Modular arithmetic II

We now look at modular arithmetic again, to prove some results that we skipped over the first time.

1 Chinese remainder theorem

We first prove what is commonly known as the “Chinese remainder theorem”. As an application, this will let us quickly calculate $\phi(m)$ in terms of the prime factorization of $m$.

Let’s go ahead and state the result about $\phi(m)$, so that we are not burying the lede.

**Theorem 1.** Suppose $m = p_1^{a_1} \cdots p_r^{a_r}$ is the prime factorization of $m$, so that $a_j \geq 1$ for $j = 1, 2, \ldots, r$. Then $\phi(m) = \prod_{j=1}^{r} \left( (p_j - 1)p_j^{a_j - 1} \right)$.

**Example 2.** Here are two special cases of the theorem:

1. Suppose $m = p_1p_2$. Then $\phi(m) = (p_1 - 1)(p_2 - 1)$. So, for example, $\phi(15) = 2 \cdot 4 = 8$, as we computed before.

2. Suppose $m = p^j$ is a power of $p$. Then $\phi(m) = (p - 1)p^{j-1}$. So, for example, $\phi(9) = 2 \cdot 3 = 6$ and $\phi(27) = 2 \cdot 9 = 18$.

**Example 3.** This is a non-example. Is there an integer $x$ that is

- $\equiv 3 \pmod{10}$
- $\equiv 2 \pmod{15}$?

The answer is “no”, because such an $x$ must on the one hand be 3 modulo 5 and on the other hand be 2 modulo 5. So, the problem, so to speak, is that 5|10 and 5|15, so there is a possibility for an obvious incompatibility between the two congruences.

This leads us to

**Theorem 4** (Chinese Remainder Theorem). Suppose $(m_1, m_2) = 1$, and $a_1, a_2$ are two integers. Then there is an $x$ with

- $x \equiv a_1 \pmod{m_1}$
- $x \equiv a_2 \pmod{m_2}$.

Moreover, such an $x$ is unique modulo $m = m_1m_2$.

**Proof.** Let’s do uniqueness first. If $x, x'$ are two solutions to the above two congruence, then $x - x'$ is $\equiv 0 \pmod{m_1}$ and $\equiv 0 \pmod{m_2}$. Thus $m_1 | (x - x')$ and $m_2 | (x - x')$. Because $(m_1, m_2) = 1$, $m = m_1m_2$ divides $x - x'$. Thus $x \equiv x' \pmod{m}$.

For the existence, one proceeds as follows. As we have shown before, $(m_1, m_2) = 1$ implies that there exists integers $y_1, y_2$ with $m_1y_1 + m_2y_2 = 1$. From this equation, we obtain

- $m_1y_1 \equiv 0 \pmod{m_1}$ and $\equiv 1 \pmod{m_2}$, while
- $m_2y_2 \equiv 0 \pmod{m_2}$ and $\equiv 1 \pmod{m_1}$.

Then $x = m_1y_1a_1 + m_2y_2a_2$ satisfies

- $x \equiv a_1 \pmod{m_1}$
- $x \equiv a_2 \pmod{m_2}$.

Thus $x$ is the unique solution modulo $m = m_1m_2$.


• $m_2y_2 \equiv 1 \pmod{m_1}$ and $\equiv 0 \pmod{m_2}$.

Set $x = a_2(m_1y_1) + a_1(m_2y_2)$. Multiplying the above congruences by $a_2$ and $a_1$, respectively, and adding, one gets the desired result for $x$.

**Example 5.** Note that $4 \cdot 7 - 3 \cdot 9 = 1$. Find an integer $x$ so that

- $x \equiv 4 \pmod{7}$
- $x \equiv 3 \pmod{9}$.

**Answer:**

- $4 \cdot 7$ is $\equiv 0 \pmod{7}$ and $1 \pmod{9}$ while
- $(-3) \cdot 9$ is $\equiv 1 \pmod{7}$ and $\equiv 0 \pmod{9}$.

Thus $3 \cdot 7 \cdot 4 + 4 \cdot 9 \cdot (-3) = 12 \cdot (7 - 9) = -24$ is equivalent to $4 \pmod{7}$ and $\equiv 3 \pmod{9}$. We could also take $x = -24 + 63 = 39$ for $x$.

We stated a simple version of the CRT. Here is the more general version:

**Theorem 6.** Suppose $m_1, m_2, \ldots, m_r$ are pairwise relatively prime, so that $(m_i, m_j) = 1$ if $i \neq j$. Let $a_1, \ldots, a_j$ be integers. Then there is an integer $x$ with $x \equiv a_j \pmod{m_j}$ for $j = 1, 2, \ldots, r$. Moreover, $x$ is unique modulo $m = m_1 \cdots m_r$.

**Proof.** Set $m_j' = \frac{m}{m_j}$. Because $m_j, m_j'$ are relatively prime, there exists an integer $b_j$ with $m_j'b_j \equiv 1 \pmod{m_j}$. Set

$$x = \sum_{j=1}^{r} m_j'b_ja_j.$$ 

Then all but the $j^{th}$ term in the sum is 0 modulo $m_j$, while the $j^{th}$-term is equivalent to $a_j$ modulo $m_j$. Thus $x \equiv a_j \pmod{m_j}$ for each $j$. The uniqueness of $x$ modulo $m$ follows just as the $m = m_1m_2$ case of the CRT proved above.

## 2 Euler’s $\phi$ function

The function $\phi(m)$ is called Euler’s $\phi$ function, or his “totient” function (not that you need to know that.) Recall

**Definition 7.** For a positive integer $m$, $\phi(m)$ is the number of integers $a$ with $1 \leq a \leq m$ and $(a, m) = 1$.

In order to prove Theorem [Euler's phi function](#), we require the following lemma.

**Lemma 8.** Suppose $m = m_1m_2$ with $(m_1, m_2) = 1$. Then $\phi(m) = \phi(m_1)\phi(m_2)$.

**Proof.** We want to count the integers $x$ with

- $1 \leq x \leq m_1m_2$
• \((x, m_1) = 1\)
• \((x, m_2) = 1\).

Equivalently, we want to count the \(x\) modulo \(m\) with \((x, m_1) = 1\) and \((x, m_2) = 1\).

Suppose

• \(a_1, \ldots, a_{\phi(m_1)}\) are the classes modulo \(m_1\) prime to \(m_1\) and
• \(b_1, \ldots, b_{\phi(m_2)}\) are the classes modulo \(m_2\) prime to \(m_2\).

Then \((x, m_1) = 1\) and \((x, m_2) = 1\) if and only if there is some \(j, k\) with

• \(x \equiv a_j \pmod{m_1}\) and
• \(x \equiv b_k \pmod{m_2}\).

By the CRT, there exists a unique \(x\) modulo \(m\) for each pair \((a_j, b_k)\). Thus, the total number of \(x\) with \(1 \leq x \leq m_1 m_2\) and \((x, m_1) = 1\), \((x, m_2) = 1\) is \(\phi(m_1)\phi(m_2)\).

Let’s do an example: Take \(m = 15 = 3 \cdot 5\).

<table>
<thead>
<tr>
<th>(x)</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>1</td>
<td>7</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>11</td>
<td>2</td>
<td>8</td>
<td>14</td>
</tr>
</tbody>
</table>

The table shows the 15 residue classes modulo 15. Which row a number sits in says what this number is modulo 3, and which column a number sits in says what this number is modulo 5. The way to make such a table is to start with the 0 in the upper left corner, and move “southeast”, writing in \(0, 1, 2, \ldots\). And then, when one reaches the bottom one “wraps around” to the top, and when one reaches the right edge, one “wraps around” to the left.

Note that all the numbers that are outside the 0th row and column are the residue classes that are relatively prime to 15. So, the picture shows that \(\phi(15) = \phi(3)\phi(5) = 2 \cdot 4\).

From Lemma 8, we can now prove Theorem 1.

**Proof of Theorem 7.** We have \(\phi(p) = p - 1\) if \(p\) is a prime. More generally, consider powers of primes. If \(1 \leq x \leq p^j\), then \(x\) is prime to \(p^j\) if and only if \(x\) is prime to \(p\). So \(\phi(p^j) = p^j - p^j - 1\) because

• \(p^j\) is the number of \(x\) with \(1 \leq x \leq p^j\)
• \(p^j - 1\) is the number of multiples of \(p\) between 1 and \(p^j\).

Thus \(\phi(p^j) = (p - 1)p^j - 1\). Theorem 1 thus follows from \(\phi(m_1 m_2) = \phi(m_1)\phi(m_2)\) when \(m_1, m_2\) are relatively prime.

We are getting closer to proving

**Theorem 9.** If \(p\) is a prime, then there exists \(g\) with \(ord_p(g) = p - 1\).

Our proof uses the following proposition about the Euler \(\phi\)-function.
Proposition 10. One has

\[ \sum_{d|m} \phi(d) = m. \]

For example

- \( m = p \), then \( \phi(1) + \phi(p) = 1 + (p - 1) = p \)
- \( m = p_1p_2 \), then

\[
\phi(1) + \phi(p_1) + \phi(p_2) + \phi(p_1p_2) = 1 + (p_1 - 1) + (p_2 - 2) + (p_1 - 1)(p_2 - 1) = p_1p_2.
\]

Proof of Proposition 10. If \( m \) is prime, we are done by the above example. Otherwise, \( m = m_1m_2 \) for some integers \( m_1, m_2 \) with \( 1 < m_j < m \) and \( (m_1, m_2) = 1 \).

Now, note that an integer \( d \mid m \) if and only if \( d = d_1d_2 \) for integers \( d_1 \mid m_1 \) and \( d_2 \mid m_2 \). Thus

\[
\sum_{d|m} \phi(d) = \sum_{d_1|m_1, d_2|m_2} \phi(d_1d_2)
= \sum_{d_1|m_1, d_2|m_2} \phi(d_1)\phi(d_2)
= \left( \sum_{d_1|m_1} \phi(d_1) \right) \left( \sum_{d_2|m_2} \phi(d_2) \right)
= m_1m_2.
\]

The last equality follows by induction. \( \square \)

3 Generators modulo \( p \)

We are almost ready to prove Theorem \( 9 \).

For \( p \) a prime, and \( h \) an integer, denote by \( N_p(h) \) the number of nonzero residue classes \( r \) modulo \( p \) with \( ord_p(r) = h \).

Lemma 11. With notation as above, \( N_p(h) \leq \phi(h) \). In fact, \( N_p(h) = 0 \) or \( N_p(h) = \phi(h) \).

Proof. If there are no elements \( r \) with \( ord_p(r) = h \), then \( N_p(h) = 0 \) and we are done. Thus, suppose \( ord_p(r) = h \). Then, \( r \) is a solution to \( x^h - 1 \equiv 0 \mod p \).

We have already proved that degree \( h \) equations have at most \( h \) roots modulo \( p \), so \( N_p(h) \leq h \). Why \( \leq \phi(h) \)?

- \( ord_p(r) = h \Rightarrow 1, r, r^2, \ldots, r^{h-1} \) are distinct modulo \( p \)
- these powers of \( r \) are solutions to \( x^h - 1 \equiv 0 \mod p \)
- Thus, these powers of \( r \) are the only solutions to \( x^h - 1 \equiv 0 \mod p \).
- However, we have already proved \( ord_p(r^d) = \frac{h}{\gcd(h,d)} \).
• Thus, $\text{ord}_p(r^d) = h$ if and only if $(d, h) = 1$.

Therefore, the classes modulo $p$ with order $h$ are exactly the $r^d$ with $(d, h) = 1$. Consequently, if $N_p(h) \geq 1$ then $N_p(h) = \phi(h)$. This proves the lemma.

Let’s show how the proof of Theorem 9 works in an example, so you get the idea:

**Example 12.** Suppose $p = 23$. Then $\phi(p) = 22 = 2 \cdot 11$. Therefore, the possible orders for elements modulo $p$ are the divisors of $p - 1 = 22$, so $1, 2, 11, 22$.

<table>
<thead>
<tr>
<th>$h$</th>
<th>$N(h)$ ≤ $\phi(1) = 1$</th>
<th>$\phi(2) = 1$</th>
<th>$\phi(11) = 10$</th>
<th>$\phi(22) = 10$</th>
</tr>
</thead>
</table>

On the one hand, the lemma puts an upper bound on the number $N_p(h)$ for each possible $h$. But on the other hand, because every element modulo $p$ has some order, $\sum_{h|p-1} N_p(h) = p - 1$. Since $1 + 1 + 10 + 10 = 22 = p - 1$, all the $\leq$ must be equalities. In particular, $\phi(22) = 10 \geq 1$, proving that there is a $g$ with $\text{ord}_{23}(g) = 22$.

**Proof of Theorem 9.** On the one hand, because every nonzero residue class modulo $p$ has some order,

- $\sum_{h|p-1} N_p(h) = p - 1$.
- On the other hand, $N_p(h) \leq \phi(h)$.

Thus

$$p - 1 = \sum_{h|p-1} N_p(h) \leq \sum_{h|p-1} \phi(h) = p - 1$$

where the last equality is by Proposition 10. Therefore, $N_p(h) = \phi(h)$ for all $h|p - 1$. In particular, $N_p(p - 1) = \phi(p - 1) \geq 1$.

Theorem 9 has the following important corollary:

**Corollary 13.** Suppose $p$ is prime, $(a, p) = 1$, and $g$ is such that $\text{ord}_p(g) = p - 1$. Then there is an integer $k$ so that $g^k \equiv a \pmod{p}$.

**Proof.** The elements $1, g, g^2, \ldots, g^{p-2}$ are distinct modulo $p$, because if $g^j \equiv g^k \pmod{p}$ with $j < k$, then $g^{k-j} \equiv 1 \pmod{p}$, violating that $\text{ord}_p(g) = p - 1$. Therefore, $1, g, g^2, \ldots, g^{p-2}$ is some rearrangement of $1, 2, \ldots, p - 1$ modulo $p$. The corollary follows.

Recall from your homework question that you experimented to determine that if $p \geq 5$ is a prime, then

- If $p \equiv 2 \pmod{3}$, the number of nonzero cubes modulo $p$ is $p - 1$
- If $p \equiv 1 \pmod{3}$, the number of nonzero cubes modulo $p$ is $\frac{p-1}{3}$

We can now prove this, using Theorem 9.

**Proof.** Let $g$ be as in theorem, so that $\text{ord}_p(g) = p - 1$.

- nonzero residue classes modulo $p$: $g, g^2, g^3, \ldots, g^{p-1}$
- the nonzero cubes modulo $p$: $g^3, g^6, g^9, \ldots, g^{3(p-1)}$.

But $\text{ord}_p(g^3) = \frac{p-1}{\gcd(p-1, 3)}$, which is $p - 1$ if $p \equiv 2 \pmod{3}$ and $\frac{p-1}{3}$ if $p \equiv 1 \pmod{3}$.
4 Quadratic residues

Using Theorem 9 and Corollary 13, one can deduce some basic properties of quadratic residues modulo a prime $p$. Recall that if $(a, p) = 1$, then $a$ is said to be a quadratic residue modulo $p$ if $a \equiv r^2 \pmod{p}$ for some $r$ and a quadratic non-reside otherwise.

The following is an important property of quadratic residues. Note that if $(a, p) = 1$, then $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$, because $(a^{(p-1)/2})^2 = a^{(p-1)} \equiv 1 \pmod{p}$. The following proposition says that $a$ is a quadratic residue if and only if one obtains 1, as opposed to $-1$.

**Proposition 14.** Suppose $p$ is prime and $(a, p) = 1$. Then $a$ is a quadratic residue if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

**Proof.** If $a \equiv r^2$, then $a^{(p-1)/2} \equiv r^{(p-1)} \equiv 1 \pmod{p}$. Conversely, suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. By Corollary 13, $a \equiv g^k \pmod{p}$ for some integer $k$. If $k$ is odd, then

$$a^{(p-1)/2} \equiv (g^{(p-1)/2})^k \equiv (-1)^k \equiv -1 \pmod{p}$$

where we have used that $g^{(p-1)/2} \equiv -1 \pmod{p}$ since $g$ has order $p-1$. Thus, $k$ is even, so $a \equiv g^{2j}$ for some integer $j$. Taking $r \equiv g^j$ proves $a \equiv r^2 \pmod{p}$. \qed

As a consequence of the proposition, note that if $x, y$ are quadratic non-residues, then $x^{(p-1)/2} \equiv -1$, $y^{(p-1)/2} \equiv -1$, and thus $(xy)^{(p-1)/2} \equiv (-1)(-1) \equiv 1 \pmod{p}$. Therefore the product $xy$ is a quadratic residue modulo $p$. 
