Zeitschrift: Elemente der Mathematik
Band: 69 (2014)

Artikel: Is every polynomial with integer coefficients near an irreducible polynomial
Autor: Filaseta, Michael
DOI: https://doi.org/10.5169/seals-515864

Elem. Math. 69 (2014) 130 – 143
0013-6018/14/030130-14
DOI 10.4171/EM/255

Elemente der Mathematik

Is Every Polynomial with Integer Coefficients Near an Irreducible Polynomial?

Michael Filaseta*

Michael Filaseta obtained his Ph.D. from the University of Illinois in 1984. He is currently a professor at the University of South Carolina, South Carolina, USA. He has broad interests in classical topics in Number Theory and often works on problems having direct or indirect connections to polynomials.

1 Posing the problem

A common exercise addressed in number theory courses is to show that there can be arbitrarily large differences between two consecutive primes. The typical argument is to observe that for every positive integer $n \geq 2$, the sequence

$$n! + 2, n! + 3, \ldots, n! + n$$

is a sequence of $n - 1$ consecutive composite numbers. Thus, the largest prime $< n! + 2$ and the smallest prime $> n! + n$ are consecutive primes differing by at least n. Since n can be arbitrarily large, so can this gap between consecutive primes.

Imagine for the moment that you were pondering the problem of showing that there are arbitrarily large gaps between the primes but, for some reason, didn't think of using the argument involving factorials above. How else might you show that the gaps between

*Supported by the National Security Agency.

Zwischen aufeinanderfolgen Primzahlen können bekanntlich Lücken beliebiger Länge auftreten. Die Situation wird deutlich komplizierter, wenn man statt Primzahlen irreduzible Polynome mit ganzzahligen Koeffizienten betrachtet. Pál Turán hat eine entsprechende Fragestellung in diesem Kontext formuliert, und der Autor der vorliegenden Arbeit diskutiert den momentanen Kenntnisstand zu Turáns Problem. Dabei stellt er Verbindungen zu Überdeckungen der ganzen Zahlen her und betrachtet die analoge Frage zu Turáns Problem über endlichen Körpern.

primes can be arbitrarily large? I ask this question because it will be relevant to another question we will be looking at shortly. My guess is that most of us would turn to the Chinese Remainder Theorem. For example, setting n to be a positive integer and letting p_j denote the jth prime, then any solution m of the system of congruences

$$x \equiv -j \pmod{p_j^2}, \quad \text{for } 1 \leq j \leq n-1,$$

has the property that $m+1, m+2, \ldots, m+n-1$ are all composite. Thus, as before, the prime just prior to these $n-1$ numbers and the prime just after these $n-1$ numbers are consecutive primes that differ by at least n. Another approach to showing that there are natural numbers that are not close to primes is to use that the asymptotic density of primes in the set of natural numbers is 0. This latter approach has interesting connections to the classical sieve of Eratosthenes and the Prime Number Theorem, but we don't elaborate on these here as they lead us too far from the main focus of the paper.

By considering natural numbers in the middle of large gaps between primes we see that there are natural numbers that are arbitrarily far from primes. In other words, given any real number C, there are natural numbers n such that any prime p satisfies $|n-p| > C$.

Now, we replace the natural numbers with polynomials having integer coefficients. We view the analog of primes here as the irreducible polynomials over $\mathbb{Q}$, that is those non-constant polynomials in $\mathbb{Z}[x]$ which cannot be written as a product of two non-constant polynomials in $\mathbb{Z}[x]$. Then is it true that there are polynomials that are arbitrarily far from irreducible polynomials? To make this more precise, we flip the question around and state the following.

> Turán's Problem: *Is there an absolute constant C such that if $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 1$, then there is a $w(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ with $\sum_{j=0}^{n} |b_j| \leq C$ such that $f(x) + w(x)$ is irreducible?*

Observe that $f(x) = x^3$ has the property that $f(x) \pm x^a$ is not irreducible for every nonnegative integer a. Indeed, if $a = 0$, then $f(x) \pm x^a$ is either $x^3+1 = (x+1)(x^2-x+1)$ or $x^3 - 1 = (x-1)(x^2+x+1)$, which are both reducible. Also, $f(x) - x^3$ is identically zero and considered neither irreducible nor reducible. Otherwise, if $a > 0$, then x is a factor of $f(x) \pm x^a$, and $f(x) \pm x^a$ will be reducible. Since $f(x) = x^3$ itself is reducible, we see that if there is a C as in Turán's problem, then necessarily $C > 1$.

2 An approach to showing $C > 2$

Next, we consider establishing that $C > 2$. In other words, we want an example of an $f(x) \in \mathbb{Z}[x]$ of some degree $n \geq 1$ such that each of $f(x)$, $f(x) \pm x^a$ and $f(x) \pm x^a \pm x^b$ is reducible for all integers a and b with $0 \leq a \leq n$ and $0 \leq b \leq n$. This seems simple enough. We just have to produce one example of such an $f(x)$ to see that $C > 2$. Surprisingly, however, there seems to be no simple example of such an $f(x)$.

Recall that we were able to show that there is no such C in the analogous problem involving integers that are far away from primes. A natural approach then for trying to show there is no such C for the polynomial problem is to consider what we did for the problem with integers and primes and generalize one of those ideas to handle the polynomial problem of

Turán. We might be able to figure out some generalization of factorials for polynomials, but a little effort in this direction should convince you that looking at our above application of the Chinese Remainder Theorem is more reasonable, especially since the Chinese Remainder Theorem can be applied to polynomials. As to an analog to using that the primes have density 0 among the natural numbers, we note that B.L. van der Waerden [13] showed that polynomials behave in a vastly different way – the density, at least in some sense of this word, of irreducible polynomials in the set $\mathbb{Z}[x]$ is 1.

So, let us see if we can use the Chinese Remainder Theorem to find an example which establishes that $C > 2$ in Turán's problem. We want a system of congruences for $f(x)$ such that if $f(x)$ satisfies all of the congruences in this system then $f(x)$, $f(x) \pm x^a$ and $f(x) \pm x^a \pm x^b$ are reducible for all integers a and b with $0 \le a, b \le n$ as above. To help with our arguments, we consider $f(x)$ with at least 4 terms. We start with the congruence

$$f(x) \equiv 0 \pmod{x}.$$

It is simple enough, and it takes care of a lot. We deduce $f(x)$ is reducible and $f(x) \pm x^a$ is reducible for all $a \ge 1$. Similarly, $f(x) \pm x^a \pm x^b$ is reducible for a and b both ≥ 1. Here, in fact, is where we use that $f(x)$ has at least 4 terms; otherwise, the example $f(x) = x^3 + x^2 + x$ would satisfy the congruence condition on $f(x)$ above and would be such that $f(x) - x^3 - x^2$ is irreducible. With $f(x)$ as above, we are left with finding other conditions on $f(x)$ that cause $f(x) \pm 1$ and $f(x) \pm x^a \pm 1$ to be reducible for all integers $a \in [0, n]$.

Next, we observe that if we want a congruence $f(x) \equiv u(x) \pmod{m(x)}$ to imply there are several polynomials of the form $f(x) \pm x^a \pm 1$ divisible by $m(x)$, then there are not a lot of choices for what $m(x)$ can be. We note first that we may suppose $m(x)$ is irreducible, since an irreducible factor of $m(x)$ will divide any polynomial that is divisible by $m(x)$. Now, for example, if $f(x) + x^a + 1$ is divisible by $m(x)$ for two different positive integers a, then the difference of two such polynomials, say $f(x) + x^{a_1} + 1$ and $f(x) + x^{a_2} + 1$ with $a_1 > a_2$, is divisible by $m(x)$. Thus, $m(x)$ divides $x^{a_1} - x^{a_2}$. Since $f(x) + x^a + 1$ is divisible by $m(x)$ and not x for $a = a_1$ and $a = a_2$, we deduce $m(x)$ divides $x^{a_1 - a_2} - 1$. In other words, $m(x)$ is cyclotomic; that is, $m(x)$ is an irreducible divisor of $x^n - 1$ for some positive integer n. A similar argument shows that if $m(x)$ is an irreducible factor of two polynomials of any one of the forms $f(x) + x^a - 1$, $f(x) - x^a + 1$ and $f(x) - x^a - 1$, then $m(x)$ is either x or is cyclotomic. The importance of considering cyclotomic polynomials is driven home by the following easily established proposition, the proof of which we leave to the reader.

Proposition 1. *If $g(x) \in \mathbb{Z}[x]$ and $m(x)$ is a divisor of $x^n - 1$ for some positive integer n with $m(x)$ dividing $g(x) + x^a$ for some integer $a \ge 0$, then $m(x)$ divides $g(x) + x^b$ for every nonnegative integer $b \equiv a \pmod{n}$.*

The same result holds with $g(x) + x^a$ and $g(x) + x^b$ replaced by $g(x) - x^a$ and $g(x) - x^b$. Taking $g(x)$ to be one of $f(x) \pm 1$, we see that we can show a congruence class of exponents a are such that, say, $f(x) + x^a + 1$ are reducible by restricting $f(x)$ to be in a congruence class modulo a cyclotomic polynomial. For example, if $f(x) \equiv 0 \pmod{x - 1}$, then $f(x) + x^a - 1$ is divisible by the first cyclotomic polynomial $\Phi_1(x) = x - 1$ for all integers

a (for all $a \equiv 0 \pmod 1$); in fact, the condition $f(x) \equiv 0 \pmod{x-1}$ implies also that $f(x) - x^a + 1$ is divisible by $x - 1$ for all a. This is a good point to remember. We have just seen that the two congruences $f(x) \equiv 0 \pmod x$ and $f(x) \equiv 0 \pmod{x-1}$, still considering $f(x)$ with at least 4 terms, are enough to guarantee that $f(x)$ and $f(x) \pm x^a$ are reducible for $a > 0$, that the polynomials $f(x) + x^a + x^b$ and $f(x) - x^a - x^b$ are reducible for all positive a and b, and that $f(x) + x^a - 1$ and $f(x) - x^a + 1$ are reducible for all $a \geq 0$. We are left with finding conditions on $f(x)$ that ensure the polynomials $f(x) \pm 1$, $f(x) + x^a + 1$ and $f(x) - x^a - 1$ are reducible for all nonnegative integers a. We will see momentarily that such conditions on $f(x)$ are already available in the existing literature. For now, we can nevertheless try to set up congruences that $f(x)$ might satisfy modulo cyclotomic polynomials to find an $f(x)$ which shows that $C > 2$ in Turán's conjecture. With a bit of careful thought, one might be led to something like the following system of congruences.

$$
\begin{array}{llll}
f(x) \equiv 0 \pmod x & & f(x) \equiv -2 & \pmod{x^2 + x + 1} \\
f(x) \equiv 0 \pmod{x-1} & & f(x) \equiv 2 & \pmod{x^2 - x + 1} \\
f(x) \equiv 0 \pmod{x+1} & & f(x) \equiv -x^4 - 1 & \pmod{x^4 - x^2 + 1} \\
f(x) \equiv 0 \pmod{x^2+1} & & f(x) \equiv x^{16} + 1 & \pmod{x^8 - x^4 + 1} \\
f(x) \equiv 0 \pmod{x^4+1} & & f(x) \equiv -x^{32} - 1 & \pmod{x^{16} - x^8 + 1} \\
f(x) \equiv 0 \pmod{x^8+1} & & f(x) \equiv x^{32} + 1 & \pmod{x^{32} - x^{16} + 1} \\
f(x) \equiv 0 \pmod{x^{16}+1} & & f(x) \equiv -1 & \pmod{x^{32} + 1} \\
 & & f(x) \equiv 1 & \pmod{x^{64} - x^{32} + 1}
\end{array}
$$

The moduli, besides x, are all cyclotomic polynomials. By Proposition 1, one can check that any $f(x)$ satisfying all of the above congruences will have the property that $f(x)$, $f(x) \pm x^a$ and $f(x) \pm x^a \pm x^b$ are reducible for all nonnegative integers a and b. Since there is no restriction here on a and b being $\leq n$, these congruences are more than sufficient for ensuring that $C > 2$ in Turán's conjecture ... or are they? We still need to check that we can apply the Chinese Remainder Theorem with the above congruences. In fact, the moduli are relatively prime so that the Chinese Remainder Theorem guarantees the existence of an $f(x)$ satisfying the above system of congruences.

The solutions in $f(x)$ to the above congruences are not easily written down, and there is no reason for the purposes of this paper to display such an $f(x)$. There is a unique solution if we restrict the degree of $f(x)$ to be less than the degree of the product of the moduli, and this solution is (in part)

$$f(x) = \frac{7x^{192}}{32} + \frac{x^{191}}{48} + \frac{x^{190}}{96} + \cdots - \frac{x^4}{32} - \frac{x^3}{24} - \frac{x^2}{48} + \frac{x}{48}.$$

Yikes! This isn't what we wanted at all. Turán's conjecture is about polynomials $f(x)$ with integer coefficients, so this example that we constructed has not provided us with a proof that $C > 2$ after all. Lesson learned. Don't forget that the Chinese Remainder Theorem for polynomials provides a solution in $F[x]$ where F is the field of coefficients for the polynomial. We have to work harder if we want an example in $\mathbb{Z}[x]$ proving $C > 2$.

3 A connection to covering systems

It is a little late to cut to the chase, but the author is ready to confess that he knows of no example which shows that $C > 2$. Furthermore, there is a result of Andrzej Schinzel [11] from 1967 that suggests that such an example might be hard to come by. To describe this result, we give a little background.

A *covering system of the integers* is a finite collection of congruences

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ \ldots,\ x \equiv a_r \pmod{m_r},$$

with the property that every integer satisfies at least one congruence in the system. Two examples of a covering system, one somewhat trivial and the other with more substance, are given in the columns below.

$$\begin{array}{ll} x \equiv 0 \pmod 2 & x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 2 & x \equiv 0 \pmod 3 \\ & x \equiv 1 \pmod 4 \\ & x \equiv 1 \pmod 6 \\ & x \equiv 11 \pmod{12} \end{array}$$

There are a variety of interesting results and open problems concerning covering systems. A classical use of complex variables to say something about the non-complex world arises in a short argument that if every integer satisfies exactly one congruence in a covering system with $r > 1$ congruences, then the largest modulus in the covering system must appear at least twice as a modulus for the system. To see this, order the moduli in the system so that $m_1 \le m_2 \le \cdots \le m_r$. The condition $r > 1$ implies each $m_j > 1$. Observe that we can restrict to $a_j \in \{0, 1, \ldots, m_j - 1\}$ in our system and that the exponents appearing on the right of

$$\frac{z^{a_j}}{1 - z^{m_j}} = z^{a_j} + z^{a_j + m_j} + z^{a_j + 2m_j} + \cdots$$

are then simply the nonnegative integers satisfying the congruence $x \equiv a_j \pmod{m_j}$. Hence, if every integer satisfies exactly one of the congruences in our system, we have

$$\frac{1}{1 - z} = \sum_{j=1}^{r} \frac{z^{a_j}}{1 - z^{m_j}}.$$

This equation holds for all $z \in \mathbb{C}$ with $|z| < 1$. Now, we see that if $m_r \ne m_{r-1}$, then as z approaches the complex number $\zeta = e^{2\pi i/m_r}$ from inside the unit disc $D = \{z \in \mathbb{C} : |z| < 1\}$, the right side has a single term which has absolute value tending to infinity whereas the left side approaches $1/(1-\zeta)$. Thus, for $z \in D$ close enough to ζ, the absolute value of the right side exceeds the absolute value of the left side, showing the above equation cannot hold.

It is possible to avoid the use of a complex variable here. For example, one can argue first that if $m_r \neq m_{r-1}$, then necessarily $m_r > 6$. Then one can take $z = 2$ in the equation above and use that $2^{m_r} - 1$ is divisible by a prime p that does not divide $2^{m_j} - 1$ for any $j < r$. Then the right side has p dividing the denominator when simplified but the left side is simply -1. Nevertheless, the above elegant and simple use of a complex variable has made a permanent mark in this subject.

Among the various open problems in the subject is the problem of determining whether the minimum modulus m_1 in a covering system with distinct moduli $m_1 < m_2 < \cdots < m_r$ can be arbitrarily large. Pál Erdős [4] wrote, "This is perhaps my favourite problem," and offered as much as $1000 for a solution to this problem (cf. [7], §F13). The current record on the largest size of m_1 was given by Pace P. Nielsen [10] who obtained a covering system with distinct moduli ≥ 40. In addition, his covering consisted of over 10^{50} congruences with each modulus only divisible by primes ≤ 103. Recall earlier that we were interested in showing that there are conditions that we could impose on $f(x)$ in addition to $f(x) \equiv 0 \pmod{x}$ and $f(x) \equiv 0 \pmod{x-1}$ that would imply $C > 2$. Although, this idea did not pan out the way we intended, leading us instead to an $f(x)$ with rational but not integral coefficients, it is worth noting that we could have used this result of Nielsen to readily establish conditions on $f(x)$, but again with the same drawback of producing a polynomial in $\mathbb{Q}[x]$ that is not in $\mathbb{Z}[x]$. Recall that we wanted to ensure that the polynomials $f(x) \pm 1$, $f(x)+x^a+1$ and $f(x)-x^a-1$ are reducible for all nonnegative integers a. By Proposition 1, if we take

$$f(x) \equiv x^{a_j} + 1 \pmod{\Phi_{m_j}(x)},$$

where $\Phi_{m_j}(x)$ is the m_jth cyclotomic polynomial, then $f(x) - x^a - 1$ will be divisible by $\Phi_{m_j}(x)$ for every nonnegative integer $a \equiv a_j \pmod{m_j}$. Recalling that earlier we saw a covering system $x \equiv a_j \pmod{m_j}$ consisting of distinct moduli m_j from the set $\{2, 3, 4, 6, 12\}$, we obtain a list of 5 congruences for $f(x)$ as above modulo $\Phi_{m_j}(x)$ where $m_j \in \{2, 3, 4, 6, 12\}$. If $f(x)$ satisfies these congruences, then $f(x) - x^a - 1$ will be divisible by a cyclotomic polynomial $\Phi_{m_j}(x)$, with $m_j \in \{2, 3, 4, 6, 12\}$, for every nonnegative integer a. Now, we take advantage of the covering system found by Nielsen, noting though that a somewhat simpler covering system would suffice in the end here. Suppose $x \equiv a'_j \pmod{m'_j}$, with $j \in \{1, 2, \ldots, r\}$, form Nielsen's covering system with minimum modulus 40. Then if we choose $f(x)$ so that

$$f(x) \equiv -x^{a'_j} - 1 \pmod{\Phi_{m'_j}(x)},$$

we see that as above $f(x) + x^a + 1$ will be divisible by one of the cyclotomic polynomials $\Phi_{m'_j}(x)$, where $j \in \{1, 2, \ldots, r\}$, for every nonnegative integer a. Since each $m'_j \geq 40$, the $r + 5$ polynomials $\Phi_{m_j}(x)$ and $\Phi_{m'_j}(x)$ appearing above are pairwise relatively prime polynomials. To ensure that the two polynomials $f(x) \pm 1$ are reducible, we simply add two more congruences involving unrelated moduli, like

$$f(x) \equiv 1 \pmod{x^2 + 2} \qquad \text{and} \qquad f(x) \equiv -1 \pmod{x^2 - 2}.$$

Combining these with the congruences $f(x) \equiv 0 \pmod{x}$ and $f(x) \equiv 0 \pmod{x-1}$ mentioned earlier, we deduce from the Chinese Remainder Theorem that there must be an

$f(x)$ (albeit in $\mathbb{Q}[x]$) such that $f(x)$, $f(x) \pm x^a$ and $f(x) \pm x^a \pm x^b$ are reducible for all nonnegative integers a and b. So this gives us an alternative way to see that such an $f(x)$ exists in $\mathbb{Q}[x]$.

Another open problem in the subject is to determine whether there is a covering system in which the moduli are all distinct odd integers > 1. Erdős offered \$25 for a proof that no such *odd covering system* exists, and John Selfridge has offered up to \$2000 for an explicit example of an odd covering system (cf. [5]). As the story goes, the two of them had disagreeing opinions as to whether an odd covering system exists, so they expressed their confidence in their contrary points of view by offering prizes to anyone who could prove the opposite point of view is correct. In particular, this means that, at the time, Erdős thought an odd covering system does exist and Selfridge believed that there are no odd covering systems. We note that no financial gain has been promised for a non-constructive proof that an odd covering system exists. Needless to say, neither Erdős nor Selfridge ever had to pay the prize money they offered to resolve this problem.

That covering systems might have something to do with Turán's conjecture should not be surprising given Proposition 1. This is certainly the case for the constructions of $f(x)$ given above, but those constructions involving covering systems led to $f(x) \in \mathbb{Q}[x]$. What happens if we require, as we want, that $f(x)$ in $\mathbb{Z}[x]$? The following helps in understanding the difficulty in finding such an $f(x)$ that will imply $C > 2$ in Turán's problem.

Theorem 1 (Schinzel [11], 1967). *In the following,* (i) *implies* (ii).

(i) *There is a polynomial* $g(x) \in \mathbb{Z}[x]$ *satisfying* $g(0) \neq 0$, $g(1) \neq -1$ *and* $G(x) = g(x) + x^a$ *is reducible for every integer* $a \geq 0$.

(ii) *There is a covering system of the integers with distinct odd moduli* > 1.

The implication is explained also in [5]. To better appreciate the connection with Turán's problem, we view $g(x)$ here as $f(x) + 1$, say, with $f(x)$ having at least 4 terms as before. As we did earlier, we take $f(x) \equiv 0 \pmod{x}$, so the condition $g(0) \neq 0$ will be satisfied. We do what we can with the cyclotomic factor $x - 1$ by requiring also that $f(x) \equiv 0 \pmod{x-1}$. This ensures $f(x) + x^a - 1$ and $f(x) - x^a + 1$ are reducible for all integers $a \geq 0$. The condition $f(x) \equiv 0 \pmod{x-1}$ also implies $g(1) \neq -1$. To establish that $C > 2$ in Turán's problem, we want to find an $f(x) \in \mathbb{Z}[x]$ that, in particular, ensures $g(x)$ satisfies (i) above. According to Schinzel's theorem, we can only find such an $f(x)$ if there is a covering system as in (ii). Thus, the existence of such an $f(x)$ implies the existence of an odd covering system, that is a covering system which, if made explicit, would have been eligible for a \$2000 prize.

As a consequence, it would seem that establishing $C > 2$ in Turán's problem is difficult, in contrast to how easy it is to demonstrate there are composite numbers that are not near primes. There is still some hope, though, of finding an example since (i) in Schinzel's theorem concerns all integers $a \geq 0$, whereas an example showing $C > 2$ in Turán's problem only requires that we consider $0 \leq a \leq \deg g$.

4 The plausibility that $C \leq 3$

If we allow for $\deg w(x) > \deg f(x)$ in Turán's problem, the following result shows that the problem can be resolved with $C = 3$.

Theorem 2 (Schinzel [12], 1970). *For every $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, there exist infinitely many polynomials $w(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$ with $\sum_{j=0}^{s} |b_j| \leq 3$ and $f(x) + w(x)$ irreducible. At least one of these satisfies $s < \exp\big((5n+7)(\|f\|+3)\big)$, where $\|f\| = \sqrt{\sum_{j=0}^{r} a_j^2}$.*

Since it is of some interest to obtain s in this result as close to n as possible, we note that Pradipto Banerjee and the author [1] established that the bound on s can be made to depend linearly on n instead of exponentially on n. However, the dependence on the sum of the squares of the coefficients, as in the bound for s above, remains exponential.

5 More convincing evidence that $C \leq 5$

Perhaps the above discussion has already persuaded the reader that there exists some C as in Turán's problem. But there is also compelling evidence of a different sort. In 1996 and 1997, Attila Bérczes and Lajos Hajdu [2, 3] viewed this problem from another point of view. Consider the analog in the field $\mathbb{F}_2$ of arithmetic modulo 2. There are only a finite number of polynomials of each degree, so for a certain degree n, we can determine the minimal distance of each polynomial in $\mathbb{F}_2[x]$ from an irreducible polynomial of degree $\leq n$ in $\mathbb{F}_2[x]$. The tables below show the polynomials of degrees 1, 2 and 3 in $\mathbb{F}_2[x]$ (in the left column) and their minimal distance from an irreducible polynomial in $\mathbb{F}_2[x]$ (in the right column).

x	0
$x+1$	0
x^2	2
x^2+1	1
x^2+x	1
x^2+x+1	0

x^3	2
x^3+1	1
x^3+x	1
x^3+x+1	0
x^3+x^2	1
x^3+x^2+1	0
x^3+x^2+x	2
x^3+x^2+x+1	1

Thus, in $\mathbb{F}_2[x]$, every polynomial of degree ≤ 3 is a distance of at most 2 from an irreducible polynomial in $\mathbb{F}_2[x]$. And, as they noted, this has a direct implication on the problem of Turán. Given any polynomial $f(x)$ of degree $n \in \{1, 2, 3\}$ in $\mathbb{Z}[x]$, we now know that there is a $w(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ with $\sum_{j=0}^{n} |b_j| \leq 3$ such that $f(x)+w(x)$ is irreducible modulo 2 and, hence, irreducible over $\mathbb{Q}$. The bound 3 on $\sum_{j=0}^{n} |b_j|$ comes

from allowing for the possibility that $f(x)$ might have an even leading coefficient, so we may need to add the term x^n to ensure that we are obtaining an irreducible polynomial of the appropriate degree. As an example, we note that if every coefficient of a cubic $f(x)$ is even, then we can take $w(x) = x^3 + x + 1$ to deduce $f(x) + w(x)$ is irreducible modulo 2 and, hence, irreducible over $\mathbb{Q}$. Considering a $w(x)$ with fewer terms may or may not work here.

Bérczes and Hajdu extended this idea to show that every polynomial in $\mathbb{F}_2[x]$ of degree ≤ 24 is within a distance 4 from an irreducible polynomial in $\mathbb{F}_2[x]$ and, hence, one may take $C = 5$ for every polynomial of degree ≤ 24 in Turán's problem. These computations have been extended further using different approaches by Gilbert Lee, Frank Ruskey and Aaron Williams [8], Michael J. Mossinghoff [9], and Mossinghoff and the author [6]. At this point, we know that one may take $C = 5$ for polynomials up to degree 40.

Independent heuristic arguments done by Lee, Ruskey and Williams and by Mossinghoff suggest how the minimal distances to irreducibles are distributed in $\mathbb{F}_2[x]$. If $\delta_k = \delta_k(n)$ denotes the density of polynomials in $\mathbb{F}_2[x]$ of degree n which have minimal distance k to an irreducible polynomial in $\mathbb{F}_2[x]$, then the heuristics give

$$\delta_0 = \frac{1}{n}, \quad \delta_1 = \frac{1-e^{-4}}{4} + \frac{1+e^{-4}}{n},$$
$$\delta_2 = \frac{2-e^{-4}}{4} - \frac{1-e^{-4}}{n},$$
$$\delta_3 = \frac{1+e^{-4}}{4}\left(1-\frac{4}{n}\right), \quad \text{and} \quad \delta_4 = \frac{e^{-4}}{4}\left(1-\frac{4}{n}\right).$$

These lead to approximate asymptotic densities of 24.54%, 49.54%, 25.46% and 0.46% for polynomials in $\mathbb{F}_2[x]$ which have minimal distance to an irreducible polynomial 1, 2, 3 and 4, respectively, with the asymptotic densities for any other distance being 0. These asymptotics agree with the actual computations amazingly accurately. Mossinghoff [9] produced Figure 1 based on his computations up to degree 34. The lined curves show the heuristic densities $\delta_k(n)$, and the points displayed with different styles for each $k \in \{0, 1, 2, 3, 4\}$ show the actual density of polynomials in $\mathbb{F}_2[x]$ of degree n which have minimal distance to an irreducible polynomial k. The second lowest curve shows the density of irreducible polynomials of degree n modulo 2 closely matches the asymptotics given by $\delta_0 = 1/n$. The number of irreducible polynomials of degree n modulo 2 is known to be approximately $2^n/n$. What we don't know, but can conjecture, is that the remaining points, concerning densities of polynomials a distance ≤ 4 from an irreducible polynomial, continue to match up well with the asymptotics δ_j. In fact, we do not even know for any fixed positive integer $k \geq 5$ that the density $\delta_k(n)$ approaches 0 as n goes to infinity. Presumably, this is the case for all $k \geq 5$.

Mossinghoff and the author [6] have shown that a positive proportion of polynomials $f(x)$ in $\mathbb{F}_2[x]$ have distance ≥ 4 to an irreducible polynomial. To clarify, for such $f(x)$ in $\mathbb{F}_2[x]$, if $g(x)$ is any irreducible polynomial in $\mathbb{F}_2[x]$ of *any* degree, then the polynomial $f(x) - g(x)$ (equivalently, $f(x) + g(x)$) in $\mathbb{F}_2[x]$ has at least 4 terms. The argument involves a

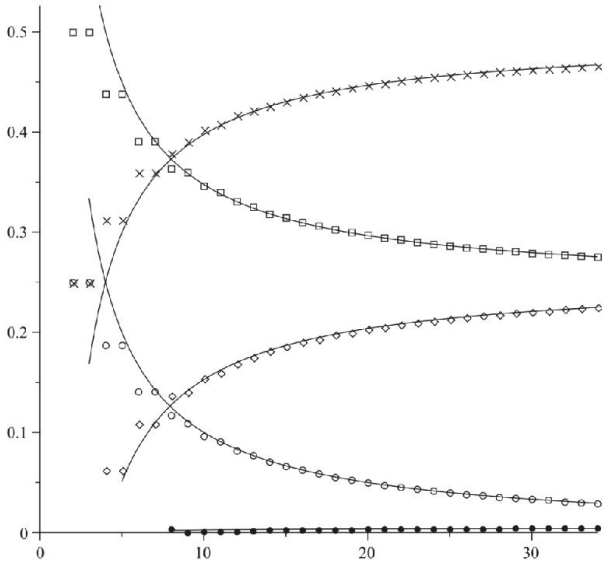

Fig. 1

covering system which produces as a particular example of such an $f(x)$ the polynomial

$$\begin{aligned} f(x) = {} & x^{243} + x^{238} + x^{233} + x^{232} + x^{231} + x^{227} + x^{225} + x^{223} + x^{222} + x^{221} \\ & + x^{217} + x^{216} + x^{214} + x^{208} + x^{206} + x^{203} + x^{202} + x^{201} + x^{199} \\ & + x^{197} + x^{196} + x^{192} + x^{186} + x^{184} + x^{180} + x^{175} + x^{174} + x^{171} \\ & + x^{169} + x^{167} + x^{164} + x^{163} + x^{162} + x^{160} + x^{157} + x^{155} + x^{149} \\ & + x^{147} + x^{146} + x^{145} + x^{143} + x^{141} + x^{136} + x^{133} + x^{130} + x^{129} \\ & + x^{125} + x^{124} + x^{116} + x^{115} + x^{114} + x^{108} + x^{103} + x^{100} + x^{99} \\ & + x^{98} + x^{95} + x^{94} + x^{92} + x^{88} + x^{83} + x^{81} + x^{72} + x^{68} + x^{63} \\ & + x^{61} + x^{55} + x^{52} + x^{50} + x^{49} + x^{47} + x^{46} + x^{43} + x^{36} + x^{35} \\ & + x^{29} + x^{26} + x^{23} + x^{22} + x^{20} + x^{18} + x^{14} + x^{10} + x^{7} + x^{6}. \end{aligned}$$

If we can show that polynomials $f(x)$ in $\mathbb{F}_2[x]$ are always a distance ≤ 4 from an irreducible polynomial in $\mathbb{F}_2[x]$ of degree $\leq \deg f$, then we can take $C = 5$ in the problem of Turán. One can try to do better by working with irreducibility over different fields. This idea, originally from Bérczes and Hajdu [2, 3], was used by Mossinghoff [9] to show that every polynomial of degree ≤ 18 in $\mathbb{F}_3[x]$ is within 3 of an irreducible polynomial. This allows one to take $C = 4$ in Turán's problem for polynomials over $\mathbb{Q}$ of degree up to 18. These authors considered working over other finite fields as well but found there was no further gain in Turán's problem from doing so.

6 Working modulo odd primes

We are ready to go full circle and return to our attempt to prove one needs $C > 2$ in Turán's problem. Recall that we gave a construction that failed to do what we wanted because it produced an $f(x)$ in $\mathbb{Q}[x]$ and not in $\mathbb{Z}[x]$. A similar construction can be used to give some new information about polynomials in $\mathbb{F}_p[x]$.

> *Let p be an odd prime. There exists an $f(x)$ in $\mathbb{F}_p[x]$ of degree ≤ 18 that is a distance ≥ 3 from every irreducible polynomial. Furthermore, a positive proportion of the polynomials $f(x)$ in $\mathbb{F}_p[x]$ are a distance ≥ 3 from every irreducible polynomial.*

In other words, for such $f(x)$, if $g(x)$ is any irreducible polynomial in $\mathbb{F}_p[x]$ (of any degree), then the polynomial $f(x) - g(x)$ in $\mathbb{F}_p[x]$ either (i) has at least 3 terms, (ii) has a coefficient in the set $\{\pm 2\}$ and another coefficient in the set $\{\pm 1, \pm 2\}$, or (iii) has a coefficient that is not in the set $\{0, \pm 1, \pm 2\}$.

We illustrate the argument for this result by considering $p = 3$. For convenience, we represent the elements of $\mathbb{F}_3$ as -1, 0 and 1. For our earlier construction, we considered, among other congruences, $f(x)$ satisfying $f(x) \equiv 0$ modulo each of the polynomials x, $x - 1$ and $x^{2^j} + 1$ where $0 \le j \le 3$. In $\mathbb{F}_3[x]$, the latter two polynomials on this list factor as

$$x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1) \quad \text{and} \quad x^8 + 1 = (x^4 + x^2 - 1)(x^4 - x^2 - 1).$$

To obtain one $f(x)$ as in the result above, one can use the Chinese Remainder Theorem over $\mathbb{F}_3[x]$ with the congruences

$$\begin{aligned}
&f(x) \equiv 0 \pmod{x} && f(x) \equiv 0 \pmod{x^2 + x - 1}\\
&f(x) \equiv 0 \pmod{x - 1} && f(x) \equiv 1 \pmod{x^2 - x - 1}\\
&f(x) \equiv 0 \pmod{x + 1} && f(x) \equiv 0 \pmod{x^4 + x^2 - 1}\\
&f(x) \equiv 0 \pmod{x^2 + 1} && f(x) \equiv -1 \pmod{x^4 - x^2 - 1}.
\end{aligned}$$

The $f(x) \in \mathbb{F}_3[x]$ having smallest possible degree satisfying these congruences is

$$x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^{11} + x^{10} - x^9 + x^7 - x^6 + x^5 + x^4 - x^3 - x^2 - x.$$

We clarify how to show every $f(x)$ satisfying the above congruences is a distance > 2 from an irreducible polynomial in $\mathbb{F}_3[x]$. Note first that $\deg f \ge 11$ since the congruences imply that $f(x)$ is non-zero and divisible by

$$x(x - 1)(x + 1)(x^2 + 1)(x^2 + x - 1)(x^4 + x^2 - 1).$$

The congruence $f(x) \equiv 0 \pmod{x}$ implies $f(x)$ itself is reducible as well as any polynomial of the form $f(x) \pm x^a$ where $a > 0$. The congruences $f(x) \equiv 1 \pmod{x^2 - x - 1}$ and $f(x) \equiv -1 \pmod{x^4 - x^2 - 1}$ imply $f(x) \pm 1$ are reducible. Let a and b be arbitrary nonnegative integers. We want to show that the various polynomials $f(x) \pm x^a \pm x^b$ are

reducible in $\mathbb{F}_3[x]$. Since $f(x) \equiv 0 \pmod{x}$, we may restrict our consideration to polynomials of the form $f(x) \pm x^a \pm 1$. To finish the argument, we now make use of the notation $f(x) \bigoplus x^a \bigoplus 1$ to represent the polynomials of the forms $f(x)+x^a+1$ and $f(x)-x^a-1$ and the notation $f(x) \bigoplus x^a \bigoplus 1$ to represent the polynomials of the forms $f(x)+x^a-1$ and $f(x)-x^a+1$. Then we have the following implications:

$$
\begin{aligned}
f(x) &\equiv 0 \pmod{x-1} &&\Longrightarrow f(x) \bigoplus x^a \bigoplus 1 \text{ are reducible} \\
f(x) &\equiv 0 \pmod{x+1} &&\Longrightarrow f(x) \bigoplus x^a \bigoplus 1 \text{ are reducible for } a \equiv 1 \pmod 2 \\
f(x) &\equiv 0 \pmod{x^2+1} &&\Longrightarrow f(x) \bigoplus x^a \bigoplus 1 \text{ are reducible for } a \equiv 2 \pmod 4 \\
f(x) &\equiv 0 \pmod{x^2+x-1} &&\Longrightarrow f(x) \bigoplus x^a \bigoplus 1 \text{ are reducible for } a \equiv 4 \pmod 8 \\
f(x) &\equiv 1 \pmod{x^2-x-1} &&\Longrightarrow f(x)+x^a+1 \text{ is reducible for } a \equiv 0 \pmod 8 \\
f(x) &\equiv 0 \pmod{x^4+x^2-1} &&\Longrightarrow f(x)-x^a-1 \text{ is reducible for } a \equiv 8 \pmod{16} \\
f(x) &\equiv -1 \pmod{x^4-x^2-1} &&\Longrightarrow f(x)-x^a-1 \text{ is reducible for } a \equiv 0 \pmod{16}.
\end{aligned}
$$

Combining the above information, we deduce every polynomial a distance ≤ 2 from $f(x)$ in $\mathbb{F}_3[x]$ is reducible, giving us what we wanted.

To show that a positive density of the polynomials in $\mathbb{F}_3[x]$ are a distance ≥ 3 from an irreducible polynomial, it suffices to show that a positive density of the polynomials satisfy the above congruences. This will be clear to some of our readers, and we appeal to [6] for details, where a similar argument is done over $\mathbb{F}_2[x]$.

The more general result for an arbitrary odd prime p can be done using a very similar argument. Of particular importance to our argument in $\mathbb{F}_3[x]$ is that the cyclotomic polynomials x^4+1 and x^8+1 were reducible in $\mathbb{F}_3[x]$. In fact, the polynomial x^4+1 is a classic example of a polynomial that factors nontrivially modulo every prime, and the reader unfamiliar with this fact will likely enjoy thinking of a proof. The fact that x^8+1 factors nontrivially modulo every prime p follows by simply replacing x with x^2 in the factorization of x^4+1. More precisely, we can write

$$x^4+1 \equiv h_1(x)h_2(x) \pmod p \quad \text{and} \quad x^8+1 \equiv h_3(x)h_4(x) \pmod p,$$

where the $h_j(x)$ are distinct, pairwise relatively prime polynomials in $\mathbb{F}_p[x]$ since p is odd. In terms of the covering argument above, one can replace the last four congruences on $f(x)$ with

$$
\begin{aligned}
f(x) &\equiv 0 \pmod{h_1(x)} & f(x) &\equiv 0 \pmod{h_3(x)} \\
f(x) &\equiv p-2 \pmod{h_2(x)} & f(x) &\equiv 2 \pmod{h_4(x)}.
\end{aligned}
$$

An additional argument is then needed to establish the reducibility of polynomials of the form $f(x) \pm 1$ in $\mathbb{F}_p[x]$. One can check that the congruences above provide an $f(x)$ satisfying $f(x) \pm 1$ is reducible in $\mathbb{F}_5[x]$. Alternatively, one can take advantage of the fact that x^2+1 factors modulo 5 to give a simpler set of congruences. For $p > 5$, we add to the congruences above the two additional congruences in $\mathbb{F}_p[x]$ given by

$$f(x) \equiv 1 \pmod{x-3} \quad \text{and} \quad f(x) \equiv -1 \pmod{x+3}.$$

The sum of the degrees of the moduli used in the construction of $f(x)$ in $\mathbb{F}_p[x]$ is in general ≤ 19, and this is enough to show the existence of an $f(x)$ as stated earlier of degree ≤ 18. The density argument for the result in $\mathbb{F}_p[x]$ as before follows along the lines of [6], and one can in fact deduce that asymptotically at least $1/p^{19}$ of the $f(x) \in \mathbb{F}_p[x]$ are a distance ≥ 3 from an irreducible polynomial.

Before ending, we note that the simple looking polynomial

$$f(x) = 5x^5 + 8x^4 + 2x^3 + 9x^2 + 10x$$

has the property that $f(x)$ has distance ≥ 3 from every irreducible polynomial in $\mathbb{F}_{17}[x]$. Thus, the existence result for polynomials of degree ≤ 18 in $\mathbb{F}_p[x]$ that are a distance ≥ 3 from every irreducible polynomial in $\mathbb{F}_p[x]$ is not sharp, at least for all primes p. In fact, one can show that the bound 18 can be replaced by ≤ 8 for every prime $p \equiv 1 \pmod 8$.

7 Wrapping up what we know and don't know

In conclusion, we have made various connections between Turán's problem and covering systems. Although Turán's problem remains a fascinating open problem, we have given some fairly strong evidence that every polynomial is within a distance 5 of an irreducible polynomial and likely within a distance 4. We have also seen that allowing more flexibility on the degree of $w(x)$ in this problem allows for a solution with $C = 3$. On the other hand, with or without this flexibility, we do not even know if one can take $C = 2$. Unlike the arbitrarily large sizes of gaps between primes in the set of natural numbers, the sizes of the gaps between irreducible polynomials in the set of polynomials with integer coefficients remain a mystery and are seemingly bounded.

Acknowledgment

The author expresses his gratitude to Mike Mossinghoff for allowing him to use a figure from [9] and for insightful comments on an early version of this paper.

References

[1] P. Banerjee and M. Filaseta, *On a polynomial conjecture of Pál Turán*, Acta Arith. 143 (2010), 239–255.

[2] A. Bérczes and L. Hajdu, *Computational experiences on the distances of polynomials to irreducible polynomials*, Math. Comp. 66 (1997), 391–398.

[3] A. Bérczes and L. Hajdu, *On a problem of P. Turán concerning irreducible polynomials*, Conference in Number Theory: Diophantine, Computational and Algebraic Aspects, in Eger, Hungary, 1996, eds. K. Győry, A. Pethő, V.T. Sós, de Gruyter, Berlin, 1998, 95–100.

[4] P. Erdős, *Some of my favourite problems in number theory, combinatorics, and geometry*, Combinatorics Week (Portuguese) (São Paulo, 1994), Resenhas **2** (1995), no. 2, 165–186.

[5] Michael Filaseta, *Coverings of the integers associated with an irreducibility theorem of A. Schinzel*, In Number theory for the millennium, II (Urbana, IL, 2000), pages 1–24, A K Peters, Natick, MA, 2002.

[6] M. Filaseta and M.J. Mossinghoff, *The distance to an irreducible polynomial, II*, Math. Comp. 81 (2012), 1571–1585.

[7] R.K. Guy, Unsolved problems in number theory, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004.

[8] G. Lee, F. Ruskey and A. Williams, *Hamming distance from irreducible polynomials over* $\mathbb{F}_2$, Discrete Math. Theor. Comput. Sci. Proc., AH (2008), 169–180.

[9] M.J. Mossinghoff, *The distance to an irreducible polynomial*, Gems in Experimental Mathematics (eds. T. Amdeberhan, L.A. Medina, V.H. Moll), Contemp. Math. 517, Amer. Math. Soc., Providence, RI, 2010, 275–288.

[10] P. P. Nielsen, *A covering system whose smallest modulus is* 40, J. Number Theory 129 (2009), 640–666.

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

[12] A. Schinzel, *Reducibility of lacunary polynomials II*, Acta. Arith. **16** (1970), 371–392.

[13] B.L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. **43** (1936), 133–147.

Michael Filaseta
Department of Mathematics
University of South Carolina
Columbia, SC 29208, USA
e-mail: filaseta@math.sc.edu