Matematiska Institutionen
KTH

Övningstal till Diskret Matematik CL torsdagen den 14 april

Uppvärmning.

1.

Betyget tre uppgifter.

2. Antag att du som deltagare i ett RSA-system har offentlig krypteringsnyckel $n = 35$ och $e = 7$.
a) Kryptera meddelandet 6.
b) Dekryptera de chiffrerade meddelandet 3.

3. Bestäm resten vid division av 3^{201} med 11.

4. Bestäm en minimal disjunktiv normalform till vart och ett av uttrycken nedan.
a) $xy + \overline{x}y + \overline{x}\,\overline{y}$.
b) $\overline{y}z + \overline{y}\,\overline{z}\,\overline{t} + \overline{z}t$.
c) $x + \overline{x}yz + x\overline{y}\,\overline{z}$.
d) $\overline{y}zt + xz\overline{t} + x\overline{y}\,\overline{z}$.

Betyget fyra uppgifter.

5. a) Klarar talet 341 Fermat-testet med bas 2?
b) Är 341 ett primtal?

6. Finn primtalen p och q, om $n = pq = 4386607$ och $m = (p-1)(q-1) = 4382136$.

Betyget fem uppgifter.

7. Låt p och q vara skilda primtal. Visa att

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Några svar och lite ledningar.

2. a) 6, b) 17.
3. 3.
4. a) $\overline{x} + y$, b) $\overline{y} + \overline{z}t$ c) $x\overline{z} + yz$. d) $x\overline{y} + z\overline{t} + \overline{y}zt$.
5. a) ja, b) nej.
6. $p = 1453$ och $q = 3019$ eller tvärtom.