Fermat's little theorem

Theorem (Fermat's little theorem)

Suppose that p is prime and p does not divide a. Then

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

- Define the Euler ϕ-function on the set of positive integers by

$$\phi(n) = \text{ the number of } k, 0 < k < n \text{ such that } \gcd(k, n) = 1.$$

Theorem (Euler's theorem)

Suppose $n > 0$ and $\gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \mod n.$$

Calculation of the ϕ-function

Lemma

For p a prime, $\phi(p^n) = p^{n-1}(p-1)$.

Lemma

Suppose that $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

Theorem

If $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ then

$$\phi(n) = p_1^{m_1-1} p_2^{m_2-1} \cdots p_k^{m_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).$$

Corollary

If p and q are distinct primes then $\phi(pq) = (p-1)(q-1)$.

Exponentiation and modular arithmetic

- How do we compute $m^e \mod n$ for large m, e and n?
- The trick is to do repeated squaring and calculate the remainder each time.
- That is, suppose that you want to compute m^{2^k}; let

$$m_0 = m, m_1 \equiv m^2 \mod n, m_2 \equiv m_1^2 \mod n \ldots$$

$$m_k \equiv m^{2^k} \equiv m_{k-1}^2 \mod n.$$

- In general, if you have e written in base 2 as

$$2^{k_1} + 2^{k_2} + \ldots + 2^{k_\ell} \text{ for } 0 \leq k_1 < k_2 \ldots < k_\ell$$

  then compute $m^{2^{k_i}} \mod n$ for each i and then multiply the results again modulo n.