndael; zie ook

`http://www.math.rug.nl/~top/compalg/CompAlgA.pdf`

(de pagina's 81 t/m 84).

(9) In Lenstra's pagina over Rijndael staat een bewering betreffende de orde van de afbeelding σ. Kan je met behulp van een software pakket deze bewering controleren? Maak hierover een verslag.

(10) Zie ook de in het college gebruikte tekst van Silverman:

`http://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf`

Gegeven een priemgetal $p > 3$. Over $\mathbb{F}_p$ nemen we de elliptische kromme $E(\mathbb{F}_p)$ behorend bij de vergelijking $y^2 = x^3 + 1$. Het punt $P = (2, 3)$ ligt op deze kromme; ga na dat $6P = \infty$.

Neem aan dat bovendien $p \equiv 2 \bmod 3$. Gebruik dit om te bewijzen dat $x \mapsto x^3 + 1$ als afbeelding van $\mathbb{F}_p$ naar $\mathbb{F}_p$ bijectief is. Gebruik dit om te bewijzen dat $E(\mathbb{F}_p)$ uit $p + 1$ elementen bestaat. Kan je, eventueel met behulp van een computer, meer zeggen over de commutatieve groep $E(\mathbb{F}_p)$ voor bijvoorbeeld

$p = 17$ en $p = 101$ en ...?

(11) Een praktisch bezwaar bij RSA is, dat decryptie, dus het berekenen van $m^d \bmod N$, en evenzo encryptie, dus het uitrekenen van $m^e \bmod N$, voor grote d, e en $n = p_1 \cdot p_2$ nogal wat tijd vergen. Experimenteer hier mee, met behulp van Maple of Mathematica, voor steeds grotere priemgetallen p_1, p_2 en paren d, e.

(12) Zie ook de in ons college gebruikte tekst over de Edwards vorm voor elliptische krommen:
`http://www.win.tue.nl/~cpeters/presentations/2008.s3cm.pdf`
Geef een voorbeeld over een niet al te klein lichaam $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, en werk de groepsstructuur uit in dit geval.