Summary on Lecture 15, May 2nd, 2016

The Chinese remainder theorem, again

Here is the main result:

Theorem. (Chinese Remainder Theorem) Let $m_1, \dots, m_k$ be a collection of relatively prime numbers, and $a_1, \dots, a_k$ be arbitrary integers. Then the system of congruences

$$(1) \qquad \begin{cases} x \equiv a_1 & \bmod m_1 \\ \cdots\cdots & \cdots\cdots \\ x \equiv a_k & \bmod m_k \end{cases}$$

has a solution $x = c$. If $x = c$ and $x = c'$ are both solutions of (1), then $c \equiv c' \bmod m_1 \cdots m_k$.

Proof. Assume that we already found a solution $x = c_i$ of the congruences

$$(2) \qquad \begin{cases} x \equiv a_1 & \bmod m_1 \\ \cdots\cdots & \cdots\cdots \\ x \equiv a_i & \bmod m_i \end{cases}$$

where $i < k$. Then we look for a solution of the conguence $x \equiv a_{i+1} \bmod m_{i+1}$ of the form $x = c_i + m_1 \cdots m_i \cdot y$. Then we have to solve the conguence

$$c_i + m_1 \cdots m_i \cdot y \equiv a_{i+1} \mod m_{i+1}$$

Since $\gcd(m_{i+1}, m_1 \cdots m_i) = 1$, we can find ℓ such that

$$\ell \cdot (m_1 \cdots m_i) \equiv 1 \mod m_{i+1}$$

We have that

$$\ell \cdot c_i + \ell \cdot (m_1 \cdots m_i) \cdot y \equiv \ell \cdot a_{i+1} \quad \text{or} \quad y \equiv \ell \cdot (a_{i+1} - c_i).$$

Then we find x as $x \equiv c_i + m_1 \cdots m_i \cdot y \bmod m_{i+1}$. □

Example. We solve the system of congruences:

$$\begin{cases} x \equiv 2 & \bmod 3 \\ x \equiv 3 & \bmod 7 \\ x \equiv 4 & \bmod 16 \end{cases}$$

We solve $x \equiv 2$ mod 3: $x = 2 + 3y$. We write $2 + 3y \equiv 3$ mod 7. We have the equation $3y \equiv 1$ mod 7. Since $3^{-1} = 5$ mod 7, we have:

$$5 \cdot 3 \cdot y \equiv 5 \mod 7, \quad \text{or} \quad y \equiv 5 \mod 7.$$

We have that $y = 5 + 7z$. We obtain $x = 2 + 3(5 + 7z) = 17 + 21z$. Then we write $17 + 21z \equiv 4$ mod 16. This is the same as $1 + 5z \equiv 4$ mod 16, or we get the congruence

$$5z \equiv 3 \mod 16.$$

We find that $5^{-1} = 13$ mod 16 (indeed, $5 \cdot 13 = 65 \equiv 1$ mod 16). Then we obtain:

$$z \equiv 13 \cdot 3 \equiv 7 \mod 16, \quad \text{or} \quad z = 7 + 16w.$$

We obtain:

$$x = 17 + 21z = 17 + 21 \cdot (7 + 16w) = 17 + 147 + 3 \cdot 7 \cdot 16w = 164 + 3 \cdot 7 \cdot 16w,$$

where w is an arbitrary interger. A minimal positive solution is $x = 164$.

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

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

Check it. Why do we have $a^4 \not\equiv 1 \bmod 15$ 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 $\gcd(a, p_1p_2) = 1$. Then $a^{\frac{(p_1-1)(p_2-1)}{d}} \equiv 1 \bmod p_1p_2$.*

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

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

Similarly we prove that $a^{\frac{(p_1-1)(p_2-1)}{d}} \equiv 1 \bmod p_2$. 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_1p_2, or $a^{\frac{(p_1-1)(p_2-1)}{d}} - 1 \equiv 0 \bmod p_1p_2$. □

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 $x^e \equiv c \bmod p$, 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 $x^e \equiv c \bmod p$ has a unique solution $x = c^d \bmod p$.*

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

$$\begin{aligned} (c^d)^e &= c^{de} \\ &= c^{1+k(p-1)} \\ &= c \cdot (c^{(p-1)})^k \\ &\equiv c \cdot 1^k \mod p \\ &\equiv c \mod p \end{aligned}$$

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

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

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