Theorems of Sylvester and Schur

T.N. Shorey

An old theorem of Sylvester states that a product of k consecutive positive integers each exceeding k is divisible by a prime greater than k. We shall give a proof of this theorem and apply it to prove a result of Schur on the irreducibility of certain polynomials.

Irreducibility of certain polynomials

We begin with

Theorem 1 (Schur [6]) Let

$$a_0, a_1, \cdots, a_n \in \mathbb{Z}$$

with

$$| a_0, |=| a_n |= 1.$$

Then

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_1 x + a_0$$

is irreducible over rationals.

The proof that we shall give depends on Newton polygons used by Coleman [2] and Filaseta [4]. I thank Professor Michael Filaseta for sending me copies of his preprints and reprints which helped me in writing this article. The text of this paper is based on my talk in Sesquicentennial Celebrations of University of Mumbai.

Newton polygons Let $p > 0$ be prime. For non-zero integer n, let

$$\nu(n) = \nu_p(n) = \mathrm{ord}_p(n).$$

Further we put

$$\nu(0) = \infty.$$

Let

$$f(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{Z}[x]$$

with

$$a_0 a_m \neq 0$$

and

$$S = \{(0, \nu(a_m)), (1, \nu(a_{m-1})), \cdots (m, \nu(a_0))\}.$$

We consider the lower edges along the convex hull of these points. The left most edge has one end point $(0, \nu(a_m))$ and the right most edge has one end point $(m, \nu(a_0))$. The end points of every edge belong to S. If $(i, \nu(a_{m-i}))$ and $(j, \nu(a_{m-j}))$ with $i < j$ are end points of such an edge, then every point $(u, v(a_{m-u}))$ of S with $i < u < j$ lie on or above the line passing through $(i, \nu(a_{m-i}))$ and $(j, \nu(a_{m-j}))$.

Definition The polygonal path formed by these edges is called the *Newton polygon associated to $f(x)$ with respect to p.*

Example: Let $p = 2$ and

$$f(x) = 2x^6 + x^4 + 2x^2 + 4x + 4.$$

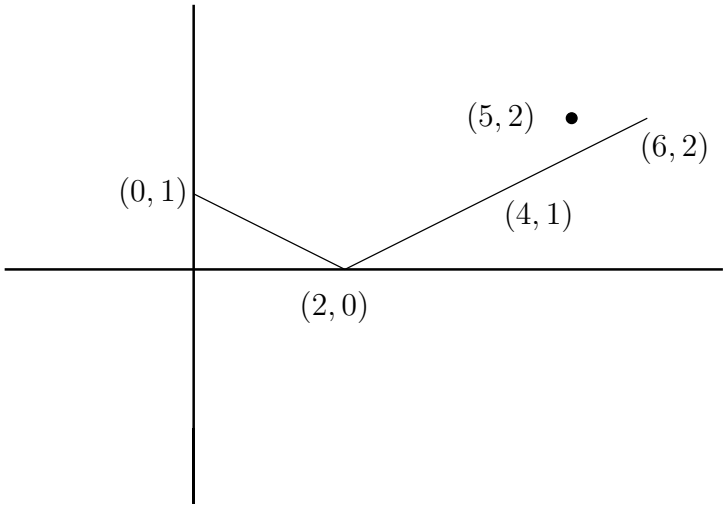
Now

$$S = \{(0, \nu(2)), (1, \nu(0)), (2, \nu(1)), (3, \nu(0)), (4, \nu(2)), (5, \nu(4)), (6, \nu(4))\}$$

i.e.

$$S = \begin{cases} (0,1), (1,\infty), (2,0), (3,\infty), \\ (4,1), (5,2), (6,2) \end{cases}$$

Newton polygon for $f(x)$



We do not allow two different edges to have the same slope. Thus the slopes of the Newton polygon are increasing when calculated from the left-most edge to the right-most edge.

We shall need the following result.

Theorem 1 (Dumas [1]) Let $p > 0$ prime and

$$g(x), h(x) \in \mathbb{Z}[x]$$

with

$$g(0)h(0) \neq 0$$

and

$$u \neq 0$$

be the leading coefficient of $g(x)h(x)$ with

$$\mathrm{ord}_p(u) = t.$$

Then the edges of the Newton polygon of $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning with $(0, t)$ and using translates of edges in the Newton polygons of $g(x)$ and $h(x)$ with respect to p (using exactly one translate from each edge). Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.

Example: Let $p = 3$ and

$$g(x) = x^3 + 3x^2 + 12x + 9,$$

$$h(x) = 2x^2 + 9x + 3.$$

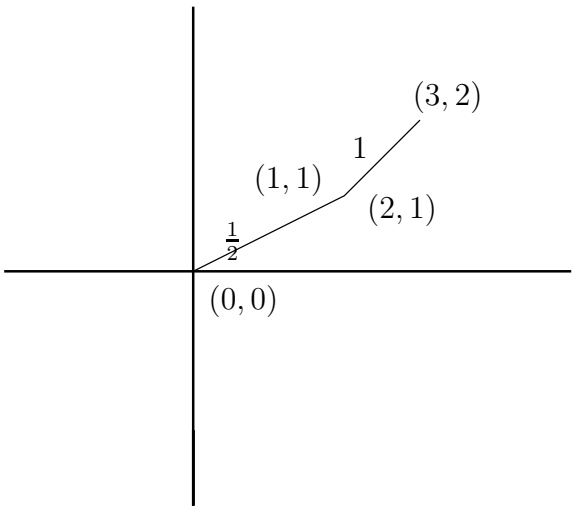
Then

$$f(x) = g(x)h(x) = 2x^5 + 15x^4 + 54x^3 + 135x^2 + 117x + 27.$$

For $g(x)$:

$$S = \{(0, 0), (1, 1), (2, 1), (3, 2)\}$$

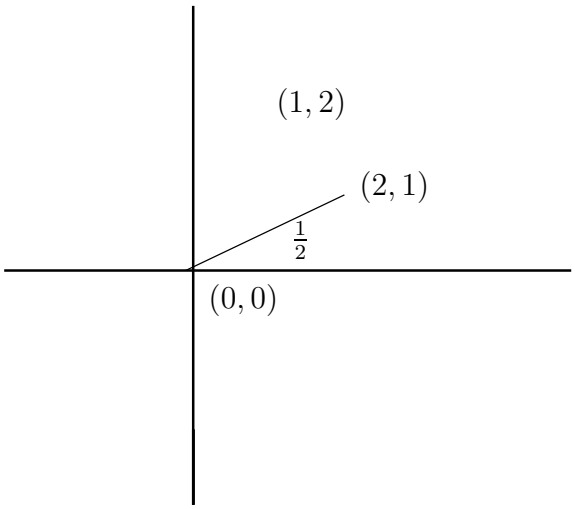
and Newton polygon.



For $h(x)$:

$$S = \{(0,0), (1,2), (2,1)\}$$

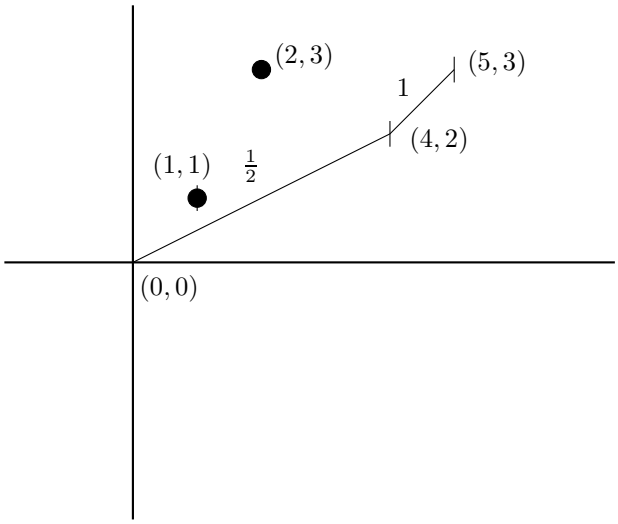
and Newton polygon.



For $f(x)$:

$$S = \{(0,0), (1,1), (2,3), (3,3), (4,2), (5,3)\}$$

and Newton polygon



$u = 2$ and $t = 0$.

$u = 2$ and $t = 0$.

The edge with slope $1/2$ of Newton polygon of f is obtained by combining the edge with slope $1/2$ of Newton polygon of g followed by a translate of the edge with slope $1/2$ of Newton polygon of h. (Here translation is obtained by shifting $(0, 0)$ to (2,1).) Then we continue with a translate of the edge with slope 1 of Newton polygon of g. (Here translation is secured by shifting $(2, 1)$ to $(4, 2)$).

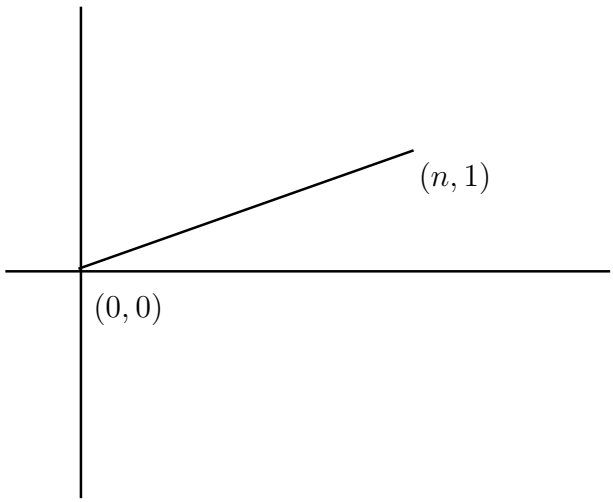
As an application of Dumas theorem, we derive

Eisenstein's Criterion for irreducibility: Let

$$F(x) = \sum_{j=0}^{n} A_j x^j \in \mathbb{Z}[x]$$

and p prime with $p \not| A_n, p \mid A_j$ for $0 \leq j < n, p^2 \not| A_0$. Then $F(x)$ is irreducible over $\mathbb{Q}$.

Proof. The Newton polygon of F with respect to p:
Here $S = \{(j, \mathrm{ord}_p(A_{n-j})) \mid 0 \leq j \leq n\}$.



The point $(j, \mathrm{ord}_p(A_{n-j}))$ lies above the edge since

$$\frac{1}{n} < \frac{\mathrm{ord}_p(A_{n-j})}{j}.$$

Assume that F is reducible. Then

$$F(x) = G(x)H(x)$$

with

$$G(x), H(x) \in \mathbb{Z}[x]$$

and

$$\mathrm{deg}G > 0, \mathrm{deg}H > 0.$$

Thus, by Dumas result, the edge of the Newton polygon of F is obtained by translating the edges of Newton polygons of G and H. In particular, the edge of Newton polygon of F has a lattice point other than $(0, 0)$ and $(n, 1)$. This is a contradiction.

The proof also depends on another result on the greatest prime factor of a product of consecutive positive integers stated in the beginning. For an integer $\nu > 1$, we write

$$P(\nu) = \max_{p|\nu} \quad p$$

and we put

$$P(1) = 1.$$

Then we have

Theorem 2 (Sylvester [7]). For $n > k > 0$, we have

$$P(n(n+1)\cdots(n+k-1)) > k.$$

Thus a product of k consecutive positive integers each exceeding k is divisible by a prime greater than k. The assumption $n > k$ is necessary since

$$P(1.2\cdots k) \leq k.$$

We use Newton polygons for the following result.

Lemma 1 Let $k > 0$. Suppose that

$$g(x) = \sum_{j=0}^{m} b_j x^j \in \mathbb{Z}[x]$$

and $p > 0$ prime with

$$p \not| b_m, p \mid b_j \text{ for } j = 0, 1, \cdots, m-k.$$

Further assume that the right most edge of the Newton polygon of $g(x)$ with respect to p has slope $< \frac{1}{k}$. Let

$$a_0, a_1, \cdots, a_m \in \mathbb{Z}$$

with

$$\mid a_0 \mid = \mid a_m \mid = 1.$$

Then

$$f(x) = \sum_{j=0}^{m} a_j b_j x^j$$

cannot have a factor of degree k.

Lemma 1 implies Schur Theorem: We take in Lemma 1

$$b_j = \frac{m!}{j!}$$

and

$$g(x) = \sum_{j=0}^{m} b_j x^j, f(x) = \sum_{j=0}^{m} a_j b_j x^j.$$

It suffices to show that $f(x)$ is irreducible. Assume that f is reducible. Let k be the smallest degree of an irreducible factor of f. Then

$$1 \leq k \leq \frac{m}{2}.$$

Thus

$$m - k \geq \frac{m}{2} \geq k.$$

Now we apply Theorem 2 to find a prime p with

$$p \geq k+1$$

such that

$$p \mid (m-k+1)\cdots m = b_{m-k}.$$

Thus

$$p \mid b_j \text{ for } j = 0, 1, \cdots, m-k$$

and

$$p \not| b_m \text{ since } b_m = 1.$$

Now we consider Newton polygon of $g(x)$ with respect to p. Here

$$S = \{(j, \nu(b_{m-j})) \mid 0 \leq j \leq m\}$$

and

$$(0, \nu(b_m)) = (0, 0)$$

is the left most end point and

$$(m, \nu(b_0)) = (m, \nu(m!))$$

is the right most end point.

For contradicting Lemma 1, we show that the slope of the right most edge is $< 1/k$. For this, we show

$$\max_{1\leq j\leq m} \frac{\nu(b_0) - \nu(b_j)}{m-(m-j)} < \frac{1}{k}$$

i.e.

$$\max_{1\leq j\leq m} \frac{\nu(m!) - \nu(\frac{m!}{j!})}{j} < \frac{1}{k}$$

i.e.

$$\max_{1\leq j\leq m} \frac{\nu(j!)}{j} < \frac{1}{k}. \qquad (*)$$

Now

$$\begin{aligned}\nu(j!) &= [\frac{j}{p}] + [\frac{j}{p^2}] + \cdots \\ &< j(\frac{1}{p} + \frac{1}{p^2} + \cdots) \\ &= j\frac{\frac{1}{p}}{1-\frac{1}{p}} = \frac{j}{p-1} \leq \frac{j}{k}\end{aligned}$$

since $p \geq k+1$. This proves (*).

Proof of Lemma 1: It is easy to see that there is no loss of generality in restricting to $a_j = 1$ for $0 \leq j \leq m$. Thus

$$f(x) = g(x).$$

Assume that $f(x)$ has a factor or degree k. Then there exist

$$u(x), v(x) \in \mathbb{Z}[x]$$

such that

$$f(x) = u(x)v(x).$$

We consider Newton polygon of $f(x)$ with respect to p. Here

$$\begin{aligned}S &= \{(0, \nu(b_m)) = (0,0), (1, \nu(b_{m-1})), \\ &\quad \cdots (k-1, \nu(b_{m-k+1})), (k, \nu(b_{m-k})), \\ &\quad \cdots (m, \nu(b_0))\}.\end{aligned}$$

We observe that y coordinates of last $m-k+1$ points in S are positive. Since the slopes of the edges are increasing when calculated from the left most edge to the right most edge, we see that the slope of each edge is $< 1/k$. Further the left most edge may have slope zero. Now we consider an edge with positive slope. Let (a,b) and (c,d) be lattice points on this edge.

Then the slope of the edge is the slope of the line passing through (a, b) and (c, d). Thus

$$\frac{1}{\mid c-a \mid} \leq \mid \frac{d-b}{c-a} \mid < \frac{1}{k}$$

implying

$$\mid c-a \mid > k.$$

Since $\deg u(x) = k$, we observe that the translates of the edges of $u(x)$ do not lie on the edges of $f(x)$ with positive slope.

Therefore, by Theorem 1, the left most edge of the Newton polygon of $f(x)$ must have slope zero and length $\geq k$. On the other hand, since the y-coordinates of all other than the first k points in S are positive, its length $< k$. This is a contradiction. This completes the proof of Theorem 1.

The above method has been applied for showing the irreducibility of several polynomials. For example, it has been used in [5] to prove that Bessel polynomials are irreducible.

1 Proof of Theorem 2

We give a proof due to Erdös [3]. We put

$$\Delta(n, k) = n(n+1)\cdots(n+k-1).$$

Let

$$n + k - 1 = x.$$

Then

$$x \geq 2k \text{ if n} > \text{k}.$$

and

$$\frac{\Delta(n, k)}{k!} = \frac{x(x-1)\cdots(x-k+1)}{k!} = \binom{x}{k}.$$

Therefore Theorem 2 implies

$$P\left(\binom{x}{k}\right) > k \text{ if } x \geq 2k. \tag{1}$$

In fact proving Theorem 2 is equivalent to showing (1).

Now we prove (1). It is enough to prove (1) when k is prime. Let

$$k_1 \leq k < k_2$$

where k_1 and k_2 are consecutive primes and (1) is valid with k replaced by k_1. Let $x \geq 2k$. Then $x \geq 2k_1$ and

$$P\left(\binom{x}{k_1}\right) > k_1.$$

Therefore

$$p := P\left(\binom{x}{k_1}\right) \geq k_2 > k.$$

Also

$$p \mid \Delta(x - k_1 + 1, k_1)$$

and

$$\Delta(x - k_1 + 1, k_1) \mid \Delta(x - k + 1, k).$$

Hence

$$p \mid \binom{x}{k}$$

The proof is by contradiction. We assume that

$$P\left(\binom{x}{k}\right) \leq k$$

Therefore

$$P(\Delta(x - k + 1, k)) = P(k!\binom{x}{k}) \leq k$$

Let $k = 2$. Then

$$P((x-1)x) \leq 2, \text{ contradiction}$$

Let $k = 3$. Then

$$P((x-2)(x-1)x) \leq 3$$

We delete the terms in which 2 and 3 appear to a maximal power. We are left with a term which is at most 2. Thus

$$x - 2 \leq 2$$

i.e.

$$x \leq 4, \text{ contradiction.}$$

Let $k = 5$. Then

$$P(x(x-1)\cdots(x-4)) \leq 5.$$

We remove the terms divisible by 5 and 3. Also we remove the term in which 2 appears to maximal power. Thus

$$x - 4 \leq 4, \text{ contradiction.}$$

Let $k = 7$. Then

$$P(x(x-1)(x-2)\cdots(x-6)) \leq 7$$

We remove the terms in which 7 and 5 appear. Further we remove the terms in which 2 and 3 appear to maximal powers. We are left with two terms. Then

$$x - 5 \leq 4.3 = 12$$

Therefore

$$14 \leq x \leq 17$$

and we check that

$$P(\Delta(x-6, 7)) > 7, \text{contradiction.}$$

Hence

$$k \geq 11.$$

Let

$$p^a \| \binom{x}{k} = \frac{x!}{k!(x-k)!}$$

and s be given by

$$p^s \leq x < p^{s+1}$$

Then

$$a = \sum_{\nu=1}^{\infty} \left(\left[\frac{x}{p^\nu} \right] - \left[\frac{x-k}{p^\nu} \right] - \left[\frac{k}{p^\nu} \right] \right) \leq s$$

Hence

$$p^a \leq p^s \leq x$$

Next we show that

$$x < \begin{cases} k^2 \text{ if k} < 37 \\ k^{3/2} \text{ if k} \geq 37 \end{cases}$$

For this, we observe

$$\binom{x}{k} = \prod_{\substack{p \leq k \\ p^a \| \binom{x}{k}}} p^a \leq x^{\pi(k)}$$

On the other hand,

$$\binom{x}{k} = \frac{x}{k} \, \frac{x-1}{k-1} \cdots \, \frac{x-k+1}{1} > \left(\frac{x}{k} \right)^k.$$

Therefore

$$\left(\frac{x}{k} \right)^k < x^{\pi(k)}.$$

Thus

$$x < k^{\frac{k}{k-\pi(k)}}.$$

and further

$$\frac{k}{k-\pi(k)} \leq \begin{cases} 2 \text{ if k} < 37 \\ 3/2 \text{ if k} \geq 37 \end{cases}$$

This proves the assertion.

Now we may assume that

$$x < k^{3/2}$$

otherwise the assertion follows by computations. Then

$$x^{\frac{1}{2\ell-1}} < k^{\frac{1}{\ell}} \text{ for } \ell \geq 2.$$

The remaining proof depends on the following result which we assume

$$\prod_{p \leq x} p \prod_{p \leq x^{1/2}} p \prod_{p \leq x^{1/3}} p \cdots < 4^x.$$

By applying the above inequality with $x = k$,

$$\prod_{p \leq k} p \prod_{p \leq k^{1/2}} p \prod_{p \leq k^{1/3}} p \cdots < 4^k.$$

Further

$$\prod_{p \leq k} p \prod_{p \leq x^{1/3}} p \prod_{p \leq x^{1/5}} p \cdots < 4^k.$$

Also

$$\prod_{p \leq x^{1/2}} p \prod_{p \leq x^{1/4}} p \prod_{p \leq x^{1/6}} p \cdots < 4^{\sqrt{x}}.$$

Hence

$$\binom{x}{k} < 4^{k+\sqrt{x}}.$$

Next we prove

(a) $x < 4k$.

(b) $k \leq 103$ if $\frac{5}{2}k < x < 4k$.

(c) $k \leq 113$ if $2k \leq x \leq \frac{5}{2}k$.

Then $k \leq 113$ and the assertion follows by computations.

First we prove (a). Let

$$x \geq 4k.$$

We observe that

$$4k \leq x < k^{3/2}$$

implying

$$k \geq 17.$$

We have

$$\frac{\binom{4k}{k}}{\binom{2k}{k}} = \frac{4k(4k-1)\cdots(3k+1)}{2k(2k-1)\cdots(k+1)} > 2^k.$$

Thus

$$\begin{aligned} \binom{x}{k} \geq \binom{4k}{k} &> \binom{2k}{k}2^k \qquad (2) \\ &\geq \frac{4^k}{2\sqrt{k}}2^k = \frac{8^k}{2\sqrt{k}}. \end{aligned}$$

On the other hand

$$\binom{x}{k} < 4^{k+\sqrt{x}} < 4^{k+k^{3/4}}.$$

Thus

$$2^{k-2k^{3/4}} < 2\sqrt{k}$$

implying $k \leq 29$ and the cases $17 \leq k \leq 29$ are excluded by (2). Now we show

$$\binom{2k}{k} > \frac{4^k}{2\sqrt{k}}$$

which has been used in the proof of (a). We have

$$\begin{aligned} 1 &> (1-\tfrac{1}{3^2})(1-\tfrac{1}{5^2})\cdots(1-\tfrac{1}{(2k-1)^2}) \\ &= \tfrac{2.4}{3^2}\tfrac{4.6}{5^2}\cdots\tfrac{(2k-2)2k}{(2k-1)^2} \\ &= \tfrac{1}{4k}(\tfrac{2^k k!}{3.5\cdots(2k-1)})^2 \\ &= \tfrac{1}{4k}(\tfrac{4^k(k!)^2}{(2k!)})^2. \end{aligned}$$

Therefore

$$\binom{2k}{k} = \frac{2k!}{(k!)^2} > \frac{4^k}{2\sqrt{k}}$$

The proof of (b) is similar. Now we turn to the proof of (c). We have

$$2k \leq x \leq \frac{5}{2}k.$$

We write

$$\binom{x}{k} = \frac{x!}{k!(x-k)!}.$$

We show

$$P(\binom{x}{k}) \leq \frac{x}{3}.$$

Let

$$\frac{x}{3} < p \leq k.$$

Then

$$\mathrm{ord}_p(x!) \leq 2.$$

Also

$$\mathrm{ord}_p(k!) = 1$$

since

$$\frac{2k}{3} < p \leq k.$$

Further

$$\mathrm{ord}_p((x-k)!) = 1$$

since

$$x - k \geq 2k - k = k \geq p$$

and

$$x - k \leq x - \frac{2}{5}x = \frac{3}{5}x < \frac{9}{5}p < 2p.$$

Thus

$$p \not| \binom{x}{k}.$$

Hence

$$P(\binom{x}{k}) \leq \frac{x}{3}.$$

Then

$$\binom{x}{k} \leq 4^{\frac{x}{3}+\sqrt{x}}.$$

Now the proof for (c) is similar to that of (a).

References

[1] G. Dumas, *Sur quelques cas d'irréductibilité des polynômes á coefficients rationnels*, Journal de Math. Pure et Appl. **2 (1906)**, 191–258.

[2] F. Coleman, *On the Galois groups of the exponential Taylor polynomials,* Enseignement Math. **33 (1987)**, 183-189.

[3] P. Erdös, *A theorem of Sylvester and Schur*, J. London Math. Soc. **9 (1934)**, 282–288.

[4] M. Filaseta, *The irreducibility of all but finitely many Bessel polynomials,* Acta Math. **174 (1995)**, 383-397.

[5] M. Filaseta and O. Trifonov, *The irreducibility of the Bessel polynomials*, Journal Reine Angew. Math. **550 (2002)**, 125–140.

[6] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I*, Sitzungsbser. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl., **14 (1929)**, 125–136.

[7] J.J. Sylvester, *On arithmetical series*, Messenger of Mathematics, XXI (1892), 1-19, 87-120, and Mathematical Papers **4 (1912)**, 687-731.

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road

Mumbai 400 005
shorey@math.tifr.res.in