Primes - Handout 1

Euler's proof of reciprocity using finite differences

Euler did not use the above 'polynomials over finite fields' idea to prove reciprocity. Instead his method was by finite differences. We outline the steps here.

Let p be a prime, and $f(x)$ be a monic polynomial of degree $d < p$. Euler showed that the congruence $f(x) \not\equiv 0 \pmod{p}$ has a solution.

We will apply this to $x^{2k}+1$, where as before $p = 4k+1$, and the degree $d = 2k < p$. We know that each $\beta \in \mathbb{Z}/p\mathbb{Z}$ is a root of $x^{4k} - 1$, but we want to find (at least one such) $\beta = [b]$ which is NOT a root of $x^{2k} - 1$. This means it must be a root of $x^{2k} + 1$,so we conclude $p \mid b^{2k} + 1$.

How to show $f(x) \not\equiv 0 \pmod{p}$ has a solution? We begin by introducing the finite difference operator

Definition 1 (Finite difference operator)**.** Let $f(x)$ be a function (polynomial, or more general). Define

$$\Delta f(x) \coloneqq f(x+1) - f(x)\,.$$

(One should think of this as some kind of 'discrete' version of the derivative. There is a corresponding theory of 'anti-finite-differencing' which allows you to evaluate certain series, much like anti-derivatives allow you to evaluate integrals.)

Lemma 2. *Let $k \geq 1$. Then $\Delta^k = \overbrace{\Delta}^{k \text{ times}} f(x)$ is an integer linear combination of $f(x), f(x+1), \ldots, f(x+k)$.*

Proof. By induction. The case $k = 1$ is true by definition. Then write

$$\Delta^k f(x) = \sum_{i=0}^{k} a_i f(x+i)\,,$$

with $a_i \in \mathbb{Z}$. Applying Δ gives

$$\Delta^{k+1} f(x) = \sum_{i=0}^{k} a_i(f(x+1+i) - f(x+i)) = \sum_{i=0}^{k+1} b_i f(x+i)\,,$$

where $b_0 = a_0$, $b_{k+1} = a_k$, and $b_i = a_i - a_{i-1}$ for $i = 1, \ldots, k$. Certainly all $b_i \in \mathbb{Z}$. □

Lemma 3. *If $f(x)$ is a degree d polynomial, then*

$$\Delta^d f(x) = d!\,.$$

Proof (Sketch). Firstly, compute that

$$\Delta x^d = (x+1)^d - x^d = \binom{d}{1} x^{d-1} + \binom{d}{2} x^{d-2} + \cdots + \binom{d}{d-1} x + \binom{d}{d}\,.$$

So, by linearity, Δ reduces the degree of a polynomial by 1. After d applications, $\Delta^d f(x)$ must be constant (degree 0). What is this constant?

Since the lower degree terms already vanish after $d-1$ steps, we can ignore them at each step and only keep the leading term, for the purposes of calculation. We see the leading term of Δx^d is $\binom{d}{1}x^{d-1}$. By induction the leading term of $\Delta^n x^d$ is

$$\tbinom{d}{1}\tbinom{d-1}{1}\cdots\tbinom{d-n}{1}x^{d-n}\,.$$

When $n=d$, we obtain

$$\Delta^d x^d = \tbinom{d}{1}\tbinom{d-1}{1}\cdots\tbinom{d-d}{1}x^0 = d(d-1)\cdots 1x^0 = d!\,.$$

Since the lower order terms vanish at step $d-1$, we conclude

$$\Delta^d f(x) = d!\,,$$

for f a *monic* polynomial of degree d. □

Now we combine these two lemmas to conclude

Proposition 4. *The congruence* $f(x) \not\equiv 0 \pmod{p}$ *has at least one solution.*

Proof. If it has no solutions, then $f(x) \equiv 0 \pmod{p}$ for every x. So $\Delta^d f(x) \equiv 0 \pmod{p}$ for every x, by writing $\Delta^d f(x)$ as an integer linear combination of $f(x+i)$, using Lemma 2. On the other hand $\Delta^d f(x) = d!$ by Lemma 3, which is a constant, and is not divisible by p for any x. (Recall: $d < p$ by assumption.)

This is a contradiction, hence there is at least one solution to $f(x) \not\equiv 0 \pmod{p}$. □

Then we can continue the proof as before.