Exercise set 8 **Number Theory**
Tuesday NOV 8 2011 at 4 pm. Sharp **in MaD-302**

1. *Do the following "baby"example of the RSA encryption method: The secret numbers are* $p = 11$, $q = 13$*; the public numbers are* $m = pq = 143$ *and* $e = 77$.
   a) *Calculate the decoding number* d.
   b) *Encode the message 50*
   c) *Decode your message. . Hope You got the original.*
   Could You have broken the code knowing only (thee) e *and* m *? How about a real life example?*

2. *Solve exercise 4.1. in Ari Lehtonen's Finnish paper.*

3. *Wrtite in the form* $D^2 \equiv a \pmod{m}$, $D = ax + b$.
   a) $x^2 + 4x + 5 \equiv 0 \pmod{10}$
   b) $x^2 + 3x + 5 \equiv 0 \pmod{10}$
   c) $x^2 + 3x + 5 \equiv 0 \pmod{9}$
   d) $3x^2 + x + 5 \equiv 0 \pmod{9}$

4. *Let* $p \in \mathbb{P} \setminus \{2\}$ *and* $(a, p) = (b, p) = 1$. *Prove that if neither* $x^2 \equiv a \pmod{p}$ *nor* $x^2 \equiv b \pmod{p}$ *has a solkution, then* $x^2 \equiv ab \pmod{p}$ *has a solution.*

5. *Which of the following have a solution??*
   a) $x^2 \equiv 7 \pmod{101}$
   b) $x^2 \equiv -7 \pmod{101}$
   c) $x^2 \equiv 7 \pmod{303}$

6. *For which* $p \in \mathbb{P}$ *does the congruence* $x^2 \equiv -3 \pmod{3p}$ *have a solution?*

7. *Solve:*
   a) $3x + 2y = 1$
   b) $3x - 2y = 1$
   c) $6x + 4y = 2$
   d) $17x - 43y = 100$
   e) $110x - 174y = 18$

8. *Let* a, b *and* c *be positive integers and ja* $(a, b) = 1$. *Prove that the linear Diophantine equation* $ax + by = c$
   a) *has a positive solution, if* $ab < c$,
   b) *has no positive solution, if jos* $a + b > c$.

9. *Determine all primitive Pythagorean triples* (x, y, z), *with* $y = 40$. *How about non-primitive ones?*

10. *Prove that in any Pythagorean triple* (x, y, z)
    a) *at least one of the numbers* x, y, z *is divisible by 3*
    b) *at least one of the numbers* x, y, z *is divisible by 4*
    c) *at least one of the numbers* x, y, z *is divisible by 5.*