Institut for Matematik og Datalogi
Syddansk Universitet, Odense

5. december 2019
JFB/RF

Eksaminatorier DM534 Uge 50

1. Is one of the following the multiplicative inverse of 49 modulo 221? Or does no multiplicative inverse exist?

   12, 56, 121, 212

2. Which of the following is a valid RSA key (ignoring the fact that the numbers are not large enough for security)?

   (a) $PK = (91, 37)$; $SK = (91, 23)$
   (b) $PK = (143, 77)$; $SK = (143, 53)$
   (c) $PK = (231, 59)$; $SK = (231, 47)$
   (d) $PK = (107, 25)$; $SK = (107, 30)$

3. In the Sieve of Eratosthenes, how many lists (including the current) have been created at the point where the number 13 is the first element in a list?

4. Consider an RSA system with Alice's public key $N = 1517$ and $e = 17$. Note that $1517 = 37 \cdot 41$.

   (a) Find Alice's secret key d. Use the Extended Euclidean Algorithm from pages 45–46 of the RSA slides used in lectures (there, e and d are called a and s (and d also is called x at top of page 46)).
   (b) Try encrypting 423. Use the algorithm for fast modular exponentiation (page 33 on the slides). How many times during the recursive execution is the "**if** k is odd" case encountered, and how many times is the "**if** k is even" case encountered? [Do not include the base cases $k = 0$ and $k = 1$ in the counts.]

(c) Decrypt the number obtained above, using fast modular exponentiation. Is the result correct? How many times during the recursive execution is the "**if** k is odd" case encountered, and how many times is the "**if** k is even" case encountered? [Do not include the base cases $k = 0$ and $k = 1$ in the counts.]

5. Why in RSA is it necessary that $gcd(e_A, (p_A - 1)(q_A - 1)) = 1$? Find an example (that is, values e_A, p_A and q_A) where this greatest common divisor is not equal to 1.

6. Try executing the Miller-Rabin primality test on 11, 15, and 561. First, what type of numbers are they (note: 561 is known from the slides)? For each, run the Miller-Rabin test for at least one value a of your own choice, preferably for more. Use e.g. Maple or a simple Java program importing the class `BigInteger` from the Java library for executing the exponentiations (first raising to a power and then using modulus should work in reasonable time for numbers this size, hence there is no need to use the fast modular exponentiation algorithm in this exercise). Which calculations showed that the composite numbers were not prime—the first line (the Fermat test) or later lines?

   With 561, be sure to try an a relatively prime to 561 (most are, 2 is a simple example). What happens differently if you try $a = 3$? Can you explain the latter?

7. Find four different square roots of 1 modulo 143, i.e., numbers which multiplied by themselves modulo 143 give 1 (and which are at least 0 and less than 143). You may consider writing a simple program for finding them.

8. [Optional] Add two of these different square roots which are not negatives of each other modulo 143 (two where adding them together does not give 143). Find the greatest common divisor of this result and 143. Subtract these same two different square roots and find the greatest common divisor of this result and 143. Think about why you get these results. (These effects are the starting point for the math behind fast primality testing algorithms.)