Exercise set 4 **Number Theory**
Tuesday OCT 11 2011 at 4 pm. Sharp **in MaD-302**

1. *Prove that*
a) no sqare ofa a n integra is of the form $4n+2$ *or* $4n+3$.
b) the product of 4 consecutive numbers is divisible by 24.
c) the product of k consecutive numbers is divisible by $k!$.

2. *Take* $x \in \mathbb{R}$, $m \in \mathbb{N}$ *ja* $p \in \mathbb{P}$.
a) Prove, that $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$
b) Prove, that $p^{\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \mid m$, *mutta* $p^{1+\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \not| m$.
c) How many zeros are at the end of tjhe decimal expansion of 169! ?
d)Prove directly from the definition that (the binoimial coefficients) $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ *are integers*

3. *Find "inverses"whenever possible*
a) for $1 \dots 10 \pmod{11}$
b) for $-12 \dots 12 \pmod{12}$

4. *Prove*

$$7 \mid n = \prod a_\mu 10^\mu \iff 7 \mid (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - \dots$$

5. *a) Write out two complete and two reduced remainder systems for* $\pmod{20}$.
b) Let $\{a_1, a_2, \dots, a_k\}$ *be a complete remainder system (tjs) modulo n. Find the smallest positive integer congruent to* $a_1 + a_2 + \cdots + a_k \pmod{n}$.
c) Let $\{a_1, a_2, \dots, a_k\}$ *be a reduced remainder system (sjs) modulo n. Find the smallest positive integer congruent to* $a_1 + a_2 + \cdots + a_k \pmod{n}$.

6. *Prove*
a) If $(m, n) = 1$, *then x goes through a t.j.s:n* $\pmod{m}$ *and y a t.j.s* $\pmod{n}$,*then the numbers* $xn + my$ *attain all posible values* $\pmod{mn}$.
b) Aivan Similarly for reduces systems.

7. **Strong pseudo primes and ja Miller's test.** *Definition: An odd non-prime n, satisfying* $n - 1 = 2^s t$, $2 \not| t$, *is a* **strong pseudo prime** *wrt. to a* (> 1) *, if either*

$$a^t \equiv 1 \pmod{n} \tag{1}$$

or

$$a^{2^j t} \equiv -1 \pmod{n} \quad \textit{jollakin } 0 \le j \le s-1. \tag{2}$$

Definition: n **passes Miller's test** *wrt. to a, if* (**??**) *tai* (**??**).

Prove that every odd prime passes Miller's test.

is a strong pseudo prim,e wrt 2 *suhteen (the smallest one). The number*

$$3215031751 = 151 \cdot 751 \cdot 28351$$

is the smallest strong pseudo prime wrt $2, 3, 5$ *jand* 7.

Thgere exist no "strong Carmichael numbers", ie Miller's test cannot fail wrt all numbers. In fact, an odd non-prime n passes Millerin testfor at most $(n-1)/4$*:lle numbers in* $[1, n-1]$.

8. *Solve* $x^2 \equiv -1 \pmod{13}$ *by Wilson.*