

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 19.

Last time: We showed how to compute $x^k \pmod{m}$ using the method of successive squaring.

Theorem. Suppose $m = pq$ where p and q are distinct primes. Suppose that $(y, m) = 1$ and $(k, \phi(m)) = 1$. Then there is a unique solution x to

$$(*) \quad x^k \equiv y, \pmod{m},$$

and x is unique modulo m . Moreover, there is an algorithm to find x which uses the Euclidean algorithm on $k, \phi(m)$ and computation of powers of y modulo m .

Proof. Since $(k, \phi(m)) = 1$, there exist a and b such that

$$1 = ak - b\phi(m).$$

The numbers a and b can be computed using the Euclidean algorithm. Then if $(x, m) = 1$ then using Euler's theorem,

$$(x^k)^a = x^{ak} = x^{1+b\phi(m)} \equiv x \cdot (x^{\phi(m)})^b \equiv x \pmod{m}$$

Hence

$$x^k \equiv y \pmod{m} \quad \Rightarrow \quad x = y^a \pmod{m}.$$

Similarly

$$x^k \equiv y \pmod{m} \quad \Leftarrow \quad x = y^a \pmod{m}.$$

The RSA Scheme. Person A makes an encryption key for person B to use to encrypt a message which only person A can decrypt. Nobody else intercepting the message can decrypt it. We show the method in the following simplified example. We will start off being person A and we make the key. We choose two primes, say 5 and 11. In reality these should be large primes, say around 200 digits long. Set $n = 55$. We have $\phi(55) = \phi(5)\phi(11) = 4 \cdot 10 = 40$. Choose e with $(e, 40) = 1$, say $e = 3$. What we give person B is the pair of numbers $(n = 55, e = 3)$. This is the encryption key which is used to encrypt a message. Suppose now that we are person B who has been given the encryption key $(55, 3)$. We want to encrypt the word "hi". First change it into a number using numerical values which we have previously agreed upon with person A (these can be made public). For example, $a = 00, b = 01, c = 02$, etc.. Then "hi" corresponds to the number 0708. This is the number we wish to send encrypt and send to person A. Break up this number into blocks of length one digit less than the length of n . In our case these blocks have only one digit each. We have

$$0708 \rightarrow 0 \ 7 \ 0 \ 8.$$

If instead $n = 1271$, the blocks would be three digits long and we would have to add zeros at the end to make a complete block. We would have

$$0708 \rightarrow 070\ 800.$$

In reality when n has hundreds of digits, so will each block so our short message 0708 will consist of one block with lots of zeros at the end. We now encrypt each block. For our example we will just encrypt the block “7”. The rule is

$$x \rightarrow x^e \pmod{n}.$$

In our case we want to compute $7^3 \pmod{55}$. Using the method of squaring,

$$7 \equiv 7, \quad 7^2 \equiv 49, \pmod{55}$$

so $7^3 \equiv 7 \cdot 49 \equiv 7 \cdot -6 \equiv -42 \equiv 13 \pmod{55}$. We ensure each of our encrypted blocks has the same length as n , for example if we had a block “4” its encryption is $4^3 \pmod{55} = 9$ which we would write as 09. (The encrypted blocks are one digit longer than the original blocks). Our message “hi” looks like

$$**13****.$$

Now let’s be person A again. We are going to decrypt this message. We split it into blocks of length n . The second block is 13. Our Theorem tells us to write

$$1 = ef - g\phi(n)$$

and then the decrypted block will be $13^f \pmod{n}$. We will check this, but we can cheat by using 20 instead of $\phi(55) = 40$. The reason we can cheat like this is because $\phi(55) = \phi(5)\phi(11) = 4 \cdot 10$, but $[4, 10] = 20$, and so we can improve Euler’s theorem to get

$$(x, 55) = 1 \quad \Rightarrow \quad x^{20} \equiv 1 \pmod{55}.$$

Using 20, we have

$$20 = 3 \cdot 6 + 2, \quad 3 = 2 + 1,$$

so

$$1 = 3 - 2 = 3 - (20 - 3 \cdot 6) = 3 \cdot 7 - 20.$$

We can take the value of f to be 7. In order to compute a value for f , you need to be able to compute the prime factorization of n . In real life when n is several hundred digits long, nobody knows how to do this. In our example we decrypt the block 13 by computing $13^7 \pmod{55}$. Using the method of squaring, since $7 = 4 + 2 + 1$ we compute

$$13^2 = 169 \equiv 4, \quad 13^4 \equiv 4^2 \equiv 16,$$

so

$$13^7 \equiv 16 \cdot 4 \cdot 13 \equiv 64 \cdot 13 \equiv 9 \cdot 13 \equiv 117 \equiv 7 \pmod{55}.$$

We remark that the decryption can fail if we happen to have a block to encrypt which is not relatively prime to n .

Proposition. If m and n are relatively prime then $\phi(mn) = \phi(m)\phi(n)$.

Proof and proof quiz.

- Define J_m to be the set of elements $\{0, 1, 2, \dots, m-1\}$. Define I_m to be the subset of J_m containing those elements x such that $(m, x) = 1$.

- Suppose $(m, n) = 1$. Define

$$F : J_{mn} \rightarrow J_m \times J_n$$

by

$$F(x) = (x \pmod{m}, x \pmod{n}),$$

where $x \pmod{m}$ and $x \pmod{n}$ are written in the standard residue system. (Note that $x \pmod{m}$ is just the remainder when x is divided by m .)

- We claim that F has an inverse. Indeed, by the Chinese Remainder Theorem for all values of y and z we can find x satisfying

$$\begin{cases} x = y \pmod{m} \\ x = z \pmod{n} \end{cases}$$

and x is unique modulo mn . By expressing x in the standard residue system modulo mn , this means if we are given $(y, z) \in J_m \times J_n$ then there exists x which is mapped by F to (y, z) . Moreover, by the uniqueness in the Chinese remainder theorem this is unique.

- Because it has an inverse, the map F sets up a bijection between J_{mn} and $J_m \times J_n$.

- We will now show that under the bijection F , I_{mn} is mapped onto $I_m \times I_n$ and so the number of elements in these sets is the same, that is $\phi(mn) = \phi(m) \cdot \phi(n)$.

- First we show that $F(I_{mn}) \subset I_m \times I_n$. Suppose $(x, mn) = 1$ and $F(x) = (y, z)$. Then $(x, m) = 1$ and so since $x \equiv y \pmod{m}$ we have $(y, m) = 1$. Similarly $(y, n) = 1$.

- To show that $(I_m \times I_n) \subset F(I_{mn})$, suppose that $(x, y) \in I_m \times I_n$ and take the unique $x \in J_{mn}$ with $F(x) = (y, z)$. Now $(y, m) = 1$ and $(z, m) = 1$. Since $x \equiv y \pmod{m}$ we have $(x, m) = 1$ and since $x \equiv z \pmod{n}$ we have $(x, n) = 1$. Hence $(x, mn) = 1$ and $(y, z) = F(x)$ where $x \in I_{mn}$.

- Putting this together, we see that $F(I_{mn}) = I_m \times I_n$.

The proof quiz:

- (1) If A and B are sets, what is the Cartesian product $A \times B$? how many elements does it contain if A contains a elements and B contains b elements?

- (2) What does it mean for a function $f : A \rightarrow B$ to be one-to-one?
- (3) What does it mean for a function $f : A \rightarrow B$ to be onto?
- (4) What does it mean for a function $f : A \rightarrow B$ to be a bijection?
- (5) Draw pictures to illustrate the following definitions: Suppose $f : A \rightarrow B$ and $g : B \rightarrow A$ are maps. Then g is a left inverse of f if $gf(a) = a$ for all $a \in A$, and g is a right inverse of f if $fg(b) = b$ for all $b \in B$.
- (6) Show that if f has a left inverse g and a right inverse h then $g = h$, and so g is a (two sided) inverse for f .
- (7) Which of the following statements are equivalent for a function $f : A \rightarrow B$?
 - (a). f is one-to-one
 - (b). f is onto
 - (c). f is a bijection
 - (d). f has a left inverse
 - (e). f has a right inverse
 - (f). f has a (two sided) inverse