Summary on Lecture 13, May 1st, 2015

Powers and roots mod p_1p_2.

Last time we proved the following result:

Lemma 1. *Let p be a prime, and e be such that $\gcd(e,p-1)=1$, giving us d be such that $de\equiv 1 \mod (p-1)$. Then the congruence $x^e\equiv c \mod p$ has a unique solution $x=c^d \mod p$.*

Now let p_1, p_2 be distinct primes. We will analyze how to solve the equation $x^e\equiv c \mod p_1p_2$. Last time we proved the following:

Theorem 2. *Let p_1 and p_2 be distinct primes, and let $d=\gcd(p_1-1,p_2-1)$. Assume an interger a is such that $\gcd(a,p_1p_2)=1$. Then $a^{\frac{(p_1-1)(p_2-1)}{d}}\equiv 1 \mod p_1p_2$.*

Here is the resut we need:

Lemma 2. Let p_1, p_2 be distinct primes, and let $e\geq 1$ be an integer satisfying $\gcd(e,(p_1-1)(p_2-1))=1$, and let d be such that $d\cdot e\equiv 1 \mod p_1p_2$. Then the congruence $x^e\equiv c \mod p_1p_2$ has a unique solution $x=c^d \mod p_1p_2$.

Proof. For simplicity, we assume that $\gcd(c,p_1p_2)=1$. Then since $\gcd(e,(p_1-1)(p_2-1))=1$, we find d such that $d\cdot e=1+k(p_1-1)(p_2-1)$. Now we check that c^d is a solution of the congruence $x^e\equiv c \mod p_1p_2$:

$$\begin{array}{rcll}(c^d)^e & = & c^{de} & \\ & = & c^{1+k(p_1-1)(p_2-1)} & \\ & = & c\cdot\left(c^{(p_1-1)(p_2-1)}\right)^k & \\ & \equiv & c\cdot 1^k & \mod (p_1p_2) \\ & \equiv & c & \mod (p_1p_2)\end{array}$$

Now we check that such a solution is unique. Assume $x=u$ is a solution of the congruence $x^e\equiv c \mod p_1p_2$. Then that c^d is a solution of the congruence $x^e\equiv c \mod p_1p_2$:

$$\begin{array}{rcll}u & = & u^{de-k(p_1-1)(p_2-1)} & \\ & = & (u^e)^d\left(u^{(p_1-1)(p_2-1)}\right)^{-k} & \\ & = & c^d\cdot 1^{-k} & \mod (p_1p_2) \\ & \equiv & c^d & \mod (p_1p_2)\end{array}$$

The case when $\gcd(c,p_1p_2)>1$ will be given as exercise. □

Example. Let $p_1=229$, $p_2=281$, $N=p_1p_2=229\cdot 281=64,349$. We solve the congruence

$$x^{17389}\equiv 43,947 \mod 64,349$$

First, we have to solve the congruence

$$d\cdot 17,389\equiv 1 \mod 63,840,$$

where $63,840=(p_1-1)(p_2-1)=228\cdot 280$. We find $d\equiv 53,509 \text{mod } 63,840$. Then Lemma 2 gives us the solution

$$x\equiv 43,947^{53,509}\equiv 14,458 \text{mod } 64,349.$$

The RSA public key cryptosystem

Now we can describe the RSA public key cryptosystem. The term RSA is named after its inventors Ron Rivest (MIT), Adi Shamir (Weizmann Institute, Israel), Leonard Adleman (MIT). They first described this algorithm in 1977 (when all of them were in their twenties).

Assume that Bob and Alice have to exchange a sensitive information over insecure communication line. Here what they do

• Bob chooses p_1, p_2 be two large primes, $N = p_1 \cdot p_2$ and an integer e such that $\gcd(e, (p_1-1)(p_2-1)) = 1$. The pair (N, e) is a **public key** which is publicly available, in particular to an unfriendly person Eve.

• Now Alice would like to send a message, an integer m to Bob. She encrypts m be computing the quantity $c \equiv m^e \mod N$. The quantity c is her ciphertext which she sends to Bob over an open communication line.

• Then Bob receives the message and easily decodes it by solving the congruence $x^e \equiv c \mod N$ since he knows the factorization $N = p_1 p_2$ and thus he can find d such that $d \cdot e \equiv 1 \mod (p_1-1)(p_2-1)$, and then just compute $x = c^d \mod N$.

• On the other hand, Eve does not know how to decode the message since it is very difficult task to factor given integer N into a product of two large primes.

Remark. As we have seen, Bob's public key includes the number $N = p_1 p_2$, which is a product of two secret primes p_1 and p_2. Clearly if Eve knows the value of $(p_1-1)(p_2-1)$, then she can solve the congruence $x^e \equiv c \mod N$, and thus can decrypt messages sent to Bob. Expanding $(p_1-1)(p_2-1)$ gives

$$(p_1-1)(p_2-1) = p_1 p_2 - p_1 - p_2 + 1 = N - (p_1 + p_2) + 1.$$

Since Bob has published the value of N, so Eve already knows N. Thus if Eve can determine the value of the sum $p_1 + p_2$, then the above identity gives her the value of $(p_1-1)(p_2-1)$, which enables her to decrypt messages.