Inför tentan: Följande satser ska kunna formuleras och bevisas

Tentan kommer att bestå av dels ett antal rena teoriuppgifter, dels av ett antal tillämpade uppgifter. Teoriuppgifterna kommer att hämtas från följande lista av satser som man ska kunna formulera och bevisa. Observare dock för det första att inga satser kan bevisas utan definitioner och att man ska känna till kursens samtliga definitioner. Observera också att i flera av bevisen ingår resultat från satser som inte står på listan, så det är nödvändigt att känna väl till även dessa satser även om man inte behöver kunna bevisa dem i detalj. Observera för det tredje att även en del tillämpade uppgifter kan vara av teoretisk karaktär och att det för att lösa dem kan vara värdefullt att ha snappat upp idéer från andra bevis än de från listan.

- Det finns oändligt många primtal.
- $\sqrt{2}$ är ett irrationellt tal.
- Binomialsatsen.
- Enkel sats om sannolikhetsmått: (a) $P(A') = 1 - P(A)$, (b) $P(\emptyset) = 0$, (c) $A \subseteq B \Rightarrow P(A) \leq P(B)$, (d) $0 \leq P(A) \leq 1$, (e) $A_1, A_2, \ldots, A_m$ disjunkta $\Rightarrow P(\cup_{i=1}^m) = \sum_{i=1}^m P(A_i)$, (f) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.
- $a|b$ och $a|c \Leftrightarrow a|nb + mc$ för alla $m, n \in \mathbf{Z}$.
- Utökade Euklides algoritm: Häri ingår förutom själva algoritmens konstruktion dels att kunna visa att det man får är $sgd(a, b)$, dels att visa hur man hittar heltal u och v så att $au + bv = sgd(a, b)$, dvs Bezouts identitet.
- Artimetikens fundamentalsats.
- $a \equiv b \bmod n$ och $c \equiv d \bmod n \Rightarrow a + c \equiv b + d \bmod n$ och $ac \equiv bd \bmod n$.
- Kinesiska restsatsen.
- Eulers sats.