NTNU
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: 21. desember 2017

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:
Eksamenen består av ti oppgaver (1, 2, 3, 4, 5a, 5b, 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

Oppgave 1 Finn alle heltallsløsninger av likningen $710x + 205y = 15$ som oppfyller ulikhetene $-200 < y < 200$.

Oppgave 2 Hva sier Eulers teorem? Regn ut 134^{36362} mod 675.

Oppgave 3 Vis ved induksjon at $\sum_{i=1}^{n} F_i = F_{n+2} - 1$ for alle naturlige tall n.

(Husk at F_n står for det n-te fibonaccitallet: $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, osv.)

Oppgave 4 Alice har et RSA-nøkkelpar der den private nøkkelen er:

$$(p, q, d) = (37, 53, 41)$$

Hun mottar meldingen $c = 310$. Dekrypter denne meldingen.

Oppgave 5

a) La a og b være heltall. Finn alle løsninger av likningssystemet

$$\begin{cases} x \equiv a \pmod{97} \\ x \equiv b \pmod{101} \end{cases}$$

b) Finn en invers til 96! modulo 9797.

Oppgave 6 Finn alle primitive pytagoreiske tripler (x, y, z) der $x = 152$.

Oppgave 7 La $p > 2$ være et primtall, og t et naturlig tall. Finn ordenen til $(p-1)$ modulo p^t.

Oppgave 8 La n være et naturlig tall. Vis at det finnes et naturlig tall m slik at $n \mid \varphi(m)$.

Oppgave 9 La p og q være primtall slik at $p \not\equiv 1 \pmod{q}$, og la a være et heltall. Vis at likningen $x^q \equiv a \pmod{p}$ har en løsning, og at løsningen er entydig modulo p.