# Notes for 2 April (Tuesday)

## 1 The road so far...

1. Proved that the converse to Lagrange's theorem is false.
2. Proved Cauchy's theorem.
3. First isomorphism theorem and as a consequence, product of two non-quadratic residues is a quadratic residue in $\mathbb{Z}_p$.

## 2 Quadratic reciprocity

An old theorem proven by Gauss helps us decide whether such an equation has a solution or not (but does not help much in finding one). This law of quadratic reciprocity is a part of a bigger conspiracy and when vastly generalised, it leads to the Langlands programme of number theory (of which Fermat's last theorem is a small corollary). The first step is to reduce the problem to a prime power.

**Theorem 1.** *Let $m = p_1^{e_1} p_2^{e_2} \ldots$. Then $a$ is a quadratic residue modulo $m$ iff it is so modulo $p_i^{e_i}$ for each $i$.*

*Proof.* If $x^2 = a + km$, obviously, $x^2 = a + np_i^{e_i}$. If $x_i^2 \equiv_{p_i^{e_i}} a \; \forall \; i$, then by the Chinese Remainder theorem (which applies because the $p_i$ are distinct), there is a unique $b \; mod \; m$ that solves $b \equiv_{p_i^{e_i}} x_i$. Thus, $b^2 \equiv_{p_i^{e_i}} a \; \forall \; i$ and hence $b^2 \equiv_m a$. □

From now onwards, we shall consider only the case where $gcd(a, m) = 1$ (because the coprime numbers form a field under multiplication). The next step is to reduce the problem to a prime. There are two cases - odd primes and 2. We first deal with odd primes.

**Theorem 2.** *Let $p$ be an odd prime such that $gcd(a, p) = 1$. Then $a$ is a quadratic residue modulo $p^e$ (where $e > 1$) iff it is so modulo $p$.*

*Proof.* If $c^2 \equiv_{p^e} a$ then $c^2 \equiv_p a$. Conversely, if $c^2 \equiv_p a$.

**Claim** : The multiplicative group of units in $\mathbb{Z}_{p^e}$ is cyclic and generated by $b$ (a primitive root). Also, such a $b$ is a primitive root modulo $p$.

Assuming the claim, $a \equiv_{p^e} b^r$ and hence $a \equiv_p b^r$. Let $c \equiv_p b^t$. Since $a \equiv_p c^2$, $b^r \equiv_p b^{2t}$. So $r = 2t + n(p-1) = 2s$. Hence, $a \equiv_{p^e} b^r = b^{2s} = (b^s)^2$. Hence we are done.
Now we prove the claim.

*Proof.* Firstly, the exponent of a finite Abelian group $G$ is the maximum of the orders of all of its elements. For example, the exponent of $U_{15}$, the group of units of $\mathbb{Z}_{15}$ is 4. The main point is that

**Theorem 3.** *Let $\lambda$ be the exponent of a finite Abelian group $G$. Then the order of every element $b \in G$ divides $\lambda$.*

*Proof.* Firstly, if $a, b \in G$, and $ord(a) = r, ord(b) = s$ such that $gcd(r, s) = 1$, then $ab$ has order $rs$. Indeed, $(ab)^{rs} = 1$ trivially. Also, if $(ab)^n = 1$, then $1 = (ab)^{nr} = b^{nr}$ and hence $nr$ is divisible by $s$. Therefore $n$ is divisible by $s$. Hence $rs$ is the smallest such integer. Now let $b \in G$ and $m = ord(b)$. $\lambda = ord(a)$ for some $a \in G$ and $m \leq \lambda$. If $m$ does not divide $\lambda$, then there is a prime $p$ such that a higher power of $p$ divides $m$ than it does $\lambda$. This assumption will be used to find an element whose order is greater than $\lambda$ thus providing a contradiction. Indeed, suppose $p^r$ is the highest power of $p$ dividing $m$ and $p^s$ that dividing $\lambda$ where $r > s$. Since $ord(b) = m$, $d = b^{m/p^r}$ has order $p^r$. Since $a$ has order $\lambda$, $c = a^{p^s}$ has order $\lambda/p^s$. But $p^r, \frac{\lambda}{p^s}$ are coprime and hence $cd$ has order $\lambda p^{r-s} > \lambda$. □

Now we inch closer to the claim through the following primitive root theorem.

**Theorem 4.** *The multiplicative group of $\mathbb{Z}_p - \{0\}$ is cyclic, i.e., there is a primitive root modulo $p$. In fact, every finite subgroup of the multiplicative group of a field is cyclic. As a consequence, the multiplicative group of a finite field is cyclic.*

*Proof.* We first prove the second statement (which implies the first). If $U$ is a finite subgroup of the group of units of a field $\mathbb{F}$ such that $\exp(U) = \lambda, |U| = n$, then $\lambda \leq n$ and $a^\lambda = 1 \ \forall \ a \in U$. By D'Alembert's theorem, $\lambda \geq n$ and hence $\lambda = n$. Therefore there is an element in $U$ with order $n$. □

We first prove the second part of the claim. that any primitive root $b$ modulo $p^e$ for some $e > 1$ is actually a primitive root for $p$. Indeed, if $0 < a < p$ then $gcd(a, p^e) = 1$. Therefore, $a$ is a unit in $\mathbb{Z}_{p^e}$. Thus $a \equiv_{p^e} b^t$ which means that $a \equiv_p b^t$ and hence $b$ is a generator for $\mathbb{Z}_p - \{0\}$.
To be continued... □

As mentioned earlier, this completes the proof (modulo the proof of the first part of the claim). □