Fermat's Little Theorem

Let \( p \) be a prime and \( a \) be an integer not divisible by \( p \). Then \( a^{p-1} \equiv 1 \pmod{p} \).

Proof: \( a, 2a, \ldots, (p-1)a \) are all distinct, modulo \( p \). (Check!) Thus \( a \cdot (2a) \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot p-1 \equiv -1 \pmod{p} \).

On the other hand,

\[ a \cdot (2a) \cdot \ldots \cdot (p-1)a \equiv a^{p-1} \cdot (-1) \pmod{p}. \]

Thus \(-a^{p-1} \equiv -1 \pmod{p}\) or equivalently, \( a^{p-1} \equiv 1 \pmod{p} \).
Corollary 1

\[ a^p \equiv a \pmod{p} \] for every integer \( a \).

Here \( p \) is a prime.

Proof: The congruence \( a^p \equiv a \pmod{p} \) holds if \( a \equiv 0 \pmod{p} \). If \( a \not\equiv 0 \pmod{p} \), then Fermat's Little Theorem tells us that \( a^{p-1} \equiv 1 \pmod{p} \).

Now multiply both sides by \( a \).

Corollary 2

Suppose \( a \not\equiv 0 \pmod{p} \).

If \( d \equiv e \pmod{p-1} \), then \( a^d \equiv a^e \pmod{p} \).

Proof: May assume \( d \geq e \), and \( d - e = (p-1)k \).

Then

\[ a^d = a^e \cdot a^{(p-1)k} = a^e \cdot (a^{p-1})^k = a^e \cdot 1^k = a^e \pmod{p} \]
Example: Compute $2^{180} \pmod{89}$

89 is a prime

$180 \equiv 4 \pmod{88}$

$2^{180} \equiv 2^4 \equiv 16 \pmod{89}$
Pollard's p-1 Factorization Method (Sect. 6.1)

Goal: Factor a given integer $n \geq 0$.

Here is how it works.

Compute $r_k = 2^k \pmod{n}$ recursively using the formula $r_k = r_{k-1} \pmod{n}$.

For each $k$, compute $\gcd(r_k - 1, n) = g_k$.

Note that $0 \leq r_k \leq n-1$, so if $g_k > 1$, we have found a proper factor of $n$.

The idea is that if $n$ has a prime factor $p$ such that $p-1$ divides $k!$, then $2^k \equiv 1 \pmod{p}$ (check!), and thus $p | 2^k - 1$ and $p | n$.

Moreover, since $r_k = 2^k \pmod{n}$, $p$ also divides $r_k - 1$ and thus $p | g_k$. $p-1$ will divide $k!$ for "small" $k$ if $p-1$ has small prime factors.
Example: \( n = 10403 \). Use Pollard's method to factor \( n \).

\[ r_2 = 2^2 \equiv 4 \pmod{n} \quad \gcd(10403, 3) = 1 \]
\[ r_3 = 4^3 \equiv 64 \pmod{n} \quad \gcd(10403, 63) = 1 \]
\[ r_4 = 64^4 \equiv 7580 \pmod{n} \quad \gcd(10403, 7579) = 1 \]
\[ r_5 = 7580^5 \equiv 4438 \pmod{n} \quad \gcd(10403, 4437) = 1 \]
\[ r_6 = 4438^6 \equiv 6862 \pmod{n} \quad \gcd(10403, 6861) = 1 \]
\[ r_7 = 6862^7 \equiv 137 \pmod{n} \quad \gcd(10403, 136) = 1 \]
\[ r_8 = 137^8 \equiv 196 \pmod{n} \quad \gcd(10403, 195) = 1 \]
\[ r_9 = 3619 \pmod{n} \quad \gcd(10403, 3618) = 1 \]
\[ r_{10} = 9798 \pmod{n} \quad \gcd(10403, 9797) = 101 \]

\[ n = 10403 = 101 \cdot 103 \]