Study guide

- (§10) Know the definition and various interpretations of the Euler ϕ function.
- (§10) The *statement* of Euler's theorem, and how to apply it.
- (§10) Understand the proof of Euler's theorem.
- (§10) How can Euler's theorem (or Fermat's little theorem, in prime modulus) used to compute roots in modular arithmetic?

1. Let a, m, n be positive integers, with $a \geq 2$. Prove that if $a^m + 1$ divides $a^n + 1$, then m divides n.

2. Suppose that a, b are two positive integers such that $\gcd(a, b) = 1$. Prove that there exists integers u, v such that the following congruences hold.

$$\begin{aligned} u &\equiv 0 \pmod{a} \quad & u &\equiv 1 \pmod{b} \\ v &\equiv 1 \pmod{a} \quad & v &\equiv 0 \pmod{b} \end{aligned}$$

   Hint Turn one congruence into an equation, and plug it into the other congruence.

3. (a) Determine $\phi(100)$. You are free to look up and use a general formula for $\phi(n)$ (or wait until it is stated in class), or reason it out in some other way. One useful observation: $\gcd(a, 100) = 1$ unless either $2 \mid a$ or $5 \mid a$, since 2 and 5 are the prime factors of 100.

   (b) Determine the last two digits (tens digit and units digit) of 19^{5085}.

4. Solve the congruence $x^{17} \equiv 5 \pmod{43}$.