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

Why does RSA work?

- Remember, for RSA, Bob chooses two distinct primes p and q, forms $n = pq$ and chooses a number e which is co-prime with $(p-1)(q-1)$. He publishes n and e.
- Alice takes her message m and computes $c \equiv m^e \bmod n$ and sends c to Bob.
- Bob determines a number d such that $ed \equiv 1 \bmod (p-1)(q-1)$ and computes $c^d \bmod n$ which recovers the original m.
- Why does this work and is it effective?
- If $\gcd(m, n) = 1$ then $m^{\phi(n)} \equiv 1 \bmod n$. Since $\phi(n) = (p-1)(q-1)$ and $ed \equiv 1 \bmod (p-1)(q-1)$, for some k, $ed = 1 + k(p-1)(q-1)$.
- So $(m^e)^d \equiv m \bmod n$ and we recover the message.

Why does RSA work?, cont'd

- Suppose that the $\gcd(m, n) = p$ (or equivalently q): Then $m^{ed} \equiv m \bmod p$ and $m^{ed} \equiv m \bmod q$ by Fermat. So by the Chinese remainder theorem, $m^{ed} \equiv m \bmod n$ and again we recover the message.
- All of these exponentiations can be effectively calculated in the number of digits of exponents.
- The only open question is how to pick primes p and q which are reasonably safe from attack; we will do that next week.