Homework 6

Suyi Liu

April 10, 2017

1 Problem 1

$\phi(p^k)$ = count of numbers relatively prime to p^k = p^k - count of numbers not relatively prime to p^k

Consider primes not relatively prime to p^k:

Since p is a prime, so p^k only has p as its prime factor > 1, any number n that is not relatively prime to p^k must have $p|n$. (Suppose n does not have $p|n$, then gcd(n,p^k) = 1 as they don't have common divisor > 1).

So we can categorize those n that is not relatively prime to p^k into the form $n = p^i * r$, where r doesn't have p as its factor. For example, $n = p^4 * r$ means that n can have at most 4 p's in its factorization.

Category $p^1 * r$ contains numbers whose r is:

1, 2, 3 ... p-1,(excluding p)

p+1,p+2,p+3...2p-1,(excluding 2p)

...

$p^{k-3}p + 1$,$p^{k-3}p + 2$,...$p^{k-2}p - 1$(excluding p^{k-2})

All of these r's are not congruent to 0 mod p, without gap, and $p^{k-2}p - 1$ is the largest possible r to make sure $(p^{k-2}p - 1) * p \leq p^k$.

There are in total $p^{k-2} * (p - 1)$ numbers in this category.

Category $p^2 * r$ contains numbers whose r is:

1, 2, 3 ... p-1,(excluding p)

p+1,p+2,p+3...2p-1,(excluding 2p)

...

$p^{k-4}p + 1$,$p^{k-4}p + 2$,...$p^{k-3}p - 1$(excluding p^{k-3})

All of these r's are not congruent to 0 mod p, without gap, and $p^{k-3}p - 1$ is the largest possible r to make sure $(p^{k-3}p - 1) * p^2 \leq p^k$.

There are in total $p^{k-3} * (p - 1)$ numbers in this category.

similarly, there are $p^{k-4} * (p - 1)$ numbers in $p^3 * r$ category, $p^{k-5} * (p - 1)$ numbers in $p^4 * r$ category... $p^{k-k} * (p - 1)$ numbers in $p^{k-1} * r$ category and 1 numbers in $p^k * r$ category(p^k itself).

Since all categories do not intersect with each other, total count of numbers not relatively prime to p^k is:

$(p^{k-2}+p^{k-3}+...p^{k-k})*(p-1)+1$
$=(p^{k-1}+p^{k-2}+...p^1+p^0)-(p^{k-2}+p^{k-3}+...p^{k-k})$
So count of numbers relatively prime to p^k
$=p^k-(p^{k-1}+p^{k-2}+...p^1+p^0)+(p^{k-2}+p^{k-3}+...p^{k-k})$
$=p^k-p^{k-1}$
(terms $p^{k-2}+...p^1+p^0$ cancel out)
$=(p-1)p^{k-1}$
Which is, $\phi(p^k)=(p-1)p^{k-1}$

2 Problem 2

See fastexp.m file and Problem2.txt file. Details are included in the function.

3 Problem 3

- Since $\phi(n)=\phi(pq)=(p-1)(q-1)=pq-p-q+1=n-p-q+1$,$p+q=n+1-\phi(n)$
  so $q=n+1-\phi(n)-p$
  Since $pq=n$, $p(n+1-\phi(n)-p)=n$
  So solving p, q is solving quadratic equation: $p^2-(n+1-\phi(n))p+n=0$.
  So $p=\frac{(n+1-\phi(n))+\sqrt{(n+1-\phi(n))^2-4n}}{2}$, or $p=\frac{(n+1-\phi(n))-\sqrt{(n+1-\phi(n))^2-4n}}{2}$.
  Then we can get the corresponding $q=\frac{n}{p}=\frac{2n}{(n+1-\phi(n))+\sqrt{(n+1-\phi(n))^2-4n}}$ or $\frac{2n}{(n+1-\phi(n))-\sqrt{(n+1-\phi(n))^2-4n}}$.
  So the formula is:
  $p=\frac{(n+1-\phi(n))+\sqrt{(n+1-\phi(n))^2-4n}}{2}$ and $q=\frac{2n}{(n+1-\phi(n))+\sqrt{(n+1-\phi(n))^2-4n}}$,
  or $p=\frac{(n+1-\phi(n))-\sqrt{(n+1-\phi(n))^2-4n}}{2}$ and $q=\frac{2n}{(n+1-\phi(n))-\sqrt{(n+1-\phi(n))^2-4n}}$
- Since if we know different prime numbers p,q such that $pq=n$, we can efficiently compute $\phi(n)=(p-1)(q-1)$. And conversely, if we know n and $\phi(n)$, we can efficiently compute p,q. So finding $\phi(n)$ is as hard as finding p,q, prime factorization of n. Since we know there (almost assuredly) isn't an efficient algorithm for factoring n into p,q, there (almost assuredly) isn't an efficient algorithm for computing $\phi(n)$ given only n.

4 Problem 4

The corresponding plaintext m is 2345678, I wrote a function solversa.m to find the plaintext. Details are included in the function file, and implementation is in Problem4.txt file.

5 Problem 5

The four square roots are : 1443540, 1234567, 8119314, 7910341.
See function squareroots.m and implementation is in Problem5.txt file. Details are written in squareroots.m file.

6 Problem 6

If a is a primitive root for q, then order(a) = $\phi(q)$, and vice versa.(This is because if a is a primitive root for q, subgroup of a = Z_q^*, which means order of a is $\phi(q)$ without a being a^x, such that $x < \phi(q)$. Also if order of a is $\phi(q)$, subgroup of a = Z_q^*, then a is a primitive root for q)

Prove that if a is primitive mod q, then $a^p = -1$ mod q:

If a is primitive mod q, order(a) = $\phi(q) = q - 1 = 2p$, since q is prime and $q = 2p + 1$. So $a^{2p} = 1$ mod q according to the definition of order. Since $a^{2p} = (a^p)^2$, so either $a^p = 1$ mod q or $a^p = -1$ mod q. But if $a^p = 1$ mod q, then order(a) = p $\neq 2p$, which is a contradiction, so then $a^p = -1$ mod q.

Prove that if $a^p = -1$ mod q, then a is primitive mod q:

This equals to prove that if $a^p = -1$ mod q, then order(a) = $\phi(q) = 2p$.

Since Z_q^* is a group, then according to Lagrange Theorem, order(a)|$\phi(q)$, order(a)|$2p$. Since p is a prime, there are four possibilities of order(a): 1,2,p or 2p.

Case order(a) = 1: then $a^1 = 1$ mod q, this contradicts with the premise that $a \neq 1$ mod q. Impossible.

Case order(a) = 2: then $a^2 = 1$ mod q, which means either $a = 1$ mod q or $a = -1$ mod q, this contradicts with the premise that $a \neq 1, -1$ mod q. Impossible.

Case order(a) = p: then $a^p = 1$ mod q. This contradicts with the premise that $a^p = -1$ mod q. Impossible.

Case order(a) = 2p: then $a^{2p} = 1$ mod q. This works because $a^p = -1$ mod q, $a^{2p} = 1$ mod q

So order(a) can only be $2p = \phi(q)$, a is primitive mod q

So a is primitive mod q, if and only if $a^p = -1$ mod q.