**Computing Science 204 (B1)**
**Fermat's Little Theorem**
Wednesday, July 12

*Fermat's Little Theorem* states that if $p$ is a prime and $a$ is a positive integer which is not divisible by $p$, then

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

In order to prove this we need the following lemmas.

**Lemma 1.** If $a$ and $b$ are integers, not both 0, then the greatest common divisor of $a$ and $b$, is the least positive integer $d$ such that $d = a \cdot s + b \cdot t$ for some integers $s$ and $t$.

**proof.** Let $S$ be the set of all positive integers of the form $a \cdot s + b \cdot t$ where $s$ and $t$ are integers. Assuming that $a \neq 0$, then at least one of $1 \cdot a + 0 \cdot b$ or $(-1) \cdot a + 0 \cdot b$ is positive, so that $S$ is nonempty.

By the well-ordering property for the positive integers, $S$ has a smallest element, say

$$d = a \cdot s + b \cdot t$$

where $s$ and $t$ are integers and $d > 0$. Now we show that $d \mid a$ and $d \mid b$.

By the division algorithm, there exist unique integers $q$ and $r$ such that

$$a = q \cdot d + r$$

where $0 \leq r < d$. Thus,

$$r = a - q \cdot d = a - q(a \cdot s + b \cdot t) = (1 - qs) \cdot a - qt \cdot b \tag{$*$}$$

and $r \geq 0$. If $r > 0$, then $(*)$ implies that $r \in S$, and $r < d$, which contradicts the fact that $d$ is the smallest element in $S$. Therefore, we must have $r = 0$, that is, $a = q \cdot d$, that is, $d \mid a$. A similar argument shows that $d \mid b$. Therefore, $d$ is a common divisor of $a$ and $b$.

In order to show that $d$ is the greatest common divisor of $a$ and $b$, we need only show that if $c$ is any other positive common divisor of $a$ and $b$, then $c \mid d$. To this end, suppose that $a = k \cdot c$ and $b = \ell \cdot c$, then

$$d = a \cdot s + b \cdot t = (ks + \ell t) \cdot c,$$

that is, $c \mid d$, and therefore, $d = a \cdot s + b \cdot t = \gcd(a, b)$.

$\square$

**Lemma 2.** If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

**proof.** Since $\gcd(a, b) = 1$, then there exist integers $s$ and $t$ such that $1 = a \cdot s + b \cdot t$, and therefore $c = ac \cdot s + bc \cdot t$, and since $a \mid bc$, then $a \mid c$.

$\square$

**Theorem (Fermat).** If $p$ is prime and $a$ is a positive integer such that $p \not| a$, then

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

**proof.** Consider the integers $a$, $2a$, $3a$, $\ldots$, $(p-1)a$. None of these are divisible by $p$, since if $p \,\big|\, ka$, the fact that $\gcd(a,p) = 1$ and the lemma imply that $p \,\big|\, k$. But this is impossible, since $1 \leq k \leq p-1$.

Also, no two of $a$, $2a$, $3a$, $\ldots$, $(p-1)a$ are congruent modulo $p$, since if $ja \equiv ka \mod p$, where $j < k$, then $p \,\big|\, (j-k)a$, and again using the fact that $a$ and $p$ are relatively prime, the lemma implies that $p \,\big|\, j-k$, that is, $j \equiv k \mod p$. But this is impossible since $1 \leq j < k \leq p-1$.

Since $a$, $2a$, $3a$, $\ldots$, $(p-1)a$ are all incongruent to 0 modulo $p$, and no two are congruent modulo $p$, then each of them is in a different congruence class modulo $p$, that is, when these integers are divided by $p$, the least positive remainders of $a$, $2a$, $3a$, $\ldots$, $(p-1)a$ are just the integers 1, 2, 3, $\ldots$, $(p-1)$ in some order. Therefore,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p,$$

that is,

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p,$$

that is, $p \,\big|\, (p-1)! \left[a^{p-1} - 1\right]$. Since $p \not| (p-1)!$, then from the lemma, $p \,\big|\, a^{p-1} - 1$, that is, $a^{p-1} \equiv 1 \mod p$.
$\square$