Notes for 3rd April (Wednesday)

1 The road so far...

1. Reduced quadratic residues to prime powers.
2. Wanted to reduce it to primes but left a claim about U_{p^e} being cyclic and the case for $p = 2$.

2 Quadratic reciprocity

Finally, we prove

Theorem 1. *For every odd prime p, and every $e > 1$, there is a primitive root modulo p^e.*

Proof. Firstly, if p is an odd prime and $gcd(r, p) = 1$, then for each $k \geq 0$, $(1 + pr)^{p^k} = 1 + p^{k+1}s$ for some s coprime to p : Indeed, for $k = 0$ it is obvious and for $k = 1$, $(1 + pr)^p = 1 + p^2r + p^2r^2\frac{p(p-1)}{2} + O(p^3) = 1 + p^2r + p^3t = 1 + p^2(r + pt)$ and hence we are done for $k = 1$.
We induct on k. Assuming truth for $1, 2 \ldots, k$. Then $(1 + pr)^{p^{k+1}} = (1 + p^{k+1}s)^p = 1 + p^{k+2}s + p^{2k+2}s^2\frac{p(p-1)}{2} + O(p^{k+3})$. Hence, $(1 + pr)^{p^{k+1}} = 1 + p^{k+2}s \ mod \ p^{k+3}$. Therefore we are done.
Now we complete the proof. Let b be a primitive root modulo p and $d = ord(b) \ mod \ p^e$. So d divides $p^{e-1}(p-1)$. So $b^d \equiv_p 1$ and hence $p-1$ divides d. So $d = p^l(p-1)$. For $e = 2$, if $ord(b) = p(p - 1)$ then b is already a primitive root modulo p^2. If $ord(b) = p - 1$, then consider $b + p$ (which is b modulo p anyway). Now $(b + p)^{p-1} \equiv_{p^2} b^{p-1} + (p - 1)b^{p-2}p \equiv 1 - pb^{p-2} \neq 1$ and hence $(b + p)$ has order $p(p - 1)$ modulo p^2. So for $e = 2$ we are done. We claim that b is actually a primitive root for p^e for all $e > 2$ as well. Indeed, since $ord(b) = (p - 1)$ modulo p and so $b^{p-1} = 1 + pr$ for some r. Also, $b^{p-1} \neq 1$ modulo p^2 and so $gcd(r, p) = 1$. Now b has order $(p - 1)p^l$ modulo p^e for some l. We claim $l = e - 1$. Indeed, since $gcd(r, p) = 1$, $(b^{p-1})^{p^{e-2}} = (1 + rp)^{p^{e-2}} = 1 + sp^{e-1} \neq 1$ modulo p^e. □

Hence, the claim and therefore, the proof of the reduction of quadratic residues to modulo primes (for odd primes) is done.
Examples and the case for even primes are in Childs' book.

The next order of business is to determine when a number is a quadratic residue modulo a prime p. To this end, we define the so-called Legendre symbol and state some rules that it obeys. These rules help us decide an answer to this question. The most important among these rules is the law of Quadratic reciprocity. Def of Legendre symbol and the rules in Childs' book once again. Here is the proof of the rules.

Proof. The first two rules are obvious. The third rule is proven by saying that if a, b are not quadratic residues, then ab is a quadratic residue (by what we did earlier using the first isomorphism theorem). Obviously the product of quadratic residues is a quadratic residue. Since quadratic residues form a group, the product of a q.r and a non-q.r is a non-q.r.
To be continued.... □