NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **MA1301 Tallteori**

Faglig kontakt under eksamen: Kristian Seip

Tlf: 911 29 136

Eksamensdato: 25. november 2020

Eksamenstid (fra–til): 09:00–13:00

Hjelpemiddelkode/Tillatte hjelpemidler: A: Alle trykte og håndskrevne hjelpemidler tillatt. Alle kalkulatorer tillatt.

Annen informasjon:
Denne prøven består av 10 delpunkt som alle teller like mye. I og med at alle hjelpemidler er tillatt, er det viktig at svarene på oppgavene er godt begrunnet.

Målform/språk: bokmål

Antall sider: 1

Antall sider vedlegg: 0

Kontrollert av:

Dato Sign

Oppgave 1 Bruk Euklids algoritme til å finne $\gcd(567, 417)$ og alle heltall x og y slik at $567x + 417y = \gcd(567, 417)$.

Oppgave 2

a) Finn det siste sifferet i p^{2020} for alle odde primtall p.

b) Hvilken rest får vi når vi deler 5^{2020} på $7^2 \cdot 13$?

c) Hvilken rest får vi når vi deler $7 \cdot (76!)$ på 79?

Oppgave 3 I et RSA-krypteringssystem er den offentlige krypteringsnøkkelen

$$\{n, e\} = (143, 11).$$

Finn den hemmelige dekrypteringsnøkkelen, og dekrypter deretter den krypterte meldingen 5.

Oppgave 4

a) Hvor mange tall mellom 1 og 66 har orden 22 modulo 67?

b) Det oppgis at 2 er en primitiv rot til 19. Bruk denne informasjonen til å vise at også 13 er en primitiv rot til 19.

Oppgave 5 Det finnes kun ett primtall p slik at også $p^2 + 20$ er et primtall. Bevis denne påstanden, og finn dette ene primtallet.

Oppgave 6 La p og q være to odde primtall. Anta at den kvadratiske kongruensen

$$x^2 \equiv p \pmod{q}$$

har en løsning. Under hvilken betingelse på p og q vil den kvadratiske kongruensen

$$x^2 \equiv q \pmod{p}$$

også ha en løsning?

Oppgave 7 For $n \geq 1$ er $\tau(n)$ er definert som antall positive divisorer til n. Finn det minste tallet n slik at $\tau(n) = 2020$. (Det holder å skrive ned primtallsfaktoriseringen av n.)