Kunnskap for en bedre verden

Institutt for matematiske fag

# Eksamensoppgave i **MA1301/MA6301 Tallteori**

**Faglig kontakt under eksamen:** Øystein Skartsæterhagen

**Tlf:** 95 92 55 96

**Eksamensdato:** 28. november 2016

**Eksamenstid (fra–til):** 09:00–13:00

**Hjelpemiddelkode/Tillatte hjelpemidler:** D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt. (Casio fx-82ES PLUS, Casio fx-82EX, Citizen SR-270X, Citizen SR-270X College, Hewlett Packard HP30S)

**Annen informasjon:**
Prøven består av ti oppgaver (1, 2, 3, 4a, 4b, 5, 6, 7, 8, 9). Hver av disse teller like mye. Alle svar må begrunnes.

**Målform/språk:** bokmål

**Antall sider:** 1

**Antall sider vedlegg:** 0

**Kontrollert av:**

| **Informasjon om trykking av eksamensoppgave** | |
|---|---|
| **Originalen er:** | |
| **1-sidig** ☒ | **2-sidig** ☐ |
| **sort/hvit** ☒ | **farger** ☐ |
| **skal ha flervalgskjema** ☐ | |

Dato Sign

Merk! Studenter finner sensur i Studentweb. Har du spørsmål om din sensur må du kontakte instituttet ditt. Eksamenskontoret vil ikke kunne svare på slike spørsmål.

**Oppgave 1** Finn alle heltallsløsninger av likningen $943x + 299y = 115$.

**Oppgave 2** Løs kongruenslikningen $34^{143} \cdot x \equiv 2 \pmod{13}$.

**Oppgave 3** Du skal lage et RSA-nøkkelpar. Du velger $p = 89$ og $q = 157$ som de to hemmelige primtallene, og $e = 5$ som krypteringseksponent. Regn ut dekrypteringseksponenten $d$. Skriv opp tallene som utgjør den offentlige nøkkelen og tallene som utgjør den private nøkkelen.

**Oppgave 4** La $m$ og $n$ være to naturlige tall som er relativt primiske.

**a)** La $k$ være et heltall. Vis at hvis $m \mid k$ og $n \mid k$, så følger det at $mn \mid k$.

**b)** La $a$ og $b$ være heltall. Vis at $a \equiv b \pmod{mn}$ hvis og bare hvis $a \equiv b \pmod{m}$ og $a \equiv b \pmod{n}$.

**Oppgave 5** Finn alle heltall $x$ mellom 0 og 1000 som er løsninger av likningssystemet

$$\begin{cases} 17x \equiv 19 \pmod{4} \\ 3x \equiv 28 \pmod{7} \\ x \equiv 14 \pmod{9} \\ x \equiv 11 \pmod{12} \end{cases}$$

**Oppgave 6** Skriv $\sqrt{72}$ som en uendelig kjedebrøk

$$[a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$$

Finn et rasjonalt tall $\frac{a}{b}$ som er en tilnærming til $\sqrt{72}$ ved å regne ut den tredje konvergenten $C_3 = [a_0; a_1, a_2, a_3]$ av denne uendelige kjedebrøken.

**Oppgave 7** Finn ordenen til 4 modulo 27, og finn det minste naturlige tallet $x$ slik at

$$4^{65x+39} \equiv 4^{107} \pmod{27}$$

**Oppgave 8** La $m$ og $n$ være naturlige tall slik at $m \mid n$. La $a$ være et heltall som har orden $k$ modulo $m$ og orden $l$ modulo $n$. Vis at $k \mid l$.

**Oppgave 9** La $m$ være et naturlig tall. Vis at $m = 2 \cdot \varphi(m)$ hvis og bare hvis det finnes et naturlig tall $n$ slik at $m = 2^n$.