Theorems of Fermat and Euler

We state and prove two important theorems by famous mathematicians, one by Pierre de Fermat and the other by Leonhard Euler. Both theorems concern powers in modular arithmetic. The results are fundamental and will be used over and over again. This material supplements T&W, pp. 79-83.

Theorem (Key Fact). We recall that if \( \gcd(z, n) = 1 \), then \( z^{-1} \pmod{n} \) exists.

Theorem (Fermat’s Little Theorem). Assume that \( p \) is prime and that \( \gcd(a, p) = 1 \) (or equivalently that \( p \) does not divide \( a \), or that \( a \) and \( p \) are relatively prime). Then

\[
a^{p-1} \equiv 1 \pmod{p}.
\]

Proof. First we apply the Key Fact with \( z = a \) and \( n = p \), concluding that \( a^{-1} \pmod{p} \) exists because \( \gcd(a, p) = 1 \). Let \( S = \{1, 2, \ldots, p-1\} \), so that \( \mathbb{Z}_p = S \cup \{0\} \). Let the map \( \psi : S \to S \) be defined by \( \psi(x) = ax \). The following three facts are true:

1. If \( x \in S \), then \( \psi(x) = ax \in S \), so \( \psi \) is well-defined. (Proof. If \( \psi(x) = ax = 0 = a \cdot 0 \), then \( a^{-1}ax \equiv a^{-1}0 \pmod{p} \) (by our Key Fact), so \( x = 0 \), a contradiction.)

2. If \( \psi(x) = \psi(y) \), then \( x = y \) (\( \psi \) is one-to-one). (Proof. From the Key Fact, if \( ax \equiv ay \pmod{p} \) in \( \mathbb{Z}_p \), then \( a^{-1}ax \equiv a^{-1}ay \pmod{p} \) so \( x = y \).)

3. \( \psi \) permutes the elements of \( S \). That is \( \{\psi(1), \psi(2), \ldots, \psi(p-1)\} \) is the same set as \( \{1, 2, \ldots, p-1\} \), possibly in a different order. (Proof. This follows from (1) and (2).)

Therefore

\[
(*) \quad 1 \cdot 2 \cdot \cdots (p-1) \equiv \psi(1) \cdot \psi(2) \cdots \psi(p-1) \quad \text{(same factors, usually rearranged)}
\]

\[
\equiv (a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \quad \text{(definition of \( \psi \))}
\]

\[
\equiv a^{p-1}(1 \cdot 2 \cdots (p-1)) \pmod{p} \quad \text{(collecting terms)}.
\]

Now \( \gcd(j, p) = 1 \) for every \( j \in S \). Once more by our Key Fact with \( z \) replaced successively by \( j = 1, 2, \ldots, p-1 \), we see that we can divide this congruence by \( j = 1, 2, \ldots, p-1 \), leaving \( 1 \equiv a^{p-1} \pmod{p} \) which was to be proved.

Examples. (1) Explicitly verify line (*) if \( p = 7 \) and \( a = 4 \). (Answer: \( 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 4 \cdot 1 \cdot 5 \cdot 2 \cdot 6 \cdot 3 \pmod{7} \) in that order.)

(2) Let \( p \) be prime and \( \gcd(a, p) = 1 \). Find \( a^{-1} \). Answer. By Fermat’s theorem, \( a^{p-1} \equiv 1 \pmod{p} \). Then \( a^{p-2} \equiv a^{-1} \pmod{p} \). Now isn’t that simple!! Fermat’s Little Theorem is a very quick way to find inverses modulo a prime.
(3) Find \( 2^{714} \pmod{11} \). **Answer.** \( 2^{10} = 1024 \equiv 1 \pmod{11} \) by easy computation. Now \( 2^{714} = 2^{710 \cdot 2^4} \equiv 1^{71} \cdot 2^4 \equiv 16 \equiv 5 \pmod{11} \).

(4) Show that \( 2^{560} \equiv 1 \pmod{561} \). **Answer.** This is a little tricky because 561 is not a prime (cf. T&W, p. 79). We will combine Fermat’s Little Theorem and the Chinese remainder theorem. 561 = 3 \cdot 11 \cdot 17. Now \( 2^2 \equiv 1 \pmod{3} \), so \( 2^{560} = (2^3)^{280} \equiv 1 \pmod{3} \) by Fermat’s theorem. Similarly, \( 2^{560} = (2^{10})^{56} \equiv 1 \pmod{11} \) and \( 2^{560} = (2^{16})^{35} \equiv 1 \pmod{17} \). This leaves

\[
2^{560} \equiv 1 \pmod{3} \\
2^{560} \equiv 1 \pmod{11} \\
2^{560} \equiv 1 \pmod{17}
\]

which we show satisfies \( 2^{560} \equiv 1 \pmod{561} \) by the Chinese remainder theorem. Fill in the details.

Now we generalize Fermat’s Little Theorem. Let \( n \) be an arbitrary positive integer. We observe that we may apply our Key Fact to compute \( a^{-1} \) any time that \( \gcd(a, n) = 1 \). This suggests that we focus on precisely those numbers \( a, 1 \leq a \leq n \) that are relatively prime to \( n \).

The first thing that we can do is count them. We let \( \phi(n) \) denote the number of integers \( 1 \leq a \leq n \) such that \( \gcd(a, n) = 1 \) (or \( 1 \leq a < n \) since \( a = n \) never satisfies \( \gcd(n, n) = 1 \)). \( \phi(n) \) is called the Euler \( \phi \)-function. It is possible to write down a formula for \( \phi(n) \) in terms of the prime factors of \( n \). First let’s look at some examples.

**Examples.** Verify that the value of \( \phi(n) \) for the given \( n \) is correct.

1. \( \phi(7) = 6 \).
2. \( \phi(6) = \phi(2 \cdot 3) = 2 \). The numbers between 1 and 6 relatively prime to 6 are 1, 6.
3. \( \phi(35) = \phi(5 \cdot 7) = 24 \). The numbers between 1 and 35 relatively prime to 35 are
   
   \[
   1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.
   \]
4. \( \phi(120) = 32 \).

**Proposition.** The following facts are true about the Euler \( \phi \)-function.

1. \( \phi(p) = p - 1 \) if \( p \) is prime.
2. \( \phi(pq) = (p - 1)(q - 1) \) if \( p \) and \( q \) are prime.
(3) In general the formula for $\phi(n)$ is:

$$\phi(n) = n \prod_{p \mid n} (1 - \frac{1}{p})$$

where the product is over distinct primes $p$ dividing $n$.

We are now in a position to state Euler’s theorem.

**Theorem** (Euler’s Theorem). If $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

**Remark.** When $n = p$ is prime, then $\phi(p) = p - 1$, and we get Fermat’s Little Theorem.

**Theorem** (Basic Principle). If you want to work mod $n$, then you should work mod $\phi(n)$ in the exponent. Specifically let $a, n, x, y$ be integers with $n \geq 1$ and $\gcd(a, n) = 1$. If $x \equiv y \pmod{\phi(n)}$, then $a^x \equiv a^y \pmod{n}$.

**Proof.** Let $x = y + \phi(n)k$. Then

$$a^x = a^{y + \phi(n)k} = a^y(a^{\phi(n)})^k \equiv a^y \pmod{n}.$$

**Remark.** Because we do so many calculations with large numbers and high powers, this Basic Principle combining modular arithmetic and powers is very important and will be used repeatedly.

**Examples.** Cf. T&W, p. 82.

1. What are the last 2 digits of $11^{84}$? 
   **Answer.** Knowing the last two digits is equivalent to working mod 100. $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$. Therefore, $11^{84} = (11^{40})^{2}11^{4} \equiv 11^{4} \equiv 14461 \equiv 61 \pmod{100}$.

2. Compute $2^{78312} \pmod{11}$. 
   **Answer.** By Fermat’s theorem, we know that $2^{10} \equiv 1 \pmod{11}$. Therefore,

$$2^{78312} \equiv (2^{10})^{7831}2^{2} \equiv 1^{7831}2^{2} \equiv 4 \pmod{11}.$$