6.5. Introduction to Euler's Function

Note. In this section, we consider numbers relatively prime to to a given positive integer n. Euler's function, $\varphi(n)$, gives a count of these relatively prime numbers. Like in the previous section, all numbers in this section are assumed to be integers. Much of this material is covered in Elementary Number Theory (MATH 3120); see my online ntoes for this class on Section 9. Euler's Theorem and Function.

Definition. Numbers (i.e., integers) a and b are *relatively prime* (or *coprime*) if their greatest common divisor is 1: $(a, b) = 1$.

Definition. If m is a positive integer, then denote the number of positive integers less than or equal to m and relatively prime to m as $\varphi(m)$, called the *Euler* φ *function* (or the *totient* function). Symbolically,

$$\varphi(m) = \#\{k \mid 1 \leq k \leq m \text{ and } (k, m) = 1\}.$$

Example 6.50/Note. Notice that $\varphi(6) = 2$ because among $1, 2, 3, 4, 5, 6$ the numbers relatively prime with 6 are 1 and 5. We have $\varphi(1) = 1$. If p is prime then (and only then) $\varphi(p) = p-1$. In Section 6.6. The Inclusion-Exclusion Principle and Euler's Function we will have a formula for computing $\varphi(n)$ in terms of the standard factorization of n given by the Fundamental Theorem of Arithmetic (Theorem 6.29).

Note. In Euler's Theorem below, we give a congruence relation involving Euler's φ function. We first need a preliminary lemma.

Lemma 6.51.

(i) If $m \mid ab$ and $(m, a) = 1$, then $m \mid b$.

(ii) **(The Cancellation Law.)** If $ax \equiv ay \pmod{m}$ and $(a, m) = 1$, then $x \equiv y \pmod{m}$.

Theorem 6.52. Euler's Theorem.

Suppose m is positive and $(x, m) = 1$. Then $x^{\varphi(m)} \equiv 1 \pmod{m}$.

Corollary 6.53. Fermat's Theorem/Fermat's Little Theorem.

If p is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Note. For given integer m, exploration of the question "Is m prime?" can be difficult. One could check all of the primes up to $\sqrt{m}$ to see if they divide m or not (this gives a conclusive answer to the question). Fermat's Theorem (with $a = 2$) implies that if m is an odd prime then $2^{m-1} \equiv 1 \pmod{m}$. By the contrapositive of this, we see that if $2^{m-1} \not\equiv 1 \pmod{m}$ then m is *not* prime. This approach is inconclusive when $2^{m-1} \equiv 1 \pmod{m}$. These claims are true, but that does not mean that they are computationally practical.

Definition. Let $m > 0$. For any x, by the Division Algorithm (Theorem 6.17), $x = mq + r$ for unique integers q and r where $0 \leq r \leq m - 1$. That is, there is unique r with $0 \leq r \leq m - 1$ such that $x \equiv r \pmod{m}$. The nonnegative integer r is the *residue of x modulo m*, denoted "$x \pmod{m}$." Replacing a number by its residue is called *reduction mod m*.

Note. Reduction mod m can greatly simplify computations. For example, suppose we want to find the residue $7^{16} \pmod{11}$. Reducing as we go and taking advantage of the fact that the exponent is a power of 2, we have:

$$\begin{aligned} 7^2 &= 49 \equiv 5 \pmod{11} \\ 7^4 &\equiv 5^2 \equiv 3 \pmod{11} \\ 7^8 &\equiv 3^2 \equiv 9 \pmod{11} \\ 7^{16} &\equiv 9^2 \equiv 4 \pmod{11}. \end{aligned}$$

So $7^{16} \equiv 4 \pmod{11}$. By the way, $7^{16} = 33{,}232{,}930{,}569{,}601$ so we see that we have definitely simplified the computation!

Example 6.54. We now apply a technique similar to that above to check if $n = 529$ is prime. We use Fermat's Theorem (Corollary 6.53) will $a = 2$ and "alleged prime" $p = 529$ to check if $2^{528} \equiv 1 \pmod{529}$. If this is false (which, as we'll see, it is), then p is not prime. Notice that $p - 1 = 528 = 512 + 16 = 2^9 + 2^4$. So we consider

(with the help of a calculator, since the numbers are ugly):

$$\begin{aligned}
2^{2^3} &= 2^8 = 256 \\
2^{2^4} &= (256)^2 = 65526 \equiv 469 \pmod{529} \\
2^{2^5} &\equiv (469)^2 = 219961 \equiv 426 \pmod{529} \\
2^{2^6} &\equiv (226)^2 = 181476 \equiv 29 \pmod{529} \\
2^{2^7} &\equiv (29)^2 = 841 \equiv 312 \pmod{529} \\
2^{2^8} &\equiv (312)^2 = 97344 \equiv 8 \pmod{529} \\
2^{2^9} &\equiv 8^2 = 64 \pmod{529}
\end{aligned}$$

This gives (by Corollary 6.43) that

$$2^{258} = 2^{2^9} \cdot 2^{2^4} \equiv 64 \cdot 469 = 30016 \equiv 392 \not\equiv 1 \pmod{529}.$$

This is the case in which Fermat's Theorem is conclusive; we conclude that 529 is not prime (in fact, $529 = (23(^2)$. Notice that this computation required only six squaring and reducing steps (followed by one multiplication step). If we had checked all primes up to $\sqrt{n} = \sqrt{529} = 23$, so this is a simplified approach. Gerstein makes an argument (see page 313) that the number of squaring and reducing steps grows logarithmically in n, whereas testing divisibility of individual primes grows (something like) $\sqrt{n}$. So for very large n, Fermat's Theorem offers a significantly more efficient algorithm for testing a number for primeness.