PROJECT SUMMARY

For Proposal by Michael Filaseta

The proposer plans to investigate several problems associated with lacunary polynomials (a polynomial is lacunary if it has a small number of non-zero terms compared to its degree). Many of the problems proposed for investigation involve the special class of lacunary polynomials having small Euclidean norm. Following the lines of what is now classical work of A. Schinzel, the proposer has recently shown that computationally it is feasible to classify lacunary polynomials with small Euclidean norm and with reducible non-reciprocal parts. Some examples are given and it is proposed to provide such a classification. The approach has applications to irreducibility testing, and another project to be investigated concerns testing the irreducibility of polynomials with small Euclidean norm. These investigations include joint work with A. Schinzel, D. Meade, and R. Murphy (a student of the proposer). The proposer also plans to investigate problems related to recent work by Ford, Konyagin, and the proposer. These include (i) connecting, for a fixed integer a, the reducibility of $f(x)x^n + a$ with systems of congruences that cover the integers and (ii) showing that a given polynomial $g(x) \in \mathbb{Z}[x]$ must be close in some sense to an irreducible polynomial. Both of these are associated with work of A. Schinzel, the latter being a problem posed by P. Turán. In addition, other problems associated with irreducibility results of I. Schur and powerfree values of polynomials are to be investigated by the proposer and his students.

PROJECT DESCRIPTION

Lacunary Polynomials and Irreducibility

This proposal concerns investigations on problems associated mainly with lacunary polynomials with integer coefficients. A lacunary polynomial $f(x) = \sum_{j=0}^{n} a_j x^j$ is a polynomial with few non-zero terms compared to its degree (no precise definition of lacunary is needed here). Many of the problems considered involve the more strict condition that the Euclidean norm $\|f\| = \sqrt{\sum_{j=0}^{n} a_j^2}$ is small (so not only are there few non-zero coefficients, those few coefficients are not too large). The project proposal begins with five sections on various problems associated with the irreducibility or factorization of lacunary polynomials and ends with two sections on some unrelated irreducibility problems.

1. Classifying Reducible Lacunary Polynomials

Results about the irreducibility of lacunary polynomials go back at least to Serret [39] who showed that $x^p - x - 1$ is irreducible for every prime p. Selmer [38] later investigated the irreducibility of polynomials of the form $x^n \pm x^a \pm 1$ and completely classified the cases where reducibility occurs when $a = 1$. Ljunggren [24] then showed that all such polynomials are irreducible unless they have a cyclotomic divisor. Moreover, he showed that if the cyclotomic divisors were removed, then the resulting polynomial would either be identically one (if all factors are cyclotomic) or irreducible. He extended his argument to obtain the analogous result for $x^n \pm x^b \pm x^a \pm 1$. The argument involved checking several cases and was not completely correct. A corrected version of the argument has been given by Mills [25]. The example

$$x^8 + x^4 + x^2 - 1 = (x^2 + 1)(x^3 + x^2 - 1)(x^3 - x^2 + 1)$$

shows that if cyclotomic factors are removed from such polynomials, then the remaining part can be reducible. Mills classified all such examples. Recently, the proposer has considered extensions of these results to more than four terms. Before addressing these extensions, we discuss an important consequence of a more general theorem of Schinzel.

Define a non-zero polynomial $w(x)$ to be reciprocal if $w(x) = \pm x^{\deg w} w(1/x)$. We refer to the non-reciprocal part of a polynomial $f(x)$ as the polynomial one obtains by taking $f(x)$ and removing each irreducible reciprocal factor (to its multiplicity) having positive leading coefficient. Now, suppose we consider $f(x) = \sum_{j=0}^{r} a_j x^{d_j}$ where the a_j are fixed non-zero integers and the d_j are viewed as integer variables satisfying $0 = d_0 < d_1 < \cdots < d_r$. As a result of a more general theorem of Schinzel [34], it follows that one can classify all choices for the d_j for which the non-reciprocal part of the polynomial $f(x)$ is reducible. Cyclotomic polynomials are reciprocal so this can be viewed as a generalization of the results above (or almost so). In particular, if one considers $f(x) = x^n \pm x^c \pm x^b \pm x^a \pm 1$ where $0 < a < b < c < n$, then it is possible in theory to determine when the non-reciprocal part of $f(x)$ is reducible. The work of Schinzel [34] does not readily make classifying the reducibility cases practical. Indeed, a direct application of the main result in [34] would imply performing over 10^{200} computations to derive at such a classification for $f(x)$ of this form. Nevertheless, joint work of Solan (a former student of the proposer) and the proposer [6] has led to a solution in the case where $f(x) = x^n + x^c + x^b + x^a + 1$ (with each coefficient $+1$). Here, it is shown that the non-reciprocal part is always irreducible. In more recent work, the proposer [7] has found an alternative approach to explaining the above consequence of Schinzel's theorem. As a result, obtaining further results about the irreducibility of the non-reciprocal part of lacunary polynomials is computationally possible. As an example, the proposer [7] established

Theorem 1: *Let a, b, c, d, and n be positive integers satisfying $a < b < c < d < n$, and let $f(x) = x^n + x^d + x^c + x^b + x^a + 1$. Then the non-reciprocal part of $f(x)$ is reducible if and only if $f(x)$ is a variation of*

$$f(x) = x^{5s+3t} + x^{4s+2t} + x^{2s+2t} + x^t + x^s + 1 = (x^{3s+2t} - x^{s+t} + x^t + 1)(x^{2s+t} + x^s + 1)$$

where s and t denote arbitrary distinct positive integers.

Details as to what "variation of" refers to can be found in [7]. The proposer dealt with considering six non-zero terms as in this theorem partially because classifying the reducible polynomials is easier when the coefficients are in $\{0, 1\}$ and fewer non-zero terms with such coefficients had previously been considered (as noted above). However, it is still reasonable to believe the general approach in [7] can be used to obtain other results of this nature.

Problem 1: Classify completely the cases where $f(x) \in \mathbb{Z}[x]$ has a reducible non-reciprocal factor and $\|f\|$ is small (perhaps only $\|f\| \le \sqrt{6}$). In particular, determine when the non-reciprocal part of $f(x) = x^n \pm x^c \pm x^b \pm x^a \pm 1$ is irreducible.

The proposer currently has a student, Robert Murphy, doing research on the above problem, and considerable progress has been made. This research constitutes part of joint work with A. Schinzel. It is only a matter of checking and running programs to verify the following:

Theorem 2: *If $n > c > b > a > 0$, then the non-reciprocal part of $f(x) = x^n \pm x^c \pm x^b \pm x^a \pm 1$ is irreducible unless $f(x)$ is a variation of one of the following:*

$$\begin{aligned}
x^{8t} - x^{7t} - x^{4t} + x^{2t} - 1 &= (x^{3t} - x^t - 1)(x^{5t} - x^{4t} + x^{3t} - x^t + 1)\\
x^{8t} - x^{6t} + x^{4t} - x^t - 1 &= (x^{3t} - x^{2t} + 1)(x^{5t} + x^{4t} - x^{2t} - x^t - 1)\\
x^{9t} - x^{7t} + x^{6t} - x^t - 1 &= (x^{3t} - x^{2t} + 1)(x^{6t} + x^{5t} - x^{2t} - x^t - 1)\\
x^{10t} - x^{7t} - x^{6t} - x^{4t} - 1 &= (x^{3t} - x^t - 1)(x^{7t} + x^{5t} + x^{2t} - x^t + 1)\\
x^{10t} - x^{9t} + x^{8t} - x^t - 1 &= (x^{3t} - x^{2t} + 1)(x^{7t} + x^{5t} - x^{2t} - x^t - 1)\\
x^{10t} - x^{6t} - x^{5t} + x^{4t} - 1 &= (x^{5t} - x^{4t} + x^{3t} - x^t + 1)(x^{5t} + x^{4t} - x^{2t} - x^t - 1)\\
x^{10t} - x^{9t} - x^{6t} + x^{3t} - 1 &= (x^{3t} - x^t - 1)(x^{7t} - x^{6t} + x^{5t} - x^{3t} + x^{2t} - x^t + 1)\\
x^{10t} + x^{7t} + x^{4t} - x^t - 1 &= (x^{3t} - x^{2t} + 1)(x^{7t} + x^{6t} + x^{5t} + x^{4t} - x^{2t} - x^t - 1)\\
x^{11t} - x^{8t} - x^{6t} - x^{5t} - 1 &= (x^{4t} - x^t + 1)(x^{7t} - x^{3t} - x^{2t} - x^t - 1)\\
x^{11t} + x^{8t} + x^{6t} - x^t - 1 &= (x^{3t} - x^{2t} + 1)(x^{8t} + x^{7t} + x^{6t} + x^{5t} - x^{2t} - x^t - 1)\\
x^{13t} - x^{11t} - x^{9t} - x^{4t} - 1 &= (x^{3t} - x^t - 1)(x^{10t} + x^{7t} - x^{6t} + x^{5t} + x^{2t} - x^t + 1)\\
x^{13t} - x^{11t} + x^{10t} - x^{2t} - 1 &= (x^{5t} - x^{4t} + x^{2t} - x^t + 1)(x^{8t} + x^{7t} - x^{2t} - x^t - 1)\\
x^{14t} - x^{11t} + x^{9t} - x^{3t} - 1 &= (x^{7t} - x^{6t} + x^{3t} - x^t + 1)(x^{7t} + x^{6t} + x^{5t} - x^{3t} - x^{2t} - x^t - 1)
\end{aligned}$$

$$x^{14t} - x^{9t} - x^{8t} + x^{7t} - 1 = (x^{7t} - x^{6t} + x^{5t} - x^{3t} + x^{2t} - x^t + 1)(x^{7t} + x^{6t} - x^{4t} - x^t - 1)$$
$$x^{2t+u} - x^{t+2u} + x^{2u} - x^t - 1 = (x^t - x^u + 1)(x^{t+u} - x^u - 1)$$
$$x^{5t+2u} - x^{4t+2u} - x^{t+u} - x^t - 1 = (x^{2t+u} - x^{t+u} - 1)(x^{3t+u} + x^t + 1)$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

The above is a complete list of the polynomials of the form $f(x) = x^n \pm x^c \pm x^b \pm x^a - 1$ which have reducible non-reciprocal part and a similar list exists in the case when the constant term -1 is replaced by $+1$. The above result is not particularly aesthetically pleasing, but it does give us an indication of how complicated a classification of the reducible lacunary polynomials satisfying $\|f\| = \sqrt{5}$ is. In fact, the existing program produces results in the case that $\|f\| = \sqrt{6}$ as well (and the coefficients needn't be restricted to ± 1), but the current output of the results in this case is considerably longer and part of the game is to determine how best to present a classification of reducible polynomials in this case. As a consequence, though, some unexpected results may follow; for example, we now know that any polynomial of the form $f(x) = x^n - x^c + x^b - x^a + 1$ with $n > c > b > a > 0$ is either irreducible or it has a reciprocal factor.

Before leaving this section, we note that recent work of Schinzel [30] suggests that similar results may be obtainable for classifying when the non-cyclotomic part (rather than the non-reciprocal part) of a polynomial is reducible. Indeed, he shows that in theory such a classification exists; however, the techniques for doing so are currently non-effective. This will likely be a future investigation of the proposer.

2. Irreducibility Testing for Lacunary Polynomials

The work in the previous section has a computational significance for irreducibility testing. It follows as a consequence of Schinzel's work, for example, that if a polynomial $f(x)$ has sufficiently small Euclidean norm, then it is possible to determine the irreducibility of the non-reciprocal part of $f(x)$ in running time that is roughly logarithmic in the degree of $f(x)$. Currently, algorithms for irreducibility testing (such as that used by MAPLE) require running time that is polynomial in $\deg f$ for most polynomials. The difference in these is quite significant. On the other hand, determining whether the non-reciprocal part of $f(x)$ is irreducible is different from determining whether $f(x)$ itself is irreducible. But how much so? Suppose one has an $f(x)$ to check for irreducibility. In the typical case where $f(x)$ is not itself reciprocal, one can check if $f(x)$ has any reciprocal factors simply by computing $\gcd(f(x), x^{\deg f} f(1/x))$. If this gcd is 1, then $f(x)$ has no reciprocal factors (this is the typical case). Here, one then merely needs to check the irreducibility of the non-reciprocal part of $f(x)$ to determine whether $f(x)$ is itself reducible. If the gcd is not 1, then in this case $f(x)$ has a reciprocal factor and is reducible. Thus, one can seemingly reduce irreducibility testing for lacunary polynomials to computing a gcd. Using the Euclidean algorithm, one can compute such a gcd, but in some ways this is unsatisfactory as the Euclidean algorithm runs roughly in $O(\deg f)$ steps. A faster algorithm that takes into account that $f(x)$ and its reciprocal are lacunary would be nice.

Problem 2: Find an efficient algorithm for determining if $\gcd(f(x), x^{\deg f} f(1/x)) = 1$ above (with running time considerably better than $O(\deg f)$). More generally, investigate the problem of computing efficiently the greatest common divisor of two lacunary polynomials.

Some steps have already been made by the proposer in joint work with Meade (in progress) for using the above ideas to test the irreducibility of lacunary polynomials. The polynomials considered thus far are those having each coefficient either 0 or 1. As discussed earlier, these are somewhat easier to handle. The gcd in Problem 2 is dealt with by working modulo small primes. This saves some time but still is the costly part of the algorithm. An interactive web page developed by the proposer and Meade is already available for testing such $f(x)$ for irreducibility. In particular, comparisons can be made with the running time for checking the irreducibility of $f(x)$ using MAPLE. The URL for this page is

`http://www.math.sc.edu/~filaseta/irreduc.html`.

The proposer in joint work with Schinzel (in progress) has also made partial progress toward investigating reciprocal factors of lacunary polynomials by considering first the special case of cyclotomic factors. We have determined that for a lacunary polynomial $f(x)$ it is possible to determine efficiently whether or not $f(x)$ has a cyclotomic divisor. An interactive web page put together by the proposer and Meade is also available for performing such tests. The URL is

`http://www.math.sc.edu/~filaseta/cyclotomic.html`.

The work with Robert Murphy giving rise to Theorem 2 suggests strongly that the irreducibility test for lacunary polynomials with Meade can be extended to polynomials having arbitrary integer coefficients (and not simply coefficients that are 0 and 1). Indeed, the algorithm for obtaining a result of the nature of Theorem 2 is fundamentally more difficult than obtaining an algorithm for irreducibility testing of lacunary polynomials. In the case of Theorem 2, the polynomials considered have variable exponents whereas, in the case of irreducibility testing of lacunary polynomials, the exponents are specific numbers given as input. It is anticipated that Robert Murphy, Meade, and the proposer will pursue then the following:

Problem 3: Find an algorithm for determining if a given lacunary polynomial $f(x)$ has an irreducible non-reciprocal part that runs better than polynomial in the degree of $f(x)$, and combine this with a gcd test as above to produce a fast irreducibility test for lacunary polynomials.

3. Lacunary Polynomials and Coverings of the Integers

A different type of problem about lacunary polynomials of interest to the proposer is related to coverings of the integers. A covering of $\mathbb{Z}$ is a system of finitely many congruences $x \equiv a_j \pmod{m_j}$, with $j = 1, \ldots, r$, having the property that every integer satisfies at least one of these congruences. Coverings have played a role in a variety of problems in Elementary Number Theory. One classical example of such an application is a demonstration that there are infinitely many positive integers k for which $k \times 2^n + 1$ is composite for every positive integer n. An open problem is whether the moduli in a covering can consist entirely of distinct odd integers > 1. Here we will call such a covering an "odd" covering (it seems afterall to be quite unusual).

Corresponding to the application of coverings mentioned above, we consider whether there are $f(x) \in \mathbb{Z}[x]$ for which $f(x)x^n + 1$ is reducible for every positive integer n. Such $f(x)$ exist. To see this, simply consider any $f(x) \in \mathbb{Z}[x]$ satisfying $\deg f(x) \geq 1$ and $f(1) = -1$; it will then follow that $f(x)x^n + 1$ is of degree ≥ 2, has $x - 1$ as a factor, and hence is reducible. Such an example might be viewed as trivial, and we ask whether or not other examples exist. This problem is motivated by the observation of Schinzel [35] that

$$\left(5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3\right) x^n + 12$$

is reducible over the rationals for every integer $n \geq 0$. Observe that such a polynomial is lacunary (at least when n is large). Furthermore, the example above has the property that for each $n \geq 0$ the polynomial has a cyclotomic divisor. It can be shown that any such example must form a list of lacunary polynomials each having a cyclotomic divisor. The proposer has been interested in establishing a new proof of the following result of Schinzel:

Theorem 3 (Schinzel [35]): *If there is an $f(x) \in \mathbb{Z}[x]$ for which $f(1) \neq -1$ and such that $f(x)x^n + 1$ is reducible for every positive integer n, then there is an odd covering of the integers.*

Indeed, the proposer mentioned the problem of finding a new proof of Theorem 3 perhaps based on ideas used in [7] in his last research proposal to NSA. A major part of such a proof was found by Ford, Konyagin, and the proposer [5]. More specifically, we showed

Theorem 4: *Let $u(x)$ and $v(x)$ be in $\mathbb{Z}[x]$ with*

$$u(0) \neq 0, \;\; v(0) \neq 0, \;\; \textit{and} \;\;\; \gcd(u(x), v(x)) = 1.$$

Let r_1 and r_2 denote the number of non-zero terms in $u(x)$ and $v(x)$, respectively. If

$$m \geq \max\left\{2 \times 5^{2N-1}, 2\max\left\{\deg u, \deg v\right\}\left(5^{N-1} + \frac{1}{4}\right)\right\}$$

where

$$N = 2\,\|u\|^2 + 2\,\|v\|^2 + 2r_1 + 2r_2 - 7,$$

then the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible unless one of the following holds:

(i) The polynomial $-u(x)v(x)$ is a pth power for some prime p dividing m.

(ii) One of $\pm u(x)$ or $\pm v(x)$ is a 4th power, the other is 4 times a 4th power, and $4|m$.

The above result without an explicit lower bound on m was given by Schinzel and was key to proving Theorem 3. The proposer is working on writing up his own connection between Theorem 3 and Theorem 4. In addition, he is pursuing the following:

Problem 4: Investigate connections between coverings and the reducibility of $f(x)x^n + a$ for all n given an integer a.

The proposer has made some further progress. It is not too hard to show that as a consequence of Schinzel's work [35], one can extend Theorem 3 to show that if a is odd and there is an $f(x) \in \mathbb{Z}[x]$ for which $f(1) \neq -a$ and such that $f(x)x^n + a$ is reducible for every positive integer n, then there is an odd covering of the integers. In addition, the author has shown by a rather complicated (perhaps more messy than complicated) covering argument that there is an $f(x) \in \mathbb{Z}[x]$ for which $f(1) \neq -4$ and such that $f(x)x^n + 4$ is reducible for every positive integer n. This example can be modified to show that the role of 4 can be replaced by an arbitrary multiple of 4. This leaves open the situation when $a \equiv 2 \pmod 4$. It can be shown that such a can be handled if $a = 2$ can be. This corresponds to solving a covering problem that can be viewed as easier than the odd covering problem but harder than the one the proposer has used to handle the case $a = 4$. This represents ongoing work that the proposer is doing.

4. A Problem of Turán

Turán asked the following problem: Is there an absolute constant C such that if $g(x)$ is an arbitrary polynomial in $\mathbb{Z}[x]$, then there is an irreducible polynomial $f(x)$ in $\mathbb{Z}[x]$ such that $\|f(x) - g(x)\|^2 \leq C$? The question, as stated here, Schinzel [33] has resolved in the affirmative and shown that one can take $C = 3$. On the other hand, as he notes, his proof relies on allowing $\deg f$ to be large compared to $\deg g$ whereas Turán was really asking whether $\|f(x) - g(x)\|^2 \leq C$ is possible with $\deg f \leq \deg g$. Schinzel showed that one can find an irreducible $f(x)$ with $\|f(x) - g(x)\|^2 \leq 3$ and such that

$$\deg f < \exp\big((5\deg g + 7)(\|g\|^2 + 3)\big).$$

Problem 5: Improve on the upper bound for $\deg f$ and, in particular, make the bound on $\deg f$ above depend less than exponentially on $\deg g$.

The proposer has already been working on decreasing the upper bound on $\deg f(x)$. Taking advantage of the lower bound given for m in Theorem 4, the proposer has shown that one can find an irreducible $f(x)$ with $\|f(x) - g(x)\|^2 \leq 5$ satisfying

$$\deg f \leq 4(\deg g)\exp\big(4\|g\|^2 + 12\big),$$

a bound which is linear in $\deg g$. The proof does not require much modification of Schinzel's original argument given the result of Theorem 4. However, if one wants a similar result with instead $\|f(x) - g(x)\|^2 \leq 3$, more work is needed. The proposer has convinced himself that in this case one can still obtain a bound on $\deg f$ that depends polynomially on $\deg g$. The basic idea is to consider $F(x) = Ax^m + Bx^n + g(x)$ with $m \in (M, 2M]$ and $n \in (N, 2N]$ where M and N are large and $M > N$. One then applies Theorem 4 with $u(x) = A$ and $v(x) = Bx^n + f(x)$ to reduce the problem to consideration of reciprocal and then to cyclotomic factors. Let

$$\mathcal{A} = \{(m,n) : M < m \leq 2M, N < n \leq 2N\},$$

and let $\mathcal{A}_p \subset A$ (arising from pairs (m,n) for which $F(\zeta_{p^k}) = 0$). Then the argument is completed by using a sieve approach to estimate the size of

$$\mathcal{A} - \bigcup \mathcal{A}_p$$

(for example, by using the approach in [32]). The details of this last step are somewhat involved and the proposer is working on completing them.

5. A Problem of Erdős and Renyi

Can a polynomial having only a few non-zero terms be the square of a polynomial having many non-zero terms? This question can be asked for polynomials having coefficients from any field. An old related problem of Erdős [3] (and independently posed by Renyi) that intrigued the proposer as a graduate student years ago is the following. Consider all polynomials $f(x) \in \mathbb{R}[x]$ having exactly n non-zero terms. Let $m(n)$ denote the minimum number of non-zero terms that the square of such a polynomial can have. Prove that $m(n)$ tends to infinity with n. It seems inconceivable that $m(n)$ could be bounded, and yet it took approximately 40 years for a proof to appear that in fact $m(n) \gg \log\log n$. This result and a generalization to kth powers is due to Schinzel [31]. The proposer is interested in seeing if the techniques used to establish Theorem 4 or a variation of them might lead to an improvement of Schinzel's lower bound on $m(n)$.

Problem 6: Improve on lower bounds for $m(n)$.

Another similar problem of interest to the proposer is whether or not there is a constant C such that every trinomial in $\mathbb{Z}[x]$ has an irreducible factor consisting of $\leq C$ non-zero terms. This problem and its obvious generalization were raised in recent work by Choudhry and Schinzel [1].

6. The Irreducibility Theorems of I. Schur

In these last two sections, we discuss problems that are not specifically related to the study of lacunary polynomials but are still associated with irreducibility. Motivated by work of the proposer [10] and recent work of Trifonov and the proposer [4] which settled the question of whether all Bessel Polynomials are irreducible, the proposer has been pursuing irreducibility results about other classes of polynomials. In 1929, I. Schur [37] showed that if $a_0, a_1, \ldots, a_n$ are arbitrary integers with $|a_n| = |a_0| = 1$ and if

$$(*) \qquad f(x) = a_n \frac{x^n}{n!} + a_{n-1}\frac{x^{n-1}}{(n-1)!} + \cdots + a_1 x + a_0,$$

then $f(x)$ is irreducible over the rationals. His approach made use of a prime ideal $\mathcal{P}$ dividing (α) in the ring of algebraic integers in $\mathbb{Q}(\alpha)$ where α is a root of $f(x)$. A few years ago, the proposer [9] showed that Schur's result follows also as an application of Newton polygons. Further, he generalized Schur's result by showing the condition $|a_n| = 1$ could be relaxed to $0 < |a_n| < n$ provided $(a_n, n) \notin \{(\pm 5, 6), (\pm 7, 10)\}$. This result is best possible in the sense that for any $n \geq 2$, there exist integers a_j with $|a_0| = 1$ and $a_n = \pm n$ such that $f(x)$ is reducible. In fact, reducible examples exist whenever n divides a_n. On the other hand, he noted that if one considers a_n not divisible by n, then for all by a finite (ineffective) list of pairs (a_n, n), the polynomial $f(x)$ is irreducible provided only $0 < |a_n| \leq Cn^{3/2}$ where C is any constant $< 1/\sqrt{2}$.

Schur had three other theorems of a similar nature. For example, he showed

Theorem 5: *Let n be an integer ≥ 1. For $j \geq 0$, let $u_{2j} = 1 \times 3 \times 5 \times \cdots \times (2j-1)$. If $a_0, a_1, \ldots, a_n$ are arbitrary integers with $|a_n| = |a_0| = 1$, then*

$$f(x) = \sum_{j=0}^{n} a_j x^{2j}/u_{2j+2}$$

is irreducible over the rationals unless $2n$ is of the form $3^u - 1$ where u is an integer > 1 in which case $f(x)$ can have the factor x^2+3 or x^2-3 and the remaining factor will be irreducible.

Such results enabled Schur to deduce that the classical Hermite polynomials are irreducible. The proposer has a student, Martha Allen, working on seeing to what extent each of the remaining three theorems of Schur follow from the use of Newton polygons and to what extent the condition $|a_n| = 1$ can be relaxed in these theorems. That each of the theorems follows from an application of Newton polygons has already been completed and steps have already been made toward relaxing the condition $|a_n| = 1$. In generalizing Theorem 5, for example, it is expected that only a finite list of pairs (a_n, n) can produce reducible $f(x)$ with the condition $|a_n| = 1$ replaced by $0 < |a_n| < 2n - 1$.

Problem 7: Generalize Schur's remaining irreducibility theorems by relaxing the condition $|a_n| = 1$.

It should be noted that if one considers relaxing the condition $|a_0| = 1$ instead of $|a_n| = 1$, the situation is different. The proposer [9] showed, for example, that even with $a_0 = 2$, there are infinitely many n for which an example can be given where $f(x)$ as in $(*)$ is reducible (with $|a_n| = 1$).

The generalized Laguerre polynomials are defined by

$$L_m^{(\alpha)}(x) = \sum_{j=0}^{m} \binom{m+\alpha}{m-j} \frac{(-x)^j}{j!} = \sum_{j=0}^{m} \frac{(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)(-x)^j}{(m-j)!j!}.$$

Schur's work on $(*)$ implies the irreducibility of $L_m^{(0)}(x)$ (the classical Laguerre polynomials) for all positive integers m. In 1931, Schur [36] considered the general Laguerre polynomials defined above and showed that $L_m^{(1)}(x)$ is irreducible for all positive integers m. The analogous result for $L_m^{(2)}(x)$ already does not hold as

$$L_2^{(2)}(x) = \frac{1}{2}(x-2)(x-6).$$

However, Lam and the proposer have already established

Theorem 6: *Let α be a rational number which is not a negative integer. Then for all but finitely many positive integers m, $L_m^{(\alpha)}(x)$ is irreducible.*

Theorem 6 is effective. It constitutes part of ongoing investigations by Lam and the proposer. We have already completed other investigations as well. For example, we can obtain results if, instead of fixing α in the above theorem, we fix m. One such result is that if m is a fixed positive integer, then for all but finitely many integers α, the polynomial $L_m^{(\alpha)}(x)$ is either irreducible or it factors as a product of a linear polynomial and an irreducible polynomial over $\mathbb{Q}[x]$. (Note that there are infinitely many integers α for which $L_2^{(\alpha)}(x)$ has a linear factor.)

Problem 8: Obtain further results about the irreducibility of classical polynomials along the lines above (continue the joint investigations with Lam).

Similar results are being pursued by one of the proposer's students, Rich Williams. He is addressing (as Schur himself did) the Galois groups associated with general Laguerre polynomials. Some work in this direction has already been done by Gow [17] in certain special cases.

7. Powerfree Values of Irreducible Polynomials

Let $f(x) \in \mathbb{Z}[x]$ be irreducible and of degree n. Let $k \geq n+1$, and assume that $\gcd(f(m) : m \in \mathbb{Z})$ is $k-$free. Then Nair [28] showed that there are infinitely many integers m for which $f(m)$ is $k-$free where k is any integer $\geq (\sqrt{2} - (1/2))n$. Previous work had been done by Nagel [26], Ricci [29], Erdős [2], and Hooley [20]. The best previous result was that any $k \geq n-1$ is admissible and it is still best when n is small. The proposer has done some related work in [12] and [14]. In particular, the former gives a new account of Nair's approach and shows how it implies a similar result for k-free values of binary forms. The approach can be viewed as a differencing method in algebraic number fields. The proposer is very much familiar with the use of differences for such problems; he has done considerable work (many joint with Trifonov) on applying differences to number theoretic problems (see [11], [13], [14], [15], [16], and especially [8]).

The proposer has a talented student, Anguel Koumtchev, who is giving thought to two problems in this direction. There is a technique of Swinnerton-Dyer [40] that has recently been developed and used by Trifonov and Huxley (see [22], [21]). The method has led to nice applications associated with differences and it is worth considering what applications could come from this technique if applied to the problem of powerfree values of polynomials.

Problem 9: Extend the Swinnerton-Dyer method to algebraic number fields with a focus on obtaining results associated with powerfree values of polynomials.

If one considers a large positive integer N and takes $f(x) = -x^n + N$, then one can hope to apply the method of Nair to show that there is an integer m which is not too small such that $f(m)$ is k-free where k is any integer $\geq (\sqrt{2} - (1/2))n$. If $m < N^{1/n}$, then it would follow that N can be written as an nth power (i.e., m^n) plus a k-free number (i.e., $f(m)$). Obtaining such a result from Nair's method, however, is far from easy. His approach makes use of class numbers and a notion of primary numbers that itself is based on knowledge of units in certain algebraic number fields. Recently, the proposer observed that one might be able to get around the class number issue, and Anguel Koumtchev has been considering carrying through with Nair's argument in other ways.

Problem 10: Show that for every positive integer $n \geq 2$ and $k \geq cn$ (for some $c < 1$), every sufficiently large positive integer N can be written as an nth power plus a k-free number.

We note that Hooley's method from [20] allows one to take $k = n - 1$ in the above problem.

References

[1] A. Choudhry and A. Schinzel, *On the number of terms in the irreducible factors of a polynomial over* $\mathbb{Q}$, Glasgow Math. J. 34 (1992), 11–15.

[2] P. Erdős, *Arithmetical properties of polynomials*, J. London Math. Soc. **28** (1953), 416–425.

[3] P. Erdős, *On the number of terms in the square of a polynomial*, Nieuw. Arch. Wisk. (2) **23** (1949), 63–65.

[4] M. Filaseta and O. Trifonov, *The irreducibility of the Bessel polynomials*, preprint.

[5] M. Filaseta, K. Ford, and S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*, Illinois Journal of Math., to appear.

[6] M. Filaseta and I. Solan, *An extension of a theorem of Ljunggren*, Math. Scand. **84** (1999), 5–10.

[7] M. Filaseta, *On the factorization of polynomials with small Euclidean norm*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 143–163.

[8] M. Filaseta and O. Trifonov, *The distribution of fractional parts with applications to gap results in number theory*, Proc. London Math. Soc. (3) **73** (1996), 241–278.

[9] M. Filaseta, *A generalization of an irreducibility theorem of I. Schur*, Analytic Number Theory: Proceedings of a Conference in Honor of Heini Halberstam, Volume 1 (eds. B.C. Berndt, H.G. Diamond, and A.J. Hildebrand), Birkhauser, Boston 1996, 371–396.

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

[11] M. Filaseta and O. Trifonov, *The distribution of squarefull numbers in short intervals*, Acta Arith. **67** (1994), 323–333.

[12] M. Filaseta, *Powerfree values of binary forms*, J. Number Theory **49** (1994), 250–268.

[13] M. Filaseta, *On the distribution of gaps between squarefree numbers*, Mathematika **40** (1993), 88–101.

[14] M. Filaseta, *Short interval results for k-free values of irreducible polynomials*, Acta Arith. **64** (1993), 249–270.

[15] M. Filaseta and O. Trifonov, *On gaps between squarefree numbers, II*, J. London Math. Soc. (2) **45** (1992), 215–221.

[16] M. Filaseta, *An elementary approach to short interval results for k-free numbers*, J. Number Theory **30** (1988), 208–225.

[17] R. Gow, *Some generalized Laguerre polynomials whose Galois groups are the alternating groups*, J. Number Theory **31** (1989), 201–207.

[18] E. Grosswald, Bessel Polynomials, Lecture Notes in Mathematics, Vol. 698, Springer-Verlag, Berlin, 1978.

[19] J.B. Holt, *The irreducibility of Legendre's polynomials I*, Proc. London Math. Soc. (2) **11** (1913), 351–356.

[20] C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21–26.

[21] M. N. Huxley, Area, lattice points, and exponential sums, London Mathematical Society Monographs, New Series, 13, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1996.

[22] M. N. Huxley and O. Trifonov, *The square-full numbers in an interval*, Math. Proc. Cambridge Philos. Soc. **119** (1996), 201–208.

[23] M. N. Huxley and M. Nair, *Power free values of polynomials III*, Proc. London Math. Soc. **41** (1980), 66–82.

[24] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.

[25] W.H. Mills, *The factorization of certain quadrinomials*, Math. Scand. **57** (1985), 44–50.

[26] T. Nagell, *Zur Arithmetik der Polynome*, Abhandl. Math. Sem. Hamburg **1** (1922), 179–184.

[27] M. Nair, *Power free values of polynomials II*, Proc. London Math. Soc. (3) **38** (1979), 353–368.

[28] M. Nair, *Power free values of polynomials*, Mathematika **23** (1976), 159–183.

[29] G. Ricci, *Ricerche arithmetiche sui polynomi*, Rend. Circ. Mat. Palermo **57** (1933), 433–475.

[30] A. Schinzel, *Reducibility of lacunary polynomials, XII*, preprint.

[31] A. Schinzel, *On the number of terms of a power of a polynomial*, Acta Arith. **49** (1987/88), 55–70.

[32] A. Schinzel, *The fundamental lemma of Bruns' sieve in a new setting*, Rocky Mountain J. Math. **15** (1985), 573–578.

[33] A. Schinzel, *Reducibility of lacunary polynomials II*, Acta Arith. **16** (1969/70), 371–392.

[34] A. Schinzel, *Reducibility of lacunary polynomials*, Acta Arith. **16** (1969/70), 123–159.

[35] A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967), 91–101.

[36] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, Journal für die reine und angewandte Mathematik **165** (1931), 52–58.

[37] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I*, Sitzungsber. Preuss. Akad. Wiss., 1929, 125–136.

[38] E. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302.

[39] J.A. Serret, Cours d'Algebre Superieur, Vol. II, 7th ed., Gauthier-Villars, Paris, 1928.

[40] H.P.F. Swinnerton-Dyer, *The number of lattice points on a convex curve*, J. Number Theory **6** (1974), 128–135.

[41] J.H. Wahab, *New cases of irreducibility of Legendre polynomials*, Duke Math J. 19 (1952), 165–176.