The arithmetic progression $15n + 1$, $n \geqslant 0$, 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 $\equiv 1 \pmod{15}$ contains infinitely many primes. Equivalently, we will see that there are infinitely many primes of the form $15n+1$, $n \geqslant 0$. To follow the proof, one must recall the expression of the discriminant of a polynomial.

Definition 1. The discriminant of a monic polynomial $A(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ 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 2. 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 $A(m)$.

1 The main Theorem

We are now able to show that there exist infinitely many primes $\equiv 1 \pmod{15}$. For this purpose, consider the polynomial

$$f(x) := \Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

We will specifically show that every prime divisor p of f either belongs to the finite set

$$T := \{3, 5\}$$

or satisfies $p \equiv 1 \pmod{15}$. To see this, consider the set $S := \{1, 2, 4, 7, 8, 11, 13, 14\}$ and the values ζ^s, 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

$$f(x) = \prod_{s \in S} \left(x - \zeta^s\right) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 = \Phi_{15}(x).$$

The discriminant of $f(x)$ can be calculated[1] to be $\Delta(f) = 3^4 \cdot 5^6$.

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

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

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

Lemma 3. *The equality $\zeta^s = \zeta^{ps}$ holds in $\mathbb{F}$.*

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

$$\zeta^s = a = a^p = \zeta^{ps}, \tag{2}$$

where we have used Fermat's little theorem in the second equality. ■

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

Lemma 4. *ζ^{ps} is also a root of $f(x)$ in $\mathbb{Q}(\zeta)$ (the smallest subfield of $\mathbb{C}$ containing ζ).*

Proof. Begin by noting that the value ζ^{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. Thus, ζ^{ps} is a root of $\Phi_{15}(x) = f(x)$ in $\mathbb{Q}(\zeta)$. ■

[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.

Lemma 5. *ζ^{ps} and ζ^s are the same root of $f(x)$ in $\mathbb{Q}(\zeta)$.*

Proof. If ζ^{ps} and ζ^s were two distinct roots of $f(x)$ in $\mathbb{Q}(\zeta)$, we know because of (**??**) that they would be the same in $\mathbb{F}$. Therefore, observing expression (**??**), it follows that $\Delta(f \pmod p) = \Delta(f) \pmod p = 0$, so p divides $\Delta(f) = 3^4 \cdot 5^6$. This is a contradiction with our choice of p. Thus, ζ^{ps} and ζ^s are in fact the same root of $f(x)$ in $\mathbb{Q}(\zeta)$. ■

Therefore, the equality

$$\zeta^{ps} = \zeta^s \tag{3}$$

holds in $\mathbb{Q}(\zeta)$.

Lemma 6. *The fact that* (**??**) *holds implies that* $p \pmod{15} = 1$.

Proof. Write the above equation in terms of $\theta := \zeta^s$. This change yields

$$\theta^p = \theta.$$

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. In conclusion, expression (**??**) only holds if $p \pmod{15} = 1$, that is, if $p \equiv 1 \pmod{15}$. ■

In conclusion, every prime divisor p of $f = \Phi_{15}$ either belongs to the finite set

$$T = \{3, 5\}$$

or satisfies $p \equiv 1 \pmod{15}$. In Section **??** we will establish that the polynomial Φ_{15} has infinitely many prime divisors. But, from the remark above, all these prime divisors must be $\equiv 1 \pmod{15}$ (except for those $p \in T$). This concludes the proof that there are infinitely many primes $\equiv 1 \pmod{15}$.

2 Property of the polynomial $\Phi_{15}(x)$

We just need the following lemma to complete the proof of the main Theorem in Section **??**.

Lemma 7. *The cyclotomic polynomial $\Phi_{15}(x) \in \mathbb{Z}[x]$ has infinitely many prime divisors.*

Proof. There is obviously at least one prime divisor of Φ_{15}, since the case $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 = \pm 1$ only happens for a finite number of integer values of x. Now suppose Φ_{15} has only a finite number of prime divisors, say $p_1, p_2, \ldots, p_k$ and let $Q := p_1 p_2 \cdots p_k$.

Observe that $\deg(\Phi_{15}) = 8$ and $\Phi_{15}(0) = 1 \neq 0$. Then, $\Phi_{15}(Qx) = g(x)$ for some $g(x) \in \mathbb{Z}[x]$ of the form $1 + c_1x + \cdots + c_8x^8$, $c_i \in \mathbb{Z}$, satisfying $Q \mid c_i$ for every $1 \leqslant i \leqslant 8$. This polynomial g must also have at least one prime divisor, say p, for the same reason as before. Therefore, p divides $g(m)$ for some $m \in \mathbb{Z}$, and this implies that p divides $\Phi_{15}(Qm)$. Since $m' := Qm \in \mathbb{Z}$, it follows that p is a prime divisor of Φ_{15}. But p does not divide Q, since p dividing Q would mean that p divides c_i, for every $1 \leqslant i \leqslant 8$ (recall that Q divides every c_i). This, together with the fact that p divides $g(m)$, would imply that p divides $g(m) - \sum_{i=1}^{8} c_i m^i = 1$, which means $p = 1$, a contradiction.

Now, p is a prime divisor of Φ_{15}, but p is not any of the primes $p_1, p_2, \ldots, p_k$, since we just proved that p does not divide $p_1p_2\cdots p_k = Q$. Thus, we found a new prime divisor of Φ_{15} not in our list. Since this argument can be repeated indefinitely, one concludes that Φ_{15} has infinitely many prime divisors. ■