Wilson's theorem & the Chinese remainder theorem

UNIVERSITY OF TORONTO

February 25th, 2021

Wilson's theorem – 1

Lemma

Let p be a prime number. Then

$$\forall a \in \mathbb{Z},\ a^2 \equiv 1 \pmod{p} \implies \left(a \equiv -1 \pmod{p} \text{ or } a \equiv 1 \pmod{p}\right)$$

Proof.
Let p be a prime number and $a \in \mathbb{Z}$ satisfying $a^2 \equiv 1 \pmod{p}$.
Then $p | a^2 - 1 = (a-1)(a+1)$.
By Euclid's lemma, either $p | a - 1$ or $p | a + 1$, i.e. $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. ∎

Wilson's theorem – 2

Wilson's theorem

Let $n \in \mathbb{N} \setminus \{0, 1\}$. Then n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Proof. Let $n \in \mathbb{N} \setminus \{0, 1\}$.

- *Assume that n is a composite number.*
  Then there exists $k \in \mathbb{N}$ such that $k|n$ and $1 < k < n$.
  Assume by contradiction that $(n-1)! \equiv -1 \pmod{n}$ then $n|(n-1)! + 1$ and hence $k|(n-1)! + 1$.
  But $k|(n-1)!$, thus $k|\left((n-1)! + 1 - (n-1)!\right)$, i.e. $k|1$. So $k = 1$ which leads to a contradiction.
- *Assume that n is prime.*
  Let $a \in \{1, 2, \dots, n-1\}$ then $\gcd(a, n) = 1$.
  Hence a admits a multiplicative inverse modulo n:
  $\exists b \in \{1, 2, \dots, n-1\}$ such that $ab \equiv 1 \pmod{n}$.
  Note that this b is unique.
  By the above lemma, $a = 1$ and $a = n - 1$ are the only a as above being their self-multiplicative inverse: otherwise $b \neq a$.
  Thus $(n-1)! = 1 \times 2 \times \cdots \times (n-1) \equiv 1 \times (n-1) \pmod{n} \equiv -1 \pmod{n}$.
  Indeed, in the above product each term simplifies with its multiplicative inverse except 1 and $n - 1$. ∎

Wilson's theorem – 3

Wilson's theorem

Let $n \in \mathbb{N} \setminus \{0, 1\}$. Then n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Examples

- Take $p = 17$ then $(17-1)! + 1 = 20922789888001 = 17 \times 1230752346353$.
- Take $p = 15$ then $(15-1)! + 1 = 87178291201 = 15 \times 5811886080 + 1$.

Remark

Wilson's theorem is a very inefficient way to check whether a number is prime or not.

The Chinese remainder theorem

Let $n_1, n_2 \in \mathbb{N} \setminus \{0, 1\}$ be such that $\gcd(n_1, n_2) = 1$ and let $a_1, a_2 \in \mathbb{Z}$.

Then there exists $x \in \mathbb{Z}$ satisfying $\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$

Besides, if $x_1, x_2 \in \mathbb{Z}$ are two solutions of the above system then $x_1 \equiv x_2 \pmod{n_1 n_2}$.

Proof.

- *Existence.* By Bézout's identity, there exist $m_1, m_2 \in \mathbb{Z}$ such that $n_1 m_1 + n_2 m_2 = 1$.
  Note that $n_1 m_1 \equiv 0 \pmod{n_1}$ and that $n_1 m_1 \equiv n_1 m_1 + n_2 m_2 \pmod{n_2} \equiv 1 \pmod{n_2}$.
  Similarly $n_2 m_2 \equiv 0 \pmod{n_2}$ and $n_2 m_2 \equiv 1 \pmod{n_1}$.
  Thus, if we set $x = a_2 n_1 m_1 + a_1 n_2 m_2$ then
  - $x \equiv a_2 \times 0 + a_1 \times 1 \pmod{n_1} \equiv a_1 \pmod{n_1}$,
  - $x \equiv a_2 \times 1 + a_1 \times 0 \pmod{n_2} \equiv a_2 \pmod{n_2}$.
- *Uniqueness modulo $n_1 n_2$.* Let $x_1, x_2 \in \mathbb{Z}$ be two solutions.
  Then $x_1 - x_2 \equiv 0 \pmod{n_1}$ so $x_1 - x_2 = k n_1$ for some $k \in \mathbb{Z}$.
  Similarly $n_2 | x_1 - x_2 = k n_1$.
  Since $\gcd(n_1, n_2) = 1$, by Gauss' lemma, $n_2 | k$. So there exists $l \in \mathbb{Z}$ such that $k = n_2 l$.
  Thus $x_1 - x_2 = l n_1 n_2$ and therefore $x_1 \equiv x_2 \pmod{n_1 n_2}$. ∎