The AKS primality test explained – Kuba Perlin    Churchill College, 23.01.2019

## Multiplicative order $o_r(n)$ [slide 7]

$o_r(n)$ is the *order* of $n$ mod $r$,
i.e. the smallest number $o_r(n)$ such that $n^{o_r(n)} = 1 \pmod r$.

- e.g. $o_7(3) = 6$:
  $3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad \underline{3^6 = 1} \pmod 7$

---

## The inefficient primality test [slide 12]

*$X + a^n \equiv (X+a)^n$ below is an equality of **polynomials**, not numbers.*

For any $a \in \mathbb{Z}$ such that $\gcd(a,n) = 1$:

$$X + a^n \equiv (X+a)^n \pmod n \iff n \text{ is prime}$$

(For the $\Leftarrow$ direction you don't need the $\gcd(a,n) = 1$ assumption.)

---

## AKS pseudocode [slide 18]

1. `if` ($n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$)`, return COMPOSITE.`
2. `Find the smallest` $r$ `such that` $o_r(n) > \log^2 n$`.`
3. `If some` $a \leq r$ `is not coprime with` $n$`, return COMPOSITE.`
4. `If` $r \geq n$`, return PRIME.`
5. `For` $a = 1$ `to` $\lfloor \sqrt{\varphi(r)} \log n \rfloor$ `do:`

   `if` $X + a^n \not\equiv (X+a)^n \pmod{X^r - 1, n}$`, return COMPOSITE.`
6. `Return PRIME.`

**Main challenge:** show that if `Line 6.` is reached, then $n$ must be prime.

---

## Plan of the final attack [slide 25]

**1.** Define a group $\mathcal{G}$ of polynomials.

**2.** Prove that $|\mathcal{G}| \geq$ `LowerBound`.

**3.** Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.

**4.** Deduce that $n = p^k$ for some $k$.

But recall `Line 1.` of `AKS`:    `if` ($n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$)`, return COMPOSITE.`

**5.** Therefore $k = 1$... and we get that $n = p^1$ is prime. $\square$

---

## Introspectiveness [slide 26]

**Definition.** $m \in \mathbb{N}$ is *introspective* for $f(X) \iff$

$$f(X^m) \equiv [f(X)]^M \pmod{X^r - 1, p}$$

**Corollary.** $n$ and $p$ are introspective for $X + a$ (for all $a \in \{0, 1, \ldots, l\}$).

---

## $G_1$ and $\mathcal{G}$ [slide 29]

$$G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$$

$$\mathcal{G} := \{\prod_{a=0}^{l} (X+a)^{e_a} \mid e_a \geq 0\} \pmod{h(X), p}$$