THE RSA ALGORITHM

DAN CIUBOTARU

1. Fermat's little theorem

(1) (Fermat's little theorem) If p is a prime number, and a is an integer such that $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(2) Use Fermat's theorem to find 3^{302} mod 5, mod 7, and mod 11.
(3) (Extension of Fermat's little theorem) If $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

(4) Compute 2^{561} mod 561 (note that 561 is not prime).

Prove the following result (it will be needed later):

Theorem. *Let p, q be two numbers (not necessarily prime) such that $\gcd(p, q) = 1$. If $a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$, then $a \equiv b \pmod{pq}$.*

Definition. *A composite integer n is called a Carmichael number if $a^{n-1} \equiv 1$ for all positive integers a such that $\gcd(a, n) = 1$.*

There exist infinitely many Carmichael numbers. Here are three examples:

(1) Prove that 561 is a Carmichael number. (In fact, this is the smallest Carmichael number). Hint: use Fermat's theorem for the prime factors of 561.
(2) Prove that 1729 is a Carmichael number.
(3) Prove that 2821 is a Carmichael number.
(4) Show that if $n = p_1 p_2 \cdots p_k$, where p_i are distinct primes that satisfy $p_j - 1$ divides $n - 1$ for $j = 1, 2, \ldots, k$, then n is a Carmichael number.
(5) Use the previous exercise to prove that any integer of the form $(6m + 1)(12m + 1)(18m + 1)$ where m is a positive integer such that $6m+1, 12m+1$, and $18m+1$ are all primes, is a Carmichael number.
(6) For example, 172947529 is a Carmichael number.

2. RSA algorithm

(1) Suppose that you chose the primes $p = 23$ and $q = 41$, and the exponent $e = 7$. Explain how the algorithm works if the other person wants to encode the message $M = 35$.
(2) Encrypt the message STOP using the RSA system with $p = 43$, $q = 59$, so that $n = 43 \cdot 59 = 2537$, and with $e = 13$.
(3) Decrypt the previous encryption using $d = 937$.
(4) With the same keys, assume you received the encrypted message 0981 0461. What is the decrypted message?
(5) You chose the primes 97 and 173 and the exponent $e = 5$. Thus you told your friend $N = 16781$ (which is pq) and $e = 5$. Your friend encodes a message (a number) for you and tells you that the encoding is 5347. What was the original message?
(6) Show that if you know n is a product of two primes p, q and you also know $(p-1)(q-1)$ then we can find easily p and q.

(D. Ciubotaru) Dept. of Mathematics, University of Utah, Salt Lake City, UT 84112
E-mail address: ciubo@math.utah.edu