8. Primitive Elements and Quadratic Reciprocity (Part I).

Fermat’s Little Theorem tells us that for all nonzero remainders \( m \),
\[ m^{p-1} \equiv 1 \mod p. \]

Thus every number from 1 to \( p-1 \) is a root of \( x^{p-1} - 1 \mod p \), so
\[ x^{p-1} - 1 \equiv (x - 1)(x - 2)(x - 3) \cdots (x - (p - 1)) \mod p \]

and since the constant term on the right is \((-1)^{p-1}(p-1)!\), we get

**Wilson’s Theorem:** If \( p \) is any prime, then:
\[ (p-1)! \equiv -1 \mod p \]

(when \( p \) is odd, \( p - 1 \) is even whereas mod 2 we have \(-1 \equiv +1\)).

**Question:** What is \((n-1)! \mod n\) when \( n \) is composite?

**Definition 8.1.** The order of any nonzero \( m \mod p \) is the smallest positive value of \( d \) such that:
\[ m^d \equiv 1 \mod p \]

The order is, of course, always \( \leq p - 1 \), but in fact it divides \( p - 1 \).
That’s because of Euclid’s Algorithm. Suppose \( m^k \equiv 1 \mod p \), and let
\( d = \text{GCD}(k, p - 1) \). Then we can solve \( d = ak + b(p - 1) \), and:
\[ m^d \equiv m^{ak+b(p-1)} \equiv m^{ak}m^{b(p-1)} \equiv (m^k)^a(m^{p-1})^b \equiv 1 \mod p \]
giving us a smaller power of \( m \) that divides \( p - 1 \).

**Definition 8.2.** \( m \mod p \) is primitive if its order is exactly \( p - 1 \). In this case, the powers of \( m \):
\[ m, m^2, m^3, m^4, \ldots, m^{p-2}, m^{p-1} \equiv 1 \mod p \]
are all the remainders mod \( p \) (in some other order) because if \( m^a \equiv m^b \)
for some \( a < b \leq p - 1 \), then \( m^{b-a} \equiv 1 \), which isn’t allowed.

For example, mod 11:
\[ m \equiv 2, m^2 \equiv 4, m^3 \equiv 8, m^4 \equiv 5, m^5 \equiv 10 \]
\[ m^6 \equiv 9, m^7 \equiv 7, m^8 \equiv 3, m^9 \equiv 6, m^{10} \equiv 1 \]
and notice that \( m^5 \equiv 10 \equiv -1 \mod 11 \).

**Lemma 8.3** For each \( d \) that divides \( p - 1 \), there are \( \phi(d) \) remainders of order \( d \). In particular, there are \( \phi(p - 1) \) primitive remainders.
**Proof:** If $m$ has order $d$, then the roots of $x^d - 1$ are exactly the remainders $m, m^2, m^3, \ldots, m^{d-1}, m^d \equiv 1$. Consider $m^k$ for some $k < d$. If $\gcd(k, d) = e \neq 1$, then $(m^k)^{d/e} = (m^{(k/e)})^d \equiv 1$ has smaller order. Thus the only possible remainders of order $d$ are the powers of $m$ that are relatively prime to $d$. Thus there are at most $\phi(d)$ remainders of order $d$ for each $d$ that divides $p - 1$. On the other hand, if you add all of the values of the $\phi$ function for divisors of $p - 1$ together:

$$\sum_{d|p-1} \phi(d) = p - 1$$

so there must be exactly $\phi(d)$ remainders of each order $d$, otherwise we wouldn’t be able to account for all the numbers from 1 to $p - 1$.

**Examples:** Mod 11, we consider the divisors of $10 = 11 - 1$:

$$\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$$
and the corresponding remainders are:

1 (order 1), 10 (order 2), 4, 5, 9, 3 (order 5), 2, 8, 7, 6 (order 10)

**Food for thought:** Why is it that $\sum_{d|n} \phi(n) = n$ for all $n$?

We next consider: “What are the perfect squares mod $p$?”

For starters, 1 is obviously always a square, with square roots 1, $-1$ (which are different from each other as long as $p$ is an odd prime).

The next easiest case is $m = -1$:

**Proposition 8.4.** Let $p$ be an odd prime, so $p \equiv 1$ or $p \equiv 3 \mod 4$.

(a) $-1$ is **not** a square mod $p$ if $p \equiv 3 \mod 4$.
(b) $-1$ **is** a square mod $p$ if $p \equiv 1 \mod 4$. Moreover, in that case:

$$\left(\frac{p - 1}{2}\right)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(\frac{p - 1}{2}\right), \quad \text{and} \quad -\left(\frac{p - 1}{2}\right)!$$

are the two square roots of $-1$ modulo $p$.

**Proof:** Suppose $m$ is a primitive remainder mod $p$. Remember that:

$$m, m^2, m^3, \ldots, m^{p-1} \equiv 1 \mod p$$
runs through all the remainders modulo $p$. Since each square mod $p$ has two different square roots ($r$ and $-r$), it follows that exactly half of the remainders mod $p$ are squares. But:

$$m^2, (m^2)^2 \equiv m^4, (m^3)^2 \equiv m^6, \ldots, (m^{\frac{p-1}{2}})^2 \equiv m^{p-1}$$

are all different, and all perfect squares, so they must be all of them!
Notice that \((mp^{-1})^2 \equiv 1\), and \(mp^{-1} \neq 1 \mod p\), so it must be \(-1\). If \(p \equiv 3 \mod 4\), then \(p^{-1}\) is odd, so \(mp^{-1}\) is NOT a square, and if \(p \equiv 1 \mod 4\), then \(p^{-1}\) is even, so it is a perfect square, and if \(p \equiv 1 \mod 4\), then \(p - 1 \equiv -1, p - 2 \equiv -2, \ldots, p - (p^{-1}) = (p^{-1}) + 1 \equiv - (p^{-1})\), so by Wilson’s Theorem:

\[-1 \equiv (p-1)! \equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{\left(\frac{p-1}{2}\right)} \left(\frac{p-1}{2}\right)! \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \mod p\]

**Examples:** The first primes \(\equiv 1 \mod 4\) are: 5, 13, 17 and 29.

(a) \((\mod 5)\ 2! = 2, \ 2^2 \equiv -1 \mod 5.\)

(b) \((\mod 13)\ 6! = 720 \equiv 5 \mod 13, \ \text{and} \ 5^2 = 25 \equiv -1 \mod 13.\)

(c) \((\mod 17)\ 8! = 40320 \equiv 13 \mod 17, \ \text{and} \ 13^2 = 169 \equiv -1 \mod 17.\)

(d) \((\mod 29)\ 14! \equiv 12 \mod 29, \ \text{and} \ 12^2 = 144 \equiv -1 \mod 29.\)

**Remark:** The nice thing about this Proposition is that it tells us whether or not \(-1\) is a perfect square without requiring us to find the square root. It just so happens that the square root is given by \((p^{-1})!\), but this is actually quite hard to calculate when \(p\) is large.

**Quadratic Reciprocity** will similarly tell us whether any remainder \(\mod p\) is a perfect square or not, with a minimal amount of checking of congruences \(\mod 4\) (and \(\mod 8\)). We will follow one of Gauss’ many proofs of this, which proceeds in stages.

**Lemma 8.5 (Stage 1):** Let \(a \mod p\) be nonzero. Then:

\[a^{(\frac{p-1}{2})} \equiv 1 \ or \ -1 \mod p\]

and \(a\) is a square if it is 1, and not a square if it is \(-1\).

**Proof:** Let \(m\) be some primitive \(\mod p\), and choose \(k\) so that \(a \equiv m^k.\)

- If \(k = 2l\) is even, then \(a\) is a square and \(a^{(\frac{p-1}{2})} \equiv m^{(p-1)l} \equiv 1 \mod p.\)

- If \(k = 2l + 1\) is odd, then \(a\) is not a square, and

\[a^{(\frac{p-1}{2})} \equiv m^{(p-1)l + (\frac{p-1}{2})} \equiv -1 \mod p. \ □\]

**Example:** \(\mod 11:\)

\[1^5 \equiv 1 \mod 11. \ \text{Perfect square (duh!).}\]

\[2^5 = 32 \equiv -1 \mod 11. \ \text{Not a perfect square.}\]

\[3^5 = 243 \equiv 1 \mod 11. \ \text{Perfect square.}\]

\[4^5 = 1024 \equiv 1 \mod 11. \ \text{Perfect square (duh!).}\]

\[5^5 = 3125 \equiv 1 \mod 11. \ \text{Perfect square.}\]
\[
6^5 \equiv (-5)^5 \equiv -1 \mod 11. \text{ Not a perfect square.}
\]
\[
7^5 \equiv (-4)^5 \equiv -1 \mod 11. \text{ Not a perfect square.}
\]
\[
8^5 \equiv (-3)^5 \equiv -1 \mod 11. \text{ Not a perfect square.}
\]
\[
9^5 \equiv (-2)^5 \equiv 1 \mod 11. \text{ Perfect square (duh!).}
\]
\[
10^5 \equiv (-1)^5 \equiv -1 \mod 11. \text{ Not a perfect square.}
\]

This is somewhat nice, but it involves too many calculations. It is, however, the key ingredient in a further extremely clever Lemma due to Gauss. For this, we consider the first half of the \textit{multiples} of \(a\):
\[
a, 2a, 3a, 4a, \ldots, \left(\frac{p-1}{2}\right)a
\]
and we choose remainders that lie between \(-\left(\frac{p-1}{2}\right)\) and \(\left(\frac{p-1}{2}\right)\) mod \(p\) (rather than the usual remainders between 1 and \(p-1\)). Let \(n\) be the number of \textit{negative} remainders.

\textbf{Gauss’ Lemma 8.6 (Stage 2):} Let \(a\) be nonzero \(\mod p\), and let \(n\) be defined as above. Then:

\begin{itemize}
    \item \(a\) is a square \(\mod p\) if \(n\) is even, and:
    \item \(a\) is not a square \(\mod p\) if \(n\) is odd.
\end{itemize}

\textbf{Proof:} Since \(-a \equiv (p-1)a\), \(-2a \equiv (p-2)a\), \ldots it follows that when \(a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\) are brought between \(-\left(\frac{p-1}{2}\right)\) and \(\left(\frac{p-1}{2}\right)\) mod \(p\), then at most one of each of the following pairs arises:
\[
1 \text{ or } -1, \quad 2 \text{ or } -2, \quad 3 \text{ or } -3, \quad \ldots, \quad \left(\frac{p-1}{2}\right) \text{ or } -\left(\frac{p-1}{2}\right)
\]
but since there are exactly \(\left(\frac{p-1}{2}\right)\) of these, it follows that one of each pair does arise. Multiply all the remainders together:
\[
(a)(2a)(3a) \cdots \left(\frac{p-1}{2}\right)a \equiv (\pm 1)(\pm 2)(\pm 3) \cdots \left(\pm \frac{p-1}{2}\right) \mod p
\]
and exactly \(n\) of the “\(\pm\)”s on the right side is a “\(-\)” As in the proof of Euler’s formula, we can now cancel \(\left(\frac{p-1}{2}\right)!\) from both sides to get:
\[
a^{\left(\frac{p-1}{2}\right)} \equiv (-1)^n \mod p
\]
which, together with Stage 1, proves Stage 2. \(\square\)

\textit{Example:} (a) Check that 2 is not a square \(\mod 11\).

\begin{align*}
2, 4, 6, 8, 10 & \text{ become } 2, 4, -5, -3, -1 \\
\text{so } n = 3 & \text{ is odd, and 2 is not a square.}
\end{align*}
(b) Check that 3 is a square mod 11.

$$3, 6, 9, 12, 15 \text{ become } 3, -5, -2, 1, 4$$

so $n = 2$ is even, and 3 is a square.

We can generalize Example (a) in a big way to get the following:

**Proposition 8.7.** If $p$ is an odd prime, $p \equiv 1, 3, 5$ or 7 mod 8, and:

(a) 2 is a square mod $p$ if $p \equiv 1$ or 7 mod 8, and

(b) 2 is not a square mod $p$ if $p \equiv 3$ or 5 mod 8.

**Proof:** As in Example (a), consider:

$$2, 4, 6, 8, \ldots, p - 1 = 2\left(\frac{p - 1}{2}\right)$$

and remember that $n$ is the number of these that are larger than $\left(\frac{p - 1}{2}\right)$ (which is $\left(\frac{p - 1}{2}\right)$ minus the number that are less than or equal to $\left(\frac{p - 1}{2}\right)$).

- If $p = 8l + 1$, then $n = 4l - 2l = 2l$ is even.
- If $p = 8l + 3$, then $n = (4l + 1) - 2l = 2l + 1$ is odd.
- If $p = 8l + 5$, then $n = (4l + 2) - (2l + 1) = (2l + 1)$ is odd.
- If $p = 8l + 7$, then $n = (4l + 3) - (2l + 1) = (2l + 2)$ is even.  □

**Examples:**

(a) 2 is not a square mod 3.
(b) 2 is not a square mod 5.
(c) $2 \equiv 3^2$ mod 7.
(d) 2 is not a square mod 11 (and 11 $\equiv$ 3 mod 8).
(e) 2 is not a square mod 13 (and 13 $\equiv$ 5 mod 8).
(f) $2 \equiv 6^2$ mod 17 (and 17 $\equiv$ 1 mod 8).
(g) 2 is not a square mod 19 (and 19 $\equiv$ 3 mod 8).
(h) $2 \equiv 5^2$ mod 23 (and 23 $\equiv$ 7 mod 8).

Again, notice that the Proposition tells us whether 2 is a perfect square or not mod $p$ simply by testing $p$ mod 8.