RSA Codes: Modular Arithmetic **5/12/03**

- In order to make and use RSA codes, you have to understand a few things about Modular Arithmetic. You will learn these things by doing this worksheet.
- Write your answers on a separate sheet. You may help each other, but write your own work. Remember that understanding is important. You will have to work with what you have learned in the next lessons!
- If you do not finish the work in class, please finish it at home. I will check it next lesson (on Friday, December 12).
- GOOD LUCK!!

Introduction

1. Think of a clock with 12 digits on it. If it is now 12 o'clock
   a. What time will it be six hours from now?
   b. What time will it be twelve hours from now?
   c. What time will it be twenty hours from now?
   d. What time will it be 124 hours from now?
   e. Can you give a general rule for finding the time after a certain number of hours?

2. If your clock had only six hours on it, and you start at 6 o'clock, answer the same questions as for the 12-hour clock in question 1.

Explanation:
Modular Arithmetic is sometimes also called 'clock arithmetic'.
The **modulus** stands for the number of hours that are shown on the clock.

In question 1 c we would write: $20 \bmod 12 \equiv 8$
You read this as "Twenty modulus twelve is the same as eight."
This means that twenty hours further is the same as 8 hours further if you have a clock with 12 hours on it.

3. Write your answers in question 2 in modular arithmetic form, like in the explanation above.

4. Can you find the answer to the following problems? (If you find this difficult, you can look at the general rule below. Be sure to show your work.)
   a. $14 \bmod 3 \equiv$
   b. $17 \bmod 14 \equiv$
   c. $1000 \bmod 7 \equiv$

General Rule:
To find '$a \bmod m$' you divide the number *a* by the number *m* and you calculate the remainder.
Example: To find $16 \bmod 5$, you divide 16 by 5. The remainder is 1.
So: $16 \bmod 5 \equiv 1$