A Geometric Construction Involving Wilson's Theorem

Kenneth J. Prevot
Metro State University of Denver
Department of Math and CS
Denver, CO 80217-3362

ABSTRACT
A long standing result in number theory is Wilson's Theorem, which states that n is a prime number if and only if $(n-1)! \equiv (-1) \bmod n$. One motivation for this study is to detect some algebraic congruence relations which naturally arise in this number theoretic context, strictly through geometric constructions. Some examples of such congruence relations are presented. Namely, than n is an odd prime if and only if $(n-2)! - n(n-3)/2 \equiv 1 \bmod (n^2 - 2n)$. Also if n is an odd prime, one has $(n-2)((n-1)!)+(n-1) \equiv 1 \bmod (n^2 - 2n)$.

General Terms
Congruence Relations, Number Theory, Geometric Constructions, Prime Numbers, Tilings, Wilson's Theorem

Keywords
Chimney, Sleeve, Wilson's Theorem, Geometric Construction

1. INTRODUCTION
A long standing result in number theory is Wilson"s Theorem [1] which states that n is a prime number if and only if the following congruence relation holds true:

$$(n - 1)! \equiv (-1) mod\ n$$

It is noted that, as a test for whether an integer is prime or not, Wilson's Theorem is not the most efficient [1]. Fermat's Little Theorem would be better, namely: If p is a prime number and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$. This paper is not intended to offer a more efficient check for whether an odd integer is prime or not, but rather to characterize other congruence relations naturally, involving prime numbers, using geometric constructions alone. The geometric construction gives the result of the main theorem, that n is an odd prime if and only if $(n-2)! - n(n-3)/2 \equiv 1 \bmod (n^2 - 2n)$.

2. PRELIMINARY COMPUTATIONS
One first notices that

$$\text{n is prime}$$
$$\Leftrightarrow (n-1)! \equiv (-1) \bmod n$$
$$\Leftrightarrow (n-1)! \equiv (n-1) \bmod n$$
$$\Leftrightarrow (n-2)! \equiv 1\ mod\ n$$
$$\Leftrightarrow n \mid ((n-2)! - 1)$$

Now represent $(n-2)! - 1$ as a rectangle with sides of length $(n-2)$ and $(n-3)!$ along with a deleted unit square notch at the top. See the depiction in the following display.

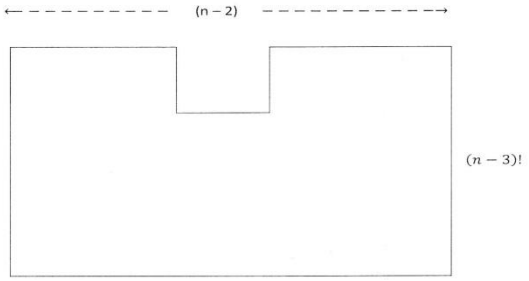

Figure 1: Basic Depiction

In the above depiction in Figure 1, the integer n is an odd prime. Since $n \mid ((n-2)! - 1)$

3. SMALL VALUES OF n
This section considers the first few odd primes to illustrate the geometric patterns.

Case n = 3: This is a vacuous case pictorially for the main theorem mentioned in the introduction. Once checks the formula

$$(3-2)! - 3(3-3)/2 \equiv 1 \bmod (3^2 - 2 \cdot 3)$$
$$\Leftrightarrow 1! - 0 \equiv 1 \bmod 3$$
$$\Leftrightarrow 1 \equiv 1 \bmod 3$$

Case n = 5: The rectangle with sides, one of length $(5-2)$ and the other of length $(5-3)!$, along with a deleted unit square may be depicted in the following Figure 2.

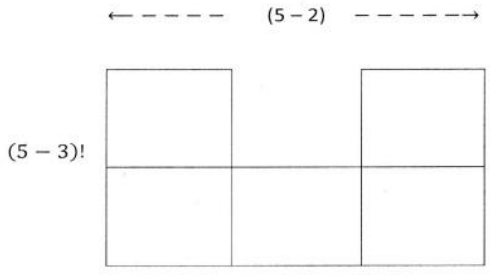

Figure 2: The Case n = 5

Since 5 is prime, the alternate representation of Wilson's Theorem is clear, *i.e.*, $5 \mid (3!-1)$. Furthermore, the equation $\bmod 15 (= 5^2 - 2(5))$ is satisfied.

$$(5-2)! - 5(5-3)/2 = 6 - 5 = 1 \equiv 1 \bmod 15.$$

Case n = 7: Consider the depiction for the case n = 7 in Figure 3.

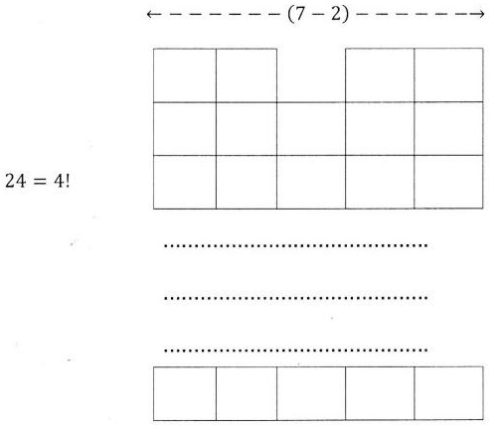

Figure 3: Preparing for n = 7

The details of the analysis will involve constructing strips of area = 7 which fill in the above "notched" rectangle. There will be two basic patterns used to fill in the depiction. One pattern will appear as a chimney, the other will appear as a cross. The sequence of configurations will consist of a chimney pattern, then an inverted chimney, a cross, a chimney pattern, an inverted chimney pattern, and will ultimately terminate in a chimney pattern. Each chimney pattern (and the inverted chimney pattern) will have area equal to 14 and each cross pattern will have an area equal to 7.

An illustration of the chimney and cross patterns within the notched rectangle for the case n = 7 follows. See Figure 4.

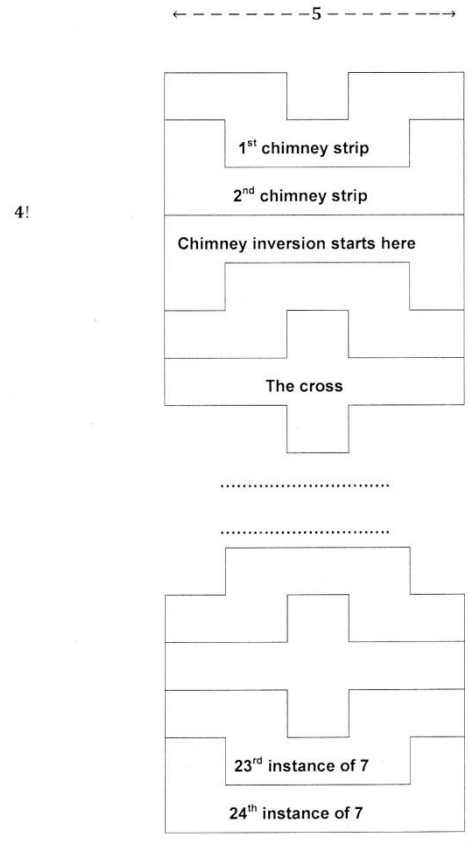

Figure 4: Pattern Illustration for n = 7

Thus, with n = 7, let n_1 = 14 = area of the first chimney and inverted chimney pattern, and let n_2 = 7 = area of the first cross pattern. It follows from the construction that

$$(n-2)! - 1 = (7-2)! - 1$$
$$= n_1 + 2(3)n_1 + 3n_2$$
$$= 14 + 2(3)14 + (3)7$$
$$= 119$$

In summary, one uses the first chimney pattern, along with 3 instances of the chimney pattern, with an inverted chimney, placing the cross between the chimney and the inverted chimney.

The number $n^2 - 2n = 7^2 - 2(7) = 35$ measures the area associated with the following union: (chimney ∪ cross ∪ inverted chimney). Also, $n(n-3)/2 = 7(4)/2 = 14$ = area of the chimney pattern.

Finally, an easy algebra check validates the equation of the main theorem mentioned in the introduction (for n = 7), namely:

$$5! - 7(4)/2 = 106 \equiv 1 \bmod (7^2 - 2(7)).$$

In other words, one has that the number 35 divides 105.

4. THE AREA OF THE CHIMNEY PATTERN AS A FUNCTION OF (n≥5)

A lemma will be presented illustrating a claim from the previous section using an inductive argument.

Lemma: Let n ≥5 be an odd integer. Then the area A_n of the chimney pattern is given by $A_n = n(n-3)/2$.

Proof: By induction. For n = 5, the validation occurs from Figure 2. One has that $A_5 = 5 = 5(5-3)/2$. Now assume inductively that $A_n = n(n-3)/2$ and show that $A_{n+2} = (n+2)(n-1)/2$. One must inductively construct the next chimney pattern from the n^{th} pattern. This consists of appending an outer sleeve of thickness equal to one. Let C_n denote the region whose area is $(n-2)! - 1$.

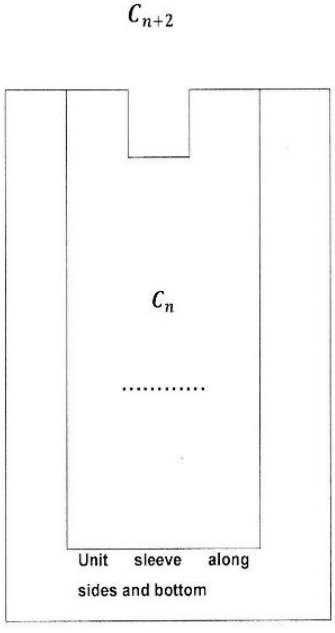

Figure 5: The Region C_{n+2} Inductive Construction

The embedded region displayed inside the above is the region C_n within the total displayed region C_{n+2}. To see how a collection of regions of area equal to n+2 would naturally fit into C_{n+2}, notice it is sufficient to prepend and append a single unit square for each strip of unit n, along with the last strip at the bottom of size n unit squares hosting unit squares above its end squares.

Now C_n is a rectangle with a deleted unit square. So the height h_n of C_n satisfies the equation

$$A_n + 1 = n(n-3)/2 + 1 = h_n(n-2).$$

It follows that the height h_n is equal to $(n-1)/2$. Hence the area A_{n+2} is given by the following

$A_{n+2} = A_n + 2h_n +$ n "the sides" + n "the bottom"

$= n(n-3)/2 + 2(n-1)/2 + n$

$= n(n-3)/2 + 2n - 1$

$= (n^2 - 3n + 4n - 2)/2$

$= (n+2)(n-1)/2.$

So we are done with the induction lemma for the area of the first chimney pattern. ■

5. THE CONGRUENCE RELATION

Previous sections have described the process for establishing the main theorem. One begins with the first chimney pattern, then one appends an even number 2j of chimney patterns with j cross patterns in between.

Theorem 1. The positive odd integer n is prime if and only if

$$(n-2)! - n(n-3)/2 \equiv 1 \bmod (n^2 - 2n).$$

Proof: Considering the area of the notched rectangle one has the following result:

$$(n-2)\cdot(n-3)! - 1 = A_n + 2j\cdot A_n + j\cdot A_n$$

For some integer $j \geq 0$ if and only if n is an odd prime. Recall that A_n is the chimney area for the prime number n. Furthermore, the congruence relation in the statement of the theorem has been validated previously for n = 3 and as a final note, when n = 5, one has that j = 0. Thus

$$(n-2)! - 1 = n(n-3)/2 + 2jn(n-3)/2 + jn$$

$$= n(n-3)/2 + j(n^2 - 2n).$$

And thus the modular relation is established, namely that

$$(n-2)! - n(n-3)/2 \equiv 1 \bmod(n^2 - 2n).$$ ■

6. ANOTHER CONGRUENCE RELATION mod $n^2 - 2n$ BY MODULAR ARITHMETIC

The result of the geometric construction provided a modular relationship modulo $n^2 - 2n$ if and only if n is an odd prime. Given that $n^2 - 2n$ naturally occurred from the construction itself, it would be interesting to check what result might occur from a straightforward calculation in modular arithmetic relative to $n^2 - 2n$. Consider the following for the prime number n.:

$(n-1)! \equiv -1 \bmod n$

$\Leftrightarrow (n-1)! + 1 = kn$ for some integer k

$\Leftrightarrow n(n-1)! + n = kn^2$ and $2(n-1)! + 2 = 2kn$

$\Rightarrow (n-2)((n-1)!) + (n-2) = k(n^2 - 2n)$

$\Leftrightarrow (n-2)((n-1)!) + (n-1) = 1 + k(n^2 - 2n)$

So one has the following

Theorem 2: If n is an odd prime, then

$$(n-2)((n-1)!) + (n-1) \equiv 1 \bmod(n^2 - 2n).$$

7. CONCLUSION

This paper has demonstrated how to geometrically construct congruence relations for prime numbers using Wilson's Theorem. The methods suggest how to effectively integrate algebraic and geometric techniques to generate results in numbers theory.

8. REFERENCES

[1] Rosen, K. H., Elementary Number Theory and its applications, 4th edition, Addison Wesley Longman, Reading, Massachusetts, 1999.

[2] Gabai, David, "Foliations and topology of 3-manifolds," J. Diff. Geom. 18 (1983) no. 3, 445-503.