NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **MA1301/MA6301 Tallteori**

Faglig kontakt under eksamen: Øystein Skartsæterhagen

Tlf: 95925596

Eksamensdato: 20. august 2016

Eksamenstid (fra–til): 09:00–13:00

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

Annen informasjon:
Dette eksamensettet har 10 deloppgaver som alle vektes likt. Les oppgavene godt; mange av deloppgavene har flere spørsmål.

Alle svar må begrunnes godt. En delvis løsning er mye bedre enn ingenting!

Du kan skrive med både penn og blyant, men husk at dersom du visker, så ødelegger du din egen kopi.

Lykke til!

Målform/språk: bokmål

Antall sider: 2

Antall sider vedlegg: 0

Kontrollert av:

Dato Sign

Oppgave 1 La p være et primtall. Vis at $\sqrt{p}$ er et irrasjonalt tall. Med andre ord, vis at $pb^2 = a^2$ ikke har heltallige løsninger (a, b).

Oppgave 2 Vis at

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} = \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} \geq \sqrt{n},$$

for alle $n \geq 1$.

Oppgave 3 Finn alle løsninger av ligningssystemet

$$\begin{aligned} 4x &\equiv 0 \pmod 2 \\ x &\equiv -1 \pmod 5 \\ 3x &\equiv 1 \pmod 7. \end{aligned}$$

Hva er det minste heltallet $x \geq 0$ som løser systemet?

Oppgave 4 Du har satt opp RSA ved å velge $n = 13 \cdot 17 = 221$, og valgt krypteringsnøkkel $(n, e) = (221, 5)$.

a) Finn dekrypteringsnøkkelen (n, d).

b) Kryptér meldinga $m = 5$.

Oppgave 5 Vis at 3 er en primitiv rot modulo 14. Hvor mange primitive røtter modulo 14 finnes det?

Oppgave 6 Produktet av to forskjellige primtall p og q er $pq = 35143$. I tillegg er $\varphi(pq) = 34720$. Finn primtallsfaktorene p og q.

Oppgave 7 La $n \geq 1$ være et naturlig tall.

a) Anta at både $2^n - 1$ og $2^n + 1$ er primtall. Vis at da er $n = 2$.

b) Vis at dersom $2^n + 1$ er et primtall, så er $n = 2^k$ for en eller annen $k \geq 0$. (Hint: Bevis det kontrapositive; det vil si, anta at n ikke er på form 2^k, så det finnes et odde primtall p slik at $n = pm$. Regn modulo $2^m + 1$ for å vise at $2^n + 1$ er et sammensatt tall.)

Oppgave 8 La (x, y, z) være et primitivt pytagoreisk trippel (som betyr at $x, y, z \geq 1$, $\gcd(x, y, z) = 1$ og $x^2 + y^2 = z^2$). Vis at $x + y$ og $x - y$ er kongruente til 1 eller -1 modulo 8. (Hint: Skriv x og y ved hjelp av parametriseringa. Hvilke rester av a^2 er mulige modulo 8?)