Summary on Lecture 12, April 28th, 2015

Generalization of the Fermat's Little Theorem.

According to the Fermat's Little Theorem, for given prime p and any integer a, $a^{p-1} \equiv 1$ unless a is divisible by p. We would like to investigate what happens with the powers mod $n = p_1 \cdot p_2$ (product of two primes).

Example. Let $n = 15 = 3 \cdot 5$. Then we have

$$\begin{array}{ll} a^4 \equiv 1 \mod 15 & \text{if } a = 1,2,4,7,8,11,13,14, \\ a^4 \not\equiv 1 \mod 15 & \text{if } a = 3,5,6,9,10,12. \end{array}$$

Check it. Why do we have $a^4 \not\equiv 1 \text{mod } 15$ for particular values $a = 3,5,6,9,10,12$? We can notice that all these numbers have common factors with 15. This suggest that some version of the the Fermat's Little Theorem should hold for a product of two primes. Here is the result which plays a fundamental role for the RSA public key cryptosystem. This theorem is also known as the Euler formula for the product of two primes.

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 $\gcd(a, p_1 p_2) = 1$. Then $a^{\frac{(p_1-1)(p_2-1)}{d}} \equiv 1 \mod p_1 p_2$.*

Proof. By assumption, d has to divide $p_2 - 1$, and $\gcd(a, p_1) = 1$. In particular, we have that $a^{(p_1-1)} \equiv 1 \mod p_1$ by the Fermat's Little Theorem. Then we have:

$$\begin{array}{rcl} a^{\frac{(p_1-1)(p_2-1)}{d}} & = & \left(a^{(p_1-1)}\right)^{\frac{(p_2-1)}{d}} \\ & \equiv & 1^{\frac{(p_2-1)}{d}} \mod p_1 \\ & \equiv & 1 \qquad \mod p_1. \end{array}$$

Similarly we prove that $a^{\frac{(p_1-1)(p_2-1)}{d}} \equiv 1 \mod p_2$. It means that the difference

$$a^{\frac{(p_1-1)(p_2-1)}{d}} - 1$$

is divisible by both p_1 and p_2. Hence it divisible by $p_1 p_2$, or $a^{\frac{(p_1-1)(p_2-1)}{d}} - 1 \equiv 0 \mod p_1 p_2$. □

Now we are almost ready to describe the RSA public key cryptosystem. Two more theoretical exercises to go.

First, let us try to solve an equation of the form $x^e \equiv c \mod p$, where x is an unknown, e, c are known integers, and p is a prime. We recall that if e is such number that $\gcd(e, p-1) = 1$, then there exists d such that

$$de \equiv 1 \mod p - 1.$$

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 $x = c^d \mod p$.*

Proof. First, assume that $c \equiv 0 \mod p$. Then $x \equiv 0 \mod p$ is the unique solution. Assume that $c \not\equiv 0 \mod p$. The congruence $de \equiv 1 \mod (p-1)$ means that there exists k such that $de = 1 + k(p-1)$. Then we have

$$\begin{array}{rcl} (c^d)^e & = & c^{de} \\ & = & c^{1+k(p-1)} \\ & = & c \cdot \left(c^{(p-1)}\right)^k \\ & \equiv & c \cdot 1^k \mod p \\ & \equiv & c \qquad \mod p \end{array}$$

We see that $x = c^d$ solves the conguence $x^e \equiv c$. □

Exercise. Prove that the solution $x = c^d \mod p$ is unique.

Example. We solve $x^{1583} \equiv 4714 \mod 7919$, where 7919 is prime. For this, we solve the congruence $d \cdot 1583 \equiv 1 \mod 7918$. We find $d \equiv 5277 \mod 7918$. Then we use Lemma 1 to find $x \equiv 4714^{5277} \mod 7919$. We find $x \equiv 6059 \mod 7919$.