Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt : Petter Andreas Bergh
Telefon: 92032532

Eksamen i MA1301 Tallteori

Bokmål
Mandag 5. desember 2011
Kl. 09.00–13.00 (4 timer)

Hjelpemidler: kode D (bestemt enkel kalkulator: HP30S eller Citizen SR-270X)

Alle svar skal begrunnes.

Oppgave 1 Hva får vi til rest når vi deler 1301^{338} på 98?

Oppgave 2 Finn alle løsninger av systemet

$$\begin{aligned} 8x &\equiv 6 \pmod 7 \\ x &\equiv -3 \pmod 9 \\ 4x &\equiv -1 \pmod{13}. \end{aligned}$$

Oppgave 3 I et RSA-kryptosystem er den offentlige nøkkelen $\{n, e\} = \{187, 21\}$. Hva blir den hemmelige nøkkelen $\{n, d\}$? Krypter meldingen $M = 20$.

Oppgave 4 La $a = 77! - 1$. Finn et tall $1 < d < a$ med $d | a$.

Oppgave 5 Vis at $32 | (n^8 - 1)$ for alle oddetall $n \geq 1$.

Oppgave 6 Fibonaccifølgen $f_1, f_2, f_3, \ldots$ defineres ved

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad \text{for } n \geq 3. \end{aligned}$$

De første leddene blir $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. Vis at

$$\sum_{i=1}^{n} f_i^2 = f_n f_{n+1}$$

for alle $n \geq 1$.

Oppgave 7 La $n \in \mathbb{N}$ og $a \in \mathbb{Z}$ med $\gcd(a, n) = 1$. Hvis k er ordenen til a modulo n, vis at

$$a^t \equiv 1 \pmod{n} \quad \Leftrightarrow \quad k|t.$$

Oppgave 8

a) Vis at for et odde primtall p er kongruensen

$$x^2 \equiv -1 \pmod{p}$$

løsbar hvis og bare hvis p er på formen $4k + 1$.

b) Vis at det finnes uendelig mange primtall på formen $4k + 1$ (hint: $(2p_1 \cdots p_t)^2 + 1$).

Oppgave 9 Er kongruensen

$$x^2 + 4x \equiv 30 \pmod{31}$$

løsbar?