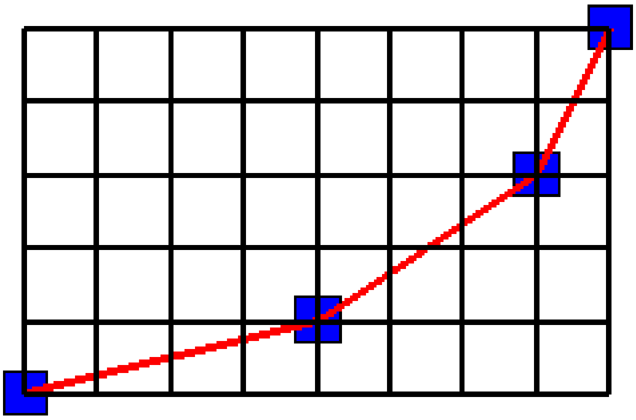
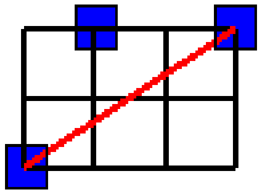
Seminar Notes: Some Proofs Associated with Irreducibility Theorems

Theorem: Let $a_0, a_1, \dots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let $f(x) = \sum_{j=0}^{n} a_j x^j / j!$. If $0 < |a_n| < n$, then $f(x)$ is irreducible unless $(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}$.

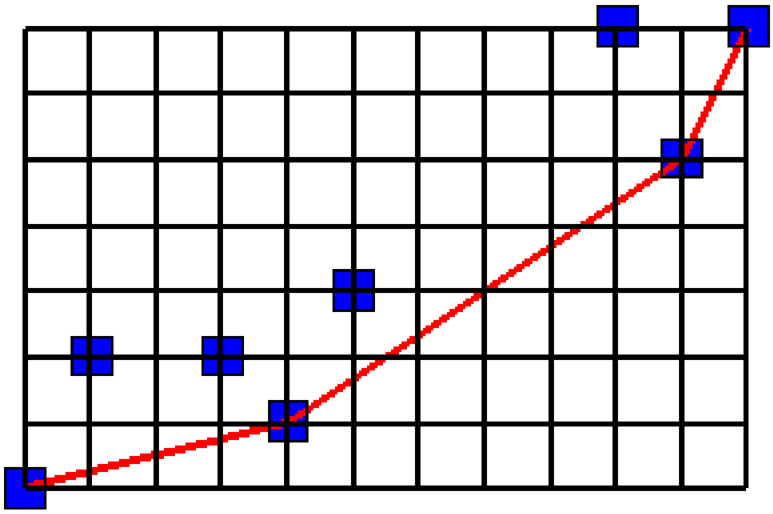
Lemma 1 (Dumas): The Newton polygon of $g(x)h(x)$ with respect to a prime is determined from the Newton polygons of $g(x)$ and of $h(x)$ with respect to the same prime as illustrated below.



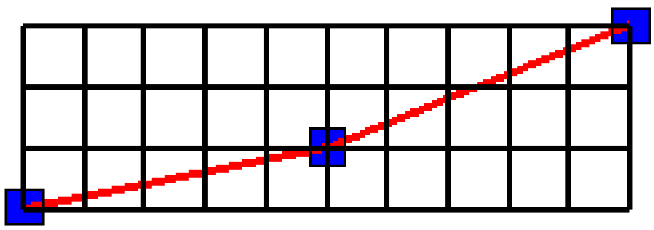
NEWTON POLYGON OF $g(x)$



NEWTON POLYGON OF $h(x)$



NEWTON POLYGON OF $g(x)h(x)$



NEWTON POLYGON OF SOME $f(x)$

Lemma 2. Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let $f(x) = \displaystyle\sum_{j=0}^{n} a_j x^j / j!$.

Let $k \in [1, n/2] \cap \mathbb{Z}$. Suppose $r \in \mathbb{Z}^+$ and a prime p satisfy:

(i) $p \geq k+1$

(ii) $p^r | n(n-1)\cdots(n-k+1)$

(iii) $p^r \nmid a_n$

Then $f(x)$ cannot have a factor of degree k.

Proof: Assume $F(x) = n! f(x)$, with coefficients $b_j = a_j n!/j!$, has a factor $g(x) \in \mathbb{Z}[x]$ of degree k, and consider the Newton polygon of $F(x)$ with respect to p.

- The $n-k+1$ right-most spots have y-coordinates $\geq r$.
- The left-most spot has y-coordinate $< r$.
- The spots $(j, \nu(b_{n-j})$ for $j \in \{k-1, k, \ldots, n\}$ are on or above edges with positive slope.
- Each edge has slope $< 1/k$.
- An edge with positive slope cannot be a translated edge of the Newton polygon of $g(x)$.
- The other edges cannot contain all the translated edges of the Newton polygon of $g(x)$.

Lemma 1 implies a contradiction. ■

The Rest of the Story: Lemma 2 and analytic estimates lead to a proof of the theorem.

Reducible Examples: Consider $f(x) = \sum_{j=0}^{n} a_j x^j/(j+1)!$ where $n = 2^k m \geq 3$ and $n+1 = 3^\ell m'$ with k, ℓ, m, and m' are positive integers and $\gcd(mm', 6) = 1$. Take $a_n = mm'$, $a_{n-1} = mr$, $a_{n-2} = s$, $a_{n-3} = a_{n-4} = \cdots = a_3 = 0$, $a_2 = -y$, $a_1 = w + y$ and rewrite $(n+1)! f(x)/(mm')$ as

$$g(x) = x^n + 3^\ell r x^{n-1} + 3^\ell 2^k s x^{n-2} - 3^{\ell-1} 2^{k-1} (n-1)! y x^2 + 3^\ell 2^{k-1} (n-1)! (w+y) x + 3^\ell 2^k (n-1)!.$$

The idea is to show $g(x)$ has the factor $q(x) = x^2 - 3x - 6$. In other words, we want to show that $g(x) \bmod q(x) = 0$. The basic approach for "determining" the value of $g(x) \bmod q(x)$ is outlined.

- For $j \geq 0$, define integers c_j and b_j by $x^j \equiv c_j + b_j x \pmod{q(x)}$.
- Observe that $c_{j+1} = 3c_j + 6c_{j-1}$ and $b_{j+1} = 3b_j + 6b_{j-1}$ for $j \geq 1$.
- Use $A^j = \begin{pmatrix} c_j & b_j \\ c_{j+1} & b_{j+1} \end{pmatrix}$ where $A = \begin{pmatrix} 0 & 1 \\ 6 & 3 \end{pmatrix}$ to get information about the c_j and b_j.
  (**Examples**: $c_j b_{j+1} - c_{j+1} b_j = \pm 6^j$ for $j \geq 0$; $\nu_2(c_j) = 1$ and $\nu_2(b_j) = 0$ for $j > 1$)

Comment: The above approach can be used to compute the remainder efficiently when dividing a sparse polynomial by a small degree polynomial.