SKOLEM-MAHLER-LECH

$\langle u_n \rangle$ is an LRS

$Z = \{ n : u_n = 0 \}$

$Z = F \cup (c_1 + N\mathbb{N}) \cup \ldots \cup (c_r + N\mathbb{N})$

$Z \subseteq \mathbb{N}$

$$u_n = \sum_{j=1}^{k} P_j(n) \lambda_j^n$$

$$u_n = Q(n)$$

Theorem (SML)

Let $\langle u_n \rangle$ be an LRS over $\mathbb{Z}$. Then its set of zeros $\{n : u_n = 0\}$ is of the form

$$F \cup (c_1 + N\mathbb{N}) \cup \dots \cup (c_k + N\mathbb{N})$$

where F is a finite set.

Exercise: Extend this result to LRS over $\mathbb{Q}$.

Let $\langle u_n \rangle$ be an LRS over $\mathbb{Z}$.

$$u_n = a_{k-1} u_{n-1} + \dots + a_1 u_{n-k+1} + a_0 u_{n-k}$$

Need to specify

assume $a_0 \neq 0$

$a_0, \dots, a_{k-1} \in \mathbb{Z}$

$u_0 \dots u_{k-1} \in \mathbb{Z}$

$\exists\, v, w \in \mathbb{Z}^k, M \in \mathbb{Z}^{k \times k}$

$u_n = v^T M^n w$

$$M = \begin{pmatrix} a_{k-1} & 1 & & & 0 \\ a_{k-2} & 0 & \ddots & & \\ \vdots & & \ddots & \ddots & \\ \vdots & 0 & & \ddots & 1 \\ a_1 & & & & \\ a_0 & & & & 0 \end{pmatrix}$$

$\det(M) = \pm a_0$

Proof of SML

$u_n = a_{k-1} u_{n-1} + \dots + a_0 u_{n-k}$

WLOG $a_0 \neq 0$. $\exists\, v, w, M$

$u_n = v^T M^n w$. $\boxed{\text{all over } \mathbb{Z}}$

$\det(M) = \pm a_0 \neq 0$

Choose p prime $(p > 2)$ s.t. $p \nmid a_0$.

Consider $M_p \in \mathbb{F}_p^{k \times k}$ $\det(M_p) \neq 0$

There are at most p^{k^2} matrices in $\mathbb{F}_p^{k \times k}$.

$M_p, M_p^2, M_p^3 \dots$

$M_p^{k_1} = M^{k_3}$ $k_3 > k_1$

$M_p^{k_3 - k_1} = M_p^0 = I$

$\exists\, N \leq p^{k^2}$ $M_p^N = I$ (in $\mathbb{F}_p$)

Over $\mathbb{Z}$: $\exists N \leq p^{k^2}$ and $M_1 \in \mathbb{Z}^{k \times k}$ s.t.

$$M^N = I + p \cdot M_1 .$$

Note: p, N, M_1 can all be found algorithmically.

Given $n \in \mathbb{N}$

$$n = m \cdot N + r \quad (0 \leq r < N)$$

$$M^n = M^{mN+r} = M^{Nm} M^r$$
$$= (I + pM_1)^m M^r$$

$$u_n = v^T M^n w$$
$$= v^T (I + pM_1)^m \underbrace{M^r w}_{w_r}$$

$$u_{mN+r} = v^T (I + pM_1)^m w_r$$

Split $\langle u_n \rangle$ into N different LRS's $\langle u_m^{(r)} \rangle$ for each $r \in \{0, \dots, N-1\}$ by letting

$$u_m^{(r)} = u_{mN+r}$$

$$= v^T (I + pM_1)^m w_r$$

$$= \sum_{i=0}^{m} \binom{m}{i} p^i \underbrace{v^T M_1^i w_r}_{d_i}$$

$$b_m = \boxed{\sum_{i=0}^{m} \binom{m}{i} p^i d_i}$$

$\langle b_m \rangle$ is a seq of $\mathbb{Z}$

Let p be a prime

Let $m \in \mathbb{Z}$

$$v_p(m) = \begin{cases} 0 & \text{if } p \nmid m \\ k & \text{if } p^k \mid m \ \& \ p^{k+1} \nmid m \end{cases}$$

$$v_p(0) = +\infty$$

$$v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$$

<u>properties:</u>

1. $v_p(a \cdot b) = v_p(a) + v_p(b)$
2. $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$
3. If $v_p(a) < v_p(b)$ then
   $$v_p(a+b) = v_p(a)$$
4. $v_p(a) = \infty \iff a = 0$.

Theorem (Hansel)

Let $p > 2$ be prime, and let $\langle d_i \rangle$ be a sequence of integers.

Let $b_n = \sum_{i=0}^{n} \binom{n}{i} p^i d_i$

If $b_n = 0$ for infinitely many n, then $b_n = 0$ for <u>all</u> n.

<u>Lemma</u>: Let $p > 2$ be prime, let $n \in \mathbb{Z}$. Then

$$v_p\left(\frac{p^n}{n!}\right) \geq n\,\frac{p-2}{p-1}.$$

$$v_p\left(\frac{p^n}{n!}\right) = v_p(p^n) - v_p(n!)$$

$$= n - v_p(n!)$$

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$$

$$\leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots$$

$$= \frac{n}{p-1}$$

So $v_p\left(\frac{p^n}{n!}\right) \geq n - \frac{n}{p-1} = n\,\frac{p-2}{p-1}$

<u>Defⁿ</u>: Given a polynomial

$$P(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Q}[x]$$

let $\omega_k(P) = \begin{cases} \min\{v_p(a_j) \mid j \geq k\} & \text{if } k \leq n \\ \infty & \text{if } k > n \end{cases}$

<u>Note</u>: $\omega_0(P) \leq \omega_1(P) \leq \omega_2(P) \dots$

<u>Note</u>: For a fixed value $t \in \mathbb{Z}$

$$v_p(P(t)) =$$

$$v_p(a_0 + a_1 t + \dots + a_n t^n) \geq$$

$$\min\{v_p(a_0), v_p(a_1 t), \dots, v_p(a_n t^n)\}$$

$$\geq \min\{v_p(a_0), \dots, v_p(a_n)\}$$

$$= \omega_0(P).$$

Lemma Let $P(x), Q(x) \in \mathbb{Q}[x]$

Let $n_1, \dots, n_k \in \mathbb{Z}$

If $P(x) = (x - n_1) \dots (x - n_k) Q(x)$

Then $\omega_k(P) \leq \omega_0(Q)$

Claim if $P(x) = (x - n_1) Q(x)$

Then $\omega_{k+1}(P) \leq \omega_k(Q)$

write $Q(x) = q_0 + q_1 x + \dots + q_n x^n$

$P(x) = p_0 + p_1 x + \dots + p_{n+1} x^{n+1}$

we have $p_{j+1} = q_j - n_1 q_{j+1}$

$\Rightarrow$

$$q_j = p_{j+1} + n_1 p_{j+2} + n_1^2 p_{j+3} + \dots + n_1^{n-j} p_{n+1}$$

$$
\begin{aligned}
v_p(q_j) &= \\
& v_p\left(p_{j+1} + n_1 p_{j+2} + \dots + n_1^{n-j} p_{n+1}\right) \\
& \geq \min\left\{ v_p(p_{j+1}), v_p(p_{j+2}), \right. \\
& \qquad \left. \dots v_p(p_{n+1}) \right\} \\
& = \omega_{j+1}(P)
\end{aligned}
$$

$$
\begin{array}{cccc}
 & v_p(q_0) & \geq & \omega_1(P) \\
 & & & \wedge\!\! \mid \\
 & v_p(q_1) & \geq & \omega_2(P) \\
 & & & \wedge\!\! \mid \\
 & v_p(q_2) & \geq & \omega_3(P) \\
 & \vdots & & \wedge\!\! \mid \\
\omega_k(Q) & v_p(q_k) & \geq & \omega_{k+1}(P) \\
\shortparallel & & & \wedge\!\! \mid \\
\min & \vdots & & \\
 & & & \wedge\!\! \mid \\
 & v_p(q_n) & \geq & \omega_{n+1}(P)
\end{array}
$$

$$\omega_k(Q) \geq \omega_{k+1}(P)$$

Fix $n \in \mathbb{N}$ Let

$R(x) \in \mathbb{Q}[x]$

$$R(x) = \sum_{i=0}^{n} d_i p^i \frac{x(x-1)\dots(x-i+1)}{i!}$$

<u>Lemma</u>: For each k, we have

$$\omega_k(R) \geq k \frac{p-2}{p-1}$$

$$R(x) = \sum_{i=0}^{n} d_i \frac{p^i}{i!} x(x-1)\dots(x-i+1)$$

$$= \sum_{i=0}^{n} d_i \frac{p^i}{i!} \sum_{j=0}^{i} s_{ij} x^j$$

$$= \sum_{j=0}^{n} \sum_{i=j}^{n} d_i \frac{p^i}{i!} s_{ij} x^j$$

[s_{ij} are integers "Stirling Numbers of the first kind"]

Coeff of x^j in $R(x)$ is given by

$$\sum_{i=j}^{n} d_i \frac{p^i}{i!} s_{ij} \quad \text{and}$$

$$v_p\left(\sum_{i=j}^{n} d_i \frac{p^i}{i!} s_{ij}\right) \geq$$

$$\min_{i \geq j} \left\{ v_p\left(d_i \frac{p^i}{i!} s_{ij}\right) \right\} \geq$$

$$\min_{i \geq j} \left\{ v_p\left(\frac{p^i}{i!}\right) \right\} \geq$$

$$\min_{i \geq j} \left\{ i \, \frac{p-2}{p-1} \right\} \geq j \, \frac{p-2}{p-1}$$

So $\omega_j(R) \geq j \, \dfrac{p-2}{p-1}$.

We have the sequence $\langle b_n \rangle$. We show if $b_n = 0$ for $n \in \{n_1, \ldots, n_k\}$ then $v_p(b_n) \geq k \frac{p-2}{p-1}$ for each b_n.

Let $n = \max\{n_1 \ldots n_k\}$

Recall

$$R(x) = \sum_{i=0}^{n} d_i p^i \frac{x(x-1)\ldots(x-i+1)}{i!}$$

Clearly, for each $t \leq n$ we have

$$R(t) = \sum_{i=0}^{n} \binom{t}{i} p^i d_i = \sum_{i=0}^{t} \binom{t}{i} p^i d_i = b_t$$

Since $R(x)$ has integer zeros $n_1, \ldots, n_k$

$$R(x) = (x-n_1) \cdots (x-n_k)\, Q(x)$$

for some $Q(x) \in \mathbb{Q}[x]$

so

$$v_p(R(t)) \geq v_p(Q(t))$$

and

$$v_p(b_t) = v_p(R(t)) \geq$$

$$v_p(Q(t)) \geq \omega_0(Q)$$

$$\geq \omega_k(R)$$

$$\geq k\,\frac{p-2}{p-1}.$$

$\blacksquare$