Exercise set 6 **Number Theory**
Tuesday OCT 25 2011 at 4 pm. Sharp **in MaD-302**

1. *Solve:*

a) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 5 \pmod{7} \\ x \equiv 8 \pmod{15} \end{cases}$ b) $\begin{cases} 2x \equiv 3 \pmod{9} \\ 4x \equiv 6 \pmod{10} \\ 6x \equiv 9 \pmod{11} \end{cases}$

2. *Prove by the Chinese Remainder Theorem: for all* $k \in \mathbb{N}$ *there exist* k *consequtive numbers* $a+1, \ldots, a+k$ *of which all are divisible whith some square (not necessarily the same).*

3. *Calculate* $\varphi(10)$, $\varphi(100)$ *and* $\varphi(10!)$.

4. *a) For which* n *is* $\varphi(n)$ *odd?*
b) For which n *is* $\varphi(n) = \varphi(2n)$*?*

5. *Find the orders of* 3, 7 *ja* $11 \pmod{20}$.

6. *Find alt least one primitive root modulo* 14.

7. 2 *is a primitive root modulo* 101. *Find* $ord_{101}(2^{32})$.

8. 2 *is a primitive root modulo* 19. *How many primitive roots modulo* 19 *exist? After finding out this, find all these primitive roots.*

9. *Let* r *be a primitive root modulo* m *and* $(m, a) = 1$. *Prove that the following are equivalent:*

(1) a *is a primitive root modulo* $\pmod{m}$.
(2) *For all prime factors* p *of* $\varphi(m)$*:*

$$a^{\varphi(m)/p} \not\equiv 1 \pmod{m}.$$

10. *Construct an index table for* 13. *(Compare with the given table) .*

11. *Which of the following congruences are solvable?*

a) $x^4 \equiv 17 \pmod{67}$
b) $x^4 \equiv 18 \pmod{67}$
c) $x^5 \equiv 17 \pmod{67}$

Solve them using that 2 is a primitive root $\pmod{67}$.