Homework 7

Suyi Liu

April 26, 2017

1 Problem 1

See expofact.m file and problem1.txt file. Details are included in the function. I consulted the fastexp.m and extendedeuclid.m functions to use fast exponentiation as well as to compute gcd of two numbers.
The factors of 68309797 is 8527 and 8011, using k = 341466300, base a = 2, as well as base a = 5.

2 Problem 2

Prove by induction on mn:

Base case:
Suppose m, n are prime numbers. Then $\phi(mn) = (m-1)(n-1) = \phi(m)\phi(n)$
Suppose m, n are 1 and 2. Then $\phi(mn) = \phi(2) = 1 * 2 = \phi(m)\phi(n)$

Inductive hypothesis:
Suppose for all x such that $x < m$, and for all y such that $y < n$, if x and y are relatively prime positive integers $\phi(xy) = \phi(x)\phi(y)$.

Induction Step:
Need to show $\phi(mn) = \phi(m)\phi(n)$
Suppose all the divisors of m are $d_1, d_2, ...d_a$, specifically, $d_1 = 1, d_a = m$. Suppose all the divisors of n are $d'_1, d'_2, ...d'_b$, specifically, $d'_1 = 1, d'_b = n$.
==
Claim: There's correspondence between $d_i * d'_j$, $1 \leq i \leq a$ and $1 \leq j \leq b$, and all the divisors of mn(All the divisors of mn are the Cartesian products of divisors of m times divisors of n).
Proof:
"=>": $d_i * d'_j$ divides mn, because $d_i|m$ and $d'_j|n$, so $m = u * d_i$, $n = v * d'_j$ for some $u, v \in Z$. So $d_i * d'_j * uv = mn$, $d_i * d'_j$ divides mn.
"<=": Suppose $x|mn$, then $x = d_i * d'_j$, where $d_i|m$ and $d'_j|n$. This is because when m, n are relatively prime, they don't share any common prime $p > 1$. Suppose the prime factorization of x is $p_1 * p_2 * ...p_z$. For all $s \in 1...z$, if $p_s|m$,

group such p_s together, and there must be a d_i equal to such product which divides m. For all $r \in 1...z$, if $p_r|n$, group such p_r together, and there must be a d'_j equal to such product which divides n. And there must not be any prime factor of x that cannot divide m or n(then x will not be able to divide mn, contradiction!), or any prime factor of x that divides both m and n in the same time because m and n are relatively prime.
==
According to the theorem from class, we can write $mn = m*n = (\sum_{i=1}^{a} \phi(d_i)) * (\sum_{j=1}^{b} \phi(d'_j))$
$= \sum_{i=1,j=1}^{i=a,j=b} \phi(d_i) * \phi(d'_j)$
Using the correspondence above, we can write $mn = \sum_{i=1,j=1}^{i=a,j=b} \phi(d_i * d'_j)$
So we get $\sum_{i=1,j=1}^{i=a,j=b} \phi(d_i) * \phi(d'_j) = \sum_{i=1,j=1}^{i=a,j=b} \phi(d_i * d'_j)$
By the inductive hypothesis, since d_i, d'_j are positive and pairwise relatively prime(divisors of two relatively prime integers are relatively prime to each other), we know $\phi(d_i) * \phi(d'_j) = \phi(d_i * d'_j)$ for all $d_i < m$, $d'_j < n$, so we can cancel out $\phi(d_i) * \phi(d'_j)$ and $\phi(d_i * d'_j)$ for all $d_i < m$, $d'_j < n$ from both sides.
Then we only have $\phi(d_i) * \phi(d'_j) = \phi(d_i * d'_j)$ left on both sides. Since $d_i = m, d'_j = n$, $\phi(mn) = \phi(m) * \phi(n)$

So if m and n are relatively prime positive integers, then $\phi(mn) = \phi(m) * \phi(n)$

3 Problem 3

Suppose the prime factorization of n is $\prod_{i=1}^{k} p_i^{e_i}$, where p_i are prime numbers.

- $\phi(n) = \phi(p_1^{e_1} * \prod_{i=2}^{k} p_i^{e_i}) = \phi(p_1^{e_1}) * \phi(\prod_{i=2}^{k} p_i^{e_i}) = ... = \phi(p_1^{e_1}) * \phi(p_2^{e_2}) * ... * \phi(p_k^{e_k}) = \prod_{i=1}^{k} \phi(p_i^{e_i})$ Since $\phi(p^k) = (p-1)p^{k-1}$ from last homework, $\phi(n) = \prod_{i=1}^{k} (p_i - 1) * p_i^{e_i - 1}$
- $\frac{\phi(n)}{n} = \frac{\prod_{i=1}^{k} (p_i-1)*p_i^{e_i-1}}{\prod_{i=1}^{k} p_i^{ei}} = \prod_{i=1}^{k} \frac{(p_i-1)*p_i^{e_i-1}}{p_i^{ei}} = \prod_{i=1}^{k} \frac{p_i-1}{p_i}$
- $\frac{\phi(n)}{n}$ is $\frac{\#units}{n} = \frac{|Z_n*|}{|Z_n|}$ So $\frac{\phi(n)}{n}$ represents the fraction of members of Z_n that are in Z_n*.

4 Problem 4

Since n, e_A and e_B are public keys known to Eve, and e_A and e_B are relatively prime, there must exists $x, y \in Z$ such that $x * e_A + y * e_B = 1$. So Eve can efficiently compute x and y using extended Euclid's algorithm.
Since Eve knows c_A, c_B, she can compute $c_A^x * c_B^y = (m^{e_A})^x * (m^{e_B})^y = m^{x*e_A + y*e_B} = m^1 = m$ mod n.
As for the case where either x or y is negative: Assume $x = -k$, $k > 0$, Eve

can compute $c_A^x = c_A^{-k} = {c_A^{-1}}^k$. And c_A^{-1} is easy to compute efficiently using Euclid's algorithm to find the inverse of c_A.
The rest of work can be computed efficiently using fast exponentiation.
So Eve can find m by computing $c_A^x * c_B^y \bmod n$ if she intercepts c_A, c_B.

5 Problem 5

According to Fermat's Little Theorem, for all $a \in Z_p*$, $a^{p-1} = 1$ mod p.
If $p_i - 1 | n - 1$ for all $i = 1, 2, ..., m$, there exists an integer x_i such that $(p_i - 1) * x_i = n - 1$ for all $i = 1, 2, ..., m$.
Thus for all $a \in Z_p*$, for all $i = 1, 2, ..., m$, $a^{n-1} = a^{(p_i-1)*x_i} = (a^{p_i-1})^{x_i} = 1^{x_i} = 1 \bmod p_i$.
Specifically, for all $a \in Z_p*$:
$a^{n-1} = 1 \bmod p_1$
$a^{n-1} = 1 \bmod p_2$
...
$a^{n-1} = 1 \bmod p_m$
which means:
$p_1 | a^{n-1} - 1$
$p_2 | a^{n-1} - 1$
...
$p_m | a^{n-1} - 1$
Since $p_1, p_2, ..., p_m$ are distinct prime numbers sharing no common factor > 1, $p_1 * p_2 * ... * p_m | a^{n-1} - 1$, So $a^{n-1} = 1 \bmod p_1 * p_2 * ... * p_m = n$
Thus for all $a \in Z_p*$, $a^{n-1} = 1 \bmod n$, so n is a Carmichael number by definition.