Tutorial 6

Question 1

(a, b, c) is a solution to $x^2 + y^2 + z^2 = 2xyz$
$a^2 + b^2 + c^2$ is even if two of a, b, c are odd or if all are even
Assume $a^2 \equiv b^2 \equiv 1 \mod 4$ and $c^2 \equiv 0 \mod 4$
then we have $2abc \equiv 0 \mod 4$ and $a^2+b^2+c^2 \equiv 2 \mod 4$, a contradiction.
$\therefore a, b, c$ are all even.
let $a = 2p$, $b = 2q$, $c = 2r$ then $p^2 + q^2 + r^2 = 4pqr$
It is clear that you can iterate the argument so $P^2 + Q^2 + R^2 = 2^k pqr$
but this cannot continue indefinitely as P, Q and R get smaller and the RHS gets larger
$\therefore P = Q = R = 0$ and the only solution is $(0, 0, 0)$

Question 2

(a, b, c) is a solution to $x^2 + y^2 + z^2 = 2xyz$

Case 1: $3 \nmid a$, $3 \mid b, c$
$a^2 \equiv 1 \pmod 3$
$b^2 \equiv 0 \pmod 3$
$a^2 + b^2 + c^2 = / = 0 \pmod 3$
(Note: This is also true if 3 does not divide a and b, but divides c)

Case 2: $3 \nmid a, b, c$
$a^2 \equiv b^2 \equiv c^2 \equiv 1 \pmod 3$
$abc \equiv 0 \pmod 3$

To show there is one-to-one correspondence, let: $3p = a$, $3q = b$, $3r = c$
$9p^2 + 9q^2 + 9r^2 = 27pqr$
$p^2 + q^2 + r^2 = 3pqr$

Question 3

Case $p = 2$:
$x^4 + 1 = (x^2 + 1)^2 - 2x^2 \equiv (x^2 + 1)^2 \mod 2$
Case p odd, $p \equiv 1 \mod 4 \therefore p = 4k + 1$, some k :
$(-1/p) = (-1)^{(p-1)/2} = 1$

there exists y such that $y^2 \equiv (-1) \mod p$
$x^4 + 1 = x^4 - (-1) \equiv x^4 - y^2 \mod p$
$\therefore (x^2 - y)(x^2 + y) \mod p$
p $\equiv 3 \mod p \therefore p = 4k + 3$, some k
$(-1/p) = (-1)^{2k+1} = -1$ $(2/p) = (-1)^{(11k^2+24k+8)/8} = 1$ if k is odd, -1 if k is even. For k odd:
$x^4 + 1 = (x^2 + 1)^2 - 2x^2 \equiv (x^2 + 1)^2 - (x^2)(y^2) \mod p \equiv (x^2 - 1 - xy)(x^2 + 1 + xy) \mod p$
For k even:
$(-2/p) = (-1/p)(2/p) = (-1)(-1) = 1$
$x^4 + 1 = (x^2 - 1)^2 - (-2x^2) \equiv ((x^2 - 1)^2 - (y^2)(x^2) \equiv (x^2 - 1 - xy)(x^2 - 1 + xp)$ mod p

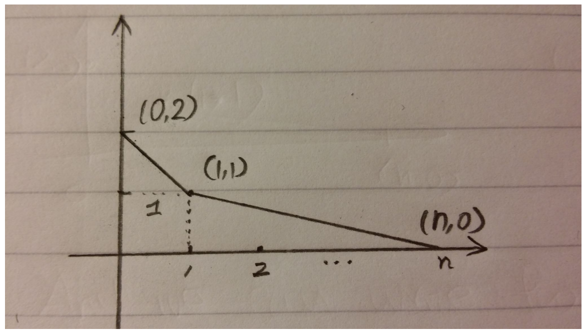
Question 4

Let f be the function defined by $f(x) = x^4 + 1$
Then: $f(x + 1) = x^4 + 4x^3 + 6x^2 + 4x + 2$
Using Eisenstein's Criterion with $p = 2$ we get:
$p \mid 4, 6, 4, 2$
$p \nmid 1$
$p^2 \nmid 2$
$\therefore f(x + 1)$ is irreducible in $\mathbb{Q}$[x]
Hence, $f(x)$ is irreducible in $\mathbb{Q}$[x]
$\therefore$ by Gauss' Lemma f(x) is irreducible in $\mathbb{Z}$[x]

Question 5

Let $f(x) = x^n + px + bp^2, p$ is a prime number, and $\gcd(b, p) = 1$,
then $p_0 = (0, \alpha_0) = (0, 2)$, $p_1 = (1, \alpha_1) = (1, 1)$, $p_n = (n, \alpha_n) = (n, 0)$.
Since f can be written as $f(x) = a_n{}' p^{\alpha_n} x^n + a_1{}' p^{\alpha_1} x + a_0{}' p^{\alpha_0}$
with $\alpha_n = 0, \alpha_1 = 1, \alpha_0 = 2, a_0{}' = b$, $a_1{}' = 0$ and $a_n{}' = 0$.

Then constructing Newton diagram of f modulo p.



Write $f(x) = (x + c)(x^{n-1} + p)$ with $cx^{n-1} + cp = bp^2$,

by Dumas theorem,
if $c \in \mathbb{Z}$, the edge diagram of f is the centre of diagrams of $(x + c)$ and $(x^{n-1} + p)$, i.e. $f(x)$ has an interger root
if $c \notin \mathbb{Z}$, it is irreducible over integers.
$\therefore$ As required.

Question 6

We have:

$$f(x) = 9x^n + 6(x^{n-1} + x^{n-2} + \cdots + x^2 + x) + 4$$

And we would like to show that f is irreducible in $\mathbb{Z}$.

We will construct the Newton diagrams of f for $p = 2$ and $p = 3$ as these are

the only primes whose positive powers divide at least some of the coefficients of

f and hence will produce useful Newton diagrams with respect to reducibility.

For each of the following cases of p we desire the form of f to be

$$f(x) = a_n p^{\gamma_n} x^n + a_{n-1} p^{\gamma_{n-1}} x^{n-1} + \cdots + a_1 p^{\gamma_1} x + a_0 p^{\gamma_0}$$

Case where $p = 2$:

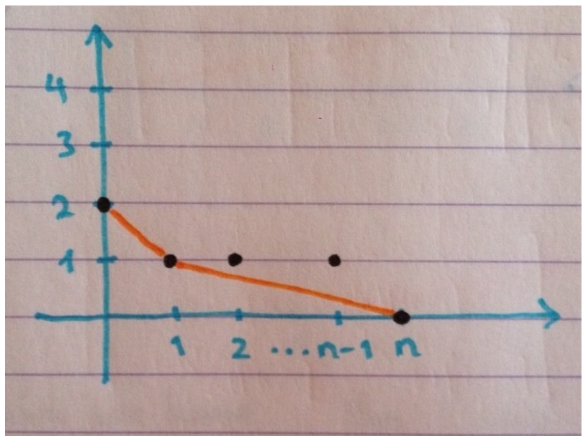
Keeping the desired form of f in mind,

$$f(x) = 9 \cdot 2^0 + 3 \cdot 2^1 (x^{n-1} + \cdots + x) + 1 \cdot 2^2$$

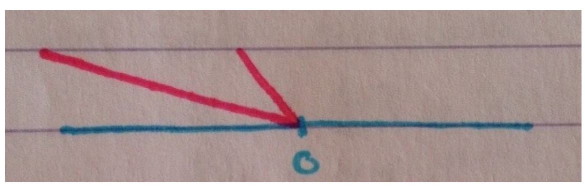
For the Newton diagram we plot the points (n, γ_n). These are

$$(0, 2), (1, 1), (2, 1), \ldots, (n - 1, 1), (n, 0)$$

Giving the Newton diagram:



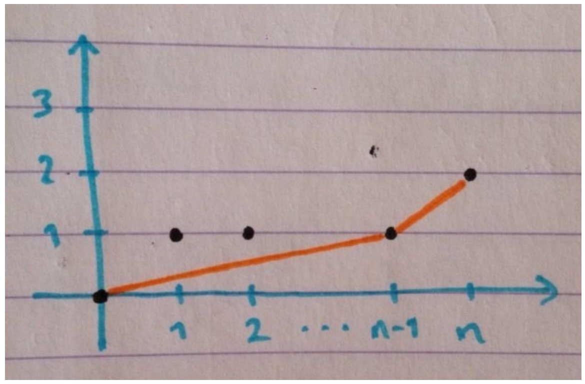
And hence the edge diagram:



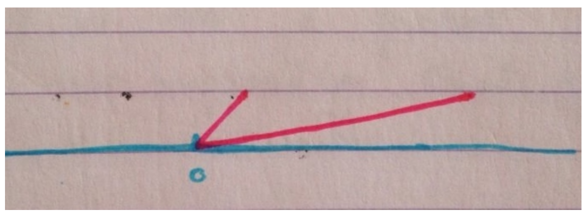
Case where $p = 3$:

$$f(x) = 1 \cdot 3^2 x^n + 2 \cdot 3^1 (x^{n-1} + \cdots + x) + 4 \cdot 3^0$$

Newton Diagram:



Edge Diagram:



Now note that the edge diagram of a product of functions is the union of the edge diagrams of those functions. So if $f = gh$ then f having an edge diagram consisting of two edges, one of degree 1 and the other of degree $n-1$, implies that $deg(g) = 1$ and $deg(h) = n-1$.

Hence, we can assume that g and h have the form

$$g = ax + b$$

and

$$h = cx^{n-1} + \sum_{i=1}^{n-2} \alpha_i x^i + d$$

And then by the values of the coefficients of f it is clear that

$$g = \pm 3x \pm 2$$

and

$$h = \pm 3x^{n-1} \pm \sum_{i=1}^{n-2} \alpha_i x^i \pm 2$$

Where we have either all coefficients are positive or all are negative.
So $(\pm 3x \pm 2)$ is a factor of f.
So $f\left(\frac{-2}{3}\right) = 0$

$$f\left(\frac{-2}{3}\right) = 9\left(\frac{-2}{3}\right)^n + 6\left(\sum_{i=1}^{n-1}\left(\frac{-2}{3}\right)^i\right) + 4 \quad = \quad 0$$

$\dfrac{(-2)^n}{3^{n-2}} - 4 + \sum_{i=2}^{n-1} \dfrac{2(-2)^i}{3^{i-1}} + 4 = 0$

$\sum_{i=2}^{n-1} \dfrac{2(-2)^i}{3^{i-1}} = \dfrac{-(-2)^n}{3^{n-2}}$

$\sum_{i=2}^{n-2} \dfrac{2(-2)^i}{3^{i-1}} = \dfrac{-(-2)^n}{3^{n-2}} - \dfrac{2(-2)^n}{3^{n-2}}$

$= \dfrac{-(-2)^n + (-2)^n}{3^{n-2}} = 0$

And so we have that

$$\sum_{i=2}^{n-2} \frac{2(-2)^i}{3^{i-1}} = 0$$

a contradiction.

So our supposition that f is of the form $f = gh$ is false, so f is irreducible in $\mathbb{Z}$.

Question 7

Assume f, g non constant
As $f^3 - g^2 = 1$, f^3 and g^2 have the same degree.
$a = \deg(f^3) = \deg(g^2)$ so $a = 3\deg(f) = 2\deg(g)$
f, g are coprime so

$$a \leq \mathrm{No}(f, g, (-1)) - 1 = \mathrm{No}(fg) - 1 \leq a/3 + a/2 - 1 = 5a/6 - 1$$

by Mason-Stothers theorem
which implies $a/6 \leq -1$
this is a contradiction,
$\therefore f, g$ are constant