Lecture 9, Feb 10, 2011, Euclid Algorithm & Chinese Reminder Theorem

Theorem 1 (Fermat’s little theorem). Let $p$ be a prime number and $a$ is an integer not divisible by $p$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Start by listing the first $p-1$ positive multiplies of $a$:

$$a, 2a, 3a, \ldots, (p-1)a$$

If $ra \equiv sa \pmod{p}$, then we have $(r-s)a$ is a multiple of $p$, so the $p-1$ multiples of $a$ above are distinct and nonzero; that is, they must be congruent to $1, 2, 3, \ldots, p-1$ in some order. Multiply all these congruences together and we find

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \ldots (p-1) \pmod{p}$$

□

Lemma 1. Let $a = bq + r$, where $a, b, q,$ and $r$ are integers, then

$$\gcd(a, b) = \gcd(b, r).$$

Proof. Suppose that $d$ divides both $a$ and $b$, then it follows that $d$ also divides $a-bq = r$. Hence, any common divisor of $a$ and $b$ is also a common divisor of $b$ and $r$.

Likewise, suppose that $d$ divides $b$ and $r$, then $d$ also divides $bq + r = a$. Hence, any common divisor of $b$ and $r$ is also a common divisor of $a$ and $b$. □

Example 1.

$$287 = 91 \times 3 + 14, \Rightarrow \gcd(287, 91) = \gcd(91, 14)$$

$$91 = 14 \times 6 + 7, \Rightarrow \gcd(91, 14) = \gcd(14, 7)$$

$$14 = 7 \times 2 + 0, \Rightarrow \gcd(14, 7) = 7, \Rightarrow \gcd(287, 91) = 7$$

We now formally prove that

The Euclidean algorithm

1 $\gcd(a, b)$
2 $x \leftarrow a$
3 $y \leftarrow b$
4 while $y \neq 0$
5 $r \leftarrow x \mod y$
6 $x \leftarrow y$
7 $y \leftarrow r$

Theorem 2. If $a$ and $b$ are positive integers, then there exists integers $s$ and $t$ such that $\gcd(a, b) = sa + tb$.

Show how to use the Euclidean algorithm to find such $s$ and $t$.

$$7 = 91 - 14 \times 6 = 91 - (281 \times 3) \times 6 = 287 \times (-6) + 91 \times 19$$

We now formally prove that
Theorem 3. If $\gcd(a, m) = 1$, then $a$ has a multiplicative inverse in $\mathbb{Z}_m$.

Proof. There exist integers $s$ and $t$ such that

$$sa + tm = 1.$$  

This implies $sa + tm \equiv 1 \pmod{m}$. Because $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$. □

The Euclidean algorithm gives a way to find the inverse of $s$ in $\mathbb{Z}_m$. It also provides a way to solve $ax \equiv b \pmod{m}$ when $\gcd(a, m) = 1$.

Theorem 4 (Chinese remainder theorem). Let $m_1$ and $m_2$ be relatively prime positive integers and $a_1, a_2$ arbitrary integers. The system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

has a unique solution modulo $m = m_1m_2$.

Proof. To construct a simultaneous solution, first let $M_k = m/m_k$, $k = 1, 2$. Because $\gcd(m_1, m_2) = 1$, then $\gcd(M_k, m_k) = 1$. Therefore, we know that there is an integer $y_k$, such that

$$M_ky_k \equiv 1 \pmod{m_k}.$$  

To construct a simultaneous solution, form the sum

$$x_0 = a_1M_1y_1 + a_2M_2y_2$$

It is clear that $x_0$ is one solution. □