We start by showing that the converse of Wilson's theorem provides a primality test.

Of Wilson's theorem, proves a primality test by large and other tests are needed.

Very large and other tests are needed for very large and other tests are needed.

The converse of Wilson's theorem, proves a primality test by large and other tests are needed.

The converse of Wilson's theorem, proves a primality test by large and other tests are needed.

Example

\[ 3 \equiv \frac{1}{1} \pmod{11} \]

By FLT, \( 3^{10} \equiv 1 \pmod{11} \)

Thus, \( \frac{1}{1} \equiv 1 \pmod{11} \)

Thus, \( \frac{1}{1} \equiv 1 \pmod{11} \)

Thus, \( \frac{1}{1} \equiv 1 \pmod{11} \)

Thus, \( \frac{1}{1} \equiv 1 \pmod{11} \)
Theorem. Let \( n \in \mathbb{Z}_+ \) satisfy \((n-1)! = -1 \pmod{n}\). Then \( n \) is a prime number.

Proof: Suppose \( n \) is composite and suppose \((n-1)! \equiv -1 \pmod{n}\). Let \( n = ab \) with \( 1 < a, b < n \).

\( a \leq n-1 \), so \( a \mid (n-1)! \). Furthermore \((n-1)! \equiv -1 \pmod{n} \) if and only if \((n-1)! + 1 \equiv 0 \pmod{n} \iff n \mid (n-1)! + 1\).

Thus since \( a \mid n \) and \( n \mid (n-1)! + 1 \) we have \( a \mid (n-1)! + 1 \) and in particular \( a \) divides the difference, \( a \mid [(n-1)! + 1 - (n-1)!] = 1 \rightarrow a = 1 \) contradicts \( a > 1 \).

Thus \( n \) must be prime.

Thus this theorem together with Wilson's theorem shows that \((n-1)! = -1 \pmod{n}\) is equivalent to \( n \) being prime. In practice computing \((n-1)! \pmod{n}\) is hard since \((n-1)! \) is so large for big \( n \). A better test is given by

Theorem \( r \) \(^{\text{(Fermat's Test)}}\). Let \( n, b \in \mathbb{Z}_{>1} \), \( 1 < b < n \).

If \( b^{n-1} \not\equiv 1 \pmod{n} \), then \( n \) is composite.
Definition: If \( b^{n-1} \equiv 1 \pmod{n} \) then we say \( n \) passes Fermat's test for base \( b \).

Proof: If \( n \) is prime, then \( (b,n) = 1 \) and \( b^{n-1} \equiv 1 \pmod{n} \) by FLT.

Example: Suppose \( n = 91 \). \( 2^{91-1} \equiv 64 \pmod{91} \) and \( 64 \equiv 1 \pmod{91} \). Fermat's test implies 91 is composite (and indeed \( 91 = 13 \cdot 7 \)).

We have seen that \( n \) is prime if and only if \( (n-1)! = -1 \pmod{n} \).

We have also seen that \( (a,n) = 1 \) and \( n \) prime always implies \( a^{n-1} \equiv 1 \pmod{n} \).

But \( a^{n-1} \equiv 1 \pmod{n} \) does not necessarily mean that \( a \) is prime.

Example: Let \( n = 341 \) and \( a = 2 \). Then \( 2^{340} \equiv 1 \pmod{341} \) but 341 is not prime since \( 341 = 11 \cdot 31 \).

Composite numbers which pass Fermat's test for base \( b \) have a special name.
Definition: If \( n \) is composite and satisfies \( b^{n-1} \equiv 1 \mod n \) for some \( 1 < b < n \), we say \( n \) is a pseudoprime to the base \( b \).

Example 1: \( 2^{340} \equiv 1 \pmod{341} \) but \( 341 = 11 \cdot 31 \) hence \( 341 \) is a pseudoprime for base \( 2 \).

Example 2: \( 341 \) is not a pseudoprime for base \( b = 3 \).

(proof of this fact) \( 3^{30} \equiv 1 \pmod{31} \) by FLT.

Thus \( 3^{340} \equiv (3^{30})^{11} \cdot 3^{10} \equiv 1^{11} \cdot 3^{10} \pmod{31} \)

\[ = (3^3)^3 \cdot 3 \equiv 27^3 \cdot 3 \equiv (-4)^3 \cdot 3 \pmod{31} \]

\[ = (-64) \cdot 3 \pmod{31} \equiv (-2) \cdot 3 \equiv -6 \equiv 25 \pmod{31} \]

Thus \( 3^{340} \equiv 1 \pmod{31} \). But \( 31 \mid 341 \) hence \( 3^{340} \equiv 1 \pmod{341} \) — since if 2 numbers are equal \( \mod m \) they are equal \( \mod \) to the divisors of \( m \). End of example.

Thus \( 341 \) passes Fermat’s test in base 2 but not in base 3.
Question: Are there integers $n$ that are composite and yet pass Fermat’s test in every base relatively prime to $n$?

Definition: An integer $n > 1$ is a Carmichael number if it is a pseudoprime for every base $b > 2$ such that $(n, b) = 1$.

It can be tricky to determine directly whether a number is a Carmichael number. However, there is a good classification theorem which makes it easy to test whether a number is a Carmichael number or not. We prove one direction here (the other direction requires primitive roots—a later chapter).

Definition: An integer is square-free if no square number divides it.