A generalisation of a congruence due to Vantieghem only holding for primes

L J P Kilford*

October 30, 2018

Abstract

In this note we present a family of congruences which hold if and only if a natural number \( n \) is prime.

The subject of primality testing has been in the mathematical and general news recently, with the announcement [AKS02] that there exists a polynomial-time algorithm to determine whether an integer \( p \) is prime or not.

There are older deterministic primality tests which are less efficient; the classical example is Wilson’s Theorem, that

\[
(n - 1)! \equiv -1 \mod n \text{ if and only if } n \text{ is prime.}
\]

Although this is a deterministic algorithm, it does not provide a workable primality test because it requires much more calculation than trial division.

This note provides another congruence satisfied by primes and only by primes; it is a generalisation of previous work. In Guy [Guy94], problem A17, the following result due to Vantieghem [Van91] is quoted:

**Theorem 1 (Vantieghem, [Van91]).** Let \( n \) be a natural number greater than 2. Then \( n \) is prime if and only if

\[
\prod_{d=1}^{n-1} (1 - 2^d) \equiv n \mod (2^n - 1).
\]

In this note, we will generalise this result to obtain the following theorem:

**Theorem 2.** Let \( m \) and \( n \) be natural numbers greater than 2. Then \( n \) is prime if and only if

\[
\frac{1}{2} : \prod_{d=1}^{n-1} (1 - m^d) \equiv n \mod \frac{m^n - 1}{m - 1}.
\]

**Proof.** We follow the method of Vantieghem, using a congruence satisfied by cyclotomic polynomials.

*Address: Mathematics 253-37, California Institute of Technology, Pasadena CA 91125.*
Lemma 3 (Vantieghem). Let $m$ be a natural number greater than 1 and let $\Phi_m(X)$ be the $m^{th}$ cyclotomic polynomial. Then

$$\prod_{\substack{d=1 \\ (d,m)=1}}^{m} (X - Y^d) \equiv \Phi_m(X) \mod \Phi_m(Y) \text{ in } \mathbb{Z}[X,Y].$$

Proof of Lemma 3. We can write

$$\prod_{\substack{d=1 \\ (d,m)=1}}^{m} (X - Y^d) - \Phi_m(X) = f_0(Y) + f_1(Y)X + f_2(Y)X^2 + \cdots$$

where the $f_i$ are polynomials over $\mathbb{Z}$.

Let $\zeta$ be a primitive $m^{th}$ root of unity. Now, if $Y = \zeta$ then we see that the left hand side of this expression is identically 0 in $X$.

This implies that the $f_i$ are zero at every $\zeta$ and every $i$. Therefore, we have $f_i(Y) \equiv 0 \mod \Phi_m(Y)$, which is enough to prove the Lemma.

If $p$ is prime, then we have that $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Therefore, if we set $m = p$ in the Lemma, we find that

$$\prod_{d=1}^{p-1} (X - Y^d) \equiv X^{p-1} + X^{p-2} + \cdots + X + 1 \mod (Y^{p-1} + \cdots + 1).$$

We now set $X = 1$ and $Y = m$, to get

$$\prod_{d=1}^{p-1} (1 - m^d) \equiv p \mod \frac{m^p - 1}{m - 1};$$

this proves that if $p$ is prime then the congruence holds.

We now prove the converse, by supposing that the congruence $\pmod{p}$ holds, and that $p$ is not prime. Therefore $p$ is composite, and hence has a smallest prime factor $q$. We write $p = q \cdot a$; now $q \leq a$, and also $p \leq a^2$.

Now we have that $m^a - 1$ divides $m^p - 1$ and $m^a - 1$ divides the product $\prod_{d=1}^{a-1} (m^d - 1)$. By combining this with the congruence $\pmod{p}$ in the Theorem, this implies that $(m^a - 1)/(m - 1)$ divides $p$. Therefore we have

$$\frac{m^a - 1}{m - 1} \leq p \leq a^2.$$

Now this is only possible, when $m \geq 3$, for $m = 3$ and $a = 2$. It can be easily checked that the congruence does not hold in this case, so we have proved the Theorem.

Guy also asks if there is a relationship between the congruence given by Vantieghem and Wilson’s Theorem. The following theorem gives an elementary congruence similar to that of Vantieghem between a product over integers and a cyclotomic polynomial. It is in fact equivalent to Wilson’s Theorem.
Theorem 4. Let $m$ be a natural number greater than 2. Then $m$ is prime if and only if

$$\diamondsuit : \Phi_m(X) \equiv F(X) := \prod_{i=1}^{m-1} (X - i - 1) + 1 \mod m.$$ 

Proof of Theorem 4. Firstly, we prove that if $m$ is not prime, the congruence $\diamondsuit$ in Theorem 4 does not hold.

Recall that $\phi(m)$ is defined to be Euler's totient function; the number of integers in the set $\{1, \ldots, m\}$ which are coprime to $m$.

The coefficient of $X^{\phi(m) - 1}$ on the right-hand side is given by the sum

$$- \sum_{i=1}^{m-1} i + 1 = -\phi(m) - \sum_{(i,m)=1}^{m-1} i \equiv -\phi(m) \mod m;$$

the final inequality holds because if $(i, m) = 1$ then $(-i, m) = 1$ as well, and the case $i \equiv -i \mod m$ does not occur because then we have $2i \equiv 0 \mod m$ and therefore $2 \equiv 0 \mod m$ which is false because $m$ is greater than 2.

We now use some theorems to be found in a paper by Gallot \[Gal01\] (Theorem 1.1 and Theorem 1.4):

Theorem 5. Let $p$ be a prime and $m$ be a natural number.

1. The following relations between cyclotomic polynomials hold:

$$\Phi_{pm}(x) = \Phi_m(x^p) \text{ if } p \mid m$$

$$\Phi_{pm}(x) = \frac{\Phi_{nm}(x^p)}{\Phi_m(x)} \text{ if } p \nmid m.$$ 

2. If $m > 1$ then

$$\Phi_n(1) = p \text{ if } n \text{ is a power of a prime } p$$

$$\Phi_n(1) = 1 \text{ otherwise.}$$

From these results, we see that if $m$ is not a prime power then we have $\Phi_n(1) \equiv 1 \mod m$, and the right hand side of the congruence $\diamondsuit$ when evaluated at $X = 1$ is

$$1 + \prod_{(i,m)=1}^{m-1} - i.$$ 

We see that this is not congruent to 1 mod $m$ because the product is over those $i$ which are coprime to $m$, so the product does not vanish modulo $m$.

If $m$ is a prime power $p^n$, then we see from Theorem 5.1 that $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$; in particular, we see that the coefficient of $x^{\phi(p^n) - 1}$ is 0, which differs from the coefficient of $x^{\phi(p^n) - 1}$ in $F(X)$. 

3
Therefore, if $m$ is not prime then the congruence does not hold. We now show that if $m$ is prime, the congruence holds.

If $m$ is prime then $\Phi_m(x) = x^{m-1} + x^{m-2} + \cdots + x + 1$. Let us consider the polynomials $\Phi_m(X + 1)$ and $F(X + 1)$. Now, modulo $m$ we have

$$\Phi_m(X + 1) = X^{m-1} \text{ and } F(X + 1) = \prod_{\substack{i=1 \atop (i,m)=1}}^{m-1} (X - i) + 1.$$ 

Now if $x \not\equiv 0 \pmod{m}$, then we see that $\Phi_m(x) \equiv 1$ and that $F(x + 1) \equiv 1$, because the product vanishes.

And if we have $x = 0$, then $\Phi_m(x) = 0$ and, by Wilson’s Theorem, $F(0) \equiv (m-1)! + 1 \equiv 0 \pmod{m}$.

Therefore we have proved the Theorem.

References

[AKS02] M. Agrawal, N. Kayal, and N. Saxena, PRIMES is in $P$, 
\url{http://www.cse.iitk.ac.in/users/manindra/primality.pdf} 
August 2002.

[Gal01] Yves Gallot, Cyclotomic Polynomials and prime numbers, 
\url{http://perso.wanadoo.fr/yves.gallot/papers/index.html} 
2001.

[Guy94] Richard K. Guy, Unsolved problems in number theory, second ed., 
Problem Books in Mathematics, Springer-Verlag, New York, 1994, Unsolved Problems in Intuitive Mathematics, I.

[Van91] E. Vantieghem, On a congruence only holding for primes, Indag. Math. (N.S.) 2 (1991), no. 2, 253–255.