COS 341: Discrete Mathematics

Precept #9 Fall 2006
For the week of: December 11

---

1. Let a, k and n be positive integers. Show how $\mathrm{rem}(a^k, n)$ can be computed in time polynomial in $\log a$, $\log k$ and $\log n$.

2. For any positive integer n, let $\phi(n)$ be the number of integers between 1 and $n-1$ that are relatively prime to n.

a. Prove Euler's Theorem which asserts that if k is relatively prime to n then

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

b. In class, we saw how RSA involves the choice of two distinct primes p and q, as well as positive integers d and e such that e is relatively prime to $s = (p-1)(q-1)$, and $ed \equiv 1 \pmod{s}$. To show that RSA works, we had to prove that

$$m^{ed} \equiv m \pmod{n}$$

for all m, where $n = pq$. Give an alternative proof of this fact based on Euler's Theorem that holds for all m which are relatively prime to n. (Why is this last assumption of relative primality reasonable?)

3. Given two positive integers a and b with $a \leq b$, Euclid's algorithm computes $\gcd(a, b)$ by repeatedly applying the rule $\gcd(a, b) = \gcd(\mathrm{rem}(b, a), a)$ until the smaller number equals zero.

a. Show that Euclid's algorithm terminates after $O(\log a)$ iterations.

b. Show how Euclid's algorithm can be modified to compute integers s and t such that $sa+tb = \gcd(a, b)$. Explain also how this technique can be used to compute multiplicative inverses modulo a prime (as an alternative to using Fermat's Little Theorem).