The arithmetic progression $15n + 11$, $n \geqslant 0$, contains infinitely many primes. A Euclidean proof

About this document

This file has been automatically generated for the user-supplied arithmetic progression. The code behind this document can be found in the url http://www.overleaf.com, and has been developed as part of a BSc Thesis in Mathematics by Joan Arenillas i Cases at the Autonomous University of Barcelona. The above link also provides full access to the complete Thesis. Please use joanarenillas01@gmail.com to report any typo or express any suggestions.

We will prove that the arithmetic progression $\equiv 11 \pmod{15}$ contains infinitely many primes. Equivalently, we will see that there are infinitely many primes of the form $15n + 11$, $n \geqslant 0$. For this purpose, consider the polynomial

$$f(x) := x^4 + 884x^3 + 293206x^2 + 43243679x + 2392743361.$$

1 The main Theorem

To prove that there exist infinitely many primes $\equiv 11 \pmod{15}$ we can proceed by contradiction. Suppose there are finitely many primes $\equiv 11 \pmod{15}$ and denote them by $p_1, p_2, \ldots, p_m$. Since $11, 41, 71 \equiv 11 \pmod{15}$, we can write the list as $11, 41, 71, p_4, p_5, \ldots, p_m$ (so $p_3 = 71$). Now, let $Q := 5 \cdot 11^2 \cdot 19 \cdot 41^2 \cdot 1091 \cdot p_4 p_5 \cdots p_m$. Consider the following congruence equation system:

$$\begin{cases} c \equiv 2 \pmod{71^2} \\ c \equiv 0 \pmod{15Q}. \end{cases}$$

The Chinese Remainder Theorem guarantees the existence of $c \in \mathbb{Z}$ that is a solution to the above system since 71 does not divide $15Q$. It follows that

$$f(c) \equiv f(2) = 2480410631 \equiv 71 \cdot 24 \pmod{71^2},$$
$$f(c) \equiv f(0) = 61 \cdot 39225301 \pmod{15Q}.$$

In particular, observe that the prime $p_3 = 71$ divides $f(c)$, but 71^2 does not.

Lemma 1. *Every prime that divides $f(c)$ is $\equiv 1 \pmod{15}$ (except for $p_3 = 71$).*

Proof. Let r be a prime divisor of $f(c)$ different from 71. In Section 2 we will establish that $r = 3,\ 5,\ 11,\ 19,\ 41,\ 1091$ or $r \equiv 1, 11 \pmod{15}$. For now, we will assume this is true. To reach a contradiction, suppose $r \not\equiv 1 \pmod{15}$. Thus, $r \equiv 11 \pmod{15}$ or $r = 3,\ 5,\ 11,\ 19,\ 41,\ 1091$, so r divides $15 \cdot 5 \cdot 11^2 \cdot 19 \cdot 41^2 \cdot 1091 \cdot p_4 p_5 \cdots p_m = 15Q$. Since $f(c) \equiv 61 \cdot 39225301 \pmod{15Q}$ and r is a divisor of $15Q$, we deduce that $f(c) \equiv 61 \cdot 39225301 \pmod{r}$. But r is a divisor of $f(c)$, so $f(c) \equiv 0 \pmod{r}$. Therefore, $61 \cdot 39225301 \equiv 0 \pmod{r}$. Thus, it must happen that $r = 61, 39225301$, which are $\equiv 1 \pmod{15}$. This forces r to be $\equiv 1 \pmod{15}$, a contradiction. Therefore, $f(c)$ is only divisible by primes $\equiv 1 \pmod{15}$ (and by $p_3 = 71$). ∎

Finally, from the fact that $f(c)$ has every prime divisor $\equiv 1 \pmod{15}$ except for $p_3 = 71$ it follows, $\pmod{15}$, that $f(c) = 1 \cdot 1 \cdots 1 \cdot 11 = 11$ (note that 11 only appears once because $p_3 = 71 \equiv 11 \pmod{15}$ and the fact that 71^2 does not divide $f(c)$). However, observe that $f(c) \equiv f(0) \equiv 1 \pmod{15}$. This is a contradiction. Therefore, the arithmetic progression $\equiv 11 \pmod{15}$ contains infinitely many primes.

2 Properties of the polynomial $f(x)$

To complete the proof of the main Theorem in Section 1 we must justify that every prime divisor p of $f(c)$ either belongs to the finite set

$$T := \{3, 5, 11, 19, 41, 1091\}$$

or satisfies $p \equiv 1, 11 \pmod{15}$. To see this, we must first recall the expression of the discriminant of a polynomial.

Definition 2. The discriminant of a monic polynomial $A(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ is given, in terms of its roots $\{r_1, r_2, \ldots, r_m\} \subset \mathbb{C}$ (not necessarily distinct), by

$$\Delta(A) = \prod_{i<j} (r_i - r_j)^2, \quad 1 \leqslant i, j \leqslant m. \tag{1}$$

It will be useful to remember that the 15th cyclotomic polynomial is $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$. We shall also define what a *prime divisor* of a given polynomial is.

Definition 3. Let $A(x) \in \mathbb{Z}[x]$ be a polynomial. We say that a prime number p is a *prime divisor* of A (or simply that p *divides* A) if there exists $m \in \mathbb{Z}$ such that p divides $A(m)$.

With the definition above, we are interested in describing the prime divisors of f.

Let's now start the proof. Consider the set $S := \{1, \ 2, \ 4, \ 8\}$ and the values $h(\zeta^s) := (\zeta^s - 15)(15 - \zeta^{11s})$, with $s \in S$ and $\zeta := e^{2\pi i/15}$, a 15th primitive root of unity (thus a root of $\Phi_{15}(x)$). A simple calculation shows that $f(x)$ can be written as

$$f(x) = \prod_{s \in S} \big(x - h(\zeta^s)\big) = x^4 + 884x^3 + 293206x^2 + 43243679x + 2392743361. \tag{2}$$

The discriminant of $f(x)$ can be calculated[1] to be $\Delta(f) = 5^3 \cdot 11^2 \cdot 19^2 \cdot 41^2 \cdot 1091^2$.

Now, suppose that p is a prime divisor of f such that $p \notin T$. Next, consider a field $\mathbb{F}$ containing both the finite field $\mathbb{F}_p$ and ζ[2]. Since p divides f, working in $\mathbb{F}$, there exists $a \in \mathbb{Z}$ such that

$$f(a) = \prod_{s' \in S} \left(a - h(\zeta^{s'})\right) = 0.$$

Since $\mathbb{F}$ is a field, there exists some $s \in S$ such that $a = h(\zeta^s)$.

Lemma 4. *The equality $h(\zeta^s) = h(\zeta^{ps})$ holds in $\mathbb{F}$.*

Proof. Observe that the following calculation holds in $\mathbb{F}$:

$$\begin{aligned} h(\zeta^s) &= a = a^p = h(\zeta^s)^p = (\zeta^s - 15)^p (15 - \zeta^{11s})^p \\ &= (\zeta^{ps} - 15^p)(15^p - \zeta^{11ps}) = (\zeta^{ps} - 15)(15 - \zeta^{11ps}) = h(\zeta^{ps}), \end{aligned} \tag{3}$$

where we have used Fermat's little theorem in the second equality. The fifth equality, on the other hand, relies on the fact that $\mathbb{F}$ has characteristic p (so that $(c+d)^p = c^p + d^p$ for every $c, d \in \mathbb{F}$) and the following one, on Fermat's little theorem. ∎

Therefore, equality (3) means that $h(\zeta^{ps}) = h(\zeta^s)$ is a root of $\overline{f(x)} \in \mathbb{F}[x]$.

Lemma 5. *$h(\zeta^{ps})$ is also a root of $f(x)$ in $\mathbb{Q}(\zeta)$ (the smallest subfield of $\mathbb{C}$ containing ζ).*

[1] One way of calculating $\Delta(f)$ is via the resultant of f and f'.

[2] For instance, consider $\mathbb{F} = \mathbb{F}_{p^n}$ with a suitable integer $n \geqslant 1$ such that Φ_{15} has a root ζ.

Proof. Begin by noting that the value $h(\zeta^{ps})$ only depends on the value of $ps \pmod{15}$ since it only appears as an exponent of ζ. Since p does not divide 15 and s is coprime to 15, ps is coprime to 15 (so $ps \pmod{15}$ is coprime to 15) and hence ζ^{ps} is a primitive 15th root of unity.

There are now only two options: either $ps \pmod{15} \in S$ or $ps \pmod{15} \notin S$. In the first case, $h(\zeta^{ps})$ is a root of $f(x)$, observing expression (2). In the latter case, note that every integer $ps \pmod{15}$ relatively prime to 15 not in S satisfies $ps \equiv 11t \pmod{15}$ for some $t \in S$ (for instance, if $ps \pmod{15} = 13$, pick $t = 8 \in S$ so that $13 \equiv 11 \cdot 8 \pmod{15}$). This means that $h(\zeta^{ps}) = h(\zeta^{11t})$. Let us prove that $h(\zeta^{11t}) = h(\zeta^{t})$, so $h(\zeta^{ps}) = h(\zeta^{11t}) = h(\zeta^{t})$ is also a root of $f(x)$. Indeed,

$$\begin{aligned} h(\zeta^{11t}) &= (\zeta^{11t} - 15)(15 - \zeta^{11^2 t}) = (\zeta^{11^2 t} - 15)(15 - \zeta^{11t}) \\ &= (\zeta^{t} - 15)(15 - \zeta^{11t}) = h(\zeta^{t}), \end{aligned}$$

where we have used that $\zeta^{11^2 t}$ only depends on the value of $11^2 t \pmod{15}$ and the fact that $11^2 \equiv 1 \pmod{15}$. Therefore, $h(\zeta^{ps}) = h(\zeta^{t})$ is always a root of $f(x)$ in $\mathbb{Q}(\zeta)$. ■

Lemma 6. *$h(\zeta^{ps})$ and $h(\zeta^{s})$ are the same root of $f(x)$ in $\mathbb{Q}(\zeta)$.*

Proof. If $h(\zeta^{ps})$ and $h(\zeta^{s})$ were two distinct roots of $f(x)$ in $\mathbb{Q}(\zeta)$, we know because of (3) that they would be the same in $\mathbb{F}$. Therefore, observing expression (1), it follows that $\Delta(f \pmod{p}) = \Delta(f) \pmod{p} = 0$, so p divides $\Delta(f) = 5^3 \cdot 11^2 \cdot 19^2 \cdot 41^2 \cdot 1091^2$. This is a contradiction with our choice of p. Thus, $h(\zeta^{ps})$ and $h(\zeta^{s})$ are in fact the same root of $f(x)$ in $\mathbb{Q}(\zeta)$. ■

Therefore, the equality

$$h(\zeta^{ps}) = \big(\zeta^{ps} - 15\big)\big(15 - \zeta^{11ps}\big) = \big(\zeta^{s} - 15\big)\big(15 - \zeta^{11s}\big) = h(\zeta^{s})$$

holds in $\mathbb{Q}(\zeta)$. Next, write the above equation in terms of $\theta := \zeta^{s}$ and multiply both sides by -1. This changes yield

$$\begin{aligned} 225 - 15\big(\theta^{p} + \theta^{11p}\big) + \theta^{(1+11)p} &= 225 - 15\big(\theta + \theta^{11}\big) + \theta^{1+11}, \\ -15\big(\theta^{p} + \theta^{11p}\big) + \theta^{12p} &= -15\big(\theta + \theta^{11}\big) + \theta^{12}. \end{aligned} \tag{4}$$

The right-hand side of the equation above does not depend on p. The left-hand side only depends on the value of $p \pmod{15}$, since p only appears as an exponent of θ. The above equality gives information about p, which is what we are interested in.

Lemma 7. *The fact that (4) holds implies that $p \pmod{15} \in H := \{1, 11\}$.*

Proof. To prove this, we will check every value of p such that $p \pmod{15} \notin H$ and conclude that (4) is not true in $\mathbb{Q}(\theta)$ in those cases. Therefore, we shall see the following:

if $p \pmod{15} \in G \setminus H = \{2, 4, 7, 8, 13, 14\}$, then $-h(\theta^p) \neq -h(\theta)$. This will automatically imply what we want to prove: since (4) holds, $p \pmod{15} \in H$. To see this, rewrite (4) as

$$-15\big(\theta^p + \theta^{11p}\big) + \theta^{12p} + 15\big(\theta + \theta^{11}\big) - \theta^{12} = 0 \tag{5}$$

and trade θ for x, since the condition (5) in $\mathbb{Q}(\theta)$ is equivalent to the condition

$$-15\big(x^p + x^{11p}\big) + x^{12p} + 15\big(x + x^{11}\big) - x^{12} = 0 \tag{6}$$

in $\mathbb{Q}[x]/(\Phi_{15}(x)) \cong \mathbb{Q}(\theta)$ ($\Phi_{15}(x)$ is also the minimal polynomial of θ, since $\theta = \zeta^s$ is a primitive 15th root of unity). We will explicitly write the case $p = 2 \pmod{15}$ (the remaining values of $p \pmod{15} \in G \setminus H$ are left as an exercise to the reader). With this value of p, equation (6) becomes

$$\begin{aligned} A(x) &:= -15\big(x^2 + x^{22}\big) + x^{24} + 15\big(x + x^{11}\big) - x^{12} \\ &= x^{24} - 15x^{22} - x^{12} + 15x^{11} - 15x^2 + 15x = 0. \end{aligned}$$

If we recall that $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(\Phi_{15}(x))$, the above equation is equivalent to $A(x)$ being a multiple of the 15th cyclotomic polynomial, $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$. Therefore, we are interested in showing that the residue $R(x)$ of the division $A(x)/\Phi_{15}(x)$ satisfies $R(x) \neq 0$, from which our result will follow. A simple Euclidean division of polynomials shows that $A(x) = B(x) \cdot \Phi_{15}(x) + (-13x^7 - 16x^6 - x^3 - 13x^2 - 1)$, with $B(x)$ a polynomial of degree 16, so $R(x) = -13x^7 - 16x^6 - x^3 - 13x^2 - 1 \neq 0$. Therefore, equality (4) implies that $p \pmod{15} \in H$, that is, $p \equiv 1, 11 \pmod{15}$. ■

In conclusion, every prime divisor p of $f(c)$ either belongs to the finite set

$$T := \{3, 5, 11, 19, 41, 1091\}$$

or satisfies $p \equiv 1, 11 \pmod{15}$, which finally settles the main Theorem in Section 1.