Week 9 List of Theorems

RSA Theorem (RSA)
Let p and q be two distinct primes. If we define the following variables

1. $n = pq$ and $\phi(n) = (p-1)(q-1)$, and
2. e is a positive integer, $2 \leq e < \phi(n)$, such that $\gcd(e, \phi(n)) = 1$, and
3. d is a positive integer, $2 \leq d < \phi(n)$, such that $ed \equiv 1 \pmod{\phi(n)}$, and
4. M is an integer such that $0 \leq M < n$, and
5. C is an integer, $0 \leq C < n$, such that $C \equiv M^e \pmod{n}$, and
6. R is an integer, $0 \leq R < n$, such that $R \equiv C^d \pmod{n}$,

then $R = M$.

Properties of Conjugates (PCJ)
If z and w are complex numbers, then

1. $\overline{z+w} = \overline{z} + \overline{w}$.
2. $\overline{zw} = \overline{z}\,\overline{w}$.
3. $\overline{\overline{z}} = z$.
4. $z + \overline{z} = 2\mathrm{Re}(z)$.
5. $z - \overline{z} = 2i\mathrm{Im}(z)$.

Properties of Modulus (PM)
If z and w are complex numbers, then

1. $|z| = 0$ if and only if $z = 0$.
2. $|\bar{z}| = |z|$.
3. $|z|^2 = z\bar{z}$.
4. $|zw| = |z|\ |w|$.
5. $|z + w| \leq |z| + |w|$.