Notes for 4th April (Thursday)

1 The road so far...

1. Reduced the problem of quadratic residues to modulo p where p is an odd prime.
2. Stated the rules for the Legendre symbol and proved three of them.

2 Quadratic reciprocity

Before we proceed to prove the other rules of the Legendre symbol, we illustrate the theory through examples.

1. Is 35 a quadratic residue mod 37 ? $(35/37) = (-2/37)$. Now $(2/37) = (-1)^{(37^2-1)/8} = -1$ and $(-1/37) = (-1)^{18} = 1$. Hence, 35 is not a quadratic residue.
2. Is -42 a q.r mod 103 ?

   $(-42/103) = (-1/103)(2/103)(3/103)(7/103) = (-1)^{(103^2-1)/8}(-1)^{102/2}(3/103)(7/103)$

   which equals $-(3/103)(7/103)$. Now $(3/103) = (103/3)(-1)^{51} = -1$ and $(7/103) = (103/7)(-1)^{51\times 3} = -(5/7) = 1$. Hence -42 is a quadratic residue.
3. Is 41 a q.r. mod 1332 ? Firstly, $1332 = 37 \times 2^2 \times 3^2$. Now $(41/3) = (2/3) = -1$ and hence 41 is not a q.r.
4. Suppose $gcd(a, p) = 1$ and we want to solve $ax^2 + bx + c \equiv_p 0$. Then $(x + \frac{b}{2a})^2 \equiv_p \frac{-4ac+b^2}{4a^2}$. Unless $b^2 - 4ac \equiv_p 0$, this equation can be solved iff $\left(\frac{b^2-4ac}{p}\right) = 1$.

We continue the proofs of the other rules. Note that if $p \equiv_4 1$ we know that -1 is a q.r mod p (using Wilson's theorem). So that proves a part of rule 4. But to prove it fully and to prove the other rules, we need a criterion due to Euler. This criterion basically gives a formula for the Legendre symbol ! The formula is slightly painful though. Nonetheless, the point of reciprocity runs deeper. Here is Euler's criterion.

Lemma 2.1. *Let p be an odd prime. If $gcd(a, p) = 1$, then $\left(\frac{a}{p}\right) \equiv_p a^{(p-1)/2}$.*

Proof. By Fermat, $a^{p-1} \equiv_p 1$ and hence either $a^{(p-1)/2} \equiv 1$ or $\equiv -1$. By D' Alembert, $a^{(p-1)/2} = 1$ has at most $\frac{p-1}{2}$ distinct solutions. Moreover, if a is a quadratic residue, then $a^{(p-1)/2} \equiv_p 1$. Also, $x^2 \equiv_p a$ has at most 2 distinct roots. If $x \neq 0$, then there are at least $\frac{p-1}{2}$ distinct values for x^2. So there are at least $\frac{p-1}{2}$ distinct quadratic residues and at most as many (and they satisfy $a^{(p-1)/2} \equiv 1$). So the remaining $\frac{p-1}{2}$ elements are non-residues and satisfy $a^{(p-1)/2} \equiv -1$. We are done. □

In fact, one of the examples above can be done relatively quickly using this. $(35/37) \equiv_{37} 35^{18} \equiv (-2)^1 8 \equiv (2^6)^3 \equiv 10^3 \equiv 260 \equiv 1$.(But the others are somewhat painful.) Now we can prove the fifth rule.

Proof. Consider $D = 2.1.2.2.2.3.\ldots.2.\frac{p-1}{2} \equiv_p 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv_p (2/p)\left(\frac{p-1}{2}\right)!$. For illustrative purposes, look at the case where $p = 19$. Then, replace all the even numbers $> \frac{19}{2}$ by smaller residues by subtracting 19. So $D \equiv_{19} 2.4.6.8.(-9).(-7).(-5).(-3).(-1) \equiv (-1)^5 9!$ which means that $(2/19) \equiv (-1)^5$. Likewise, subtract p from all the even numbers $> \frac{p}{2}$. Let t be the number of odd numbers $< \frac{p}{2}$. This subtraction procedure gives the negative of all odd numbers $< \frac{p}{2}$. So $D \equiv (-1)^t \frac{p-1}{2}!$ and hence $(2/p) = (-1)^t$. If $\frac{p-1}{2}$ is even, then $t = \frac{p-1}{4}$ and if not then $t = \frac{p+1}{4}$. So a brute-force check shows rule 5. □

Now we finally prove quadratic reciprocity. It has several proofs. (Gauss himself gave more than 5.) The proof we follow is in Childs' book and is based on the Chinese Remainder theorem, Euler's criterion, and a little bit of quotient groups.