We present a family of congruences which hold if and only if a natural number \( n \) is prime.

2000 Mathematics Subject Classification: 11A51, 11A07.

The subject of primality testing has been in the mathematical and general news recently, with the announcement [1] 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

\[
(n-1)! \equiv -1 \mod n
\]

if and only if \( n \) 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 family of congruences satisfied by primes and only by primes; it is a generalization of previous work. They could be used as examples of primality tests for students studying elementary number theory.

In Guy [3, Problem A17], the following result due to Vantieghem [4] is quoted as follows.

**Theorem 1** (Vantieghem [4]). Let \( n \) be a natural number greater than 1. 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 generalize this result to obtain the following theorem.

**Theorem 2.** Let \( m \) and \( n \) be natural numbers greater than 1. Then \( n \) is prime if and only if

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

We note that these congruences are also much less efficient than trial division.

**Proof.** We follow the method of Vantieghem, using a congruence satisfied by cyclotomic polynomials.
**Lemma 3** (Vantieghem). Let $m$ be a natural number greater than 1 and let $\Phi_m(X)$ be the $m$th cyclotomic polynomial. Then

$$\prod_{d=1}^{m} (X - Y^d) \equiv \Phi_m(X) \mod \Phi_m(Y) \text{ in } \mathbb{Z}[X,Y]. \tag{4}$$

**Proof of Lemma 3.** We can write

$$\prod_{d=1}^{m} (X - Y^d) - \Phi_m(X) = f_0(Y) + f_1(Y)X + f_2(Y)X^2 + \cdots. \tag{5}$$

(Here 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.

Suppose that the natural number $n$ in Theorem 2 is prime. Let $p := n$. We have that $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Therefore, if we set $m = p$ in Lemma 3, we find that

$$\prod_{d=1}^{p-1} (X - Y^d) \equiv X^{p-1} + X^{p-2} + \cdots + X + 1 \mod (Y^{p-1} + \cdots + 1). \tag{6}$$

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

$$\prod_{d=1}^{p-1} (1 - m^d) \equiv p \mod \frac{m^p - 1}{m - 1}. \tag{7}$$

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

We now prove the converse, by supposing that the congruence (3) 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 $\prod_{d=1}^{p-1} (m^d - 1)$. By combining this with the congruence (3) in Theorem 2, this implies that $(m^a - 1)/(m - 1)$ divides $p$. Therefore we have

$$2^a - 1 \leq \frac{m^a - 1}{m - 1} \leq p \leq a^2. \tag{8}$$

The inequality $2^a - 1 \leq a^2$ forces $a$ to be either 2 or 3; this means that $p \in \{4, 6, 9\}$ and $m \in \{2, 3\}$; one can check by hand that the congruence does not hold in this case, so we have proved Theorem 2.

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. Define the product \( F(X) \) by

\[
F(X) := \prod_{i=1 \atop (i,m)=1}^{m-1} (X - i - 1) + 1. \tag{9}
\]

Then \( m \) is prime if and only if

\[
\Phi_m(X) \equiv F(X) \mod m. \tag{10}
\]

**Proof of Theorem 4.** Firstly, we prove that if \( m \) is not prime, the congruence (10) 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 \( X^{\phi(m)-1} \) in \( F(X) \) is given by the sum

\[
- \sum_{i=1 \atop (i,m)=1}^{m-1} (i + 1) = -\phi(m) - \sum_{i=1 \atop (i,m)=1}^{m-1} i. \tag{11}
\]

We find that the following congruence holds:

\[
-\phi(m) - \sum_{i=1 \atop (i,m)=1}^{m-1} i \equiv -\phi(m) \mod m. \tag{12}
\]

This follows from the following identity:

\[
\sum_{i=1 \atop (i,m)=1}^{m-1} i = \frac{m\phi(m)}{2}. \tag{13}
\]

Because \( m > 2 \), \( \phi(m) \) is divisible by 2, the sum on the left-hand side of (12) is a multiple of \( m \). We now use some theorems to be found in a paper by Gallot [2, Theorems 1.1 and 1.4].

**Theorem 5.** Let \( p \) be a prime and \( m \) a natural number.

1. The following relations between cyclotomic polynomials hold:

\[
\Phi_{pm}(x) = \begin{cases} 
\Phi_m(x^p) & \text{if } p \mid m, \\
\Phi_m(x) & \text{if } p \nmid m.
\end{cases} \tag{14}
\]

2. If \( m > 1 \), then

\[
\Phi_n(1) = \begin{cases} 
p & \text{if } n \text{ is a power of a prime } p, \\
1 & \text{otherwise.}
\end{cases} \tag{15}
\]
From these results, we see that if \( m \) is not a prime power, we then have \( \Phi_n(1) \equiv 1 \mod m \), and \( F(1) \) is given by

\[
1 + \prod_{i=1 \atop (i,m)=1}^{m-1} (-i). \tag{16}
\]

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 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 \( F(X) \).

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 \( \Phi_m(x) = x^{m-1} + x^{m-2} + \cdots + x + 1 \). We consider the polynomials \( \Phi_m(X+1) \) and \( F(X+1) \). Now, modulo \( m \) we have

\[
\Phi_m(X+1) = X^{m-1}, \quad F(X+1) = \prod_{i=1 \atop (i,m)=1}^{m-1} (X - i) + 1. \tag{17}
\]

Now if \( x \neq 0 \mod m \), then we see that \( \Phi_m(x+1) \equiv 1 \) 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, \( F(0) \equiv (m-1)! + 1 \equiv 0 \mod m \).

Therefore we have proved Theorem 4. \( \square \)

REFERENCES


