# Cyclotomic factors of Serre polynomials

Florian Luca

**November 8, 2017**

## The Ramanujan $\tau$-function

Let $\tau(n)$ be the Ramanujan function given by

$$\sum_{n\geq 1}\tau(n)q^n = q\prod_{i\geq 1}(1-q^i)^{24} \qquad (|q|<1).$$

Ramanujan observed but could not prove the following three properties of $\tau(n)$:

(i) $\tau(mn)=\tau(m)\tau(n)$ whenever $\gcd(m,n)=1$.

(ii) $\tau(p^{r+1})=\tau(p)\tau(p^r)-p^{11}\tau(p^{r-1})$ for $p$ prime and $r\geq 1$.

(iii) $|\tau(p)|\leq 2p^{11/2}$ for all primes $p$.

These conjectures were proved by Mordell and Deligne.

## Zero values of $\tau(n)$

Lehmer conjectured that $\tau(n) \neq 0$ for all $n$. This is still unknown. It is known that

$$\tau(n) \neq 0 \qquad \text{for} \qquad n \leq 22798241520242687999.$$

Serre proved that

$$\#\{p \leq x \;:\; \tau(p) = 0\} = O\left(\frac{x}{(\log x)^{3/2}}\right).$$

## Today's problem

The Dedekind eta function is a modular form:

$$\eta(\tau) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n), \qquad \left(q := e^{2\pi i\tau},\ \mathrm{Im}(\tau) > 0\right).$$

Euler and Jacobi studied $\eta(\tau)^k$ and proved that

$$\prod_{m=1}^{\infty} (1 - q^m) = \sum_{m=-\infty}^{\infty} (-1)^m q^{\frac{3m^2+m}{2}}, \qquad (1)$$

$$\prod_{m=1}^{\infty} (1 - q^m)^3 = \sum_{m=0}^{\infty} (-1)^m (2m+1) q^{\frac{m^2+m}{2}}. \qquad (2)$$

More powers of $\eta$ were studied by Serre.

## A family of interesting polynomials

We look at the Fourier coefficients simultaneous for all powers of the Dedekind eta function. We define a family of polynomials $P_m(X)$ for $m \geq 0$ with interesting properties. Consider the identity

$$\prod_{m\geq 1}(1-q^m)^{-z} = \sum_{m=0}^{\infty} P_m(z)\, q^m \quad (z \in \mathbb{C})\,. \tag{3}$$

The roots of $P_m(z)$ dictate the vanishing properties of the Fourier coefficients. These polynomials have degree $m$ and

$$A_m(X) := m!\, P_m(X) \in \mathbb{Z}[X]$$

is normalized. It follows also from the definition that $P_m(X)$ are integer-valued polynomials.

The polynomials can be defined also recursively. We put $P_0(X) := 1$ and define

$$P_m(X) = \frac{X}{m}\left(\sum_{k=1}^{m}\sigma(k)P_{m-k}(X)\right), \qquad m \geq 1. \tag{4}$$

Here, as before, $\sigma(k)$ denotes the sum of the divisors of $k$.

To illustrate the complexity of these polynomials here are the first ten:

$$\begin{aligned}
P_1(X) &= X;\\
2!P_2(X) &= X^2+3X = X(X+3);\\
3!P_3(X) &= X\left(X^2+9X+8\right)\\
&= X(X+8)(X+1);\\
4!P_4(X) &= X\left(X^3+18X^2+59X+42\right)\\
&= X(X+14)(3+X)(X+1);\\
5!P_5(X) &= X\left(X^4+30X^3+215X^2+450X+144\right)\\
&= X(3+X)(X+6)\left(X^2+21X+8\right);
\end{aligned}$$

$$
\begin{aligned}
6!P_6(X) &= X\left(X^5+45X^4+565X^3+2475X^2+3394X+1440\right) \\
&= X(X+10)(X+1)\left(X^3+34X^2+181X+144\right); \\
7!P_7(X) &= X(X^6+63X^5+1225X^4+9345X^3 \\
&\quad +28294X^2+30912X+5760) \\
&= X(X+8)(3+X)(X+2)\left(X^3+50X^2+529X+120 \right. \\
8!P_8(X) &= X(X^7+84X^6+2338X^5+27720X^4+147889X^3 \\
&\quad +340116X^2+293292X+75600) \\
&= X(X+6)(3+X)(X+1) \\
&\quad \left(X^4+74X^3+1571X^2+9994X+4200\right); \\
9!P_9(X) &= X^9+108X^8+4074X^7+69552X^6+579369X^5 \\
&\quad +2341332X^4+4335596X^3+3032208X^2+524160 \\
&= (X+14)(X+26)(X+4)(3+X)(X+1) \\
&\quad \left(X^3+60X^2+491X+120\right); \\
10!P_{10}(X) &= X^{10}+135X^9+6630X^8+154350X^7+1857513X^6 \\
&\quad +11744775X^5+38049920X^4+57773700X^3 \\
&\quad +36290736X^2+6531840X \\
&= X(X+1)\ R(X).
\end{aligned}
$$

In the last example, $R(X)$ is an irreducible polynomial given by

$$R(x) = X^8 + 134\,X^7 + 6496\,X^6 + 147854\,X^5 + 1709659\,X^4 + 10035116\,X^3 + 28014804\,X^2 + 29758896\,X + 6531840.$$

The initial motivation for this work was the following question:

**Question**

*Does there exist $m \geq 0$, such that $P_m(i) = 0$?*

Considering $i$ as a root of unity, what about the values $P_m(\zeta)$ for root of unities $\zeta$ of general order $N$? Note that in the case $N = 2$ due to Euler we already have that

$$(X + 1) \mid P_m(X) \text{ for infinitely many } m.$$

Note also that the Lehmer's conjecture is equivalent to

$$P_m(-24) \neq 0 \qquad \text{for all} \qquad m \geq 0.$$

Let $N$ be a natural number. Let $\Phi_N(X)$ be the $N$-th cyclotomic polynomial:

$$\Phi_N(X) := \prod_{\substack{1\le k\le N\\ (k,N)=1}} (X - e^{2\pi ik/N})$$

The polynomial $\Phi_N(X)$ is irreducible of degree $\varphi(N)$.

The following result was obtained jointly with Heim and Neuhauser:

**Theorem**

*There is no pair of positive integers $(N, m)$ with $N \ge 3$ such that $\Phi_N(X) \mid P_m(X)$.*

The theorem is equivalent to $P_m(\zeta) \neq 0$ for any root of unity $\zeta$ of order $N \ge 3$.

It maybe worth to mention, that although the proof does not reveal much about the distribution of the roots of $P_m(X)$ in the complex plane, it reveals a very interesting property of these roots modulo $p$ for every prime number $p$. Namely, it shows that if $m = p\ell + r$, where $\ell = \lfloor m/p \rfloor$ and $r = m - p\lfloor m/p \rfloor \in \{0, 1, \ldots, p-1\}$, then

$$A_m(X) \equiv Q_{r,p}(X)(X(X^{p-1} - 1))^{\ell} \pmod{p},$$

where $Q_{r,p}(X)$ is a polynomial of degree $r$. In particular, the roots of $A_m(X)$ modulo $p$ are always among the roots of

$$X(X^{p-1} - 1) \prod_{1 \le r \le p-1} Q_r(X)$$

a polynomial of bounded degree $p(p+1)/2$. Furthermore, the splitting field of $A_m(X)$ over the finite field $\mathbb{F}_p$ with $p$ elements is of degree at most $p - 1$ no matter how large $m$ is. This is certainly a very surprising phenomenon and we do not have an explanation for such regularity.

The polynomials $Q_{r,p}(X)$ play an important role in our proof. Our proof proceeds to show that if there is $N \geq 3$ such that $P_m(\zeta) = 0$ for some root of unity $\zeta$ of order $N$, then $N$ must be even. Then a multiple of 3. Then of 5. And so on, which of course is impossible. The proof proceeds by induction. For the induction step, we need to show that if $p$ is a prime and $q \mid N$ for all primes $p < q$, then also $p \mid N$. For this, we show that none of the polynomials $Q_{r,p}(X) \pmod{p}$ has an irreducible factor of degree $d$ such that $p^d - 1$ is a multiple of $N$. When $p$ is small ($p \leq 11$), we show this by computing all polynomials $Q_{r,p}(X)$ and their irreducible factors modulo $p$. For $p \geq 13$, we appeal to general methods of analytic number theory (for $p \geq 5 \times 10^9$). Finally a computation for $p$ in the intermediary range $[13, 5 \cdot 10^9]$ proves our theorem.

## The work-horse lemma

From now on, $N \geq 3$ is an integer and $\zeta$ is a root of unity of order $N$. Throughout the paper $p$ and $q$ are prime numbers.

**Lemma**

*Let $Q(X) \in \mathbb{Z}[X]$. Let $p$ be a prime and $\zeta$ be a root of unity of order $N \geq 3$. Assume that $k, a, M_1, \ldots, M_k$ are positive integers, such that:*

(i) $p \nmid N$;

(ii) $N \nmid M_i$ for $i = 1, \ldots, k$;

(iii) Modulo $p$ we have $Q(X) \mid \left(X(X^{M_1} - 1) \cdots (X^{M_k} - 1)\right)^a$.

*Then, $Q(\zeta) \neq 0$.*

Condition (iii) tells us that

$$\Big(X(X^{M_1}-1)\cdots(X^{M_k}-1)\Big)^a = Q(X)R(X)+pS(X) \quad (5)$$

for some polynomials $R(X), S(X) \in \mathbb{Z}[X]$. Assuming that $Q(\zeta)=0$, we evaluate equation (5) in $X=\zeta$ getting

$$(\zeta(\zeta^{M_1}-1)\cdots(\zeta^{M_k}-1))^a = pS(\zeta). \quad (6)$$

The algebraic integer $\zeta_i := \zeta^{M_i}$ is a root of unity of order

$$N_i = N/\gcd(N, M_i) > 1$$

for $i=1,\ldots,k$ by condition (ii). Taking norms over $\mathbb{K}=\mathbb{Q}(\zeta)$, we get

$$(N_{\mathbb{K}/\mathbb{Q}}(\zeta))^a \prod_{i=1}^{k}(N_{\mathbb{K}/\mathbb{Q}}(\zeta_i-1))^a = N_{\mathbb{K}/\mathbb{Q}}(pS(\zeta)). \quad (7)$$

In the left–hand side of (7), we have $N_{\mathbb{K}/\mathbb{Q}}(\zeta) = \pm 1$, and

$$N_{\mathbb{K}/\mathbb{Q}}(\zeta_i - 1) = \pm(\Phi_{N_i}(1))^{\varphi(N)/\varphi(N_i)}, \qquad \text{for} \quad i = 1, \ldots, k.$$

Hence, we get

$$\pm \prod_{i=1}^{k} \Phi_{N_i}(1)^{a_i} = p^{\varphi(N)} S, \tag{8}$$

where $a_i = a\,\varphi(N)/\varphi(N_i)$ for $i = 1, \ldots, k$ and $S = N_{\mathbb{K}/\mathbb{Q}}(S(\zeta))$ is an integer. The above relation is impossible since the left–hand side is divisible only by primes dividing $N_i$ for $i = 1, \ldots, k$; hence, $N$, whereas by (i), $p$ is not a factor of $N$. Here, we used the well-known fact that for every integer $m > 1$, $\Phi_m(1)$ is an integer whose prime factors divide $m$.

Further we need the following fact.

**Lemma**

*If $p \geq 2$ is prime, then*

$$p!P_p(X) \equiv X(X^{p-1} - 1) \pmod{p}.$$

**Proof.**

Note that $P_m(x)$ is an integer valued polynomial. Hence,

$$p!P_p(k) \equiv 0 \pmod{p}$$

for all $k \in \mathbb{Z}$. It follows that the polynomial $p!P_p(X)$ has roots modulo $p$ at all positive integers $k$. Hence, all residue classes modulo $p$ are roots of $p!P_p(X)$. Since $p!P_p(X)$ is monic of degree $p$, it follows that

$$p!P_p(X) \equiv \prod^{p-1}(X - k) \equiv X(X^{p-1} - 1) \pmod{p}.$$

## The strategy of the proof

Let $A_m(X) = m!P_m(X)$, then $A_0(X) = 1$, $A_1(X) = X$, and

$$A_m(X) = X\left(\sum_{k=1}^{m} \sigma(k)(m-1)\cdots(m-k+1)A_{m-k}(X)\right), \qquad m \geq 2.$$

In particular, $A_m(X) \in \mathbb{Z}[X]$.

Let us look at $A_m(X)$ modulo 2. Since $\sigma(2) = 3 \equiv 1 \pmod 2$ and $2 \mid m(m-1)$ for all $m \geq 1$, we only have the recurrence

$$A_m(X) \equiv X\,(A_{m-1}(X) + (m-1)A_{m-2}(X)) \qquad \text{for all} \qquad m \geq 1.$$

In particular, if $m$ is odd then $2 \mid m-1$ and

$$A_m(X) \equiv XA_{m-1}(X) \pmod 2,$$

while if $m$ is even then

$$A_m(X) \equiv X(A_{m-1}(X)+A_{m-2}(X)) \equiv X(X-1)A_{m-2}(X) \pmod 2.$$

In particular, writing $m = 2\ell + r$, $\ell = \lfloor m/2 \rfloor$, $r = m - 2\lfloor m/2 \rfloor$, and putting $Q_0(X) := 1$, $Q_1(X) := X$, we get that

$$\begin{aligned} A_m(X) &\equiv A_{2\ell+r}(X) \equiv Q_r(X)A_{2\ell}(X) \\ &\equiv Q_r(X)(X(X-1))A_{2(\ell-1)}(X) \equiv \cdots \\ &\equiv Q_r(X)(X(X-1))^{\ell}A_0(X) \equiv X^{r+\lfloor m/2 \rfloor}(X-1)^{\lfloor m/2 \rfloor} \pmod 2 \end{aligned}$$

Assume now that $P_m(\zeta) = 0$ for some root of unity $\zeta$ of order $N > 1$. Then $A_m(\zeta) = 0$. Assuming that $N$ is odd, we have that $N \geq 3$. Lemma 3 gives a contradiction. Hence, $2 \mid N$.

Let us record this.

**Lemma**

*If $P_m(\zeta) = 0$ for some $m \geq 1$ and root of unity $\zeta$ of order $N \geq 3$, then $N$ is even.*

There is nothing mysterious about the prime $p = 2$ in the above argument.

Let's try the prime $p = 3$. That is, we reduce the recurrence for the sequence of general term $A_m(X)$ modulo 3. Since $3 = \sigma(2)$, and $3 \mid (m-1)(m-2)(m-3)$ for all $m \geq 3$, we get that

$$A_m(X) \equiv X(A_{m-1}(X) + 4(m-1)(m-2)A_{m-3}(X)) \pmod 3, \quad m \geq 2.$$

In particular,

$$A_m(X) \equiv \begin{cases} XA_{m-1}(X) & \pmod 3 \quad m \not\equiv 0 \pmod 3, \\ X(A_{m-1}(X) + 2A_{m-3}(X)) & \pmod 3 \quad m \equiv 0 \pmod 3. \end{cases}$$

We then get

$$\begin{aligned} A_{3\ell+1}(X) &\equiv XA_{3\ell}(X) \pmod 3, \\ A_{3\ell+2}(X) &\equiv XA_{3\ell+1}(X) \equiv X^2 A_{3\ell}(X) \pmod 3, \\ A_{3\ell+3}(X) &\equiv X(A_{3\ell+2}(X) + 2A_{3\ell}(X)) \pmod 3 \end{aligned}$$

$$\equiv X(X^2 - 1)A_{3\ell}(X) \pmod 3.$$

Recursively, we get that if we put
$Q_0(X) := 1,\ Q_1(X) := X,\ Q_2(X) := X^2$, $m = 3\ell + r$,
$\ell = \lfloor m/3 \rfloor,\ r = m - 3\lfloor m/3 \rfloor \in \{0, 1, 2\}$, then

$$\begin{aligned} A_m(X) &\equiv Q_r(X)A_{3\ell}(X) \equiv Q_r(X)(X(X^2-1))^2 A_{3\ell-3}(X) \equiv \cdots \\ &\equiv Q_r(X)(X(X^2-1))^{\ell} \pmod 3. \end{aligned}$$

Hence,

$$A_m(X) \equiv X^{r+\lfloor m/3 \rfloor}(X^2-1)^{\lfloor m/3 \rfloor} \pmod 3. \tag{9}$$

Assume now that $P_m(\zeta) = 0$ for some root of unity $\zeta$ of order $N$. Then $A_m(\zeta) = 0$. Assume $3 \nmid N$. Lemma 3 with $Q(X) = A_m(X)$, $p = 3,\ a = r + \lfloor m/3 \rfloor,\ k = 1,\ M_1 = 2$ gives a contradiction. Note that $N \nmid M_1$ because $N \geq 4$ (since $N \geq 3$ is even). This contradiction shows that $3 \mid N$.

Let us record what we proved.

**Lemma**

*If* $P_m(\zeta) = 0$ *for some* $m \geq 1$ *and root of unity* $\zeta$ *of order* $N \geq 3$*, then* $3 \mid N$*.*

Let us continue for a few more steps. We now take $p = 5$ and consider the recurrence for $A_m(X)$ modulo 5. As before, we obtain the recursion formula:

$$\begin{aligned} A_m(X) \equiv\ & X\,(A_{m-1}(X) + 3\,(m-1)\,A_{m-2}(X) \\ & +4\,(m-1)\,(m-2)\,A_{m-3}(X) \\ & +7\,(m-1)\,(m-2)\,(m-3)\,A_{m-4}(X) \\ & +6\,(m-1)\,(m-2)\,(m-3)\,(m-4)\,A_{m-5}(X)) \pmod 5. \end{aligned}$$

Treating the cases $m = 5\ell + r$, $r \in \{1, 2, 3, 4, 5\}$, we get

$$\begin{aligned}
A_{5\ell+1}(X) &\equiv XA_{5\ell}(X) \pmod 5;\\
A_{5\ell+2}(X) &\equiv \left(X^2 + 3X\right) A_{5\ell}(X) \equiv X\,(X+3)\,A_{5\ell}(X) \pmod 5;\\
A_{5\ell+3}(X) &\equiv X\left(X^3 + 4\,X^2 + 3X\right) A_{5\ell}(X)\\
&\equiv X\,(X+1)\,(X+3)\,A_{5\ell}(X) \pmod 5;\\
A_{5\ell+4}(X) &\equiv X\left(X^3 + 3\,X^2 + 4\,X + 2\right) A_{5\ell}(X)\\
&\equiv X\,(X+1)\,(X+3)\,(X+4)\,A_{5\ell}(X) \pmod 5;\\
A_{5\ell+5}(X) &\equiv \left(X\left(X^4 - 1\right)\right) A_{5\ell}(X) \pmod 5.
\end{aligned}$$

Thus, putting

$$\begin{aligned} Q_0(X) &= 1, \quad Q_1(X) = X, \quad Q_2(X) = X(X+3), \\ Q_3(X) &= X(X+1)(X+3), \quad Q_4(X) = X(X+1)(X+3)(X+4), \end{aligned}$$

we have that if we write

$$r = m - 5\lfloor m/5 \rfloor \in \{0,1,2,3,4\},$$

then

$$A_m(X) \equiv Q_r(X)(X(X^4-1))^{\lfloor m/5 \rfloor} \pmod 5.$$

Note that $Q_r(X) \mid X(X^4-1)$. Assume now that $5 \nmid N$. We then apply Lemma 1 with $Q(X) = A_m(X)$, $p = 5,\ a = \lfloor m/5 \rfloor + 1,\ k = 1,\ M_1 = 4$ and note that $N \nmid M_1$ since $N \geq 6$ (because $N$ is a multiple of 6), and we obtain a contradiction.

Let us record what we proved.

**Lemma**

*If* $P_m(\zeta) = 0$ *for some* $m \geq 1$ *and root of unity* $\zeta$ *of order* $N$*, then* $5 \mid N$*.*

We apply the same program for $p=7$. We skip the details and only show the results. For $r \in \{0,1,2,3,4,5,6\}$, we get $Q_0(X)=1$,

$$\begin{aligned} Q_1(X) &= X, \quad Q_2(X)=X(X+3), \quad Q_3(X)=X(X+1)^2, \\ Q_4(X) &= X^2(X+1)(X+3), \quad Q_5(X)=X(X+3)(X+6)(X^2+1), \\ Q_6(X) &= X(X+1)(X+3)(X^3+6X^2+6X+4), \end{aligned}$$

where the factors shown above are irreducible modulo 7. Since $X^2+1 \mid X^4-1$ and $X^3+6X^2+6X+4 \mid X^{7^3-1}-1$, and every root of $Q_r(X)$ is of multiplicity at most 2, it follows that

$$Q_r(X) \mid \left(X(X^6-1)(X^4-1)(X^{342}-1)\right)^2.$$

Further, writing $m=7\ell+r$, where $\ell=\lfloor m/7\rfloor$ and $r=m-7\lfloor m/7\rfloor$, we get that

$$A_m(X) \equiv Q_r(X)\left(X(X^6-1)\right)^{\lfloor m/7\rfloor} \pmod 7.$$

Thus, modulo 7,

$$A_m(X) \mid \Big(X(X^4-1)(X^6-1)(X^{342}-1)\Big)^a,$$

where $a = \lfloor m/7 \rfloor + 2$. Assume now that $7 \nmid N$. We apply Lemma 1 with $Q(X) = A_m(X)$,
$p = 7,\ a = \lfloor m/7 \rfloor + 2,\ k = 3,\ M_1 = 4,\ M_2 = 6,\ M_3 = 342.$
Since $30 \mid N$, it follows that $N \nmid M_i$ for $i = 1, 2, 3$. Lemma 1 gives a contradiction.

Thus, we proved the following.

**Lemma**

*If $P_m(\zeta) = 0$ for some $m \geq 1$ and root of unity $\zeta$ of order $N \geq 3$, then $7 \mid N$.*

For $p = 11$, we have

$$
\begin{aligned}
Q_0(X) &= 1, \quad Q_1(X) = X, \quad Q_2(X) = X(X+3),\\
Q_3(X) &= X(X+1)(X+8),\\
Q_4(X) &= X(X+1)(X+3)^2,\\
Q_5(X) &= X(X+3)(X+6)(X^2+10X+8),\\
Q_6(X) &= X(X+1)(X+10)(X^3+X^2+5X+1),\\
Q_7(X) &= X(X+2)(X+3)(X+8)(X+9)(X^2+8X+6),\\
Q_8(X) &= X(X+1)(X+3)(X+6)(X+10)(X^3+9X^2+7X+2),\\
Q_9(X) &= X(X+1)(X+3)^2(X+4)^2(X+10)(X^2+6X+1),\\
Q_{10}(X) &= X(X+1)(X+8)(X^7+5X^6+10X^5+6X^3+10X^2+X
\end{aligned}
$$

All factors shown are irreducible modulo 11. We note that the multiplicity of any root of $Q_r(X)$ is at most 2. Further, the irreducible factors of the above polynomials which are not linear are of of degrees $2, 3$, or 7 over $\mathbb{F}_{11}$.

Hence,

$$Q_r(X) \mid \left(X(X^{11-1}-1)(X^{11^2-1}-1)(X^{11^3-1}-1)(X^{11^7-1}-1)\right)^2.$$

Writing $m = 11\ell + r$ with $r \in \{0, 1, \ldots, 10\}$, where $\ell = \lfloor m/11 \rfloor$, we get that

$$A_m(X) \equiv Q_r(X)\left(X(X^{10}-1)\right)^{\lfloor m/11 \rfloor} \pmod{11},$$

so modulo 11, $A_m(X)$ divides

$$\left(X(X^{10}-1)(X^{11^2-1}-1)(X^{11^3-1}-1)(X^{11^7-1}-1)\right)^a,$$

where $a = \lfloor m/11 \rfloor + 2$. Assume now that $11 \nmid N$. Then we apply Lemma 3 with $Q(X) = A_m(X)$, $p = 11,\ a = \lfloor m/11 \rfloor + 2$, $k = 4$, $M_1 = 11 - 1 = 10,\ M_2 = 11^2 - 1 = 120,\ M_3 = 11^3 - 1 = 1330,\ M_4 = 11^7 - 1 = 19487170$. Since $2 \cdot 3 \cdot 5 \cdot 7 \mid N$, we get that $N \nmid M_i$ for $i = 1, 2, 3, 4$. Now Lemma 1 yields to a contradiction.

Thus, we record what we proved.

**Lemma**

*If* $P_m(\zeta) = 0$ *for some* $m \geq 1$ *and root of unity* $\zeta$ *of order* $N \geq 3$*, then* $11 \mid N$*.*

## The case of the general prime $p$

Assume now that $p \geq 13$ and that we proved that $q \mid N$ holds for all primes $q < p$. We would like to prove that $p \mid N$. For this, we compute for $r \in \{0, \ldots, p-1\}$,

$$Q_r(X) \equiv \prod_{i=1}^{s_r} Q_{r,i}(X)^{\alpha_{r,i}} \pmod{p},$$

where $Q_{r,i}(X)$ are distinct irreducible factors of $Q_r(X)$ modulo $p$. Assume $Q_{r,i}(X)$ is of degree $d_{r,i}$. Let

$$\mathcal{D}_p = \left\{ d_{r,i} : 1 \leq i \leq s_r,\ 1 \leq r \leq p-1 \right\}.$$

Let $\alpha = \max\{\alpha_{r,i} : 1 \leq i \leq s_r,\ 1 \leq r \leq p-1\}$.

Then, writing $m = p\ell + r$ with $r \in \{0, 1, \ldots, p-1\}$, we have

$$A_m(X) \equiv Q_r(X)\,(A_p(X))^{\ell} \pmod{p}.$$

This follows by induction from the recursion formula

$$\begin{aligned} A_{p\ell+r}(X) &\equiv X\left(\sum_{k=1}^{r} \sigma(k)\,(p\ell+r-1)\cdots(p\ell+r-k+1)\,A_{p\ell+r-k}(X \\ &\equiv X\left(\sum_{k=1}^{r} \sigma(k)\,(r-1)\cdots(r-k+1)\,A_{r-k}(X)\right)(A_p(X))^{\ell} \\ &\equiv A_r(X)\,(A_p(X))^{\ell} \pmod{p}. \end{aligned}$$

By using Lemma 2 we thus get that

$$A_m(X) \equiv Q_r(X) \left( X(X^{p-1} - 1) \right)^{\lfloor m/p \rfloor} \pmod{p}.$$

Hence modulo $p$, $A_m(X)$ divides

$$\left( X \prod_{d \in \mathcal{D}_p} (X^{p^d - 1} - 1) \right)^a,$$

where we can take $a := \lfloor m/p \rfloor + \alpha$.

Assume that $p \nmid N$. We can then apply Lemma 1 with $Q(X) = A_m(X)$, the prime $p$, the number $a$, $k = \#\mathcal{D}_p$ and $M_j = p^{d_j} - 1$ for $j = 1, \ldots, k$, where $\mathcal{D}_p = \{d_1, \ldots, d_k\}$. We need to ensure that $N \nmid M_j$ for all $j = 1, \ldots, k$. We know that $\prod_{q<p} q \mid N$. Thus, it suffices to show that $\prod_{q<p} q$ is not a divisor of $M_j$ for any $j = 1, \ldots, k$. Until now, namely for the primes $p \in \{2, 3, 5, 7, 11\}$, we checked that this was case by case. To complete the induction, it suffices to show the following lemma.

**Lemma**

*If $p \geq 13$, there does not exist a positive integer $1 \leq d \leq p - 1$ such that*

$$p^d - 1 \equiv 0 \pmod{\prod_{q<p} q}.$$

For $p = 11$, this is not true since

$$11^6 - 1 \equiv 0 \pmod{2 \cdot 3 \cdot 5 \cdot 7}.$$

Assume that we proved the lemma. The above argument shows that if $q \mid N$ for all $q < p$ and $p \geq 13$, then $p \mid N$. Replacing $p$ by the next prime, we get, by induction, that $N$ is divisible by all possible primes, which is a contradiction.
So, it suffices to prove Lemma 10. This will be proven by analytic methods.

Assume $p \geq 13$ and for some $d \leq p-1$, we have $q \mid p^d - 1$ for all primes $q < p$. Then $d$ is divisible by the $o_q(p)$, which is the order of $p$ modulo $q$. We split $q < p$ into two subsets:

$$Q_1 = \{q < p : o_q(p) \leq p^{1/2}\}, \qquad Q_2 = \{q < p : o_q(p) > p^{1/2}\}.$$

For $Q_1$, we have

$$\prod_{q \in Q_1} q \;\Big|\; \prod_{\substack{e \mid d \\ e \leq p^{1/2}}} (p^e - 1).$$

The above leads to

$$\sum_{q \in Q_1} \log q < \sum_{\substack{e \mid d \\ e \leq p^{1/2}}} \log(p^e - 1) < \log p \sum_{\substack{e \mid d \\ e \leq p^{1/2}}} e \leq p^{1/2} \tau_1(d) \log p.$$

Here and in what follows we use $\tau_1(d)$ for the number of divisors of $d$ which are $\le p^{1/2}$. For $Q_2$, let $e \mid d$ with $e > p^{1/2}$ and assume that $q \le p-1$ is such that $o_p(q) = e$. Then $e \mid q-1$. Thus, $q \equiv 1 \pmod{e}$. Since $q \le p-1$, it then follows, by counting the number of positive integers less than or equal to $p-1$ which are larger than 1 in the arithmetic progression $1 \pmod{e}$ and even ignoring the information that they should also be prime, it follows that the number of choices for such $q$ is at most $(p-1)/e < p^{1/2}$. This was for a fixed divisor $e$ of $d$ which exceeds $p^{1/2}$. Thus,

$$\sum_{q\in Q_2} \log q \le p^{1/2} \left( \sum_{\substack{e|d \\ e>p^{1/2}}} 1 \right) \log p < p^{1/2}\tau_2(d) \log p,$$

where $\tau_2(d)$ is the number of divisors of $d$ which are $> p^{1/2}$.

Thus letting $\theta$ be the Chebyshev function, we get

$$\theta(p) := \sum_{q<p} \log p \leq p^{1/2}\tau(d) \log p,$$

where $\tau(d) = \tau_1(d) + \tau_2(d)$ is the total number of divisors of $d$. Assume now that $p > 10^9$. A theorem of Rosser, Schoenfeld shows that

$$\sum_{q \leq p} \log q > 0.99\ p.$$

Further,

$$\frac{\tau(d)}{d^{1/3}} = \prod_{q^{\alpha_q} \| d} \left( \frac{\alpha_q + 1}{q^{\alpha_q/3}} \right).$$

The factors on the right above are all $< 1$ if $q \geq 11$, just because in that case $q^\alpha \geq 11^\alpha \geq (\alpha + 1)^3$ for all $\alpha \geq 1$.

For $q \in \{2, 3, 5, 7\}$ and positive integers $\alpha$, we have that

$$\frac{\alpha+1}{2^{\alpha/3}} \le 2, \qquad \frac{\alpha+1}{3^{\alpha/3}} < 1.45, \qquad \frac{\alpha+1}{5^{\alpha/3}} < 1.17, \qquad \frac{\alpha+1}{7^{\alpha/3}} < 1.05.$$

This analysis and the fact that $2 \times 1.45 \times 1.17 \times 1.05 < 1.79$ shows that

$$\tau(d) < 1.79\, d^{1/3} < 1.79\, p^{1/3}.$$

We thus get that

$$0.99\, p < \sum_{q \le p} \log q \le (p^{1/2}\tau(d) + 1) \log p < (1.79 p^{5/6} + 1) \log p,$$

and inequality which implies that $p < 5 \cdot 10^9$. So, we have obtained the following result.

**Lemma**

*Lemma 10 holds for $p > 5 \cdot 10^9$.*

It remains to cover the range $[13, 5 \cdot 10^9]$ for $p$. In a few minutes with Mathematica we compute for all $p \in [13, 30000]$, that

$$\mathrm{lcm}[o_p(q) : q < p] > p,$$

so we may assume that $p > 30000$. In the interval $[100, 1000]$ there are 27 primes numbers $q$ such that $2q + 1$ is also prime. They are the following:

$$113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431,$$
$$443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953$$

Let $p > 30000$ and consider one of the primes $2q + 1$ with $q$ in the above set. The order of $p$ modulo $2q + 1$ is a divisor of $2q$, so it is 1, 2 or a multiple of $q$. If it is 1 or 2, then $q$ divides $p - 1$ or $p + 1$. Since $q > 100$ and $p < 10^{10}$, there are at most four values of $q$ for which it can be a divisor of $p - 1$ and at most four values of $q$ for which it can be a divisor of $p + 1$. Thus,

$$\mathrm{lcm}[o_p(q) : q < p] > 100^{19} = 10^{38} > 10^{10} > p,$$

which finishes the proof.

THANK YOU!