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. ϕ is called the *Euler Phi or totient function*.

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

The standard RSR modulo m is

$$\{1 \leq r \leq m; \gcd(r, m) = 1\}.$$

Example: $\phi(12) = 4$ because $\{1, 5, 7, 11\}$ is the standard RSR modulo 12.

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

Some special formulas for ϕ: Let p be prime. Then

$$\phi(p) = p - 1,$$

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1},$$

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

When $p \neq q$ are primes, we have

$$\phi(pq) = (p-1)(q-1).$$

Proof: Begin with the CSR $\{0, 1, \ldots, pq-1\}$. Delete all q multiples of p. Delete all p multiples of q. 0 was deleted twice, so add 1 back. Get $pq - p - q + 1 = (p-1)(q-1)$.

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 $\{ai \bmod p; i = 1, \ldots, p-1\}$ is the same as the set $\{1, \ldots, p-1\}$. Therefore,

$$a^{p-1} \prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (ai) \equiv \left(\prod_{i=1}^{p-1} i \right) \cdot 1 \pmod{p}.$$

Since $\gcd\left(\prod_{i=1}^{p-1} i, p\right) = 1$, 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. Therefore, for all i, there is a unique j so that $r_i \equiv ar_j \pmod{m}$. Then

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i = \prod_{i=1}^{\phi(m)} (ar_i) \equiv \left(\prod_{i=1}^{\phi(m)} r_i \right) \pmod{m}.$$

Since $\gcd\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1$, 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} mod m by this formula requires roughly the same number of bit operations as computing a^{-1} mod 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 *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 *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 $p = 341 = 11 \cdot 31$ and $a = 2$. We have $2^{340} \equiv 1 \pmod{341}$.

It is even worse than that because there are infinitely many *Carmichael numbers*. These are composite numbers like $p = 561 = 3 \cdot 11 \cdot 17$ for which $a^{p-1} \equiv 1 \pmod{p}$ for *every* integer a with $\gcd(a, p) = 1$.