Test 2, March 27, 2006

1. Compute the following in $\mathbb{Z}_7$ if it exists (bring the end result in the range $0, \ldots, 6$. If there are multiple correct answers then it is enough to give just one answer)

   (a) -2

   (b) 3^{-1}

   (c) $-2/3$

   (d) $\sqrt{2}$

   (e) $\sqrt{-3}$

   (f) 3^{48}

2. Which of the following rings are fields: $\mathbb{Z}_2$ $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$
   (no computation is necessary here, it is enough to write down the answer).

3. In the following questions, give all solutions (not just one) (if there are no solutions, indicate that too).

   (a) Solve $x^3 + 2x + 2 = 0$ in $\mathbb{Z}_7$.

   (b) Solve $x^2 + x + 1 = 0$ in $\mathbb{F}_4$.

   (c) Solve $x^2 + x + 1 = 0$ in $\mathbb{Z}_7$.

   (d) Solve $3x + 2 = 0$ in $\mathbb{Z}_7$.

4. (a) Write down Fermat's little theorem. Let p be a prime number and let a .... Then .....

   (b) How do we use Fermat's little theorem to test if a number n is prime or not?

5. Compute 333^{-1} in $\mathbb{Z}_{1003}$. Show your steps.

6. (a) Let $n = 55$. Let $e = 17$ and let $m = 13$. Compute m^e in $\mathbb{Z}_n$. Show your computation.

   (b) If we use $n = 5 \cdot 11 = 55$ and $e = 17$ in RSA, then what is the decryption exponent d?

   (c) If the encrypted message is $c = 8$ (this is not the same as in part (a)) then the decrypted message is $m = \ldots$.