Name:Chao Jiang
ECE5563 — Spring 2015 **HW 5** Due: Mar. 25

Problem 8.3

Why is $gcd(n, n+1) = 1$ for two consecutive integers n and $n+1$?

Proof by contradiction - suppose $gcd(n, n+1) = p > 1$.
Then n is a multiple of p, so $n = a * p$ for some integer a.
Similarly, $n + 1 = b * p$ for some integer b.
Now the next multiple of p after n will be $(a+1)p = n+p$, which is greater than $n+1$.
We have:
$n = ap < n + 1 = bp < n + p = (a + 1)p$ Dividing everything by p we get
$a < b < a + 1$ meaning that b is an integer sandwiched between a and $a + 1$. This is impossible.

Problem 8.4

Using Fermats theorem, find $3^{201} mod 11$.

11 is a prime, according to the corollary of Fermat's lettle theorem: $n^{p-1} \equiv 1 \bmod p$.
$3^{10} \equiv 1 \bmod 11$. So for $3^{201} \equiv (3^{10}....3^{10}) * 3 \bmod 11 \equiv 3 \bmod 11 = 3$.

Problem 8.20

Find all primitive roots of 25.

We know that 2 is a primitive root. The others are 2^i where i is relatively prime to $\phi(25) = 20$. So the primitive roots are $2, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}$, *and* 2^{19}. Because $\phi(20) = \phi(4)\phi(5) = 2 * 4 = 8$. So $\{2, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}\} \bmod 25$. we can write all of them as $2, 3, 8, 12, 13, 17, 22, 23$.

Problem 9.2

Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:

a. $p = 3; q = 11, e = 7; M = 5$

   For the given information, we first get $n = p * q = 33; \phi(n) = (p-1)(q-1) = 20$, thus the $C \equiv M^e \bmod n = 14$;
   $d \equiv e^{-1} \bmod 20$ then we get $d = 3$. Therefor, $M \equiv c^d \bmod n \equiv 14^3 \bmod 33 = 5$.

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

Problem 9.3

In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5, n = 35$. What is the plaintext M?

For $n = 35, p = 5, q = 7$, so $\phi(n) = 4 * 6 = 24$. $d \equiv e^{-1} \bmod 24$. then $d = 5$, So the $M \equiv c^d \bmod 35 \equiv 10^5 \bmod 35 = 5$.

Problem 9.11

Ans:
3rd element, 4^k mod N$\equiv (2^k)^2$ mod N,because it equals to the 1st squared,
5th element, because it equals to the product of 1st and 2nd
7th element, because it equals to the cube of 1st,
etc.

Problem 9.13

Consider the following scheme:

1. Pick an odd number, E.
2. Pick two prime numbers, P and Q, where $(P-1)(Q-1)-1$ is evenly divisible by E.
3. Multiply P and Q to get N.
4. Calculate $D = \frac{(P-1)(Q-1)(E-1)+1}{E}$

Is this scheme equivalent to RSA? Show why or why not.

Yes. it is equivalent to RSA.For encryption $C = M^e$ mod N, where $N = (P-1)(Q-1)$. From the given information above, we know that $(P-1)(Q-1)-1 = mE$. so we need to prove that $d \equiv e^{-1} \bmod \phi(N)$. $E * D = (P-1)(Q-1)(E-1)+1 \bmod (P-1)(Q-1) \equiv 1 \bmod \phi(N)$. So it is equivalent as RSA.