Summary on Lecture 11, April 27th, 2015

More on the Fermat's Little Theorem.

Last time we proved the Fermat's Little Theorem:

Theorem 1. Let p be a prime number. Then

$$a^{p-1} \equiv \begin{cases} 1 \mod p & \text{if } a \neq 0 \mod p \\ 0 \mod p & \text{if } a = 0 \mod p \end{cases}$$

We notice that this theorem and fast powering algorithm provide us with new way to compute inverses mod p. We can see that

$$a^{-1} \equiv a^{p-2} \mod p.$$

Indeed, we multiply $a \cdot a^{p-2} = a^{p-1} \equiv 1 \mod p$.

Example. We can compute $7814^{-1} \mod 17449$ in two ways. First we use the fast powering algorithm to get:

$$7814^{-1} \equiv 7814^{17447} \equiv 1284 \mod 17449.$$

Secondly, we can use the Euclidian algorithm to solve the equation

$$7814 \cdot t + 17449 \cdot s = 1.$$

We get $t = 1284$, $s = -575$. The result is the same: $7814^{-1} \equiv 1284 \mod 17449$.

Example. Now we'll see that the Fermat's Little Theorem can help us to decide whether a given integer is a prime or not. Let $n = 15485207$. Assume that $n = 15485207$ is a prime. Then we can compute $2^{n-1} = 2^{15485206} \mod 15485207$. We get:

$$2^{15485206} \equiv 4136685 \mod 15485207.$$

Thus n is not a prime since $2^{n-1} \not\equiv 1 \mod n$. We did prove that 15485207 is not a prime, however, we do not know any of its factors! Actually, 15485207 is a product of two primes: $15485207 = 3853 \cdot 4019$.

Let us think again about the statement of the Fermat's Little Theorem: it gives us that $a^{p-1} \equiv 1 \mod p$ if a is not divisible by p. However, for given a there could be an integer $k < p-1$ such that $a^k \equiv 1 \mod p$. We choose a minimal k such $a^k \equiv 1 \mod p$ and call such k the order of $a \mod p$. We would like to examine this:

Lemma 1. Let p be a prime and a be an integer not divisible by p, and k be the order of $a \mod p$. Then k divides $(p-1)$.

Proof. Let k be a minimal positive integer such that $a^k \equiv 1 \mod p$. We have that $a^n \equiv 1 \mod p$ for $n = p-1$. We divide n by k:

$$n = k \cdot d + r, \quad 0 \leq r < k.$$

Then we have:

$$1 \equiv a^n \equiv a^{k \cdot d + r} \equiv a^{k \cdot d} \cdot a^r \equiv (a^k)^d \cdot a^r \equiv 1 \cdot a^r \equiv a^r.$$

Thus $a^r \equiv 1 \mod p$. However, $r < k$, and k is a minimal positive integer such that $a^k \equiv 1 \mod p$. This means that $r = 0$, i.e. k divides $n = p-1$. $\square$

Example. We look at powers of 2 mod 11:

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10,\ 2^6 \equiv 9, 2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6,\ 2^{10} \equiv 1.$$

In this case, $10 = 11 - 1$ is the order of 2 mod 11.

We look at the powers of 2 mod 17:

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 16,\ 2^5 \equiv 15,\ 2^6 \equiv 13, 2^7 \equiv 9,\ 2^8 \equiv 1, \ldots.$$

Here we see that 8 is the order of 2 mod 17.

The Chinese remainder theorem.

Here is a problem studied in China in late third century:

We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?

We translate this into modern mathematical lenguage. Let x be the "number of things". Then we have two equations:

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$$

The first equation gives us that $x = 3y + 2$ for some integer y. Then we conclude from the second equation that $x = 3y + 2 \equiv 3 \mod 5$. We obtain the equation

$$3y \equiv 1 \mod 5$$

Since $3^{-1} = 2 \mod 5$, we obtain that $y \equiv 2 \mod 5$, i.e. $y = 5k+2$, and then we obtain that $x = 3y+2 = 15z+8$. Then we should find z such that $15z + 8 \equiv 2 \mod 7$. This means that

$$14z + z + 1 + 7 \equiv 2 \mod 7, \quad \text{or} \quad z \equiv 1 \mod 7.$$

We obtain $z = 1 + 7w$, and then $x = 15z + 8 = 15(1 + 7w) + 8 = 23 + 3 \cdot 5 \cdot 7w$, where w is an integer. This gives all solutions of the ancient problem. The minimal positive solution is $x = 23$.

Exercise. Solve the system of congruences

$$\begin{cases} x \equiv 1 & \mod 5 \\ x \equiv 9 & \mod 11 \end{cases}$$

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

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ \cdots\cdots & \cdots\cdots \\ x \equiv a_k & \mod m_k \end{cases} \tag{1}$$

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

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

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ \cdots\cdots & \cdots\cdots \\ x \equiv a_i & \mod m_i \end{cases} \tag{2}$$

where $i < k$. Then we look for a solution of the conguence $x \equiv a_{i+1} \mod m_{i+1}$ 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 $x \equiv c_i + m_1 \cdots m_i \cdot y \mod m_{i+1}$. $\square$

Example. We solve the system of congruences:

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

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 $x = 164$.