Chapter 7 notes

Quadratic Reciprocity

- We focus exclusively on odd primes p.
- General fact: A degree n equation can have at most n solutions modulo p.
- The number a is a *quadratic residue* modulo p iff it is the square of a number modulo p, i.e there is a solution to the equation $x^2 = a \mod p$.
  - If x is a solution then $-x$ also is a solution. And since p is odd, x and $-x$ are NOT congruent modulo p, unless $x = 0 \mod p$.
  - The equation $x^2 = a \mod p$ can have at most 2 solutions. It has exactly two solutions unless $a = 0$.
  - The squares of the numbers modulo p produce exactly $1 + \frac{p-1}{2}$ possible numbers.
- The numbers modulo p are therefore classified in three groups (7.6):
  - zero
  - non-zero quadratic residues ($\frac{p-1}{2}$ of them)
  - non-zero quadratic non-residues (the remaining $\frac{p-1}{2}$ of them)
- Check modulo 13: There are 6 quadratic residues: $1, 2, 4, 9, 3, 12$
- Multiplicative relation (7.7):
  - Residue times Residue is a Residue
  - Residue times Non-residue is a Non-residue
  - Non-residue times Non-residue is a Residue
  - Proof:
    * Residue times Residue is obvious $x^2y^2 = (xy)^2$
    * Multiplying the numbers by a specific non-zero Residue is 1-1 function, so it must take the Non-residues to the Non-residues.
    * Now consider multiplying by a Non-residue: It is 1-1, and take the Residues onto all the Non-residues. Therefore it must take the Non-residues onto the Residues.
- Legendre Symbol (7.8)
- Euler's criterion (7.9): $a^{(p-1)/2} = 1 \mod p$ for quadratic residues, and equals $-1 \mod p$ for non-residues (for $a \neq 0 \mod p$).
  - Proof:
    * First off, note that $a^{(p-1)/2}$ squared must equal $a^{p-1} = 1 \mod p$. Therefore $a^{(p-1)/2}$ must be $\pm 1 \mod p$.

* The equations $x^{(p-1)/2} = 1 \mod p$ and $x^{(p-1)/2} = 1 \mod p$ have at most $(p-1)/2$ solutions each, and together must account for all $p-1$ non-zero numbers modulo p, therefore they each must have *exactly* $(p-1)/2$ solutions.
* If $a = x^2 \mod p$ is a quadratic residue, the $a^{(p-1)/2} = x^{p-1} = 1 \mod p$, therefore the quadratic residues are *exactly* those solving the "equals to 1" equation.
* Therefore the non-residues must be solving the "equals to -1" equation.

- Application (7.10): Use for $a = -1$. Then if $p = 1 \mod 4$ then $(p-1)/2$ is even and $a^{(p-1)/2} = 1 \mod p$, so -1 is a quadratic residue. If $p = 3 \mod 4$ then $(p-1)/2$ is odd and therefore -1 is a quadratic non-residue.

- Gauss' lemma (7.13 and 7.14)

  - We start by choosing different representatives for the equivalence classes, using the numbers from $-\frac{p-1}{2}$ up to $\frac{p-1}{2}$.
  - For $p = 13$ this would be $-6, -5, -4, \ldots, 5, 6$.
  - For a number a multiply the postive representatives $(1, 2, \ldots, \frac{p-1}{2}$ by a: This function is 1-1. Denote by g the number of negative representatives.
    * Example $p = 13$ and $a = 3$. Products are $3, 6, 9 = -4, 12 = -1, 15 = 2, 18 = 5$. So $g = 2$.
    * Example $p = 13$ and $a = 5$. Products are $5, 10 = -3, 15 = 2, 20 = -6, 25 = -1, 30 = 4$. So $g = 3$.
  - This function also never produces a number and its negative: If $ax = -ay \mod p$ then $x = -y \mod p$ but we started with only the positive representatives.
  - So the numbers obtained as $a \cdot 1, a \cdot 2, \ldots, a \cdot (\frac{p-1}{2})$ are up to their order the same as $1, 2, \ldots, \frac{p-1}{2}$ with exactly g of them having negative signs instead.
  - Multiply together to obtain $a^{(p-1)/2}\left(\frac{p-1}{2}\right)! = (-1)^g \left(\frac{p-1}{2}\right)! \mod p$ or else $a^{(p-1)/2} = (-1)^g \mod p$.
  - Gauss' lemma: The Legendre symbol of a modulo p equals $(-1)^g$. Therefore a is a quadratic residue iff g is even.
  - Check with example from earlier.

- Application (7.16):

  - Special case of $a = 2$:
  - Multiplying by 2 produces the numbers $2, 4, \ldots p-1$. We have to simply count how many of those are greater than $\frac{p-1}{2}$.
    * If $\frac{p-1}{2}$ is even, then it's exactly half of them, or $\frac{p-1}{4}$. This happens when $p = 1 \mod 8$ or $p = 5 \mod 8$, in which cases $\frac{p-1}{4}$ is even and odd respectively.
    * If $\frac{p-1}{2}$ is odd, it's $\frac{p+1}{4}$ of them. This happens when $p = 3 \mod 8$ or $p = 7 \mod 8$, in which cases $\frac{p+1}{4}$ is odd and even respectively.

- So g is odd if $p = 3 \mod 8$ or $p = 5 \mod 8$ and g is even if $p = 1 \mod 8$ or $p = 7 \mod 8$.

- Quadratic Reciprocity for p, q (7.19).
  - Proof (not in the book, see Eisenstein's proof here[1]):
  - Sketch of proof:
    * Statement 7.19 is equivalent to: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$
    * We will define something we will denote by $T(q,p)$, with the property that $\left(\frac{q}{p}\right) = (-1)^{T(q,p)}$.
    * We will also show that $T(q,p) + T(p,q) = \frac{p-1}{2}\frac{q-1}{2}$.
    * These two properties of $T help us prove the equivalent statement.
  - Statement 7.19 is equivalent to: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$
  - Now we establish a certain way to compute $\left(\frac{p}{q}\right)$.
    * For a odd we consider the products $a \cdot 1, a \cdot 2, \ldots, a \cdot \frac{p-1}{2}$. From Gauss' lemma we consider $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ their representatives in the set $-\frac{p-1}{2}, -1, \ldots, 1, \frac{p-1}{2}$. It will be exactly half of them. Denote by g the number of those that are negative. We already know $\left(\frac{a}{p}\right) = (-1)^g$.
    * We consider the same products, and divide them each by p. So we have division formulas $a \cdot k = d_k p + s_k$, where s_k is the usual remainder in range 0 to $p-1$.
      - These remainders s_k are either equal to r_k or $p - r_k$ depending on whether r_k was positive or negative. Exactly g of them will equal $p - r_k$.
    * Now we consider the sum of all the $a \cdot k$ (there are $\frac{p-1}{2}$ of them). By the divisions this is equal to the sum of $d_k p$ plus the sum of s_k.
    * We now separately compute the two sides modulo 2. The sum of the $a \cdot k$ for $k = 1, \ldots, \frac{p-1}{2}$ is going to equal a times the sum of the ks. Since a is odd, it is equal to 1 modulo 2, so this sum will equal just the sum of the ks.
    * The other side has the sum of the $d_k p$ terms and the sum of the s_k terms. Since p is an odd prime, it is the same as 1 modulo 2 so the first sum is just the sum of the d_k terms, modulo 2.
    * The sum of the s_k terms is related to the sum of the r_k terms.
      - Remember that each s_k was either equal to r_k or to $p - r_k$, and exactly g terms had the second property.
      - Note that modulo 2 the expression $p - r_k$ is the same as $1 + r_k$.
      - Therefore the sum of the s_k equals the sum of the r_k plus g.
      - Further note that the r_k are just the ks but just in different order and some of them negated. But when we consider the sum modulo 2, none of these two factors matter. so the sum of the r_k is equal to the sum of the k, modulo 2.
    * So to sum up, the left side is equal to the sum of the ks while the right side has the sum of the d_k plus the sum of the k plus g, and these sides are equal modulo 2.

[1] https://en.wikipedia.org/wiki/Proofs_of_quadratic_reciprocity#Eisenstein's_proof

    * We can cancel out the sum of the k, which is common to both sides, then move one of the remaining terms to the other side, and we end up with g equaling the sum of the d_ks, modulo 2.
    * The end result of all this is that $(-1)^g$ is equal to -1 raised to the sum of the d_ks. We will denote this sum by $T(a, p)$.
    * We therefore have $\binom{q}{p} = (-1)^{T(q,p)}$.

- Now we can rewrite our $\binom{p}{q}\binom{q}{p} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ statement, which we are still trying to prove, as:
    * $(-1)^{T(q,p)}(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$
- We will now use a geometric argument to show that $T(q, p) + T(p, q) = \frac{p-1}{2} \cdot \frac{q-1}{2}$.
    * In the $x - y$-plane consider the points with integer coordinates (x, y) where $x = 1, 2, \ldots, \frac{p-1}{2}$ and $y = 1, 2, \ldots, \frac{q-1}{2}$.
    * Consider the line $y = \frac{q}{p}x$ on this plane. It divides the points in two parts (it has to miss all the points because q and p are relatively prime).
    * If we consider a particular k, there are exactly d_k integer points lying directly below the point $y = \frac{q}{p}k$.
    * So the points below the line add up to $T(q, p)$.
    * Symmetrically, looking at things with the axes reversed and the equation $x = \frac{p}{q}y$, we see that the points above the line in the original picture add up to $T(p, q)$.
    * Therefore $T(q, p) + T(p, q)$ equals the total number of integers points, which is $\frac{p-1}{2} \cdot \frac{q-1}{2}$.