NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **MA1301/MA6301 Tallteori**

Faglig kontakt under eksamen: Petter Andreas Bergh

Tlf: 92032532

Eksamensdato: 15. august 2019

Eksamenstid (fra–til): 09:00–13:00

Hjelpemiddelkode/Tillatte hjelpemidler: Kode D (bestemt enkel kalkulator).

Annen informasjon:
Alle svar skal begrunnes.

Målform/språk: bokmål

Antall sider: 2

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 løsningene til den diofantiske ligningen $72x - 244y = 60$.

Oppgave 2 Definer Eulers φ-funksjon. Hva sier Eulers teorem? Hva får vi til rest når vi deler tallet $121^{24000002} - 66$ på 525?

Oppgave 3 Finn alle løsningene til systemet

$$\begin{aligned} x &\equiv -7 \pmod 8 \\ 5x &\equiv 1 \pmod 3 \\ x &\equiv -2 \pmod 5 \end{aligned}$$

Oppgave 4 Vis at ethvert oddetall kan skrives som differansen mellom to kvadrattall: hvis n er et oddetall, så finnes to heltall a, b med $n = a^2 - b^2$.

Oppgave 5 La n være et naturlig tall og a et heltall med $\gcd(a, n) = 1$. Hva mener vi med ordenen til a modulo n? Hvis k er ordenen til a modulo n, vis at

$$a^t \equiv 1 \pmod n \iff k|t$$

Oppgave 6 For hvilke tall $a \in \{1, 2, \ldots, 12\}$ er den kvadratiske kongruensen

$$x^2 \equiv a \pmod{13}$$

løsbar? Regn ut summen

$$\sum_{a=1}^{12} \left(\frac{a}{13}\right) = \left(\frac{1}{13}\right) + \left(\frac{2}{13}\right) + \cdots + \left(\frac{12}{13}\right)$$

hvor $\left(\frac{a}{13}\right)$ betegner Legendre-symbolet.

Oppgave 7

a) I et RSA-kryptosystem er den offentlige krypteringsnøkkelen $\{n, e\}$ gitt ved $n = 209$ og $e = 49$. Finn den hemmelige dekrypteringseksponenten d.

b) Anta vi har konstruert et RSA-kryptosystem med offentlig krypteringsnøkkel $\{n, e\}$, hemmelig dekrypteringsnøkkel $\{n, d\}$, og la M være en melding (dvs. et tall). Forklar hvorfor $(M^e)^d \equiv M \pmod{n}$, dvs. når vi krypterer M og deretter dekrypterer den krypterte meldingen, får vi M tilbake. Du kan bruke uten bevis at dersom m er et kvadratfritt naturlig tall (dvs. m er et produkt av ulike primtall), så er $a^{k\varphi(m)+1} \equiv a \pmod{m}$ for alle heltall a og $k \geq 1$.

Oppgave 8 La p være et primtall.

a) Vis at p deler binomialkoeffisienten $\binom{p}{i}$ dersom $1 \leq i \leq p-1$. Hint: se på produktet

$$\binom{p}{i} \cdot (p-i)! \cdot i!$$

b) Vis ved induksjon at $a^p \equiv a \pmod{p}$ for alle $a \geq 1$.