Notes for 26 Feb (Tuesday)

1 The road so far...

1. Proved Wilson's theorem.
2. Proved that $[-1]_p = [q^2]_p$ for some integer q if $p \equiv_4 1$.
3. Proved that $p = a^2 + b^2$ iff $[p]_4 = [1]_4$ using the Euclidean algorithm in the Gaussian integer ring $\mathbb{Z}[\sqrt{-1}]$.

2 Rings and fields

Now we return back to Fermat's and Euler's theorems and prove them using the Binomial theorem. To do this we need a lemma.

Lemma 2.1. *If p is a prime, then p divides $\binom{p}{r}$ for all $0 < r < p$.*

Proof. Clearly $r!(p-r)!$ divides $p!$. However, p does not divide $r!, (p-r)!$ and hence $gcd(r!(p-r)!, p) = 1$. So $r!(p-r)!$ divides $(p-1)!$ thus implying the result. □

The binomial theorem and the above lemma shows that

$$[(x+y)^p]_p = [x^p + y^p]$$

. Now, we prove Fermat's little theorem : $[a^p]_p = [a]_p$ for every integer a.

Proof. This is proven by induction on a. For $a = 1$ it is trivial. Assume truth for $1, 2, \ldots, a$. Then $[(a+1)^p]_p = [a^p + 1]_p = [a+1]_p$. This shows truth for all positive integers a. For negative integers, every such integer is congruent to a positive one. □

Now we can prove Euler's theorem too : $[a^{\phi(m)}]_m = [1]_m$ when $gcd(m, a) = 1$.

Proof. Let $m = p_1^{e_1} p_2^{e_2} \ldots p_g^{e_g}$. So $\phi(m) = \Pi_i \phi(p_i^{e_i})$. Hence, if we show the theorem for $m = p_i^{e_i}$ for all i, then $[a^{\phi(m)}]_m = [1]_{p_i^{e_i}}$. So $a^{\phi(m)} - 1$ is a common multiple of $p_i^{e_i}$ $\forall$ i and is hence divisible by their lcm which is m.

Now we shall show the theorem for $m = p^e$ by inducting on e. For $e = 1$ we have Fermat's little theorem. Assume truth for $1, 2 \ldots, e$. Then $a^{p^{e-1}(p-1)} \equiv_{p^e} 1$. Thus, $a^{p^{e-1}(p-1)} = 1 + p^e n$. Then, $a^{p^e(p-1)} = (1 + p^e n)^p = 1 + p^{e+1} n^p + p^e q$ for some integer q by the Binomial theorem and the divisibility result above. □

Actually, we can prove another result using the above techniques.

Theorem 1. *Let $m = p_1 p_2 \dots p_g$ where the primes are distinct, i.e., m is squarefree. Let $\lambda(m) = lcm(p_1 - 1, p_2 - 1, \dots, p_g - 1)$. Then for every integer a and $k \in \mathbb{N}$, $a^{\lambda(m)k+1} \equiv_m a$.*

Proof. As before, it suffices to show the result for $m = p_i$ for each i. If $a \equiv_{p_i} 0$ it is obvious. If not, $[a]_{p_i}$ is a unit. Since $\lambda(p_i) = (p_i - 1)$, by Fermat, $a^{\lambda(m)k+1} \equiv_{p_i} a$. □

Since $\phi(m)$ is a multiple of $\lambda(m)$, the following corollary holds.

Theorem 2. *If m is squarefree, then for every a and k, $a^{\phi(m)k+1} \equiv_m a$.*

Note that this theorem is not true in general if m is not squarefree. Indeed, $[2]_4^3 = [0]_4$.

3 Ring homomorphisms

The so-called Frobenius map $T([a]) = [a]^p$ on $\mathbb{Z}_p$ "respects" addition and multiplication, i.e., $T([a][b]) = T([a])T([b])$ and $T([a] + [b]) = T([a]) + T([b])$. Moreover, $T([1]) = [1]$ and $T([0]) = [0]$. Unfortunately, by Fermat's little theorem, this map T is simply the identity map ! However, keep this map in mind because a version of this will not be as trivial later on. This sort of a map between rings (respecting the ring structure) is quite important :
A ring homomorphism $T : R \to S$ between rings R and S is a function satisfying

1. $T(1) = 1$.
2. $T(a + b) = T(a) + T(b)$
3. $T(ab) = T(a)T(b)$.