Exercise set 7 **Number Theory**
Tuesday NOV 1 2011 at 4 pm. Sharp **in MaD-302**

1. *Prove for all odd primes p*
   a) $(p-2)! \equiv 1 \pmod{p}$.
   b) $2 \cdot (p-3)! \equiv 1 \pmod{p}$.

Hint: In a group all elements are invertible. When is $a \neq a^{-1} \in Z_p^*$*?*

2. *(jatkoa?) Prove for all odd primes p*

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \dots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

3. *Determine all quadratic residues* $\pmod{23}$. *What are their representatives of smallest absolute value?. What do you notice??*

4. *Use Euler'scriterion to determine whether 2 is a quadratic residue* $\pmod{17}$. *How about 5?*

5. *How many (non-congruent) solutions has* $x^2 \equiv 2$
   a) $\pmod{17}$
   b) $\pmod{17^2}$

   (How bout c) $\pmod{17^{100}}$*, or* d $\pmod{10}$*?) Hint: 2,2,(2,0).*

6. *Does 2 have a sqare root*
   a) *in the field* $\mathbb{Z}_{29}$
   b) *in the field* $\mathbb{Z}_{31}$
   c) *in the field* $\mathbb{Z}_{97}$
   d) *in the field* $\mathbb{Z}_{101}$
   e) *in the field* $\mathbb{Z}_{111}$?

7. *Calculate* $\left(\frac{61}{31}\right)$, $\left(\frac{33}{31}\right)$, $\left(\frac{29}{31}\right)$, $\left(\frac{8}{31}\right)$ *and* $\left(\frac{128}{821}\right)$.

8. *find* $\left(\frac{3}{17}\right)$
   a) *By Gauss's lemma*
   b) *Using Euler's criterion*
   c) *Using reciprocity*

9. *Let p be annodd prime and* $ab \equiv 1 \pmod{p}$. *Prove that if the congruence* $x^2 \equiv a \pmod{p}$ *has a solution, then also* $x^2 \equiv b \pmod{p}$ *has a solution.*