22. THE EULER φ-FUNCTION

We began with a discussion of the homework problem. Lisa A. and Gabe came up with the correct formula for \( \phi(pq) \), where \( p \) and \( q \) are distinct primes. The class as a whole provided the proof:

**Theorem:** Let \( p \) and \( q \) be distinct primes. Then

\[
\phi(pq) = (p-1)(q-1) = pq - p - q + 1.
\]

**Proof:** As in the proof of \( \phi(p^k) \), we start with the set \( \{1, 2, \ldots, pq\} \) and take out all those numbers which are not relatively prime to \( pq \). An integer is not relatively prime to \( pq \) if and only if it is a multiple of \( p \) or \( q \) (or both). Since every \( p \)th integer is a multiple of \( p \) and the list ends with a multiple of \( p \), we conclude that there are \( \frac{1}{p}(pq) = q \) integers in the list which are multiples of \( p \). By the same reasoning, there are \( \frac{1}{q}(pq) = p \) multiples of \( q \) in the list. However, we’ve counted \( pq \) twice as it is a multiple of both \( p \) and \( q \). Since \( p \) and \( q \) are primes, \( pq \) is the only number in our range which is a multiple of both \( p \) and \( q \). Thus,

\[
\phi(pq) = pq - (\# \text{ of multiples of } p) - (\# \text{ of multiples of } q) + (\# \text{ of multiples of } pq) \\
= pq - q - p + 1 \\
= (p-1)(q-1).
\]

Next, we applied the same reasoning to get a formula for \( \phi(pqr) \), where \( p, q \) and \( r \) are distinct primes?

**Theorem:** Let \( p, q \) and \( r \) be distinct primes. Then

\[
\phi(pqr) = pqr - pr - qr - pq + p + q + r - 1 = (p-1)(q-1)(r-1).
\]

**Proof:** Reasoning as before, we start with the list \( \{1, 2, \ldots, pqr\} \). We want to subtract out all integers in this list which are not relatively prime to \( pqr \), i.e., integers which are multiples of \( p \) or \( q \) or \( r \). As before, we get \( \frac{1}{p}(pqr) = qr \) multiples of \( p \), \( \frac{1}{q}(pqr) = pr \) multiples of \( q \), and \( \frac{1}{r}(pqr) = pq \) multiples of \( r \). We subtract them out to get \( pqr - qr - pr - pq \). But, we’ve counted multiples of \( pq \) twice (since they are multiples of both \( p \) and \( q \)) and there are \( \frac{1}{pq}(pqr) = r \) of those. So we add \( r \) back to the total. Similarly, we counted the multiples of \( pr \) (\( q \) of them) and \( qr \) (\( p \) of them) back in, to get \( pqr - pq - qr - pr + p + q + r \). Finally, in our ‘adding back in stage’, we added the multiples of \( pqr \) (of which there is only one) back in 3 times (being a multiple of \( pq \), \( pr \) and \( qr \)) after it was subtracted out 3 times (being a multiple of \( p, q, \) and \( r \)). So we still need to subtract it out, since it is not relatively prime to \( pqr \). Thus, our final number for the number of integers between 1 and \( pqr \) which are relatively prime to \( pqr \) is

\[
pqr - pq - pr - qr + p + q + r - 1.
\]

We can also use this reasoning to do more cases, such as \( \phi(pqr) \) where \( p, q, r, \) and \( s \) are distinct primes. However, the arguments become increasingly more complicated. Instead, we will get a general formula by a different route. For now, we will just state the formula and prove it later:
**Theorem:** Let $m = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ be the prime factorization of $m$, where $p_1, \ldots, p_t$ are distinct primes. Then

$$
\phi(m) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \cdots \phi(p_t^{k_t}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_t^{k_t} - p_t^{k_t-1}).
$$

**Example:** Assuming the above formula is true, then $\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 120 = 480$. Thus, there are 480 integers between 1 and 1000 which are relatively prime to 1000.

Next, we did another numerical experiment: We calculated the value of $a^{\phi(m)} \pmod{m}$ for various values of $m$ and $a$ with $\gcd(a, m) = 1$. For example, we found:

$$
4^{\phi(9)} \equiv 1 \pmod{9} \\
9^{\phi(14)} \equiv 1 \pmod{14} \\
2^{\phi(15)} \equiv 1 \pmod{15} \\
11^{\phi(16)} \equiv 1 \pmod{16}
$$

If we tried values of $a$ which were not relatively prime to $m$, we got entirely different results:

$$
3^{\phi(9)} \equiv 0 \pmod{9} \\
7^{\phi(14)} \equiv 7 \pmod{14} \\
3^{\phi(15)} \equiv 12 \pmod{15}
$$

Ryan made the following conjecture:

**Conjecture:** (Ryan) Let $m \geq 2$ be an integer and $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Huy noticed that this conjecture looks similar to Fermat’s (Little) Theorem: If $p$ is prime and $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$. In fact, if $m = p$ in the above conjecture, we get exactly Fermat’s Theorem, since $\phi(p) = p - 1$ and $\gcd(a, p) = 1$ if and only if $a \not\equiv 0 \pmod{p}$.

Next, we set out to prove Ryan’s conjecture. To do so, we attempted to mimic the (second) proof we gave for Fermat’s Theorem. We reintroduced some notation:

For an integer $m \geq 2$, we let $S_m$ be the set of integers between 1 and $m - 1$ which are relatively prime to $m$. For example, we have:

$$
S_4 = \{1, 3\} \\
S_8 = \{1, 3, 5, 7\} \\
S_9 = \{1, 2, 4, 5, 7, 8\} \\
S_{10} = \{1, 3, 7, 9\}
$$
In general, we know there are $\phi(m)$ elements in $S_m$, so we can write the set $S_m$ as \{x_1, x_2, \ldots, x_{\phi(m)}\}. If we wrote these elements in ascending order (there is no real reason to, however), we would have $x_1 = 1$ and $x_{\phi(m)} = m - 1$.

Now let $a \in S_m$; i.e., gcd$(a, m) = 1$. We claim that for all $x \in S_m$, $ax \% m \in S_m$. To see this, suppose not. Let $r = ax \% m$. Certainly $r$ is between 0 and $m - 1$. So if $r \not\in S_m$, we must have gcd$(r, m) > 1$. This means there is a prime $p$ such that $p$ divides both $r$ and $m$. Now, since $r = ax \% m$, we have $ax = mq + r$ for some $q \in \mathbb{Z}$. Since $p$ divides both $m$ and $r$, $p$ divides $mq + r$ and hence $ax$. But since $p$ is prime, this means that $p$ divides $a$ or $p$ divides $x$. But this can’t happen, since gcd$(a, m) = 1$ and gcd$(x, m) = 1$. Thus, we must have gcd$(r, m) = 1$.

As with the proof of Fermat’s Theorem, for $a \in S_m$ define a function $f_a^m : S_m \to S_m$ by $f_a^m(x) = ax \% m$ for each $m \in S_m$. By the preceding paragraph, since gcd$(ax \% m, m) = 1$, we have $f_a^m(x) \in S_m$.

Let’s do an example with $m = 9$. We have $S_9 = \{1, 2, 4, 5, 7, 8\}$. Choose a random element in $S_9$, say 4. Then

\[
\begin{align*}
f_4^1(1) &= 4 \cdot 1 \% 9 = 4 \\
f_4^1(2) &= 4 \cdot 2 \% 9 = 8 \\
f_4^1(4) &= 4 \cdot 4 \% 9 = 7 \\
f_4^1(5) &= 4 \cdot 5 \% 9 = 2 \\
f_4^1(7) &= 4 \cdot 7 \% 9 = 1 \\
f_4^1(8) &= 4 \cdot 8 \% 9 = 5
\end{align*}
\]

Notice that, just as with the case $m = p$ is prime (which we did before) every element in $S_9$ was ‘hit’; that is, the map is one-to-one and onto.

We made the following conjecture

**Conjecture:** Suppose $m$ is prime and $a \in S_m$. Then the map $f_a^m : S_m \to S_m$ is one-to-one and onto.

**Proof:** By the Pigeonhole Principle, it suffices to prove that $f_a^m$ is one-to-one. Suppose $f_a^m(i) = f_a^m(j)$ for some elements $i \neq j$ in $S_m$. Then $ai \% m = aj \% m$, which means $ai \equiv aj \pmod{m}$. Since gcd$(a, m) = 1$, by cancellation we have that $i \equiv j \pmod{p}$. But, since $i$ and $j$ are between 1 and $m - 1$, this means that $i = j$, a contradiction. Hence, $f_a^m$ must be one-to-one (and thus onto). \[\square\]

We now are in a position to prove Ryan’s conjecture (again, mimicking the proof from Fermat’s Theorem). The result is known as **Euler’s Theorem**:

**Theorem:** (Euler’s Theorem) Let $m \geq 2$ be an integer and $a$ an integer such that gcd$(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

**Proof:** It is enough to prove this in the case $a \in S_m$, since by the reasoning above (three paragraphs ago) $a$ is relatively prime to $m$ if and only if its remainder upon dividing $a$ by
$m$ is relatively prime to $m$. By the conjecture above, $f_m^a : S_m \to S_m$ is one-to-one and onto, we have

$$S_p = \{x_1, x_2, \ldots, x_{\phi(m)}\} = \{f_m^a(x_1), f_m^a(x_2), \ldots, f_m^a(x_{\phi(m)})\} = \{ax_1 \%(m), ax_2 \%(m), \ldots, ax_{\phi(m)} \%(m)\}$$

Since the elements in these sets are the same (with just the order scrambled), the products of their elements are the same:

$$x_1 x_2 \cdots x_{\phi(m)} = (ax_1 \%(m))(ax_2 \%(m))\cdots(ax_{\phi(m)} \%(m)).$$

Instead of using the ‘$\%$ $m$’ notation, we can instead write this as a modular equation:

$$x_1 x_2 \cdots x_{\phi(m)} \equiv (ax_1)(ax_2)\cdots(ax_{\phi(m)}) \pmod m$$

$$\equiv x_1 x_2 \cdots x_{\phi(m)} a^{\phi(m)} \pmod m$$

Since each $x_i$ is relatively prime to $m$, we can cancel it from both sides of the modular equation. (Equivalently, we could multiply both sides of the equation by the inverse of $x_i$.) Doing this for all $x_i$, we obtain:

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

\[\square\]

There was no homework assigned for Tuesday.