1. Leerstof

De leerstof bestaat uit de nota's en het hoorcollege met de volgende uizonderingen:

(1) Opmerking 4.5.2 is geen leerstof.
(2) §4.8 (de Montgomery vermenigvuldiging) is geen leerstof.
(3) Voorbeeld 5.2.9 is geen leerstof.
(4) §7 (het bewijs van de kwadratische wederkerigheidswet) is geen leerstof.
(5) §8.3 (het moeilijke geval) is geen leerstof.
(6) §9.5 (bit security) is geen leerstof.
(7) §10.4 (DSA) is geen leerstof.
(8) §11.8 (priemcertificaten) is geen leerstof.
(9) §12.9 (de kwadratische zeef) is geen leerstof.
(10) §13 (kettingbreuken extra's) is geen leerstof.
(11) §14.4 (dubbel periodieke functies) is geen leerstof.
(12) Enkel weten dat er formules zoals (15.1) bestaan. De formules zelf moeten niet gekend zijn.
(13) §16 (gebruik van elliptische krommen in cryptografie): lezen.
(14) §18 (het congruente getallen probleem) is geen leerstof.
(15) §19 (de j-invariant) is geen leerstof.

2. Examenvorm

Het examen bestaat uit een theorie- en een oefeningengedeelte. Het theorie examen is gesloten boek en het oefeningen examen is open boek. Eerst worden de theorievragen uitgedeeld. Na afgave van de antwoorden worden de oefeningenvragen uigedeeld. Er mag voor deze laatste gebruik gemaakt worden van de nota's en de bundel met uitgewerkte oefeningen.