# Math. 304 Number Theory (Spring 2019)
# Preparation No. 3

March 04, 2019

- 일반 강의로 들을 학생은 퀴즈를 제출하지 않고 나중에 과제물을 제출하면 됨.

- Study the following materials from the text:

(a) Section 3.5: (1) Lagrange's theorem, statement and proof, (2) Another proof of Wilson's theorem using Lagrange's theorem, (3) The converse of Lagrange's theorem does not hold.

(b) First half of Section 3.6: (1) Definition of primitive root modulo $n$, (2) Primitive root theorem and its proof for $n = p,$ and $p^j$.

- Quiz ♯3.

**1.** Show that $2^{2^5} + 1$ is divisible by 641.

**2.** Let $p$ be a prime such that $n < p < 2n$. Prove that

(i) $\binom{2n}{n} \equiv 0(\mod p)$.

(ii) $\binom{2n}{n}$ is not equivalent to $0(\mod p^2)$.

**3.** Let $p$ be an odd prime.

(i) Show that $2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv (-1)^{\frac{(p+1)}{2}}(\mod p)$.

(ii) Show that $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv 2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2(\mod p)$.

**4.** Find an example of $m$ such that the congruence $x^3 - 1 \equiv 0(\mod m)$ has more than 4 solutions.

**The End**