On Special Cases of Dirichlet's Theorem on Arithmetic Progressions

Johan Jönsson

January 2015

Abstract

Dirichlet's theorem regarding existence of infinitely many primes in progressions on the form a, $a+n$, $a+2n\ldots$ when $(a,n)=1$ is well known and proved by using Dirichlet series. This thesis will mainly treat the special case when $a=1$ without the use of such series. In the first section of the thesis we show existence of an upper bound as a function of n for when the first prime occurs in progressions of this form. The second section contains proofs of the existence of infinitely many primes in progressions when $a=1$ and n being $4, 6, 8$ and finally n being an arbitrary integer, using only elementary methods. In the last section we look into some results in algebraic number theory.

Contents

0 Introduction

After the dark ages mathematical development made its way back into Europe. It was during this time the well known mathematician Pierre de Fermat studied primes of the form $p = x^2 + ny^2$ and their characterization. In his investigations he used two steps, the descent step and the reciprocity step. The problem of generalizing the latter led others, such as Euler and Legendre, to work on what is today known as quadratic reciprocity. While Legendre was trying to prove a version of today's law of quadratic reciprocity, he encountered the problem of guaranteeing the existence of primes in certain residue classes. The lemma he needed was the following.

Lemma 0.1. *Let a and n be positive integers; if they are co-prime, then there exist infinitely many primes $\equiv a \mod n$.*

This lemma was proved by Dirichlet and became known as Dirichlet's theorem on arithmetic progressions, which we will call Dirichlet's theorem for short. If Legendre's lemma and the invalid proof that he presented was the reason for Dirichlet to study such progressions is not certain. It is worth noting however that Ernest Kummer, one of Dirichlet contemporaries, called Dirichlet's theorem "an offspring of the study of quadratic reciprocity". In the first section of this thesis we prove the existence of an upper bound for when the first prime of Dirichlet's theorem occurs in progressions when $a = 1$; to do this we use something called cyclotomic polynomials.

In the second section we present proofs of Dirichlet's theorem for a few special cases. The cases $a = 1$ and $n = 4, 6, 8$ are proved using quadratic residues. The case when $a = 1$ and n is arbitrary, is proved in two ways. For the first proof we need a few lemmas. We start by proving a Lemma 2.2 using fixed-point sets in connection to function iterations, which can be regarded from a graph-theoretic perspective. The lemma is then used to establish a divisibility relation which is exploited in the proof of this special case together with cyclotomic polynomials. In the last subsection we prove the previous case once more but in a much shorter version, this time following a remark made in [9]. All proofs in this section ultimately follow Euclid's classic proof-by-contradiction method which he used to prove that there are infinitely many primes.

In the third and last section we look into the remark made by the authors of [9]. This remark is regarding the behavior of certain primes when they are lifted into field extensions were the minimal polynomial is cyclotomic. These fields are called cyclotomic fields and have been studied extensively in connection to higher reciprocity laws. The primes we investigate are those that split completely. We start by treating the well-known Gaussian and Eisenstein integers which are rings of integers of quadratic as well as cyclotomic extensions over $\mathbb{Q}$. In this case the splitting is proved using quadratic reciprocity. In the last subsection we study what happens with the prime 11 when its lifted into the cyclotomic field generated by a fifth root of unity, which is of degree four. In order to follow the splitting process in such extensions in general, one needs to be familiar with Galois theory. However the extension field we get in this case is rather simple in

comparison to other extensions of high degree; it is in fact simple by definition. In order to establish the splitting in this case we use Maple, which simplifies the needed computations.

To follow the proofs and ideas in this text one only needs the knowledge from introductory courses in number theory and abstract algebra, even though we touch upon more complicated theory in the last section. The significant results of the thesis and the main idea of their proofs are found in the references, in particular [10], [9], [4] and [7]. I present these results in an order and fashion which I find suitable. Still, a few proofs are entirely my own, which will be clear from the text. The statements on the history of Dirichlet's theorem are based on the first chapters of [3] and [6]. At last I want to thank my supervisor Prof. Arne Meurman for the guidance and exciting assignments he has given me.

1 The smallest prime $\equiv 1 \mod n$

In this first section we prove the following,

Theorem 1. *For all $n \geq 1$ the least prime $p \equiv 1 \pmod{n}$ satisfies*

$$p \leq 2^{\phi(n)+1} - 1.$$

In order to prove Theorem 1 we need a few definitions and lemmas.

1.1 Definitions

Definition 1.1. *An integral domain is a commutative unital ring without zero divisors.*

Definition 1.2. *The greatest common divisor of $a, b \in \mathbb{Z}$ will be denoted (a, b).*

Definition 1.3. *A function $f(x)$ from $\mathbb{Z}$ into $\mathbb{C}$ is called an arithmetical function.*

Definition 1.4. *An arithmetical function $f(x)$ is called multiplicative if*

$$f(nm) = f(n)f(m)$$

when $(n, m) = 1$.

Definition 1.5. *For $n \geq 1$ we define Euler's ϕ-function. Let $\phi(n)$ denote the number of positive integers $a \leq n$ such that $(a, n) = 1$.*

Euler's ϕ-function is multiplicative. See [2] for proof.

Definition 1.6. *For positive integers n, we define Möbius' μ-function as*

$$\mu(n) = \begin{cases} 1 & if \quad n = 1 \\ 0 & if \quad p^2 \,|n \text{ for some prime } p \\ (-1)^r & if \quad n = p_1 p_2 \cdots p_r. \end{cases}$$

Möbius' μ-function is multiplicative. See [2] for proof.

Definition 1.7. *The nth cyclotomic polynomial is defined as*

$$\Phi_n(x) = \prod_{\substack{0 \leq k < n \\ (k,n)=1}} \left(x - e^{2i\pi \frac{k}{n}} \right).$$

1.2 Lemmas

In addition to these definitions we need a few lemmas in order to simplify the proof of Theorem 1.

Lemma 1.1. *If f, g are two arithmetical functions such that*

$$f(n) = \sum_{d|n} g(d),$$

then

$$g(n) = \sum_{d|n} f(d)\mu\Big(\frac{n}{d}\Big).$$

This is known as Möbius' inversion formula. See [2] for proof.

Lemma 1.1 has a multiplicative version,

Lemma 1.2. *If f, g are two arithmetical functions such that*

$$f(n) = \prod_{d|n} g(d),$$

then

$$g(n) = \prod_{d|n} f\Big(\frac{n}{d}\Big)^{\mu(d)} = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}.$$

Proof. By hypothesis $f(n) = \prod_{d|n} g(d)$ and therefore

$$\prod_{d|n} f\Big(\frac{n}{d}\Big)^{\mu(d)} = \prod_{d|n} \Big(\prod_{c|\frac{n}{d}} g(c)\Big)^{\mu(d)}.$$

Since $d \mid n$ and $c \mid \frac{n}{d}$ if and only if $c \mid n$ and $d \mid \frac{n}{c}$ we get,

$$\prod_{d|n} \Big(\prod_{c|\frac{n}{d}} g(c)\Big)^{\mu(d)} = \prod_{c|n} \Big(\prod_{d|\frac{n}{c}} g(c)^{\mu(d)}\Big) = \prod_{c|n} g(c)^{\sum_{d|\frac{n}{c}} \mu(d)}.$$

It is proved in [2] that the exponent vanishes for all values of c but $c = n$ and in this case it equals 1, hence

$$\prod_{d|n} f\Big(\frac{n}{d}\Big)^{\mu(d)} = g(n).$$

By letting $d = \frac{n}{d'}$ we get the seemingly different result. This follows since for each $d \mid n$ there exists a d' and vice versa. □

Lemma 1.2 implies an equality regarding the cyclotomic polynomials namely,

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

since

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Next we establish some further properties of cyclotomic polynomials. We start with a lemma regarding polynomials with coefficients in some integral domain. If D is an integral domain, then it is well-known that $D[x]$ is an integral domain. See [5] for proof.

Lemma 1.3. *Let D be an integral domain. If $f, g \in D[x]$ and g is monic, then there exist unique $q, r \in D[x]$ such that $f = gq + r$ and $\deg(r) < \deg(q)$ or $r = 0$.*

Proof. If $f = 0$ or $\deg(f) < \deg(g)$ let $q = 0$. Suppose the theorem is true for g such that $\deg(g) = m$ and for all f such that $\deg(f) < k$ for some $k \geq m$. Let $f(x) = a_k x^k + \cdots + a_0$ and $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$. Set $h(x) = f(x) - a_k x^{k-m} g(x)$ which belongs to $D[x]$ since $D[x]$ is a ring. We then get

$$\begin{aligned} h(x) &= a_k x^k + \cdots + a_0 - a_k x^{k-m}(x^m + b_{m-1}x^{m-1} + \cdots + b_0) \\ &= a_k x^k + \cdots + a_0 - a_k x^{k-m+m} - a_k b_{m-1} x^{k-m+m-1} - \cdots - a_k b_0 x^{k-m} \\ &= (a_{k-1} - a_k b_{m-1}) x^{k-1} - \cdots + a_0. \end{aligned}$$

By assumption $h = q_h g + r_h$ for some unique q_h and r_h, $r_h = 0$ or $\deg(r_h) < m$ both in $D[x]$. This implies that

$$q_h g + r_h = f - a_k x^{k-m} g.$$

Or equivalently

$$f = q_h g + a_k x^{k-m} g + r_h, \tag{1}$$

where $\deg(r_h) < m$ or $r_h = 0$. Since g was fixed we can factor the right-hand side of (1) to $f = (q_h + a_k x^{k-m})g + r_h$ where $q_h, a_k x^{k-m}$ and r_h all belong to $D[x]$. For uniqueness:
Suppose $f = q_1 g + r_1 = q_2 g + r_2$. Then $0 = (q_1 - q_2)g + r_1 - r_2$. Since $g \neq 0$ it follows that $q_1 = q_2$ and $r_1 - r_2$ has to be zero which implies that r_1 and r_2 are equal as well. □

Lemma 1.4. *If $n \in \mathbb{Z}$ and $n \geq 1$, then $\Phi_n(x) \in \mathbb{Z}[x]$.*

Proof. By Lemma 1.2,

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

This implies that,

$$(x^{d_1}-1)\cdots(x^{d_s}-1)\Phi_n(x) = (x^{d_{s+1}}-1)\cdots(x^{d_{s+t}}-1).$$

The right-hand side belongs to $\mathbb{Z}[x]$ and since $(x^{d_1}-1)\cdots(x^{d_s}-1)$ is monic we get from Lemma 1.3 that,

$$\Phi_n(x) \in \mathbb{Z}[x].$$

□

Lemma 1.5. *If $\Phi_n(x)$ is the nth cyclotomic polynomial then $\Phi_n(x)\Big|\frac{x^n-1}{x^{\frac{n}{q}}-1}$ in $\mathbb{Z}[x]$, for all $q \mid n$.*

Proof. By definition we have $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Factoring out $\Phi_n(x)$ we end up with

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d\neq n}} \Phi_d(x). \tag{2}$$

We also have

$$x^{\frac{n}{q}} - 1 = \prod_{s|\frac{n}{q}} \Phi_s(x). \tag{3}$$

Combining (2) and (3) we get

$$\frac{x^n-1}{x^{\frac{n}{q}}-1} = \Phi_n(x) \prod_{\substack{d|n \\ d\neq n \\ dq\nmid n}} \Phi_d(x)$$

which establishes the divisibility relation. □

Next we prove a somewhat different version of the previous lemma which is needed at the end of the proof of our next lemma.

Lemma 1.6. *If $\Phi_n(x)$ is the nth cyclotomic polynomial and $n > 2, n \equiv 2 \mod 4$, then $\Phi_n(x)\Big|\frac{x^{\frac{n}{2}}+1}{x+1}$.*

Proof. We start off just as in the proof of the previous lemma,

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d\neq n}} \Phi_d(x).$$

Using the identity for the difference of two squares we get,

$$(x^{\frac{n}{2}}-1)(x^{\frac{n}{2}}+1) = \Phi_n(x) \prod_{\substack{d|n \\ d\neq n}} \Phi_d(x).$$

Canceling

$$x^{\frac{n}{2}} - 1 = \prod_{d|\frac{n}{2}} \Phi_d(x),$$

we get

$$x^{\frac{n}{2}} + 1 = \Phi_n(x) \prod_{\substack{d|n \\ d\neq n \\ 2d\nmid n}} \Phi_d(x).$$

Next we use that different cyclotomic polynomials do not share roots and $n > 2$ was assumed. We can therefore divide by $\Phi_2(x) = x + 1$ without changing the relation of divisibility. Hence,

$$\Phi_n(x) \Big| \frac{x^{\frac{n}{2}} + 1}{x + 1}$$

□

The proof of the upcoming lemma is described in [9].

Lemma 1.7. *For all $b \in \mathbb{Z}$, $b \geq 2$, the prime divisors of $\Phi_n(b)$ are either prime divisors of n or are $\equiv 1 \mod n$. Moreover, if $n > 2$ then every prime divisor of n only divides $\Phi_n(b)$ to the power of one.*

Proof. We begin by proving the first statement. Suppose $p \mid \Phi_n(b)$, which by Lemma 1.5 gives us $p \mid b^n - 1$ or equivalently $b^n \equiv 1 \mod p$. This congruence relation implies that $(b, p) = 1$, hence we can define the order of $b \mod p$ as t. From elementary number theory we have that $t \mid n$. As it turns out, our two cases in the first statement of the lemma correspond to $t = n$ and $t \neq n$. Let us consider these two cases:
Case(i):
Suppose the order of $b \mod p$ is n. As mentioned above, the order of an integer mod p divides $\phi(p)$. In addition $\phi(p) = p - 1$, since p is prime. Hence $n \mid p - 1$ or equivalently $p \equiv 1 \mod n$.
Case(ii):
Suppose the order of $b \mod p$ is not n. Then there exists at least one prime q such that $q \mid n$ and $p \mid b^{\frac{n}{q}} - 1$. According to Lemma 1.5, $\Phi_n(b)$ divides

$$\frac{b^n - 1}{b^{\frac{n}{q}} - 1} = 1 + b^{\frac{n}{q}} \cdots + b^{\frac{n(q-1)}{q}}.$$

Since it was assumed that $p \mid b^{\frac{n}{q}} - 1$ we get

$$1 + b^{\frac{n}{q}} + \cdots + b^{\frac{n(q-1)}{q}} \equiv q \mod p.$$

By transitivity of division we have,

$$p \mid 1 + b^{\frac{n}{q}} + \cdots + b^{\frac{n(q-1)}{q}}.$$

Therefore $q \equiv 0 \mod p$. Since p and q are both primes we conclude that $p = q$. Since q was a proper divisor of n, so is p. This proves the first statement in our

lemma. We proceed with the proof of the second statement. For Case(i), note that $n \mid p-1$ and therefore $p \nmid n$. In Case(ii) we use the notation q as above. It was established above that $b^{\frac{n}{q}} \equiv 1 \mod q$, since $p = q$. This is equivalent to

$$b^{\frac{n}{q}} = 1 + c \cdot q \text{ for some } c \in \mathbb{Z}. \tag{4}$$

Raising both sides of (4) to the j'th power and using the binomial theorem we get:

$$(b^{\frac{n}{q}})^j = (1+c\cdot q)^j = \sum_{k=0}^{j} \binom{j}{k} 1^{j-k} \cdot (cq)^k = 1 + j\cdot c\cdot q + a_2(c\cdot q)^2 + \cdots + a_j(c\cdot q)^j$$

where $a_2, \ldots, a_j \in \mathbb{Z}$. Regarding this as a $\mod q^2$ congruence we get

$$b^{\frac{n\cdot j}{q}} \equiv 1 + c \cdot j \cdot q \mod q^2 \text{ for all } j \in \mathbb{Z},$$

since every term beyond the second in the binomial expansion is a multiple of q^2. Using this congruence relation,we get

$$\begin{aligned} \frac{b^n - 1}{b^{\frac{n}{q}} - 1} &= 1 + b^{\frac{n}{q}} \ldots + b^{\frac{n(q-1)}{q}}, \\ &\equiv 1 + 1 + c\cdot q + 1 + 2\cdot c\cdot q + \ \ldots + 1 + c(q-1)q \mod q^2, \\ &\equiv q + c\cdot q\Big(\frac{q(q-1)}{2}\Big) \mod q^2. \end{aligned}$$

If q is odd then q is not divisible by 2 and the last congruence reduces to q mod q^2. Hence

$$\frac{b^n - 1}{b^{\frac{n}{q}} - 1} \equiv q \mod q^2,$$

which implies

$$\frac{b^n - 1}{b^{\frac{n}{q}} - 1} = q + q^2 \cdot k = q(1 + qk).$$

Therefore $q^2 \nmid \frac{b^n-1}{b^{\frac{n}{q}}-1}$. As this is an integer multiple of $\Phi_n(b)$, we get that

$$q^2 \not| \Phi_n(b).$$

The remaining case is if $q = 2$. That would give us

$$\frac{b^n - 1}{b^{\frac{n}{2}} - 1} \equiv 2(1 + c) \mod 4, \qquad \text{for some } c \in \mathbb{Z}.$$

If c is even we are done. If c is odd then

$$b^{\frac{n}{2}} \equiv 3 \mod 4,$$

which follows from

$$\begin{aligned}\frac{b^n-1}{b^{\frac{n}{2}}-1} &\equiv 2(1+(2t+1)) \mod 4,\\ b^{\frac{n}{2}}+1 &\equiv 2(2+2t) \mod 4,\\ b^{\frac{n}{2}}+1 &\equiv 0 \mod 4,\\ b^{\frac{n}{2}} &\equiv 3 \mod 4.\end{aligned}$$

This implies that b and $\frac{n}{2}$ are odd. But if $\frac{n}{2}$ is odd then,

$$\Phi_n(b)\Big|\sum_{i=0}^{\frac{n}{2}-1}(-b)^i.$$

To prove this divisibility relation we consider the following,

$$\Phi_n(b)\Big|\frac{b^{\frac{n}{2}}+1}{b+1}=\sum_{i=0}^{\frac{n}{2}-1}(-b)^i.$$

Lemma 1.6 gives us the divisibility and equality follows from use of geometric series. But $\sum_{i=0}^{\frac{n}{2}-1}(-b)^i$ is odd since $(b,4)=1$ and $\frac{n}{2}$ is odd, which implies that that $\sum_{i=0}^{\frac{n}{2}-1}(-b)^i$ is a sum of an odd number of odd integers which is odd. But $\Phi_n(b)$ is even, since $p \mid \Phi_n(b)$ was assumed, and $p=q=2$ so $2 \mid \Phi_n(b)$. Since the divisibility relation is impossible c cannot be odd and we have therefore proved the case for $q=2$ as well. This completes the proof of the second statement. □

Lemma 1.8. *For all $n \in \mathbb{Z}$ such that $n>2$ and $n \neq 6$ the following holds, $\sqrt{n} \leq \phi(n)$.*

Proof. Suppose $n \in \mathbb{Z}_+$ and let $n = 2^{k_1}3^{k_2}\cdots p_t^{k_t}$, $p_i \in \mathbb{P}, k_i \in \mathbb{Z}$. Since ϕ is multiplicative we get,

$$\begin{aligned}\phi(n) &= \phi(2^{k_1}3^{k_2}\cdots p_t^{k_t})\\ &= \phi(2^{k_1})\phi(3^{k_2})\cdots\phi(p_t^{k_t})\\ &= (2^{k_1}-2^{k_1-1})(3^{k_2}-3^{k_2-1})\cdots(p_t^{k_t}-p_t^{k_t-1})\\ &= 2^{\frac{k_1}{2}}(2^{\frac{k_1}{2}}-2^{\frac{k_1}{2}-1})3^{\frac{k_2}{2}}(3^{\frac{k_2}{2}}-3^{\frac{k_2}{2}-1})\cdots p^{\frac{k_t}{2}}(p_t^{\frac{k_t}{2}}-p_t^{\frac{k_t}{2}-1}).\end{aligned}$$

Hence proving the following is sufficient:

$$2^{\frac{k_1}{2}}(2^{\frac{k_1}{2}}-2^{\frac{k_1}{2}-1})3^{\frac{k_2}{2}}(3^{\frac{k_2}{2}}-3^{\frac{k_2}{2}-1})\cdots p^{\frac{k_t}{2}}(p_t^{\frac{k_t}{2}}-p_t^{\frac{k_t}{2}-1}) \geq 2^{\frac{k_1}{2}}3^{\frac{k_2}{2}}\cdots p_t^{\frac{k_t}{2}}=\sqrt{n}.$$

Canceling $p_i^{\frac{k_i}{2}}$ on both sides we see that this follows from

$$p_i^{\frac{k_i}{2}}-p_i^{\frac{k_i}{2}-1} \geq 1 \quad \text{for all } p_i^{k_i} \text{ including } 2^{k_1} \text{ and } 3^{k_2}.$$

This holds for all $p_i^{k_i} > 2$, since $f(x,k) = x^{\frac{k}{2}} - x^{\frac{k}{2}-1}$ is an increasing function in both arguments, combined with $1 < 3^{\frac{1}{2}} \cdot (1 - \frac{1}{3}) = f(3,1)$. The monotone increase is proved by taking partial derivatives of f with respect to x and k.

$$\frac{\partial}{\partial x} f(x,k) = \frac{k}{2} x^{\frac{k}{2}-1} - \Big(\frac{k}{2} - 1\Big) x^{\frac{k}{2}-2} = x^{\frac{k}{2}} \Big(\frac{k}{2} x^{-1} - \Big(\frac{k}{2} - 1\Big) x^{-2}\Big) = \frac{x^{\frac{k}{2}}}{2x} \Big(k - \frac{k}{x} + \frac{2}{x}\Big).$$

We have

$$\frac{x^{\frac{k}{2}}}{2x} > 0 \text{ since } x > 0$$

and

$$\Big(k - \frac{k}{x} + \frac{2}{x}\Big) > 0 \text{ since } \Big(k - \frac{k}{x} + \frac{2}{x}\Big) > 0 \iff k - \frac{k+2}{x} > 0 \iff$$
$$\iff xk > k - 2 \iff xk - k + 2 > 0 \iff k(x-1) + 2 > 0.$$

This holds for all $x \in \mathbb{R}, x \geq 1$ and $k \in \mathbb{Z}, k > 0$ and therefore $f(x,k)$ increases monotonically in x for fixed k, in particular for integral x. To verify monotone increase in k for fixed x we consider the following.

$$\frac{\partial}{\partial k} f(x,k) = \ln(x)(x^{\frac{k_i}{2}} - x^{\frac{k_i}{2}-1})$$

We have $\ln(x) > 0$ for all $x \in \mathbb{R}$, $x > 1$. Furthermore $x^{\frac{k_i}{2}} - x^{\frac{k_i}{2}-1} > 0$ for all $x \in \mathbb{R}$, $x > 1$ and $k \in \mathbb{Z}$. Hence f increases monotonically in the second argument as well. It remains to prove the inequality when 2^1 is part of the factorization of n. If $n = 2^1 3^k$, then $k_2 \geq 2$ since $n \neq 6$ is assumed. We have monotone increase in the second argument and therefore prove this case by calculating $(2^1 - 2^{1-1})(3^2 - 3^{2-1}) > 1.4 > 1$. The smallest possible prime factor other then 3 to some power is 5^1. Therefore we need to prove the following:

$$1 \leq \frac{\sqrt{2}}{2}(p_i^{\frac{k_i}{2}}(1 - \frac{1}{p_i})) \text{ for all } p_i \geq 5, k_i \geq 1.$$

We proceed as above and establish:

$$1 < 0.7 \cdot 1.79 = 1,24671 < \frac{\sqrt{2}}{2}(5^{\frac{1}{2}}(1 - \frac{1}{5})).$$

We now use the monotone increase of f once more, together with the fact that any additional prime factors will keep the product above 1. This establishes the lemma for the case when n has a prime factor 2^1. The lemma is therefore proved for all n in our statement. □

The proof of the next lemma which is taken directly from [10], uses the following inequality.

$$-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \leq x + x^2 + x^3 + \cdots = \frac{x}{1-x}, \qquad (5)$$

which holds for $0 < x < 1$.

Lemma 1.9. *For any integers $n \geq 2$ and $b \geq 2$ we have*

$$\frac{1}{2} \cdot b^{\phi(n)} \leq \Phi_n(b) \leq 2 \cdot b^{\phi(n)}.$$

Proof. From Lemma 1.2, we have

$$\Phi_n(b) = \prod_{d|n} (b^d - 1)^{\mu(\frac{n}{d})} = b^{\sum_{d|n} d \cdot \mu(\frac{n}{d})} \prod_{d|n} \Big(1 - \frac{1}{b^d}\Big)^{\mu(\frac{n}{d})}.$$

Let

$$S = \frac{\Phi_n(b)}{b^{\phi(n)}} = \prod_{d|n} \Big(1 - \frac{1}{b^d}\Big)^{\mu(\frac{n}{d})}.$$

Then

$$\log S = \sum_{d|n} \mu(\frac{n}{d}) \log(1 - b^{-d}). \tag{6}$$

It suffices to show $\frac{1}{2} \leq S \leq 2$, which is equivalent to,

$$-\log 2 \leq \log S \leq \log 2.$$

For the upper bound we have two cases to consider, $\mu(n) \geq 0$ and $\mu(n) < 0$.
Case (i) :
Suppose $\mu(n) \geq 0$. Then we get by (6)

$$\begin{aligned}
\log S &= \mu(n) \log(1 - b^{-1}) + \sum_{\substack{d|n \\ d \geq 2}} \mu(\frac{n}{d}) \log(1 - b^{-d}) \\
&\leq -\mu(n) \log(\frac{b}{b-1}) + \sum_{\substack{d|n \\ d \geq 2}} -\log(1 - b^{-d}) \\
&\leq \sum_{d \geq 2} \Big[b^{-d} + \frac{b^{-2d}}{2} + \frac{b^{-3d}}{3} + \cdots \Big] \\
&\leq \sum_{d \geq 2} \Big[b^{-d} + \frac{b^{-2d}}{2} (1 + b^{-d} + b^{-2d} + \cdots) \Big] \\
&= \sum_{d \geq 2} \Big[b^{-d} + \frac{b^{-2d}}{2} (1 - b^{-d})^{-1} \Big] \\
&= \sum_{d \geq 2} \Big(\frac{1}{b^d} + \frac{1}{2b^{2d}} \cdot \frac{b^d}{b^d - 1} \Big) \\
&\leq \sum_{d \geq 2} \Big(\frac{1}{b^d} + \frac{1}{6b^d} \Big) = \frac{7}{6} \cdot \frac{1}{b(b-1)} \\
&\leq \frac{7}{12} < \log 2.
\end{aligned}$$

The second case, namely $\mu(n) < 0$, is done in the same spirit. In this case n has an odd number of prime divisors. Furthermore $\mu(\frac{n}{p}) = 1$ for all primes dividing n. Let $D = \{d; d \mid n \text{ and } d \text{ has } \geq 2 \text{ prime factors } \}$ and let q be the least prime dividing n. Then any $d \in D$ satisfies $d \geq q^2$. Hence we get,
Case(ii):

$$\begin{aligned}
\log S &= \mu(n)\log(1-b^{-1}) + \sum_{p|n}\mu(\frac{n}{p})\log(1-b^{-p}) + \sum_{d\in D}\mu(\frac{n}{d})\log(1-b^{-d}) \\
&= -\log\Big(\frac{b-1}{b}\Big) + \sum_{p|n}\log(1-b^{-p}) + \sum_{d\in D}\mu(\frac{n}{d})\log(1-b^{-d}) \\
&\leq -\log\Big(\frac{b-1}{b}\Big) + \log(1-b^{-q}) + \sum_{d\geq q^2} -\log(1-b^{-d}) \\
&\leq \log\Big(\frac{b}{b-1}\Big) + \log(1-b^{-q}) + \sum_{d\geq q^2}\frac{b^{-d}}{1-b^{-d}} \qquad \text{by (5)} \\
&\leq \log\Big(\frac{b}{b-1}\Big) + \log(1-b^{-q}) + \sum_{d\geq q^2}\frac{1}{b^{d-1}} \\
&\leq \log\Big(\frac{b}{b-1}\Big) + \log(1-b^{-q}) + \frac{1}{b^{q^2-2}(b-1)} \\
&\leq \log 2 - \frac{1}{b^q} + \frac{1}{b^{q^2-2}} \\
&\leq \log 2
\end{aligned}$$

since $q^2 - 2 \geq q$. The upper bound is therefore established. The lower bound is established by reversing the inequalities and doing the same thing all over again. □

1.3 Proof of Theorem 1

We are now ready to present the proof of Theorem 1 which is found in [10], a few comments are added for clarity.

Theorem 1. *For all integers $n \geq 2$, the least prime $p \equiv 1 \mod n$ satisfies*

$$p \leq 2^{\phi(n)+1} - 1.$$

Proof. Since our proof depends on Euler's ϕ-function, we treat $n = 2$ separately at the end. The low value of $\phi(n)$ for this number causes problems in an estimate during the proof. Therefore suppose $b > 1$, $n > 2$ and $n < \Phi_n(b)$. Then we get from Lemma 1.7 that there exists a prime p such that $p \mid \Phi_n(b)$ and $p \equiv 1 \mod n$. Since $p \mid \Phi_n(b)$ it follows that $p \leq \Phi_n(b)$. Using Lemma 1.9 we get,

$$p \leq \Phi_n(b) \leq 2b^{\phi(n)}.$$

Letting $b = 2$ will not only give us our theorem, but also the smallest possible upper bound using our argument. Hence what needs to be proved is what we

assumed above, namely $n < \Phi_n(b)$ but with $b = 2$ and for all $n > 2$. We do this using calculus for the case $n \geq 40$ and then we proceed by inspection for the remaining n. Starting with the case $n \geq 40$, we get the following by combining Lemma 1.8 and Lemma 1.9,

$$2^{\sqrt{n}-1} \leq 2^{\phi(n)-1} \leq \Phi_n(2) \text{ for all } n > 2 \text{ and } n \neq 6 \ .$$

Thus proving $n < 2^{\sqrt{n}-1}$ will be the next step. Now,

$$n < 2^{\sqrt{n}-1} \iff \frac{\log n}{\log 2} < \sqrt{n} - 1.$$

We prove this inequality by considering the real valued function $f(x) = \sqrt{x} - 1 - \frac{\log x}{\log 2}$ and further its derivative $f^{'}(x) = \frac{1}{2\sqrt{x}} - \frac{1}{\log 2}\frac{1}{x}$. We investigate for which x

$$\frac{1}{2\sqrt{x}} - \frac{1}{\log 2}\frac{1}{x} > 0.$$

Now

$$\frac{1}{2\sqrt{x}} - \frac{1}{\log 2}\frac{1}{x} > 0 \iff \frac{1}{2\sqrt{x}} > \frac{1}{\log 2}\frac{1}{x} \iff \frac{x}{2\sqrt{x}} > \frac{1}{\log 2} \iff$$

$$\frac{x}{\sqrt{x}} > \frac{2}{\log 2} \iff \sqrt{x} > \frac{2}{\log 2} \iff x > \frac{4}{(\log 2)^2} \iff x > 8.2.$$

Hence f is strictly increasing for all $x \geq 9$. The first integer for which f is positive is 40. Therefore f is positive for all integers greater then 40 and we have established that

$$n < \Phi_n(2) \text{ for all } n \geq 40.$$

We treat,

$$n < \Phi_n(2) \text{ for } 2 < n < 40,$$

by direct inspection. This proves Theorem 1 for all n except 2. In this case we find a suitable prime which satisfies our theorem. One does not have to look far since the bound holds for $n = 2$ with $p = 3$. At this point we have,

$$p \leq 2^{\phi(n)+1}.$$

We justify the -1 in the theorem by the fact that 2^t is always even and every prime but 2 is odd. Letting $p = 2$ one realizes that -1 would not violate the inequality since $\phi(n) \geq 2$ for $n \geq 3$. From our brute force argument for the case $n = 2$ one infers that we can subtract 1 in that case as well. We have now proved the bound for all $n \geq 2$ and hence Theorem 1 is true. □

While working towards proving Theorem 1, using articles [9] and [10] we encountered an error. The authors of [9] are assuming $\sum_{q|n}(q-1) \leq \phi(n)$, but $n = 2p$ is a counterexample.

2 Special cases of a theorem of Dirichlet

In this section we prove the existence of infinitely many primes in progressions of certain forms. We start by proving that there exist infinitely many primes of the forms $4k+1, 6k+1$ and $8k+1$ using Fermat's little theorem, Wilson's theorem and quadratic reciprocity. We proceed by proving existence of infinitely many primes of the form $nk+1$ using some graph theoretic ideas and fixed-points of function iterations. At the end of the section we use results from the first part of this thesis to prove that there are infinitely many primes of the form $nk+1$ once more.

2.1 Definitions and lemmas

Definition 2.1. *An integer a is a quadratic residue modulo n if*

$$x^2 \equiv a \mod n,$$

for some integer x.

Definition 2.2. *For p prime and a any integer we define the Legendre symbol as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & if \quad \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \mod p \\ -1 & if \quad \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & if \quad a \equiv 0 \mod p. \end{cases}$$

2.2 There are infinitely many primes of the forms $4k+1$, $6k+1$ and $8k+1$

In this subsection we present proofs of existence of infinitely many primes of the forms $4k+1$, $6k+1$ and $8k+1$. We start with a lemma which all three cases rest upon. The proofs and the lemma can be found in [8].

Lemma 2.1. *Let p be a prime and $f(x) \in \mathbb{Z}[x]$ be non-constant. Then,*

$$f(x) \equiv 0 \mod p,$$

is solvable for infinitely many p.

Proof. The statement is equivalent to that there exist infinitely many primes p_i such that for $f(x) \in \mathbb{Z}[x]$ we have,

$$p_i \mid f(c), \tag{7}$$

for some $c \in \mathbb{Z}$. We use Euclid's classic proof-by-contradiction idea which he used to establish the cardinality of the primes. If $f(x)$ has constant term zero the lemma becomes trivial. This follows from that $p \mid f(p)$ in such a case. Therefore let $f(x) = a_n x^n + \cdots + a_0$ where $a_0 \neq 0$ and let $p_1 \dots p_r$ be all

the primes satisfying divisibility relation (7). Let $b = p_1 \cdots p_r a_0$ and define $a_0 g(y) = f(by)$. Then $g(y) = A_m y^m + \cdots + 1$ where A_i are integers. Now every coefficient A_i of $g(y)$ but the constant term is divisible by all the p_i's in (7). Hence none of the finitely many p_i's can be a prime divisor of $g(m)$ for any integer m. For each integer m, $g(m) \mid f(bm)$, hence $g(m) = \pm 1$ for all $m \in \mathbb{Z}$. But $g(m) = \pm 1$ has at most $2m$ roots. It is therefore possible to find some $m_{r+1} \in \mathbb{Z}$ such that some prime $p_{r+1} \neq p_i, 1 \leq i \leq r$, divides $g(m_{r+1})$. Our initial assumption is contradicted and the lemma is proved. □

Next we prove the three cases mentioned above.

Theorem 2.1. *There are infinitely many primes of the form* $4k + 1$

Proof. Using Fermat's little theorem and Wilson's theorem one can deduce that the quadratic congruence $x^2 + 1 \equiv 0 \mod p$ where p is an odd prime has a solution if and only if $p \equiv 1 \mod 4$. See [2] for proof. It follows that every p for which $x^2 + 1 \equiv 0 \mod p$ is solvable is of the form $4k + 1$. By Lemma 2.1 there will be infinitely many such primes. Our statement is therefore established. □

Theorem 2.2. *There are infinitely many primes of the form* $6k + 1$

Proof. Consider the congruence $x^2 + 3 \equiv 0 \mod p$. This will have solutions for those p for which -3 is a quadratic residue and these solutions will be infinitely many by Lemma 2.1. Consider the following equation of Legendre symbols,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right).$$

From [2] we have,

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & if \quad \text{if } p \equiv 1 \mod 3 \\ -1 & if \quad \text{if } p \equiv 2 \mod 3. \end{cases}$$

Clearly we have $p \equiv 1 \mod 2$ for all primes except 2. Further we get from the Chinese Remainder Theorem that every integer satisfying this system is of the form $6k + 1$, hence so are those primes for which -3 is a quadratic residue. □

Theorem 2.3. *There are infinitely many primes of the form* $8k + 1$

Proof. We begin by establishing that the odd primes p for which $x^4 + 1 \equiv 0 \mod p$ admits solutions are of the form $8k + 1$. We know that $p = 4k + 1$ since x^4 is also a square, $x^4 \equiv -1$ can be regarded as $y^2 \equiv -1$ where $y = x^2$. Further suppose a was a solution to $x^4 \equiv -1 \mod p$. Fermat little theorem gives us,

$$1 \equiv a^{p-1} \equiv (a^4)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}} \mod p.$$

The only way for this equation to hold is if $p = 8k + 1$ and since $x^4 + 1 \equiv 0 \mod p$ for infinitely many primes by Lemma 2.1 we know that there are infinitely many such primes. □

2.3 There are infinitely many primes of the form $nk+1$ for all $n \geq 2, n \in \mathbb{Z}$

We start with the following lemma, which is a generalization of what is proved in [7].

Lemma 2.2. *Let f be a function from any set S into itself such that f^n fixes only finitely many points for each $n \in \mathbb{Z}_+$. If we let $T(n)$ denote the number of points that f^n fixes, then*

$$n \Big| \sum_{d|n} \mu(\frac{n}{d}) T(d).$$

Proof. Let n be a positive integer. Let

$$X_n = \{s \in S; f^n(s) = s\},$$

so that $|X_n| < \infty$. By definition $f^n(s) = s$ will hold for $T(n)$ elements $s \in S$. Further, each $s \in X_n$ will have a least iterate of f call it f^d such that $f^d(s) = s$. This d which will be called the order of s will divide n which follows from the following considerations. Let $f^n(s) = s$ and let $f^t(s) \neq s$ for all $t < d$. Suppose we have $r \neq 0$ such that $n = qd + r$ where $r < d$ then we have $f^n(s) = f^{qd+r}(s) \iff s = f^r(s), r < d$ which is a contradiction on our assumption on d being the least integer fixing s, hence $r = 0$ and therefore $d \mid n$. Next consider

$$Z_n = \{s \in S; f^n(s) = s \text{ and } f^t(s) \neq s \, \forall t < n\}$$

If $s \in Z_n$ then $f^i(s) \in Z_n$ for all $i \in \{0, \ldots, n-1\}$. Further $f^i(s) \neq f^j(s)$ for all i, j such that $0 \leq i < j \leq n-1$ since n was the least integer such that f^n fixes s. We proceed by defining an equivalence relation on Z_n in terms of f. For $a, b \in Z_n$ let $a \sim b$ if $b = f^t(a)$ for some t. The partitions that this equivalence relation induces are of the form,

$$\{s, f(s), \ldots, f^{n-1}(s)\}$$

each containing n elements. Since equivalence classes are identical or disjoint we get that $|Z_n| = nt$ where t is the number of partitions. This implies that $n \mid |Z_n|$. Now since $\bigcup_{d|n} Z_d = X_n$ is a disjoint union we get,

$$\sum_{d|n} |Z_d| = T(n),$$

since each point has unique order. Using Lemma 1.1 i.e Möbius inversion formula on this gives us

$$|Z_n| = \sum_{d|n} \mu(\frac{n}{d}) T(d).$$

Our previous result that $n \mid |Z_n|$ now implies that $n \mid \sum_{d|n} \mu(\frac{n}{d}) T(d)$ which was to be shown. □

The next lemma is from [4].

Lemma 2.3. *Let $a, n > 1$ and $n = p_1^{k_1} \cdots p_r^{k_r}$. Further let q be a common divisor of $\frac{a^n-1}{a^{\frac{n}{p_i}}-1}$ for all $1 \leq i \leq r$. Then $n \mid \frac{(a^n-1)(q-1)}{q}$.*

Proof. For integers $x_1, \ldots, x_n$ such that $0 \leq x_i \leq a-1$, let $(x_1 \ldots x_n)_a = x_1 a^{n-1} + \cdots + x_{n-1}a + x_n$. This we call an n-digit number in base a. Let S be the set of all n digit numbers in base a such that $q \nmid x_1 a^{n-1} + \cdots + x_{n-1}a + x_n$. We define $f(x) = (x_2 x_3 \ldots x_n x_1)_a$ for any n-digit number x. This implies $f(x) = ax - x(a^n - 1)$. Since $q \mid a^n - 1$, f maps S into S. Now assume $f^{\frac{n}{p_i}}$ fixes some $x \in S$ then,

$$\begin{aligned} x &= (x_1 \ldots x_{\frac{n}{p_i}} \ldots x_1 \ldots x_{\frac{n}{p_i}})_a \\ &= (x_1 \ldots x_{\frac{n}{p_i}})_a (1 + a^{\frac{n}{p_i}} + \cdots + a^{(p_i-1)\frac{n}{p_i}}) \\ &= (x_1 \ldots x_{\frac{n}{p_i}})_a \frac{a^n - 1}{a^{\frac{n}{p_i}} - 1}. \end{aligned}$$

This implies that $q \mid x$ since $q \mid \frac{a^n-1}{a^{\frac{n}{p_i}}-1}$ and hence $x \notin S$. The same argument is used for all d such that $d \mid n$. Looking back on notation and conclusion from Lemma 2.2 we get that $T(d) = 0$ for all non-trivial divisors of d of n and hence, that $n \mid T(n)$. But $T(n) = |S|$, which implies that $n \mid |S|$. Now S was all the $(x_1 \ldots x_n)_a$ not divisible by q and therefore we get $|S|$ by the following argument. The number of non-zero n-tuples with entries in $\mathbb{Z}_a$ is $a^n - 1$ using elementary combinatorics. Call this set $\mathbb{X}$. Next we calculate the number of elements in $\mathbb{X}$ divisible by q. Since $q \mid a^n - 1$ we get $a^n - 1 = qt$ and hence,

$$\mathbb{X} = \{1, 2 \ldots, q, \ldots, 2q, \ldots, tq\}.$$

The number t of multiples of q in $\mathbb{X}$ is given by the equation $t = \frac{a^n-1}{q}$. Further $\mathbb{X} \setminus (\mathbb{X} \cap q\mathbb{Z}) = S$ and hence $|S| = a^n - 1 - \frac{a^n-1}{q}$. Now $n \mid |S|$ hence,

$$n \Big| \frac{(a^n - 1)(q-1)}{q}. \qquad \square$$

In the upcoming proof we use the following well known lemma which is known as Euclid's lemma. See [2] for proof.

Lemma 2.4. *If $a \mid bc$, with $(a, b) = 1$, then $a \mid c$.*

The next proof is from [4]. What is called $g(x)$ in that article we identify as $\Phi_n(x)$.

Theorem 2.4. *Let $n \geq 2$ be an integer. Then there exist infinitely many primes of the from $nk + 1$.*

Proof. Suppose $q_1, \ldots, q_r$ are all the primes of the form $nk+1$. Let $n = p_1^{k_1} \cdots p_s^{k_s}$ and consider the polynomials,

$$\frac{x^n-1}{x^{\frac{n}{p_1}}-1}, \ldots, \frac{x^n-1}{x^{\frac{n}{p_s}}-1}.$$

By Lemma 1.5,

$$\Phi_n(x) \Big| \frac{x^n-1}{x^{\frac{n}{p_i}}-1}, \quad 1 \leq i \leq s.$$

Now for $x = 0$, $\Phi_n(0) = \pm 1$, hence $(\Phi_n(b), b) = 1$ for all $b \in \mathbb{Z}$. Since $\Phi_n(x)$ is monic there exists $t \in \mathbb{Z}$ such that $\Phi_n(x) > 1$ for all $x > t$. Let now $a = ntq_1 \cdots q_r$. Then $a > t$ and $\Phi_n(a) > 1$. Further let q be a prime divisor of $\Phi_n(a)$, the integers a, q and n all satisfy the conditions of Lemma 2.3 and hence,

$$n \mid (a^n - 1)(q-1).$$

But $a = ntq_1 \cdots q_r$ so $n \mid a$ and hence $(a^n - 1, n) = 1$. Next we use Lemma 2.4 to conclude that $n \mid q-1$ or equivalently $q = nk+1$. Since $q \mid \Phi_n(a)$ and $(\Phi_n(a), a) = 1$ we get $(q, a) = 1$ which imply $q \neq q_i$ for all $i = 1, \ldots, r$. This contradicts that $q_1, \ldots, q_r$ are the only primes of the form $nk+1$. □

2.4 Section 1 revisited

What was just proved can, as we mentioned above, be proved in a somewhat different way. Following a comment from [9] we prove the following.

Theorem 2.5. *Let $n \geq 2$ be an integer. Then there exist infinitely many primes of the form $nk+1$.*

Proof. Just as in the argument in Theorem 2.4 we use Euclid's old idea. We proved in Section 1 that there exist a prime of the form $nk+1$ below a certain bound. The existence of that prime will serve as a starting case in our induction argument below. Therefore, suppose $p_1, \ldots, p_r$ are all the primes of the form $nk+1$. Let $\prod_{i=1}^{r} p_i$ be an integer and consider

$$a = \Phi_n\Big(\prod_{i=1}^{r} p_i\Big),$$

which is an integer since $\Phi_n(x) \in \mathbb{Z}[x]$. Next we establish the following,

$$(\prod_{i=1}^{r} p_i, a) = 1.$$

This is realized by letting q be a divisor of a. Hence $(\prod_{i=1}^{r} p_i)^n \equiv 1 \mod q$ since $\Phi_n(x) \mid x^n - 1$. Therefore $(p_i, q) = 1$ for all p_i. We know from Theorem 1 that there exists some prime $\equiv 1 \mod n$ dividing $\Phi_n(\prod_{i=1}^{r} p_i)$. This prime is, since it is a divisor just as q above, also relatively prime to all p_i and therefore we have contradicted the assumption that there only were finitely many primes of the form $nk+1$. □

3 Some results in algebraic number theory

In this section we look into a comment at the end of [9]. The comment is regarding the remarkable behavior of some primes in $\mathbb{Z}$ when they are lifted into cyclotomic fields. In order to look into this we need some definitions from algebraic number theory.

3.1 Definitions and lemmas

Definition 3.1. *Let $\omega = e^{\frac{2\pi i}{n}}$ and consider the extension $\mathbb{Q}[\omega] : \mathbb{Q}$ and its subring $\mathbb{Z}[\omega]$. If for a prime $p \in \mathbb{Z}$*

$$p\mathbb{Z}[\omega] = P_1 \cdots P_{\phi(n)}$$

and

$$P_j \cap \mathbb{Z} = p\mathbb{Z}$$

for $j = 1 \dots \phi(n)$ and P_j are prime ideals in $\mathbb{Z}[\omega]$, we say that p splits completely *in $\mathbb{Z}[\omega]$.*

The splitting of a prime when lifted into an extension of degree two can be viewed as in the following diagram.

$$\begin{array}{ccc} \mathbb{Z} & \subset & \mathbb{Z}[\alpha] \\ \cup & & \cup \\ p\mathbb{Z} & \longrightarrow & P_1, P_2 \end{array}$$

Definition 3.2. *The ring $\mathbb{Z}[\sqrt{-1}]$ is known as the Gaussian integers.*

Definition 3.3. *The ring $\mathbb{Z}[e^{\frac{2\pi i}{6}}]$ is known as the Eisenstein integers.*

Definition 3.4. *If $\mathbb{Q}[\alpha]$ is of degree two with minimal polynomial $\alpha^2 + b\alpha + c$ we define the norm $N : \mathbb{Q}[\alpha] \to \mathbb{Q}$ by*

$$N(s + t\alpha) = (s + t\alpha)(s - t(b + \alpha)) = s^2 - bst + t^2c.$$

Lemma 3.1. *Let $\mathbb{Q}[\alpha]$ be of degree two with norm N. Then $u \in \mathbb{Z}[\alpha]$ is a unit if and only if $N(u) = \pm 1$.*

Lemma 3.2. *If $t \in \mathbb{Z}[\alpha]$ and $N(t)$ is a prime in $\mathbb{Z}$, then t is irreducible.*

The two lemmas above are slight generalizations of theorems in [5], the proofs remain the same.

Lemma 3.3. *Let p be prime and let $(a, p) = 1$. Then the congruence*

$$ax \equiv y \mod p$$

admits a solution x_0, y_0, where

$$0 < |x_0| < \sqrt{p} \text{ and } 0 < |y_0| < \sqrt{p}.$$

This is known as Thue's Lemma. See [2] for proof.

3.2 Splitting of primes $\equiv 1 \mod 4$ in the ring of Gaussian integers

Theorem 3.1. *Let p be a prime $\equiv 1 \mod 4$. Then p splits completely in $\mathbb{Z}[i]$.*

Proof. Suppose $p \equiv 1 \mod 4$. Then there exist integers x and y such that $p = x^2 + y^2$ by Fermat's theorem for sums of two squares, see [2] for proof. Let $P_1 = (x+iy)$ and $P_2 = (x-iy)$ be principal ideals in $\mathbb{Z}[i]$. We start by showing $P_1P_2 = p\mathbb{Z}[i]$. Let $a \in P_1P_2$, then $a = \sum_{finite} b_k c_k$ for $b_k \in P_1$ and $c_k \in P_2$. Hence,

$$a = \sum_{finite} b_k c_k = \sum_{finite} r_k s_k (x+iy)(x-iy) \qquad b_k, c_k, r_k, s_k \in \mathbb{Z}[i]$$

Since

$$(x+iy)(x-iy) = p, \tag{8}$$

we factor this out and get $\sum_{finite} u_k p$ where $u_k \in \mathbb{Z}[i]$. Hence $a \in p\mathbb{Z}[i]$ and therefore we get,

$$P_1P_2 \subseteq p\mathbb{Z}[i].$$

The reverse inclusion follows by reversing the implications. Hence

$$P_1P_2 = p\mathbb{Z}[i].$$

Next we show $P_j \cap \mathbb{Z} = p\mathbb{Z}$ for $j = 1, 2$. We start by verifying that $P_1 \cap \mathbb{Z}$ is a proper ideal in $\mathbb{Z}$. That $P_1 \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$, follows from straightforward verification that it satisfies the definition. Let $x \in P_1 \cap \mathbb{Z}$ and $n \in \mathbb{Z}$. Using that both P_1 and $\mathbb{Z}$ are abelian groups under addition we get that they absorb any $n \in \mathbb{Z}$. Since both ideals do, so does their intersection and therefore we have that $P_1 \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$. By (8)

$$p \in P_1 \cap \mathbb{Z},$$

hence

$$p\mathbb{Z} \subseteq P_1 \cap \mathbb{Z}.$$

Which also implies that $P_1 \cap \mathbb{Z} \neq (0)$. Next we prove $P_1 \cap \mathbb{Z} \neq \mathbb{Z}$ which is equivalent to $1 \notin P_1$. If $1 \in P_1$ then there exist solutions to the following equation in $\mathbb{Z}[i]$.

$$(\alpha + i\beta)(x+iy) = 1.$$

The solution to this equation is $\frac{x-iy}{p}$, which does not belong to $\mathbb{Z}[i]$. Therefore $1 \notin P_j$ and hence $P_j \cap \mathbb{Z}$ is proper. We now have, $p\mathbb{Z} \subseteq P_j \cap \mathbb{Z} \subset \mathbb{Z}$. Since $p\mathbb{Z}$ is prime in $\mathbb{Z}$, and since all prime ideals except (0) are maximal in any commutative unital principal ideal domain by [1], such as $\mathbb{Z}$, we get from maximality of $p\mathbb{Z}$ in $\mathbb{Z}$ that,

$$p\mathbb{Z} = P_j \cap \mathbb{Z}.$$

We proceed by proving that P_1 and P_2 are prime ideals in $\mathbb{Z}[i]$. It is well known that an ideal is prime if and only if the factor ring that it induces is an integral

domain and that an ideal is maximal if and only if the factor ring it induces is a field. We show that P_j, $j = 1, 2$, are maximal and therefore prime since every field is an integral domain. A sufficient condition for maximality of an ideal A in a ring R is :

$$A + (t) = R \text{ for all } t \notin A.$$

Therefore suppose $t \notin P_1$. By Lemma 3.2 we have that if $N(a + ib)$ is a prime in $\mathbb{Z}$, then $a + ib$ is irreducible in $\mathbb{Z}[\sqrt{-1}]$. Since we know that $N(x + iy) = p$ we get that $(x + iy)$ is irreducible and all divisors of $x + iy$ are therefore improper. Improper divisors are either units or associates. If t is an associate of $x + iy$ then $t = a(x + iy)$ for some unit a, this contradicts that $t \notin P_1$. If t is a unit we have $(t) = \mathbb{Z}[i]$ and hence $(t) + P_1 = \mathbb{Z}[i]$ which would give us maximality of P_1. This implies that $x + iy$ and t lack common non-unit factor in the case where we don't have maximality immediately. Therefore their gcd is 1, up to a unit. Since $\mathbb{Z}[i]$ is a Euclidean domain we know from [5] that there exist elements $u, v \in \mathbb{Z}[i]$ such that $(t, x + iy) = ut + v(x + iy)$. Hence we have that some unit belongs to the sum of ideals $P_1 + (t)$ which is therefore all of $\mathbb{Z}[i]$. Since this was for an arbitrary $t \notin P_1$ we have that P_1 is maximal and therefore prime. The case for P_2 is analogous. □

3.3 Splitting of primes $\equiv 1 \mod 6$ in the ring of Eisenstein integers

Theorem 3.2. *Let $\omega = e^{\frac{2\pi i}{6}}$ and p be a prime $\equiv 1 \mod 6$. Then p splits completely in $\mathbb{Z}[\omega]$.*

Proof. We begin by showing that $p = x^2 - xy + y^2$ if and only if $4p = A^2 + 3B^2$ for $x, y, A, B \in \mathbb{Z}$.

$$\begin{aligned}
&p = x^2 - xy + y^2 \iff p = (x - \frac{y}{2})^2 - (\frac{y}{2})^2 + y^2 \iff \\
&4p = 4(x - \frac{y}{2})^2 - 4(\frac{y}{2})^2 + 4y^2 \iff \\
&4p = (2x - y)^2 - y^2 + 4y^2 \iff 4p = (2x - y)^2 + 3y^2 \iff \\
&4p = A^2 + 3B^2
\end{aligned}$$

where $A = 2x - y$ and $B = y$. Next we prove that $p \equiv 1 \mod 6$ if and only if $4p = A^2 + 3B^2$ and therefore if and only if $p = x^2 - xy + y^2$. Suppose,

$$4p = A^2 + 3B^2. \tag{9}$$

We have that $p \nmid B^2 = y^2$ by the following argument. Since $p = x^2 - xy + y^2$ we need to have one of x and y odd. Since x and y play identical roles in our expression we choose y to be odd. Furthermore we have $(x, y) = 1$ else $p = ab$ with $a, b \neq 1$. Hence, since y is odd,

$$(A, B) = (2x - y, y) = (2x, y) = (x, y) = 1.$$

We are now at

$$4p = A^2 + 3B^2 \text{ where } (A, B) = 1.$$

Suppose $p \mid B$. Then $B = pu$ for some $u \in \mathbb{Z}$ which implies,

$$4p = A^2 + (3pu)^2.$$

Therefore we have $p \mid A$, but since $(A, B) = 1$ we have a contradiction and hence $p \nmid B$. This implies that there exists an integer C such that $BC \equiv 1 \mod p$. Multipliying (9) by C^2 we get,

$$4pC^2 = (AC)^2 + 3(BC)^2.$$

This becomes

$$(AC)^2 \equiv -3 \mod p.$$

Hence -3 is a quadratic residue of p. From the proof of Theorem 2.2 we have the following equation of Legendre symbols,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right).$$

Combined with that $p \equiv 1 \mod 2$ and the Chinese Remainder Theorem we get that $p = 6n + 1$. Now for the converse, let $p \equiv 1 \mod 6$. From the proof of Theorem 2.2 we know this implies $\left(\frac{-3}{p}\right) = 1$. Hence that there exists some a such that $a^2 \equiv -3 \mod p$. Furthermore $(a, p) = 1$ and hence $ax \equiv y \mod p$ has solutions α_0, β_0 for which Thue's lemma holds. This gives us,

$$-3\alpha_0^2 \equiv a^2\alpha_0^2 \equiv (a\alpha_0)^2 \equiv {\beta_0}^2 \mod p$$

or equivalently,

$$3\alpha_0^2 + {\beta_0}^2 \equiv 0 \mod p.$$

This implies,

$$3\alpha_0^2 + {\beta_0}^2 = pk \text{ for some } k \in \mathbb{Z}\ . \tag{10}$$

The bounds of α_0 and β_0 from Thue's lemma gives us, $3\alpha_0^2 + {\beta_0}^2 < 4p$. This reduces the possibilities for k in (10) to $k \in \{1, 2, 3\}$. Suppose $k = 3$, then $3p = 3{\alpha_0}^2 + {\beta_0}^2$. Therefore $3 \mid \beta_0$ and hence

$$3p = 3{\alpha_0}^2 + (3{\beta_0}')^2 \iff p = {\alpha_0}^2 + 3{\beta_0}'^2,$$

which essentially is $k = 1$. Next suppose $k = 2$, then $2p = 3{\alpha_0}^2 + {\beta_0}^2$. This can be regarded as a congruence modulo 3 of the following form,

$$2p \equiv {\beta_0}^2 \mod 3.$$

In Legendre symbols this is equivalent to,

$$1 = \left(\frac{2p}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{p}{3}\right) = -1.$$

This follows from that $p \equiv 1 \mod 6$ which implies that $\left(\frac{p}{3}\right) = 1$ and that $\left(\frac{2}{3}\right) = -1$, both of which are proved in [2]. Therefore letting $k = 2$ implies a contradiction. Furthermore since 4 is a square, we multiply $p = 3\alpha_0^2 + {\beta_0}^2$ by 4 to get $4p = D^2 + 3E^2$. The remaining part of the proof is identical to the case $p \equiv 1 \mod 4$ and the split of p in $\mathbb{Z}[\sqrt{-1}]$. The only difference is that we got a new algebraic element $\omega = e^{\frac{2\pi i}{6}}$, our prime ideals have the form $P_1 = (x + y\omega)$ and $P_2 = (x + y\bar{\omega})$ and proving that P_j is prime is done by using the norm $N(a + \omega b) = a^2 - ab + b^2$ on $\mathbb{Z}[\omega]$. □

3.4 Splitting of 11 in the ring of integers in the cyclotomic field generated by a fifth root of unity

In the two previous cases we dealt with field extensions of degree two. If we let $\omega = e^{\frac{2\pi i}{5}}$ we get an extension $\mathbb{Q}[\omega] : \mathbb{Q}$ which is of degree 4. Since this increases the number of steps in the splitting we stick to investigating what happens with the prime 11 when lifted the two steps from $\mathbb{Z}$ into $\mathbb{Z}[e^{\frac{2\pi i}{5}}]$. To do this we used Maple. The process can now be viewed in the following way:

$$\begin{array}{ccccc} \mathbb{Z} & \subset & \mathbb{Z}[\frac{-1+\sqrt{5}}{2}] & \subset & \mathbb{Z}[\omega] \\ \cup & & \cup & & \cup \\ p\mathbb{Z} & \longrightarrow & A_1, A_2 & \longrightarrow & B_1, B_2, B_3, B_4 \, . \end{array}$$

Here $A_1, A_2, B_1, B_2, B_3, B_4$, are prime ideals in their respective rings.

Theorem 3.3. *Let $\omega = e^{\frac{2\pi i}{5}}$. Then 11 splits completely in $\mathbb{Z}[\omega]$.*

Proof. What we want to establish is that we can find distinct prime ideals P_i such that $P_1 \cdots P_4 = 11\mathbb{Z}[\omega]$. In the previous cases we used conjugation in order to find suitable prime ideals. The first step is finding a suitable automorphism on $\mathbb{Z}[\omega]$ that does something similar. Let $\sigma : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]$ be the automorphism defined by $\sigma(\omega) = \omega^2$. Since ω and ω^2 share minimal polynomial we get from [5] Corollary 10.8 that this is a $\mathbb{Z}$-automorphism. We also know that $\mathbb{Z}[\omega]$ is free as a $\mathbb{Z}$-module and therefore σ is determined by how it acts on the basis. Observe that

$$\sigma^2(\omega^i) = \omega^{4i} = \bar{\omega^i}.$$

This property is essential. Lets factor 11 the two steps into $\mathbb{Z}[\omega]$. We start in the extension $\mathbb{Z}[\frac{-1+\sqrt{5}}{2}]$ which is of rank two. Here we can split 11 into $(4 + \sqrt{5})$ and $(4 - \sqrt{5})$ by conjugation of the algebraic element $\sqrt{5}$. Next we consider the splitting of $(4 + \sqrt{5})$ into $\mathbb{Z}[\omega]$. Letting this factorization be the usual complex conjugation we get two elements γ and $\bar{\gamma}$. By finding similar elements for $(4 - \sqrt{5})$ we get a final expression

$$11 = (4 + \sqrt{5})(4 - \sqrt{5}) = \gamma\bar{\gamma}\gamma'\bar{\gamma'}.$$

In terms of σ and after commuting the factors we get,

$$\gamma\bar{\gamma}\gamma'\bar{\gamma'} = \gamma\sigma(\gamma)\sigma^2(\gamma)\sigma^3(\gamma).$$

Proceeding as in the two previous cases we get that $P_1 \cdots P_4 = 11\mathbb{Z}[\omega]$. Letting $P_1 = (\gamma)$ we obtain the remaining ideals by applying σ to it. To show that these ideals are distinct we use Maple. In order to do the necessary computations we need an actual element γ. After trying some random coefficients for elements of $\mathbb{Z}[\omega]$ we find that the element $\gamma = -1 + \omega + \omega^2 + \omega^3$ multiplied by its conjugate equals $(4 + \sqrt{5})$. The following computations are sufficient to establish that the ideals are distinct. We have

$$\frac{\sigma(\gamma)}{\gamma} = \frac{13}{11}\omega^3 + \frac{1}{11}\omega^2 + \frac{7}{11}\omega + \frac{15}{11},$$

$$\frac{\sigma^2(\gamma)}{\gamma} = \frac{6}{11}\omega^3 + \frac{3}{11}\omega^2 + \frac{10}{11}\omega + \frac{12}{11},$$

$$\frac{\sigma^3(\gamma)}{\gamma} = \frac{9}{11}\omega^3 + \frac{10}{11}\omega^2 + \frac{4}{11}\omega + \frac{18}{11}.$$

Since these are not elements of $\mathbb{Z}[\omega]$ for $i = 1, 2, 3$ we know that the ideals are not identical. Next we show that all four ideals are prime in $\mathbb{Z}[\omega]$. Just as in the previous cases we prove that the ideals are maximal. This will imply that they are prime by the same argument as in those cases. The idea is to show that we have the ring isomorphism,

$$\tilde{f} : \frac{\mathbb{Z}[\omega]}{(\gamma)} \to \frac{\mathbb{Z}}{11\mathbb{Z}}.$$

Since 11 is a prime we know that $\frac{\mathbb{Z}}{11\mathbb{Z}}$ is a field. The problem is therefore finding a suitable ring homomorphism $f : \mathbb{Z}[\omega] \to \frac{\mathbb{Z}}{11\mathbb{Z}}$ where the kernel is (γ). Since both structures are free $\mathbb{Z}$-modules we know that any $\mathbb{Z}$-homomorphism f is determined by how it acts on the basis of $\mathbb{Z}[\omega]$. Clearly $f(1) = 1$ and since the remaining elements are multiples of ω we only need to decide where to map ω. Let $f(\omega) = 5$, since $\omega \equiv 5 \mod \gamma$ we get $\omega^k \equiv 5^k \mod \gamma$ for all $k \in \mathbb{Z}$ and hence we have the $\mathbb{Z}$-homomorphism defined for the basis. By extending this $\mathbb{Z}$-homomorphism defined for the basis we get that it preserves the additive group structure. It remains to show that f also preserves the multiplicative structure in order for it to be a ring homomorphism. Because of bilinearity we only need to verify the following,

$$f(\omega^k\omega^l) = f(\omega^{k+l}) = f(\omega^k)f(\omega^l).$$

Here $0 \leq k, l \leq 3$. This gives us three cases to consider. The first $0 \leq k+l \leq 3$ is clear from definitions. In second case $k+l = 4$ we use that $\omega^4+\omega^3+\omega^2+\omega+1 = 0$ and hence,

$$\begin{aligned} f(\omega^{k+l}) = f(\omega^4) &= f(-\omega^3 - \omega^2 - \omega - 1) \\ &= -[1]_{11} - [5]_{11} - [5^2]_{11} - [5^3]_{11} = [5]_{11}^4 \\ &= ([5]_{11})^{k+l} = f(\omega^k)f(\omega^l). \end{aligned}$$

For the last case $5 \leq k+l \leq 6$ we use that $\omega^5 = 1$, $0 \leq k+l-5 \leq 3$ and $[5]_{11}^5 = 1$ hence,

$$\begin{aligned} f(\omega^{k+l}) &= f(\omega^{k+l-5}) \\ &= [5]_{11}^{k+l-5} = [5]_{11}^{k+l} \\ &= f(\omega^k) f(\omega^l). \end{aligned}$$

To see that we have a well defined homomorphism with respect to the multiplicative structure consider the following:

$$\begin{aligned} f(\sum_{k=0}^{3} a_k \omega^k \sum_{l=0}^{3} b_l \omega^l) &= f(\sum_{l,k=0}^{3} a_k b_l \omega^{k+l}) \\ = \sum_{l,k=0}^{3} [a_k b_l] f(\omega^{k+l}) &= \sum_{l,k=0}^{3} [a_k][b_l] f(\omega^k) f(\omega^l) \\ = \sum_{k=0}^{3} [a_k] f(\omega^k) \sum_{l=0}^{3} [b_l] f(\omega^l) &= f(\sum_{k=0}^{3} [a_k]\omega^k) f(\sum_{l=0}^{3} [b_l]\omega^l). \end{aligned}$$

Next consider,

$$\begin{aligned} f(\gamma) &= f(-1+\omega+\omega^2+\omega^3) \\ &= f(-1) + f(\omega) + f(\omega^2) + f(\omega^3) = 10+5+3+4 \equiv 0 \mod 11. \end{aligned}$$

This implies $(\gamma) \subseteq \ker(f)$. For the reverse inclusion note that,

$$f : \mathbb{Z}[\omega] \to \frac{\mathbb{Z}}{11\mathbb{Z}}$$

is a surjective ring homomorphism as established above. Therefore we have $|\frac{\mathbb{Z}[\omega]}{ker(f)}| = 11$ by the first isomorphism theorem. Further since we have $(\gamma) \subseteq \ker(f)$ we have,

$$11 = \Big|\frac{\mathbb{Z}[\omega]}{ker(f)}\Big| \leq \Big|\frac{\mathbb{Z}[\omega]}{(\gamma)}\Big|.$$

Moreover, for every element $\alpha \in \mathbb{Z}[\omega]$ we have

$$\alpha \equiv r \mod \gamma$$

where $0 \leq r \leq 10$. This follows because $\omega^k \equiv 5^k$ for all $k \in \mathbb{Z}$ and since $11 \in (\gamma)$. Hence $|\frac{\mathbb{Z}[\omega]}{(\gamma)}|$ is bounded by 11 which proves the reverse inclusion. We therefore have our needed homomorphism and hence P_1 is prime. In order to prove that $P_i \quad i \in 2,3,4$ are prime we use different isomorphisms. For $P_2 = (\gamma')$ we define f_2 by $f_2(\omega) = 4$, $P_3 = (\bar{\gamma})$ we define f_3 by $f_3(\omega) = 9$, $P_4 = (\bar{\gamma'})$ we define f_4 by $f_4(\omega) = 3$. The arguments that these are isomorphic to the field $\frac{\mathbb{Z}}{11\mathbb{Z}}$ are identical to the case of P_1. It remains to show that $11\mathbb{Z} = P_j \cap \mathbb{Z}$. The inclusion

$11\mathbb{Z} \subseteq P_j \cap \mathbb{Z}$ is proved just as in the two previous cases. To prove $1 \notin P_i$ is a bit more complicated but we can use Maple to get,

$$\begin{aligned}
\frac{1}{\gamma} &= -\frac{4}{11}\omega^3 - \frac{2}{11}\omega^2 - \frac{3}{11}\omega - \frac{8}{11} \\
\frac{1}{\gamma'} &= \frac{2}{11}\omega^3 - \frac{1}{11}\omega^2 - \frac{2}{11}\omega - \frac{6}{11} \\
\frac{1}{\bar{\gamma}} &= \frac{1}{11}\omega^3 - \frac{1}{11}\omega^2 + \frac{3}{11}\omega - \frac{5}{11} \\
\frac{1}{\bar{\gamma'}} &= \frac{1}{11}\omega^3 + \frac{4}{11}\omega^2 + \frac{2}{11}\omega - \frac{4}{11}.
\end{aligned}$$

Since none of these belongs to $\mathbb{Z}[\omega]$ we reason just as in the case of the Gaussian and Eisenstein integers to get,

$$11\mathbb{Z} = P_j \cap \mathbb{Z}$$

This proves the splitting of 11 in $\mathbb{Z}[\omega]$. □

References

[1] P.B. Bhattacharya, S.K. Jain and S.R. Nagpaul, *Basic Abstract Algebra*, 2 ed., Cambridge University press (1994).

[2] D.M Burton, *Elementary Number Theory*, McGraw-Hill (2002).

[3] D.A Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons Inc (1989).

[4] H.Gauchman, *A Special Case of Dirichlet's Theorem on Primes in an Arithmetic Progression*, Mathematics Magazine **74** (2001), 397-399.

[5] T.W Hungerford, *Abstract Algebra An Introduction*, 2 ed., Brooks/Cole (1997).

[6] F.Lemmermeyer *Reciprocity Laws, From Euler to Eisenstien*, Springer (2000).

[7] L.Levine, *Fermat's Little Theorem: a proof by function iteration*, Mathematics Magazine **72** (1999), 308-309.

[8] T.Nagell, *Introduction to Number Theory*, Almqvist & Wiksells boktryckeri (1951).

[9] J.Sabia and S.Tesauri, *The Least Prime in Certain Arithmetic Progressions*, Amer Math. Monthly **116** (2009), 641-643.

[10] R.Thangadurai and A.Vatwani, *The Least Prime Congruent to One Modulo n*, Amer. Math. Monthly **118** (2011), 737-742.