Fermat and Euler’s Theorems

**Definition:** A reduced set of residues (RSR) modulo $m$ is a set of integers $R$ so that every integer relatively prime to $m$ is congruent to exactly one integer in $R$.

**Fact.** $a \equiv b \pmod{m}$ implies $\gcd(a, m) = \gcd(b, m)$.

**Fact.** All RSR’s modulo $m$ have the same size.

**Definition:** $\phi(m)$ is the size of a RSR modulo $m$. $\phi$ is called the *Euler Phi or totient function.*

The standard CSR modulo $m$ is $\{0, \ldots, m - 1\}$.

The standard RSR modulo $m$ is $\{1 \leq r \leq m; \gcd(r, m) = 1\}$.

**Fact.** $\phi$ is *multiplicative*, that is, $\phi(ab) = \phi(a)\phi(b)$ whenever $a$ and $b$ are relatively prime.

Some special formulas for $\phi$: Let $p$ be prime. Then $\phi(p) = p - 1$, $\phi(p^2) = p^p - p^{p-1}$, $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$.

When $p \neq q$ are primes, we have $\phi(pq) = (p - 1)(q - 1)$. 
Fermat’s “Little” Theorem

**Theorem.** Let \( p \) be prime and \( a \) be an integer which is not a multiple of \( p \). Then

\[
a^{p-1} \equiv 1 \pmod{p}.
\]

**Proof:** Since \( \gcd(a, p) = 1 \), the set \( \{ ai \mod p; i = 1, \ldots, p-1 \} \) is the same as the set \( \{1, \ldots, p-1\} \). Therefore,

\[
a^{p-1} \prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} (ai) \equiv (\prod_{i=1}^{p-1} i) \cdot 1 \pmod{p}.
\]

Since \( \gcd(\prod_{i=1}^{p-1} i, p) = 1 \), we can cancel and get

\[
a^{p-1} \equiv 1 \pmod{p}.
\]
Euler’s Theorem

**Theorem.** Let \( m > 1 \) and \( \gcd(a, m) = 1 \). Then
\[
a^{\phi(m)} \equiv 1 \pmod{m}.
\]

**Proof:** Let \( \{r_1, \ldots, r_{\phi(m)}\} \) be a RSR modulo \( m \). Then \( \{ar_1, \ldots, ar_{\phi(m)}\} \) is a RSR modulo \( m \), too (by a Lemma). Therefore, for all \( i \), there is a unique \( j \) so that \( r_i \equiv ar_j \pmod{m} \). Then
\[
a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i = \prod_{i=1}^{\phi(m)} (ar_i) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.
\]
Since \( \gcd(\prod_{i=1}^{\phi(m)} r_i, m) = 1 \), we can cancel and get
\[
a^{\phi(m)} \equiv 1 \pmod{m}.
\]
A Corollary of Euler’s Theorem

Here is an alternate way to compute the multiplicative inverse $a^{-1}$ of $a$ modulo $m$: Recall that $a^{-1}$ is the residue class mod $m$ such that $a^{-1}a \equiv aa^{-1} \equiv 1 \pmod{m}$. It is defined only when $\gcd(a, m) = 1$. In that situation we have $a^{\phi(m)} \equiv 1 \pmod{m}$ by Euler’s Theorem.

Factoring out one $a$ gives

$$aa^{\phi(m)-1} \equiv 1 \pmod{m},$$

whence $a^{-1} \equiv a^{\phi(m)-1} \pmod{m}$. For a prime modulus $p$ we have $a^{-1} \equiv a^{p-2} \pmod{p}$.

For large $m$, computing $a^{-1} \pmod{m}$ by this formula requires roughly the same number of bit operations as computing $a^{-1} \pmod{m}$ by the Extended Euclidean Algorithm. (The latter must be used if one does not know $\phi(m)$.)
How to compute $a^n$ mod $m$ swiftly

Here is an algorithm for computing $a^n$ in $O(\log_2 n)$ multiplications. To use it to compute $a^n$ mod $m$ while keeping the numbers small (smaller than $m$, that is), reduce modulo $m$ after each multiplication.

procedure power(a, n)
    e = n;
    y = 1;
    z = a;
    repeat {
        if (e is odd) y = y*z;
        if (e <= 1) return (y);
        z = z*z;
        e = floor(e/2);
    }
end power;
Another Corollary of Euler’s Theorem

**Corollary.** Let $m > 1$, $x$, $y$ and $g$ be positive integers with $\gcd(g, m) = 1$. If $x \equiv y \pmod{\phi(m)}$, then $g^x \equiv g^y \pmod{m}$.

**Proof:** We have $x = y + k\phi(m)$ for some integer $k$, so

$$g^x = g^{y+k\phi(m)} = g^y (g^\phi(m))^k \equiv g^y \pmod{m}.$$
Finding large primes

Fermat’s Little Theorem says that if \( p \) is prime and \( p \nmid a \), then \( a^{p-1} \equiv 1 \pmod{p} \).

This theorem gives a test for \textit{compositeness}: If \( p \) is odd and \( p \nmid a \) and \( a^{p-1} \not\equiv 1 \pmod{p} \), then \( p \) is not prime.

If the converse of Fermat’s theorem were true, it would give a fast test for \textit{primality}. The converse would say, if \( p \) is odd and and \( p \nmid a \) and \( a^{p-1} \equiv 1 \pmod{p} \), then \( p \) is prime.

Unfortunately, this converse is not a true statement, although it is true for most \( p \) and most \( a \). Consider \( p = 341 = 11 \cdot{27}{31} \) and \( a = 2 \).

\[
2^{340} \equiv 1 \pmod{341}.
\]

It is even worse than that because there are infinitely many \textit{Carmichael numbers}. These are composite numbers like \( p = 561 = 3 \cdot 11 \cdot 17 \) for which \( a^{p-1} \equiv 1 \pmod{p} \) for \textit{every} integer \( a \) with \( \gcd(a, p) = 1 \).
Here is a true converse of Fermat’s Little Theorem.

**Theorem.** Let $n > 3$ be odd. If for every prime $p|n−1$ there exists an $a$ such that $a^{n−1} \equiv 1 \pmod{n}$, but $a^{(n−1)/p} \not\equiv 1 \pmod{n}$, then $n$ is prime.

This theorem may be used iteratively to construct large, random primes.

Begin with a prime $p_1$. Let $i = 1$. Repeat the following steps until $p_i$ is large enough.

For random small integers $k$, let $n = 2kp_i + 1$. If $2^{n−1} \not\equiv 1 \pmod{n}$, then $n$ is composite by Fermat’s Little Theorem, so try another $k$. Otherwise, $n$ is probably prime, so try to prove $n$ is prime using the theorem just stated. Note that $n−1 = 2kp_i$ is easy to factor completely. If you succeed in finding $a$’s which satisfy the conditions of the theorem, then $n$ is proved prime, and let $p_{i+1} = n$ and let $i = i + 1$. Otherwise, try a new random $k$. 