On Coverings of the Integers Associated with an Irreducibility Theorem of A. Schinzel

Michael Filaseta[1]

Mathematics Department

University of South Carolina

Columbia, SC 29208

May 22, 2001

[1]The author gratefully acknowledges support from the National Security Agency.

1 Introduction

The purpose of this paper is to give a partially expository account of results related to coverings of the integers (defined below) while at the same time making some new observations concerning a related polynomial problem. The polynomial problem we will consider is to determine whether for a given positive integer d there exists an $f(x) \in \mathbb{Z}^+[x]$ such that $f(x)x^n + d$ is reducible over the rationals for every non-negative integer n. We begin with some background material.

A *covering of the integers* is a system of congruences $x \equiv a_j \pmod{m_j}$, with a_j and m_j integral and $m_j \geq 1$, such that every integer satisfies at least one of the congruences. Four examples are as follows:

$x \equiv 0 \pmod{2}$	$x \equiv 0 \pmod{2}$	$x \equiv 0 \pmod{2}$	$x \equiv 0 \pmod{2}$
$x \equiv 1 \pmod{2}$	$x \equiv 1 \pmod{4}$	$x \equiv 2 \pmod{3}$	$x \equiv 0 \pmod{3}$
	$x \equiv 3 \pmod{8}$	$x \equiv 1 \pmod{4}$	$x \equiv 1 \pmod{4}$
	$x \equiv 7 \pmod{16}$	$x \equiv 1 \pmod{6}$	$x \equiv 3 \pmod{8}$
	$\vdots$	$x \equiv 3 \pmod{12}$	$x \equiv 7 \pmod{12}$
			$x \equiv 23 \pmod{24}$

Two open problems concerning coverings are

Open Problem 1: For every $c > 0$, does there exist a finite covering with distinct moduli and with the minimum modulus $\geq c$?

Open Problem 2: Does there exist a finite covering consisting of distinct odd moduli > 1?

We shall call a covering as in the second problem an "odd covering". According to Richard Guy [3], Paul Erdős has offered \$500 for a proof or disproof that a c exists as in the first problem and has offered \$25 for a proof that there is no odd covering. John Selfridge has offered \$900 for an explicit example of an odd covering. In private communication, Selfridge has indicated to the author that he will now pay \$2000 for an explicit odd covering. Observe that in the odd covering problem no direct financial gain is made for a non-constructive proof that an odd covering exists. In [5], R. Morikawa announced that a covering exists as in the first problem with $c = 24$.

We stress the importance of the word "finite" in the above problems with a simple example of an infinite covering with relatively prime odd moduli that are arbitrarily large. Fix $c > 0$, and let $M = \{m_1, m_2, \ldots\}$ be an arbitrary infinite set of relatively prime integers $> c$ (for example, M could be the set of primes $> c$). Let $a_1, a_2, \ldots$ be some ordering of the integers. Then the infinite system $x \equiv a_j \pmod{m_j}$ clearly covers the integers.

One of the now classical examples of the use of coverings is in a disproof that Erdős gave of the following conjecture.

Polignac's Conjecture: For every sufficiently large odd integer $k > 1$, there is a prime p and an integer n such that $k = 2^n + p$.

The Prime Number Theorem would suggest that this is a reasonable conjecture, but small $k > 1$ not the sum of a prime and a power of two are easy to find. The smallest such k is 127 and the smallest composite k is 905. Erdős's argument is based on the last example given of a covering in the first display above. A variation on Erdős's argument is as follows. One considers any positive integer k satisfying the congruence $k \equiv 1 \pmod 2$ so that k is odd and the congruences $k \equiv 1 \pmod 3$, $k \equiv 1 \pmod 7$, $k \equiv 2 \pmod 5$, $k \equiv 8 \pmod{17}$, $k \equiv 11 \pmod{13}$, and $k \equiv 121 \pmod{241}$ (such k exist by the Chinese Remainder Theorem). The key idea then is to consider what happens if n satisfies one of the congruences in the last covering displayed above. For example, if $n \equiv 7 \pmod{12}$, then $2^n \equiv 2^7 \equiv 11 \pmod{13}$ so that $k - 2^n$ is divisible by 13. Since every integer n satisfies one of the congruences listed above, one can deduce that $k - 2^n$ must be divisible by at least one element of $S = \{3, 7, 5, 13, 17, 241\}$. From an analytic point of view, we are through. The Chinese Remainder Theorem gives that for some $\delta > 0$ and for x sufficiently large, there are $> \delta x$ different $k \le x$ as above. On the other hand, for any such k, the only possible prime values of $k - 2^n$ are elements of S so that k will be of the form $2^n + s$ where $s \in S$. Since $|S| = 6$, one easily deduces that there are $\ll (\log x)^6$ such $k \le x$. It follows that a positive proportion of positive integers k cannot be written in the form $2^n + p$.

Another classical application of the use of coverings was given by Waclaw Sierpiński.

Sierpiński's Theorem: A positive proportion of odd positive integers ℓ satisfy $\ell \times 2^n + 1$ is composite for all non-negative integers n.

It is unknown what the smallest such ℓ is. It is probably $\ell = 78557$ (attributed to Selfridge). Extensive computations are being done to check that for each odd $\ell < 78557$ there is a prime of the form $\ell \times 2^n + 1$, but it may be some time before they are completed. There are apparently 19 values of ℓ left to eliminate at the time of writing this paper; see

`http://vamri.xray.ufl.edu/proths/sierp.html`.

The question of whether there are infinitely many prime Fermat numbers is related to the existence of even ℓ as above. For example, if $F_n = 2^{2^n} + 1$ is composite for $n \ge 5$, then for $\ell = 2^{17} = 131072$ one has $\ell \times 2^n + 1$ is composite for all non-negative integers n.

Andrzej Schinzel noted Sierpiński's Theorem follows from the above solution to Polignac's Conjecture. Take $\ell = -k$. For each $n \ge 0$, consider $p \in \{3, 5, 7, 13, 17, 241\}$ such that $\ell + 2^{239n} \equiv 0 \pmod p$. Then $\ell + 2^{239n} \equiv \ell + 2^{-n}$

$\pmod p$ so that $\ell \times 2^n + 1 \equiv 0 \pmod p$. By considering $k < 0$ satisfying the congruences imposed on k above, one obtains the result of Sierpiński.

In this paper, we consider a polynomial variant of Sierpiński's result. In its most simplest form, the problem we consider is as follows.

The Analogous Polynomial Problem: Find $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -1$ such that $f(x)x^n + 1$ is reducible over the rationals for all $n \geq 0$.

The condition $f(1) \neq -1$ makes the problem non-trivial. Otherwise, one could simply consider any $f(x)$ of degree > 1 satisfying $f(1) = -1$ as then $f(x)x^n + 1$ will always have the factor $x - 1$. Schinzel [7] first considered this problem in a slightly different form with $f(x)x^n + 1$ replaced by $x^n + f(x)$ (and with the added condition $f(0) \neq 0$). His version was chosen as an approach to understanding a conjecture of Turán that every reducible polynomial is in some sense near an irreducible polynomial. Modifying an example of Schinzel's, we note that

$$f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$$

has the property that $f(x)x^n + 12$ is reducible for all $n \geq 0$. The argument for this is based on the third covering example displayed in the second opening paragraph. Indeed, that $f(x)x^n + 12$ is reducible for all $n \geq 0$ can be obtained by noting that every non-negative integer satisfies at least one of the congruences given there and that the following implications all hold:

$$\begin{aligned}
n \equiv 0 \pmod 2 &\implies f(x)x^n + 12 \equiv 0 \pmod{x+1} \\
n \equiv 2 \pmod 3 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1} \\
n \equiv 1 \pmod 4 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1} \\
n \equiv 1 \pmod 6 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2-x+1} \\
n \equiv 3 \pmod{12} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^4-x^2+1}.
\end{aligned}$$

Observe that the moduli on the right are the cyclotomic polynomials $\Phi_2(x)$, $\Phi_3(x)$, $\Phi_4(x)$, $\Phi_6(x)$, and $\Phi_{12}(x)$, respectively. The implications are easily justified. For example, if $n \equiv 1 \pmod 6$, then $x^n \equiv x \pmod{\Phi_6(x)}$ so that by a direct computation

$$f(x)x^n + 12 \equiv f(x)x + 12 \equiv 0 \pmod{\Phi_6(x)}.$$

The dual role of 12 here (as the least common multiple of the moduli in the covering and as the constant term in $f(x)x^n + 12$ for $n > 0$) is misleading. The main new result in this paper is in fact a demonstration that a suitable covering (considerably more complicated than those given in the examples above) can give rise to an $f(x) \in \mathbb{Z}^+[x]$ with $f(x)x^n + 4$ reducible for all $n \geq 0$. More generally, we obtain

Theorem 1. *Let d be a positive integer divisible by 4. There is an $f(x) \in \mathbb{Z}^+[x]$ with $f(x)x^n + d$ reducible for all $n \geq 0$.*

Observe that the condition $f(1) \neq -d$, that would prevent trivial examples of polynomials $f(x)$ with $f(x)x^n + d$ having $x - 1$ as a factor for all $n \geq 0$, is replaced by the condition that $f(x)$ have positive coefficients. Our condition seemingly makes a stronger result, but we really only choose this formulation to simplify the statement of the result.

We are left with the question

Open Problem 3: For what positive integers d does there exist an $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -d$ such that $f(x)x^n + d$ is reducible over the rationals for all $n \geq 0$?

The author is unable to establish more d with this property than what the theorem states above. Schinzel [7] already established a result that at least suggests that the existence of such $f(x)$ when $d = 1$ would be difficult to establish. We modify his ideas to show

Theorem 2. *Let d be an odd positive integer. If there is an $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -d$ and $f(x)x^n + d$ reducible for all $n \geq 0$, then there is an odd covering of the integers.*

We emphasize that this can be obtained by a simple variation on Schinzel's work in [7] and that, in fact, Schinzel's work gives a necessary and sufficient condition (somewhat more complicated than the existence of an odd covering) for such an $f(x)$ to exist in the case that $d = 1$. Nevertheless, we will give a proof of the above result, a proof that is similar in flavor but still somewhat different from Schinzel's original work on the subject.

2 A Result Concerning Cyclotomic Polynomials

We make use of the notation

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \tag{1}$$

so that $\Phi_n(x)$ denotes the nth cyclotomic polynomial. It is well-known and easy to establish from (1) that

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n. \end{cases} \tag{2}$$

We also set $\zeta_n = e^{2\pi i/n}$. Throughout this paper, d will denote a positive integer.

The example given by Schinzel of a polynomial $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -12$ and $f(x)x^n + 12$ reducible for all $n \geq 0$ has a clear connection to cyclotomic polynomials. Indeed, we saw in the introduction that there is a finite list of polynomials P, all cyclotomic, such that each $f(x)x^n + 12$ is divisible by some element of P. To demonstrate the important role of cyclotomic polynomials in our investigations here, suppose that $f(x)x^n + d$ is divisible by $g(x)$ for some irreducible $g(x) \in \mathbb{Z}[x]$ and for at least two different non-negative integers n, say $n = u$ and $n = v$ with $u > v$. Then $g(x)$ also divides

$$\big(f(x)x^u + d\big) - \big(f(x)x^v + d\big) = f(x)x^v\big(x^{u-v} - 1\big).$$

Since $d \neq 0$, we deduce that $g(x)$ divides $x^{u-v} - 1$ and, therefore, is cyclotomic. It follows that if we want to establish that $f(x)x^n + d$ is reducible for all non-negative integers n by finding a finite list of polynomials P such that each $f(x)x^n + d$ is divisible by an element of P, then P must contain cyclotomic polynomials. Another simple result in this direction is the following:

Lemma 1. *Suppose $f(x)x^a + d$ is divisible by $\Phi_m(x)$ for some positive integer m. Then $f(x)x^n + d$ is divisible by $\Phi_m(x)$ if and only if $n \equiv a \pmod{m}$.*

Proof. Let $F(x) = f(x)x^n + d$. If $n \equiv a \pmod{m}$, then clearly $F(\zeta_m) = f(\zeta_m)\zeta_m^a + d = 0$ so that $F(x)$ is divisible by $\Phi_m(x)$. If $F(x)$ is divisible by $\Phi_m(x)$, the equality

$$0 = \zeta_m^{n-a}\big(f(\zeta_m)\zeta_m^a + d\big) - F(\zeta_m) = d\big(\zeta_m^{n-a} - 1\big)$$

implies $n \equiv a \pmod{m}$. □

The lemma alluded to in the title of this section is the following.

Lemma 2. *Let n and m be positive integers with $n > m$. If n/m is not a power of a prime, then for every integer a, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ satisfying*

$$\Phi_n(x)u(x) + \Phi_m(x)v(x) = a. \tag{3}$$

If for some prime p and some positive integer t we have $n/m = p^t$, then there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ satisfying (3) if and only if $p|a$.

Momentarily, we turn to some preliminary lemmas (some quite well-known) that will not only give us what we need for the above result but also keep our arguments self-contained. Schinzel has pointed out, however, that Lemmas 3-6 and the proof of Lemma 2 can be replaced by applications of a result of Tom Apostol [1] on the resultant of two cyclotomic polynomials. Therefore, we present here Schinzel's alternative approach as well as the author's more self-contained approach. We begin with Schinzel's argument for Lemma 2. The remaining use of Apostol's work, as suggested by Schinzel, is presented in Concluding Remarks at the end of this paper.

First Proof of Lemma 2. Let $R(n,m)$ denote the resultant of $\Phi_n(x)$ and $\Phi_m(x)$. Then it is well-known that there exist polynomials $u_1(x)$ and $v_1(x)$ in $\mathbb{Z}[x]$ such that

$$\Phi_n(x)u_1(x) + \Phi_m(x)v_1(x) = R(n,m).$$

In the case that n/m is not a power of a prime, Apostol's work [1] implies that $R(n,m) = \pm 1$. We deduce immediately that, for every integer a, there are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ satisfying (3).

In the case that $n/m = p^t$ as in the statement of the lemma, Apostol establishes that $R(n,m) = \pm p^{\phi(m)}$. Note that $n = p^t m$ implies $\phi(m)|\phi(n)$. We consider the polynomial

$$h(x) = \frac{1}{p}\big(\Phi_n(x) - \Phi_m(x)^{\phi(n)/\phi(m)}\big).$$

From (2), it follows that $\Phi_n(x) \equiv \Phi_m(x)^{\phi(n)/\phi(m)} \pmod{p}$ so that $h(x) \in \mathbb{Z}[x]$. Observe that the resultant of $\Phi_m(x)$ and $h(x)$ can be expressed as

$$\prod_{\substack{1\le k\le m\\ \gcd(k,m)=1}} h(\zeta_m^k) = p^{-\phi(m)} \prod_{\substack{1\le k\le m\\ \gcd(k,m)=1}} \Phi_n(\zeta_m^k) = p^{-\phi(m)} R(n,m) = \pm 1.$$

Hence, there exist polynomials $u_2(x)$ and $v_2(x)$ in $\mathbb{Z}[x]$ such that

$$h(x)u_2(x) + \Phi_m(x)v_2(x) = 1.$$

Given the definition of $h(x)$, we deduce

$$\Phi_n(x)u_2(x) + \Phi_m(x)\big(pv_2(x) - \Phi_m(x)^{\phi(n)/\phi(m)-1}u_2(x)\big) = p.$$

We deduce in this case that, for every integer a divisible by p, there are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ satisfying (3). Furthermore, if polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ exist satisfying (3), then we must have $a \equiv 0 \pmod{p}$ since otherwise $\Phi_n(x)$ and $\Phi_m(x)$ would be relatively prime in the finite field with p elements contradicting that $R(n,m)$ is 0 in this field. $\square$

Lemma 3. *Suppose n and m are integers with $n/m = p^r$ for some prime p and some positive integer r. Then $\Phi_n(\zeta_m) = pw$ for some unit $w \in \mathbb{Z}[\zeta_m]$.*

Proof. We consider three cases: (i) $n = pm$ and $p \nmid m$, (ii) $n = p^r m$ with $r > 1$ and $p \nmid m$, and (iii) $n = p^u t$ and $m = p^v t$ with $u > v > 0$. Let ξ denote an arbitrary primitive mth root of 1 (so $\xi \in \mathbb{Z}[\zeta_m]$). For (i), observe that (2) implies $\Phi_n(x) = \Phi_m(x^p)/\Phi_m(x)$. Hence,

$$\Phi_n(\xi) = \lim_{x\to\xi} \frac{\Phi_m(x^p)}{\Phi_m(x)} = \frac{p\xi^{p-1}\Phi_m'(\xi^p)}{\Phi_m'(\xi)}.$$

Since ξ^{pj} and ξ^j range over the same set of values for $1 \le j \le m$ and $\gcd(j,m) = 1$, we deduce that $\Phi'_m(\xi^p)$ and $\Phi'_m(\xi)$ have the same norm in the field $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$. Also, the norm of ξ is ± 1. We deduce that the norm of $\Phi_n(\xi)$ is $\pm p^{\phi(m)}$. On the other hand,

$$\begin{aligned}\Phi_n(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} &= \prod_{\substack{1\le k\le m\\ \gcd(k,m)=1}} \left(\frac{x^p - \xi^{kp}}{x - \xi^k}\right)\\ &= \prod_{\substack{1\le k\le m\\ \gcd(k,m)=1}} \left(x^{p-1} + \xi^k x^{p-2} + \xi^{2k} x^{p-3} + \cdots + \xi^{(p-1)k}\right).\end{aligned}$$

By considering the factor corresponding to $k=1$, we deduce that $\Phi_n(\xi) = pu$ for some $u \in \mathbb{Z}[\zeta_m]$. It follows that there are $u_k \in \mathbb{Z}[\zeta_m]$ such that $\Phi_n(\zeta_m^k) = pu_k$ for each positive integer $k \le m$ with $\gcd(k,m) = 1$. Therefore,

$$p^{\phi(m)} \prod_{\substack{1\le k\le m\\ \gcd(k,m)=1}} u_k = \prod_{\substack{1\le k\le m\\ \gcd(k,m)=1}} \Phi_n(\zeta_m^k) = \pm p^{\phi(m)}.$$

We deduce that each u_k is a unit in $Z[\zeta_m]$. Hence, (i) follows.

For (ii), use (2) again to obtain $\Phi_n(\zeta_m) = \Phi_{pm}\left(\zeta_m^{p^{r-1}}\right)$ and apply the argument for (i) with $\xi = \zeta_m^{p^{r-1}}$. For (iii), use (2) as before to obtain $\Phi_n(\zeta_m) = \Phi_{p^{u-v}t}\left(\zeta_m^{p^v}\right) = \Phi_{p^{u-v}t}(\zeta_t)$. Now, cases (i) and (ii) imply $\Phi_n(\zeta_m) = pw$ for some unit $w \in \mathbb{Z}[\zeta_t] \subseteq \mathbb{Z}[\zeta_m]$ (since $\zeta_t = \zeta_m^{p^v}$). □

Lemma 4. *Let m be an integer > 1. Then*

$$\Phi_m(1) = \begin{cases} p & \text{if } m = p^r \text{ for some } r \in \mathbb{Z}^+\\ 1 & \text{otherwise.}\end{cases}$$

Proof. Clearly, $\Phi_p(1) = p$. If $m = p^r k$ with k and r positive integers such that $p \nmid k$, then (2) implies $\Phi_m(1) = \Phi_{pk}(1^{p^{r-1}}) = \Phi_{pk}(1)$. The lemma follows if $k = 1$. If $k > 1$, then applying (2) again we obtain $\Phi_m(1) = \Phi_{pk}(1) = \Phi_k(1^p)/\Phi_k(1) = 1$. □

Lemma 5. *Let m and ℓ be integers with $m \ge 1$ and $\ell \ge 0$. For $\alpha \in \mathbb{Q}(\zeta_m)$, let $N(\alpha) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)$ denote the norm of α. Then $N\left(\zeta_m^\ell - 1\right)$ is divisible by a prime p if and only if $m/\gcd(\ell,m)$ is a power of p.*

Proof. The idea is to apply Lemma 4 and use that

$$N\left(\zeta_m^\ell - 1\right) = \pm \Phi_{m/\gcd(\ell,m)}(1)^{\phi(m)/\phi(m/\gcd(\ell,m))}.$$

This last equation can be seen as follows. Note that $N\big(\zeta_m^\ell - 1\big) = \pm N\big(1 - \zeta_m^\ell\big)$. The value of $N\big(1 - \zeta_m^\ell\big)$ is the product of its $\phi(m)$ field conjugates $1 - \zeta_m^{k\ell}$ where $1 \le k \le m$ and $\gcd(k, m) = 1$. Observe that $1 - \zeta_m^\ell = 1 - \zeta_{m/d}^{\ell/d}$ where $d = \gcd(m, \ell)$, and $\zeta_{m/d}^{\ell/d}$ is a primitive (m/d)th root of unity. The field conjugates associated with $1-\zeta_m^\ell$ are thus the same as the numbers $1-\zeta_{m/d}^t$ where $1 \le t \le m/d$ and $\gcd(t, m/d) = 1$ with each $1 - \zeta_{m/d}^t$ appearing among the $1 - \zeta_m^{k\ell}$ precisely $\phi(m)/\phi(m/d)$ times (see Theorem 2-5 of William LeVeque's book [4]). Finally, observe that

$$\prod_{\substack{1 \le t \le m/d \\ \gcd(t, m/d)=1}} \big(1 - \zeta_{m/d}^t\big) = \Phi_{m/d}(1).$$

The result now follows. □

Observe that Lemma 5, using the notation there, implies that $\zeta_m^\ell - 1$ is a unit in $\mathbb{Z}[\zeta_m]$ if and only if $m/\gcd(\ell, m)$ is not a power of a prime.

Lemma 6. *Let $n > 1$ and a be positive integers with $\gcd(a, n) = 1$. Then the quotient $(\zeta_n^a - 1)/(\zeta_n - 1)$ is a unit in $\mathbb{Z}[\zeta_n]$.*

Proof. Let $\beta = (\zeta_n^a - 1)/(\zeta_n - 1)$. Observe that

$$\beta = 1 + \zeta_n + \zeta_n^2 + \cdots + \zeta_n^{a-1}$$

so that $\beta \in \mathbb{Z}[\zeta_n]$. The condition $\gcd(a, n) = 1$ implies that the set of values of ζ_n^{ja} and the set of values of ζ_n^j are the same as j varies over the positive integers $\le n$ that are relatively prime to n. It follows that the norm of β in the field $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is 1. Hence, β is a unit in $\mathbb{Z}[\zeta_n]$. □

Second Proof of Lemma 2. Since $n > m$, there is a prime p and non-negative integers r and s with $r > s$ satisfying $n = p^r n'$ and $m = p^s m'$ for some integers n' and m' each not divisible by p. The condition $n/m = p^t$ in the lemma is satisfied precisely when $n' = m'$ (with $t = r - s$). We use that

$$\Phi_m(\zeta_n) = \prod_{d|m} \big(\zeta_n^d - 1\big)^{\mu(m/d)}.$$

Given that $d|m$, observe $n/\gcd(d, n)$ can be a power of a prime only if $n'|d$. It follows from Lemma 5 (see the comment after its proof) that if $n' \nmid d$, then $\zeta_n^d - 1$ is a unit in $\mathbb{Z}[\zeta_n]$. Thus, there is a unit $w \in \mathbb{Z}[\zeta_n]$ such that

$$\Phi_m(\zeta_n) = w \prod_{\substack{d|m \\ n'|d}} \big(\zeta_n^d - 1\big)^{\mu(m/d)}.$$

In particular, if $n' \nmid m'$, then $\Phi_m(\zeta_n)$ is a unit in $\mathbb{Z}[\zeta_n]$. If $n'|m'$, then we set $k = m'/n'$, take $d = p^j n' d'$ where $d'|k$, and rewrite the above to obtain

$$\Phi_m(\zeta_n) = w \prod_{j=0}^{s} \prod_{d'|k} \left(\zeta_{p^{r-j}}^{d'} - 1\right)^{\mu(p^{s-j}k/d')}.$$

If $k > 1$ and $j \in \{s-1, s\}$, we use that

$$\sum_{d'|k} \mu(p^{s-j}k/d') = \pm \sum_{d'|k} \mu(k/d') = 0$$

to deduce that

$$\Phi_m(\zeta_n) = w \prod_{j=s-1}^{s} \prod_{d'|k} \left(\frac{\zeta_{p^{r-j}}^{d'} - 1}{\zeta_{p^{r-j}} - 1} \right)^{\mu(p^{s-j}k/d')}.$$

Note that for each $j \in \{0, 1, \ldots, s\}$, we have $\mathbb{Z}[\zeta_{p^{r-j}}] \subseteq \mathbb{Z}[\zeta_n]$. We deduce from Lemma 6 that if $n' \neq m'$, then $\Phi_m(\zeta_n)$ is a unit in $\mathbb{Z}[\zeta_n]$. In this case, for some $v_0(x) \in \mathbb{Z}[x]$, we obtain $\Phi_m(\zeta_n)v_0(\zeta_n) = 1$. In other words, $\Phi_m(x)v_0(x) - 1$ has ζ_n as a root. It follows that $\Phi_m(x)v_0(x) - 1 = \Phi_n(x)u_0(x)$ for some $u_0(x) \in \mathbb{Z}[x]$ so that (3) holds by multiplying through by a (i.e., taking $u(x) = -au_0(x)$ and $v(x) = av_0(x)$). If $n' = m'$, then we apply Lemma 3 to obtain that $\Phi_n(\zeta_m) = pw_0$ for some unit w_0 in $\mathbb{Z}[\zeta_m]$. Therefore, taking $u_0(\zeta_m) \in \mathbb{Z}[\zeta_m]$ to be the inverse of w_0, we obtain $\Phi_n(x)u_0(x) - p$ is divisible by $\Phi_m(x)$. We deduce in this case that if $p|a$, then (3) has a solution in polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$. Lemma 3 also implies the necessity of having $p|a$ when $n' = m'$ as follows. Take $x = \zeta_m$ in (3) to obtain $\Phi_n(\zeta_m)u(\zeta_m) = a$. By Lemma 3, the norm of $\Phi_n(\zeta_m)u(\zeta_m)$ (in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$) is divisible by p so that the norm of a must also be divisible by p. Thus, $p|a$, concluding the proof. ☐

3 How Coverings Produce Reducible Polynomials

Let d be a positive integer. Suppose we wish to find an $f(x)$ with positive integer coefficients such that $f(x)x^n + d$ is reducible for every non-negative integer n. The purpose of this section is to show how certain coverings of the integers can be used to obtain such $f(x)$. This is achieved through the following result.

Theorem 3. *Let d be a positive integer. Suppose that S is a system of congruences*

$$x \equiv 2^{j-1} \pmod{2^j} \qquad \text{for } j \in \{1, 2, \ldots, k\} \tag{4}$$

for some positive integer k together with

$$x \equiv a_j \pmod{m_j} \qquad \text{for } j \in \{1, 2, \ldots, r\} \tag{5}$$

for some positive integer r satisfying:

(i) The system S is a covering of the integers.

(ii) The moduli in (4) and (5) are all distinct and > 1.

(iii) For each $j \in \{1, 2, \dots, r\}$,

$$\Bigg(\prod_{\substack{1 \le i \le r \\ i \ne j}} a(i,j) \Bigg) \Bigg(\prod_{i=1}^{k} b(i,j) \Bigg) \text{ divides } d$$

where

$$a(i,j) = \begin{cases} p & \text{if } m_i/m_j = p^t \text{ for some prime } p \text{ and some integer } t \\ 1 & \text{otherwise} \end{cases}$$

and

$$b(i,j) = \begin{cases} p & \text{if } m_j/2^i = p^t \text{ for some prime } p \text{ and some integer } t \\ 1 & \text{otherwise.} \end{cases}$$

(iv) The double product $\prod_{i=1}^{k} \prod_{j=1}^{r} b(i,j)$ divides d.

Then there exists $f(x) \in \mathbb{Z}[x]$ with positive coefficients such that $f(x)x^n + d$ is reducible over the rationals for all non-negative integers n.

Proof. Fix d now as in the statement of the theorem. We consider as we may that $0 \le a_j < m_j$ in (5). Suppose for the moment that we have an $f(x)$ satisfying the system of congruences consisting of

$$f(x) \equiv d \pmod{w(x)}, \tag{6}$$

where $w(x) = \prod_{j=1}^{k} \Phi_{2^j}(x)$, together with

$$f(x) \equiv -dx^{m_j - a_j} \pmod{\Phi_{m_j}(x)} \qquad \text{for } j \in \{1, 2, \dots, r\}. \tag{7}$$

Let n be a non-negative integer. By (i), n must satisfy at least one of the congruences in (4) and (5). If there is a $j \in \{1, 2, \dots, k\}$ such that $n \equiv 2^{j-1} \pmod{2^j}$, then for some $\ell \in \mathbb{Z}$ we have $n = 2^{j-1} + 2^j \ell$. Since $\Phi_{2^j}(x) = x^{2^{j-1}} + 1$, we obtain from (6) that

$$f(x)x^n + d \equiv d\big(x^{(2\ell+1)2^{j-1}} + 1\big) \equiv 0 \pmod{x^{2^{j-1}} + 1}.$$

We deduce that $f(x)x^n + d$ is divisible by $\Phi_{2^j}(x)$. On the other hand, if there is a $j \in \{1, 2, \ldots, r\}$ such that $n \equiv a_j \pmod{m_j}$, then $n = a_j + m_j\ell$ for some integer ℓ. Since $\Phi_{m_j}(x)$ divides $x^{m_j} - 1$, we obtain from (7) that

$$f(x)x^n + d \equiv -d\bigl(x^{(\ell+1)m_j} - 1\bigr) \equiv 0 \pmod{\Phi_{m_j}(x)}.$$

Thus, $f(x)x^n + d$ is divisible by $\Phi_{m_j}(x)$.

To finish the proof, it suffices to show that we can find an $f(x)$ with positive integral coefficients satisfying the congruences in (6) and (7) and such that, for every non-negative integer n, $f(x)x^n + d$ is not a constant times $\Phi_{2^j}(x)$ for $j \in \{1, 2, \ldots, k\}$ and not a constant times $\Phi_{m_j}(x)$ for $j \in \{1, 2, \ldots, r\}$. To do this, we show that there is an $f(x)$ with positive integral coefficients satisfying the congruences in (6) and (7) and such that $\deg f$ is greater than both 2^k and $\max_{1 \le j \le k}\{m_j\}$.

We apply Lemma 2 to deduce that, for i and j in $\{1, 2, \ldots, r\}$ with $i \ne j$, there are polynomials $u_{i,j}(x)$ and $v_{i,j}(x)$ in $\mathbb{Z}[x]$ such that

$$\Phi_{m_i}(x)u_{i,j}(x) + \Phi_{m_j}(x)v_{i,j}(x) = a(i,j). \tag{8}$$

Also, by that lemma, for $i \in \{1, 2, \ldots, k\}$ and $j \in \{1, 2, \ldots, r\}$, there are polynomials $u'_{i,j}(x)$ and $v'_{i,j}(x)$ in $\mathbb{Z}[x]$ such that

$$\Phi_{2^i}(x)u'_{i,j}(x) + \Phi_{m_j}(x)v'_{i,j}(x) = b(i,j). \tag{9}$$

We fix $j \in \{1, 2, \ldots, r\}$ and expand

$$c \prod_{\substack{1 \le i \le r \\ i \ne j}} \bigl(\Phi_{m_i}(x)u_{i,j}(x) + \Phi_{m_j}(x)v_{i,j}(x)\bigr) \times \prod_{1 \le i \le k} \bigl(\Phi_{2^i}(x)u'_{i,j}(x) + \Phi_{m_j}(x)v'_{i,j}(x)\bigr)$$

where

$$c = \frac{d}{\Biggl(\displaystyle\prod_{\substack{1 \le i \le r \\ i \ne j}} a(i,j)\Biggr)\Biggl(\displaystyle\prod_{i=1}^{k} b(i,j)\Biggr)}.$$

From (iii), (8), and (9), we deduce that

$$\Biggl(\prod_{\substack{1 \le i \le r \\ i \ne j}} \Phi_{m_i}(x)\Biggr) w(x)u_j(x) + \Phi_{m_j}(x)v_j(x) = d$$

for some polynomials $u_j(x)$ and $v_j(x)$ in $\mathbb{Z}[x]$. Similarly, combining (iv) and (9), one obtains $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ satisfying

$$\Big(\prod_{1 \le j \le r} \Phi_{m_j}(x) \Big) u(x) + w(x)v(x) = d.$$

Let $M = 2^k m_1 m_2 \cdots m_r$, and let $k(x) \in \mathbb{Z}[x]$. It follows that

$$f(x) = \sum_{j=1}^{r} \Big(\prod_{\substack{1 \le i \le r \\ i \ne j}} \Phi_{m_i}(x) \Big) w(x) u_j(x) \big(-x^{m_j - a_j} \big) + \Big(\prod_{1 \le j \le r} \Phi_{m_j}(x) \Big) u(x) + k(x) \Big(\frac{x^M - 1}{x - 1} \Big)$$

satisfies the congruences in (6) and (7). Furthermore, we may take $k(x)$ appropriately (for example, $k(x) = b(x^s - 1)/(x - 1)$ with b and s sufficiently large positive integers) so that $f(x)$ has positive integral coefficients and $\deg f$ is greater than both 2^k and $\max_{1 \le j \le k}\{m_j\}$. This completes the proof. □

4 A Preliminary Covering and Theorem 1

In this section, we establish

Theorem 4. *There is a covering of the integers consisting of moduli $m_1, m_2, \dots, m_r$ satisfying:*

(i) For each positive integer m, there exist at most three $\ell \in \{1, 2, \dots, r\}$ for which $m_\ell = m$.

(ii) Each m_ℓ is odd and > 1.

(iii) Each m_ℓ has at least two distinct prime factors.

Observe that Theorem 4 implies that an odd covering exists if we allow up to three congruences for each odd modulus. The existence of an $f(x) \in \mathbb{Z}^+[x]$ such that $f(x)x^n + 2$ is reducible for all integers $n \ge 0$ would follow if one can establish the existence of a covering as in Theorem 4 but with "three" replaced by "two" in (i) above.

Before turning to the proof of Theorem 4, we explain how it is used with Theorem 3 to deduce Theorem 1. Let $x \equiv a_j \pmod{m_j}$ for $j \in \{1, 2, \dots, r\}$ denote the r congruences given by Theorem 4. We suppose as we may (by (i) in Theorem 4) that if $m_i = m_j$ for some integers i and j with $1 \le j < i \le r$, then $i = j + 1$ or $i = j + 2$. In particular, for j fixed, the conditions $i \neq j$ and $m_j = m_i$ imply there are at most two possibilities for i. Define

$$m'_j = 2^j m_j \qquad \text{for } j \in \{1, 2, \dots, r\}.$$

By the Chinese Remainder Theorem, for each $j \in \{1, 2, \dots, r\}$, there is an integer b_j satisfying

$$b_j \equiv a_j \pmod{m_j} \qquad \text{and} \qquad b_j \equiv 0 \pmod{2^j}.$$

We consider the congruences

$$x \equiv 2^{j-1} \pmod{2^j} \qquad \text{for } j \in \{1, 2, \dots, r\} \tag{10}$$

together with

$$x \equiv b_j \pmod{m'_j} \qquad \text{for } j \in \{1, 2, \dots, r\}. \tag{11}$$

We show that these congruences form a system S of congruences satisfying the conditions of Theorem 3 (so $k = r$ in Theorem 3 and the m_j have been replaced by m'_j there) provided d is divisible by 4.

Let n be an arbitrary integer that does not satisfy one of the congruences in (10). Then $n \equiv 0 \pmod{2^r}$ (otherwise, n would satisfy the congruence in (10) corresponding to the largest positive integer j, necessarily $\leq r$, for which 2^{j-1} divides n). Also, since the congruences $x \equiv a_j \pmod{m_j}$ for $j \in \{1, 2, \dots, r\}$ form a covering of the integers, $n \equiv a_j \pmod{m_j}$ for some $j \in \{1, 2, \dots, r\}$. By the definition of b_j, we have for that choice of j that $x \equiv b_j \pmod{m'_j}$. Hence, n satisfies one of the congruences in (11). Thus, S satisfies the condition (i) of Theorem 3. Condition (ii) of Theorem 3 is easily checked for the congruences in (10) and (11). To verify conditions (iii) and (iv) of Theorem 3 for the congruences in (10) and (11), we alter the definitions of $a(i, j)$ and $b(i, j)$ accordingly so that m_i and m_j are replaced by m'_i and m'_j. Since m'_j is 2^j times the odd number m_j, if the ratio $m'_j/m'_i = p^t$ for some prime p and some integer t, then $p = 2$ and, consequently, $m_j = m_i$. Recall that for j fixed, the conditions $i \neq j$ and $m_j = m_i$ imply there are at most two possibilities for i. We deduce that for each $j \in \{1, 2, \dots, r\}$,

$$\prod_{\substack{1 \leq i \leq r \\ i \neq j}} a(i, j) \ \text{ divides } \ 4.$$

By conditions (ii) and (iii) in Theorem 4, each m_j and, hence, each m'_j has at least two odd prime divisors. It follows that $b(i, j) = 1$ for every choice of i and j in $\{1, 2, \dots, r\}$. Conditions (iii) and (iv) of Theorem 3 now easily follow since d is divisible by 4.

We turn now to establishing Theorem 4.

Lemma 7. *Let p be a prime, and let E be a positive integer. Suppose that n is an integer which is not congruent to -1 modulo p^E. Then n satisfies at least one of the congruences*

$$x \equiv p^{e-1}(j+1) - 1 \pmod{p^e} \qquad \text{where } 0 \le j \le p-2 \text{ and } 1 \le e \le E.$$

Proof. Consider the positive integer e satisfying $p^{e-1} || (n+1)$. Then $1 \le e \le E$, and for some integer $n' \not\equiv 0 \pmod{p}$ we have $n + 1 = p^{e-1}n'$. Let $j \in \{0, 1, \ldots, p-2\}$ be such that $n' \equiv j + 1 \pmod{p}$. Then $n' = j + 1 + pn''$ for some integer n''. Thus, $n + 1 = p^{e-1}(j+1) + p^e n''$ so that n satisfies the congruence $x \equiv p^{e-1}(j+1) - 1 \pmod{p^e}$, as required. $\square$

Lemma 8. *Let p be a prime, and let E be a positive integer not divisible by p. Suppose that n is an integer $\equiv -1 \pmod{p^E}$. Then n satisfies at least one of the congruences*

$$x \equiv b_j \pmod{p^j E} \qquad \text{with } 1 \le j \le E,$$

where

$$b_j \equiv -1 \pmod{p^j} \quad \text{and} \quad b_j \equiv j \pmod{E}.$$

Proof. Consider $j \in \{1, 2, \ldots, E\}$ such that $n \equiv j \pmod{E}$. $\square$

Proof of Theorem 4. As we shall demonstrate, the specific covering is given by Tables 1 and 2. We begin by explaining the entries in the tables. Each modulus is of the form

$$m = q_1^{e(1)} q_2^{e(2)} \cdots q_{12}^{e(12)},$$

where q_k denotes the kth odd prime (so $q_1 = 3, q_2 = 5, \ldots, q_{12} = 41$) and the $e(k)$ denote non-negative integers. Each tuple under the heading "Congruences" in Table 1 indicates a list of congruences $x \equiv a \pmod{m}$ as follows. Fix a value of j from the range indicated in the third column of the table (each j will produce one or more congruences). We consider m of the form indicated above. Let T denote the set of positive integers k for which the kth component in the tuple is a "$*$". If $k \in T$, set $e(k) = 0$. If the kth component in the tuple is of the form $b : (t)$, then we define $b_k = b$ and set $e(k) = t$. If $k \notin T$ and the kth component in the tuple is not of the form $b : (t)$, then we define b_k as the value of that component and $e(k)$ is as indicated in Table 2, with each choice of $e(k)$ in Table 2 determining a different modulus m. For each such m, we determine a by the Chinese Remainder Theorem from the congruences

$$a \equiv b_k \pmod{q_k^{e(k)}}$$

where k ranges over those positive integers ≤ 12 that are not in T. As an example, we note that Row 1 in Table 1 corresponds to $41 \times 31 \times 3 = 3813$ congruences; further, if $e(1) = 1$, $e(2) = 3$, and $j = 1$, then the congruence determined by this row is $x \equiv 174 \pmod{375}$. Note that each of the three values of j in Row 1 gives a congruence modulo m where $m = 3^{e(1)}5^{e(2)}$ so that moduli can occur three times as indicated in (i) of Theorem 4. A quick look through Table 1 shows that the two sets of primes q_k with $e(k) > 0$ associated with congruences from any two distinct rows of Table 1 are distinct sets. One easily sees then that condition (i) of the theorem is satisfied by the complete collection of congruences given in the table. Similarly, it is easy to check that conditions (ii) and (iii) are satisfied by this collection of congruences. What remains to be established is that this collection of congruences, say $\mathcal{C}$, is in fact a covering of the integers.

We begin by considering the congruences $\mathcal{C}_1$ in Rows 2-5 of Table 1 with $e(1)$, $e(2)$, and $e(4)$ fixed but with $e(5)$ varying over its values in Table 2. By Lemma 7, if n is an integer satisfying

$$\begin{gathered} x \equiv 3^{e(1)-1} - 1 \pmod{3^{e(1)}}, \qquad x \equiv 5^{e(2)-1}4 - 1 \pmod{5^{e(2)}}, \\ x \equiv 11^{e(4)-1} - 1 \pmod{11^{e(4)}} \end{gathered} \tag{12}$$

and $x \not\equiv -1 \pmod{13^{23}}$, then n is *covered by* at least one of the congruences in $\mathcal{C}_1$ (i.e., n satisfies one of the congruences in $\mathcal{C}_1$). By Lemma 8, the congruences in Row 6 of Table 1 cover the integers $\equiv -1 \pmod{13^{23}}$. Thus, the congruences indicated in Table 1 cover every integer satisfying all three congruences in (12). Note that by the Chinese Remainder Theorem the congruences in (12) correspond to a single congruence modulo $3^{e(1)}5^{e(2)}11^{e(4)}$.

Observe that the last congruence in (12) is the same as

$$x \equiv 11^{e(4)-1}(j+1) - 1 \pmod{11^{e(4)}} \qquad \text{where } j = 0.$$

Consider now the congruences $\mathcal{C}_2$ in Rows 7-9 of Table 1 together with the single congruence corresponding to (12) with $e(1)$ and $e(2)$ fixed but with $e(4)$ varying over its values in Table 2. Appealing to Lemma 7 again, we deduce that if n is an integer satisfying

$$x \equiv 3^{e(1)-1} - 1 \pmod{3^{e}}, \qquad x \equiv 5^{e(2)-1}4 - 1 \pmod{5^{e(2)}}, \tag{13}$$

and $x \not\equiv -1 \pmod{11^{29}}$, then n is covered by at least one of the congruences in $\mathcal{C}_2$ (and, hence, one of the congruences determined by Rows 2-9 of Table 1). By Lemma 8, the congruences in Row 10 of Table 1 cover the integers $\equiv -1 \pmod{11^{29}}$. Thus, the congruences indicated in Table 1 cover every integer satisfying both congruences in (13) (which, by the Chinese Remainder Theorem, corresponds to a single congruence modulo $3^{e(1)}5^{e(2)}$).

Observe that the last congruence in (13) is the same as

$$x \equiv 5^{e(2)-1}(j+1) - 1 \pmod{5^{e(2)}} \qquad \text{where } j = 3.$$

TABLE 1: THE COVERING FOR THEOREM 4

	Congruences	j **Range**
1	$\left(3^{e(1)-1}-1, 5^{e(2)-1}(j+1)-1, *, \ldots\right)$	$0 \le j \le 2$
2	$\left(3^{e(1)-1}-1, *, *, 11^{e(4)-1}-1, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$0 \le j \le 2$
3	$\left(*, 5^{e(2)-1}4-1, *, 11^{e(4)-1}-1, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$3 \le j \le 5$
4	$\left(3^{e(1)-1}-1, 5^{e(2)-1}4-1, *, 11^{e(4)-1}-1, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$6 \le j \le 8$
5	$\left(*, *, *, 11^{e(4)-1}-1, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$9 \le j \le 11$
6	$(*, *, *, *, -1 : (j), *, *, j : (1), *, \ldots)$	$1 \le j \le 23$
7	$\left(3^{e(1)-1}-1, *, *, 11^{e(4)-1}(j+1)-1, *, \ldots\right)$	$1 \le j \le 3$
8	$\left(*, 5^{e(2)-1}4-1, *, 11^{e(4)-1}(j+1)-1, *, \ldots\right)$	$4 \le j \le 6$
9	$\left(3^{e(1)-1}-1, 5^{e(2)-1}4-1, *, 11^{e(4)-1}(j+1)-1, *, \ldots\right)$	$7 \le j \le 9$
10	$(*, *, *, -1 : (j), *, *, *, *, j : (1), *, \ldots)$	$1 \le j \le 29$
11	$(*, -1 : (j), *, *, *, *, *, *, j : (1), *, *)$	$1 \le j \le 31$
12	$\left(3^{e(1)-1}2-1, *, 7^{e(3)-1}(j+1)-1, *, \ldots\right)$	$0 \le j \le 2$
13	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}-1, 7^{e(3)-1}(j+1)-1, *, \ldots\right)$	$3 \le j \le 5$
14	$(*, *, -1 : (j), *, *, *, *, *, *, j : (1), *)$	$1 \le j \le 37$
15	$\left(*, 5^{e(2)-1}2-1, 7^{e(3)-1}(j+1)-1, *, \ldots\right)$	$3 \le j \le 5$
16	$\left(3^{e(1)-1}2-1, *, *, *, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$0 \le j \le 2$
17	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}3-1, *, *, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$3 \le j \le 5$
18	$\left(*, 5^{e(2)-1}3-1, *, *, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$6 \le j \le 8$
19	$\left(3^{e(1)-1}2-1, *, 7^{e(3)-1}4-1, *, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$9 \le j \le 11$
20	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}3-1, 7^{e(3)-1}5-1, *, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$9 \le j \le 11$
21	$\left(*, 5^{e(2)-1}3-1, 7^{e(3)-1}6-1, *, 13^{e(5)-1}(j+1)-1, *, \ldots\right)$	$9 \le j \le 11$
22	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}4-1, 7^{e(3)-1}4-1, j : (1), *, \ldots\right)$	$0 \le j \le 2$
23	$\left(3^{e(1)-1}2-1, *, 7^{e(3)-1}4-1, j : (1), *, \ldots\right)$	$3 \le j \le 5$
24	$\left(*, 5^{e(2)-1}4-1, 7^{e(3)-1}4-1, j : (1), *, \ldots\right)$	$6 \le j \le 8$
25	$\left(*, *, 7^{e(3)-1}4-1, j : (1), *, \ldots\right)$	$9 \le j \le 10$
26	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}4-1, 7^{e(3)-1}5-1, *, *, j : (1), *, \ldots\right)$	$0 \le j \le 2$
27	$\left(3^{e(1)-1}2-1, *, *, *, *, j : (1), *, *, *\right)$	$3 \le j \le 5$
28	$\left(*, 5^{e(2)-1}4-1, *, *, *, j : (1), *, *, *\right)$	$6 \le j \le 8$
29	$\left(*, *, 7^{e(3)-1}5-1, *, *, j : (1), *, *, *\right)$	$9 \le j \le 11$
30	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}4-1, *, *, *, j : (1), *, \ldots\right)$	$12 \le j \le 14$
31	$\left(3^{e(1)-1}2-1, *, 7^{e(3)-1}5-1, *, *, j : (1), *, \ldots\right)$	$15 \le j \le 16$
32	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}4-1, 7^{e(3)-1}6-1, *, *, *, j : (1), *, \ldots\right)$	$0 \le j \le 2$
33	$\left(3^{e(1)-1}2-1, *, *, *, *, *, j : (1), *, \ldots\right)$	$3 \le j \le 5$
34	$\left(*, 5^{e(2)-1}4-1, *, *, *, *, j : (1), *, \ldots\right)$	$6 \le j \le 8$
35	$\left(*, *, 7^{e(3)-1}6-1, *, *, *, j : (1), *, \ldots\right)$	$9 \le j \le 11$
36	$\left(3^{e(1)-1}2-1, 5^{e(2)-1}4-1, *, *, *, *, j : (1), *, \ldots\right)$	$12 \le j \le 14$
37	$\left(3^{e(1)-1}2-1, *, 7^{e(3)-1}6-1, *, *, *, j : (1), *, \ldots\right)$	$15 \le j \le 17$
38	$\left(*, 5^{e(2)-1}4-1, 7^{e(3)-1}6-1, *, *, *, j : (1), *, \ldots\right)$	$j = 18$
39	$(-1 : (j), *, *, *, *, *, *, *, *, *, *, j : (1))$	$1 \le j \le 41$

TABLE 2: THE EXPONENTS RANGES

$1 \leq e(1) \leq 41$	$1 \leq e(2) \leq 31$	$1 \leq e(3) \leq 37$	$1 \leq e(4) \leq 29$	$1 \leq e(5) \leq 23$

Consider now the congruences $\mathcal{C}_3$ in Row 1 of Table 1 together with the single congruence corresponding to (13) with $e(1)$ fixed but with $e(2)$ varying over its values in Table 2. By Lemma 7, if n is an integer satisfying

$$x \equiv 3^{e(1)-1} - 1 \pmod{3^e}, \tag{14}$$

and $x \not\equiv -1 \pmod{5^{31}}$, then n is covered by at least one of the congruences in $\mathcal{C}_3$. By Lemma 8, the congruences in Row 11 of Table 1 cover the integers $\equiv -1 \pmod{5^{31}}$. Thus, the congruences indicated in Table 1 cover every integer satisfying (14).

The congruence in (14) is the same as $x \equiv 3^{e(1)-1}(j+1) - 1 \pmod{3^{e(1)}}$ with $j = 0$. The idea now is to appeal to Lemmas 7 and 8 after showing that the congruences in Table 1 cover the integers satisfying $x \equiv 3^{e(1)-1}(j+1) - 1 \pmod{3^{e(1)}}$ with $j = 1$. In other words, we will show that the congruences in Table 1 cover the integers satisfying $x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}$. Then, by letting $e(1)$ vary over the values indicated in Table 2, Lemma 7 will imply that every integer $n \not\equiv -1 \pmod{3^{41}}$ is covered by a congruence from $\mathcal{C}$. Using the congruences corresponding to Row 39 of Table 1 and appealing to Lemma 8, we can then deduce that every integer is covered by some congruence from $\mathcal{C}$. Hence, the theorem will follow.

We cover (by congruences from $\mathcal{C}$) the integers satisfying simultaneously both

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}} \quad \text{and} \quad x \equiv 5^{e(2)-1} - 1 \pmod{5^{e(2)}} \tag{15}$$

in a manner identical to the approach above. We apply Lemma 7 with the congruences in Rows 12 and 13; and then we apply Lemma 8 with the congruences in Row 14. We can likewise cover integers satisfying simultaneously

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}} \quad \text{and} \quad x \equiv 5^{e(2)-1}2 - 1 \pmod{5^{e(2)}} \tag{16}$$

by applying Lemma 7 with the congruences in Rows 12 and 15 and Lemma 8 with the congruences in Row 14.

Lemma 7 with the congruences in Rows 16-19 and Lemma 8 with the congruences in Row 6 imply that the integers satisfying simultaneously the congruences

$$\begin{gathered} x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}, \quad x \equiv 5^{e(2)-1}3 - 1 \pmod{5^{e(2)}}, \\ \text{and} \quad x \equiv 7^{e(3)-1}4 - 1 \pmod{7^{e(3)}} \end{gathered} \tag{17}$$

are covered by congruences from $\mathcal{C}$. Lemma 7 with the congruences in Rows 16, 17, 18, and 20 and Lemma 8 with the congruences in Row 6 imply that the integers satisfying simultaneously the congruences

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}, \quad x \equiv 5^{e(2)-1}3 - 1 \pmod{5^{e(2)}}, \\ \text{and} \quad x \equiv 7^{e(3)-1}5 - 1 \pmod{7^{e(3)}} \tag{18}$$

are also covered. Lemma 7 with the congruences in Rows 16, 17, 18, and 21 and Lemma 8 with the congruences in Row 6 imply that the integers satisfying simultaneously the congruences

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}, \quad x \equiv 5^{e(2)-1}3 - 1 \pmod{5^{e(2)}}, \\ \text{and} \quad x \equiv 7^{e(3)-1}6 - 1 \pmod{7^{e(3)}} \tag{19}$$

are covered. We apply now Lemma 7 with the congruences in Row 12 together with those given by (17), (18), and (19); and then we appeal to Lemma 8 with the congruences in Row 14. We deduce that all integers satisfying simultaneously the congruences

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}} \quad \text{and} \quad x \equiv 5^{e(2)-1}3 - 1 \pmod{5^{e(2)}} \tag{20}$$

are covered by congruences from $\mathcal{C}$.

Since every integer is congruent to one of $0, 1, \ldots, 10$ modulo 11, the congruences given in Rows 22-25 cover all integers satisfying simultaneously the congruences

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}, \quad x \equiv 5^{e(2)-1}4 - 1 \pmod{5^{e(2)}}, \\ \text{and} \quad x \equiv 7^{e(3)-1}4 - 1 \pmod{7^{e(3)}}. \tag{21}$$

Similarly, since every integer is congruent to one of $0, 1, \ldots, 16$ modulo 17, the congruences given in Rows 26-31 cover all integers satisfying simultaneously the congruences

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}, \quad x \equiv 5^{e(2)-1}4 - 1 \pmod{5^{e(2)}}, \\ \text{and} \quad x \equiv 7^{e(3)-1}5 - 1 \pmod{7^{e(3)}}; \tag{22}$$

and since every integer is congruent to one of $0, 1, \ldots, 18$ modulo 19, the congruences given in Rows 31-38 cover all integers satisfying simultaneously the congruences

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}, \quad x \equiv 5^{e(2)-1}4 - 1 \pmod{5^{e(2)}}, \\ \text{and} \quad x \equiv 7^{e(3)-1}6 - 1 \pmod{7^{e(3)}}. \tag{23}$$

We use Lemma 7 with the congruences given in Row 12 together with (21), (22), and (23) and we use Lemma 8 with the congruences in Row 14 to deduce that all integers satisfying simultaneously the congruences

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}} \quad \text{and} \quad x \equiv 5^{e(2)-1}4 - 1 \pmod{5^{e(2)}} \qquad (24)$$

are covered.

Finally, we appeal to the congruences in (15), (16), (20), and (24). We apply Lemma 7 with these and apply Lemma 8 with the congruences in Row 11 to obtain that every integer satisfying

$$x \equiv 3^{e(1)-1}2 - 1 \pmod{3^{e(1)}}$$

is covered by a congruence from $\mathcal{C}$. As discussed earlier in this proof, the theorem now follows. $\square$

No real attempt was made to keep the number of congruences in our proof for Theorem 4 at a minimum; the author feels that regardless any such covering for Theorem 4 must in some sense be complicated. We note that the number of congruences used in our proof is 6928899.

5 The Connection with the Odd Covering Problem

In this final section, we give a proof of Theorem 2. For this purpose, we define a non-zero polynomial $f(x) \in \mathbb{Q}[x]$ as being reciprocal if $f(x) = \pm x^{\deg f} f(1/x)$. The non-reciprocal part of $f(x)$ is $f(x)$ removed of its irreducible reciprocal factors. For example, the non-reciprocal part of

$$2x^5 - 5x^4 + 9x^3 - 9x^2 + 5x - 2 = (x-1)(x^2 - x + 2)(2x^2 - x + 1)$$

is $(x^2 - x + 2)(2x^2 - x + 1) = 2x^4 - 3x^3 + 6x^2 - 3x + 2$. As this example illustrates, the non-reciprocal part of a polynomial may in fact be reciprocal (as only the *irreducible* reciprocal factors are removed).

We make use of the following result:

Lemma 9. *Let d be a positive integer, and let $f(x)$ be in $\mathbb{Z}[x]$. Suppose that n is sufficiently large (depending on f). Then the non-reciprocal part of $f(x)x^n + d$ is irreducible over $\mathbb{Q}$ or identically ± 1 unless one of the following holds:*

(i) $-f(x)/d$ is a pth power in $\mathbb{Q}[x]$ for some prime p dividing n.

(ii) $f(x)/d$ is 4 times a 4th power in $\mathbb{Q}[x]$ and n is divisible by 4.

The above lemma is key to the ideas in this section. Schinzel's argument in [7] also made use of this result. A proof of the lemma, which we do not include here, can be found in Schinzel [6]. An alternative proof has recently been given by Ford, Konyagin, and the author [2].

In addition, we make use of the following results.

Lemma 10. *Suppose that n_0 is a real number such that every integer $n \geq n_0$ satisfies at least one of the congruences*

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

where the a_j's and m_j's are arbitrary integers with each $m_j > 0$. Then this system of congruences forms a covering of the integers (i.e., every integer $n < n_0$ also satisfies at least one of the congruences).

Proof. Let $M = \operatorname{lcm}(m_1, m_2, \dots, m_r)$. Let $n \in \mathbb{Z}$. Consider a positive integer k such that $n + kM \geq n_0$. Then $n \equiv n + kM \equiv a_j \pmod{m_j}$ for some integer $j \in \{1, 2, \dots, r\}$, establishing the lemma. $\square$

Lemma 11. *Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \zeta_m$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.*

Proof. Let $\zeta = \zeta_m$. The roots of $x^p - \zeta = 0$ are $\zeta_{pm}\zeta_p^k$ where $0 \leq k \leq p-1$. Note that $\zeta_p = \zeta_m^{m/p} \in \mathbb{Q}(\zeta)$. Thus, $x^p = \zeta$ and $x \in \mathbb{Q}(\zeta)$ imply $\zeta_{pm} \in \mathbb{Q}(\zeta)$, a contradiction (for example, since ζ_{pm} is a root of an irreducible polynomial of degree $\phi(pm) = p\phi(m)$ which exceeds the degree of the extension $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$). $\square$

Lemma 12. *Let d be a positive integer. Suppose that $-f(x)/d = g(x)^p$ for some prime p and $f(x)x^n + d$ is divisible by $\Phi_m(x)$ where $p|m$. Then $n \equiv 0 \pmod{p}$.*

Proof. We set $\zeta = \zeta_m$, and assume $p \nmid n$. Then there are integers u and v such that $-nu + pv = 1$. Since also $f(\zeta)\zeta^n + d = 0$, we deduce that $-f(\zeta)/d = \zeta^{-n}$. Hence,

$$\big(g(\zeta)^u \zeta^v\big)^p = \zeta^{-nu+pv} = \zeta.$$

Thus, $x^p = \zeta$ has a solution $x \in \mathbb{Q}(\zeta)$, contradicting Lemma 11. $\square$

Proof of Theorem 2: We suppose (as we may) that $f(0) \neq 0$. Since $x^{2^t} + 1 = \Phi_{2^{t+1}}(x)$ is irreducible for every $t \in \mathbb{Z}^+$, we deduce $f(x) \not\equiv 1$. Let $\tilde{f}(x) = x^{\deg f} f(1/x)$. Then each reciprocal factor $g(x)$ of $F(x) = f(x)x^n + d$ divides

$$\begin{aligned} f(x)\widetilde{F}(x) - dx^{\deg f} F(x) &= f(x)\big(dx^{n+\deg f} + \tilde{f}(x)\big) - dx^{\deg f}\big(f(x)x^n + d\big) \\ &= f(x)\tilde{f}(x) - d^2 x^{\deg f}. \end{aligned}$$

In particular, there is a finite list of irreducible reciprocal factors that can divide $f(x)x^n + d$ as n varies. Each reciprocal non-cyclotomic irreducible factor divides at most one polynomial of the form $f(x)x^n + d$ (see the comment before Lemma 1). By Lemma 9, we deduce that there are $\Phi_{m_1}(x), \dots, \Phi_{m_r}(x)$ such that if n is sufficiently large and both (i) and (ii) of Lemma 9 do not hold, then $\Phi_{m_j}(x) | \big(f(x)x^n + 1\big)$ for some j. Note that (ii) does not hold since otherwise $f(x)x^n + d$ could not be divisible by a cyclotomic polynomial (if $\Phi_m(x)$ were a factor, then $f(\zeta_m)\zeta_m^n = -d$, contradicting that the left side has even norm and the right side has odd norm) so that $f(x)x^n + d$ is irreducible by Lemma 9 whenever n is a sufficiently large prime. We may suppose that for each $j \in \{1, 2, \dots, r\}$ there is an a_j such that $\Phi_{m_j}(x) | \big(f(x)x^{a_j} + 1\big)$. Let $\mathcal{P}$ denote the set of primes p for which $f(x)$ is minus a pth power. We remove from consideration any m_j divisible by a $p \in \mathcal{P}$ (but abusing notation we keep the range of subscripts). Then Lemmas 1, 10 and 12 imply that the congruences

$$x \equiv 0 \pmod{p} \ \text{ for } p \in \mathcal{P} \quad \text{and} \quad x \equiv a_j \pmod{m_j} \ \text{ for } j \in \{1, 2, \dots, r\}$$

cover the integers.

Claim: Suppose $m_j = p^t m_0$ and $m_i = p^s m_0$, where p is a prime not dividing d, m_0 is an integer > 1 such that $p \nmid m_0$, and t and s are integers with $t > s \geq 0$. Then $a_j \equiv a_i \pmod{m_0}$.

For the moment, suppose the claim holds. Take $p = 2$ in the claim. Since d is odd, clearly p does not divide d. We replace $x \equiv a_j \pmod{m_j}$ and $x \equiv a_i \pmod{m_i}$ with $x \equiv a_j \pmod{m_0}$. If for some j there is no i as above, we still replace $x \equiv a_j \pmod{m_j}$ with $x \equiv a_j \pmod{m_0}$. Then we are left with a covering with moduli that are distinct odd numbers together with possibly powers of 2. Observe that $\sum_{j=1}^{\infty} 1/2^j = 1$ implies that there is an $a \in \mathbb{Z}$ and a $k \in \mathbb{Z}^+$ such that no integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Denote by $x \equiv a'_j \pmod{m'_j}$ the congruences with m'_j odd. Let u and v be integers such that

$$2^k u + v\Big(\prod m'_j\Big) = 1.$$

For any $n \in \mathbb{Z}$, consider the number $m = a + 2^k u(n - a)$. Then $m \equiv n \pmod{m'_j}$ for every m'_j and $m \equiv a \pmod{2^k}$. It follows that $n \equiv m \equiv a'_j \pmod{m'_j}$ for some m'_j. Therefore, every $n \in \mathbb{Z}$ satisfies one of the congruences $x \equiv a'_j \pmod{m'_j}$. So these congruences form an odd covering of the integers, and we are left with establishing the claim.

Let $k \in \mathbb{Z}^+ \cup \{0\}$ such that

$$a_i + (k-1)m_i < a_j \leq a_i + k m_i.$$

Let $\ell = a_i + km_i - a_j$. Then $\ell \in [0, m_i)$. Since $\Phi_{m_i}(x)$ divides $f(x)x^{a_i+km_i} + d$ by Lemma 1 and $\Phi_{m_j}(x)$ divides $f(x)x^{a_j} + d$, we deduce that there are $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that

$$f(x)x^{a_i+km_i} + d = -\Phi_{m_i}(x)u(x)$$

and

$$f(x)x^{a_i+km_i} = f(x)x^{\ell+a_j} = -dx^{\ell} + \Phi_{m_j}(x)v(x).$$

Hence,

$$\Phi_{m_i}(x)u(x) + \Phi_{m_j}(x)v(x) = d\big(x^{\ell} - 1\big).$$

Letting $x = \zeta_{m_i}$ above and applying Lemma 3, we obtain $pw = d\big(\zeta_{m_i}^{\ell} - 1\big)$ for some $w \in \mathbb{Z}[\zeta_{m_i}]$. Applying Lemma 5 and using that $p \nmid d$, we deduce that m_0 divides ℓ. The definition of ℓ and the fact that m_0 divides both ℓ and m_i imply the claim. □

Concluding Remarks: In the closing arguments above, we used Lemmas 3 and 5 to justify that m_0 divides ℓ. Schinzel has pointed out that instead one can apply the work of Apostol [1] on the resultants of two cyclotomic polynomials. By (2), $\Phi_{m_0}(x)$ divides both $\Phi_{m_i}(x)$ and $\Phi_{m_j}(x)$ modulo p. Since $p \nmid d$, the last equation displayed above implies $\Phi_{m_0}(x)$ divides $x^{\ell} - 1$ modulo p. Hence, $\Phi_{m_0}(x)$ and some divisor $\Phi_{\ell'}(x)$ of $x^{\ell} - 1$ in $\mathbb{Z}[x]$ have a factor in common modulo p. In other words, there is a positive integer ℓ' dividing ℓ such that the resultant of $\Phi_{m_0}(x)$ and $\Phi_{\ell'}(x)$ is divisible by p. Recall from above that $p \nmid m_0$. Apostol's work implies that ℓ'/m_0 is a power of p. It follows that m_0 divides ℓ' and, hence, ℓ.

The author expresses his gratitude to Andrzej Schinzel for taking an interest in this work and for supplying the author with alternative approaches to some of the arguments.

References

[1] T. M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457–462.

[2] 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.

[3] R. K. Guy, Unsolved Problems in Number Theory (Second Ed.), Springer-Verlag, New York, 1994

[4] W. J. LeVeque, Topics in Number Theory, Vol. II, Addison-Wesley, Reading, 1956

[5] R. Morikawa, *Some examples of covering sets*, Bull. Fac. Liberal Arts Nagasaki Univ. **21** (1981), 1–4.

[6] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. **11** (1965), 1–34; Errata, ibid., vol. 12.

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