# 1. Calculating $a^b$ mod $c$ for large $b$

*Emir Habul*

**Lemma 1.** *Assuming* $gcd(a, b) = 1$

$x \equiv y \pmod{ab}$ *iff* $x \equiv y \pmod{a}$ *and* $x \equiv y \pmod{b}$.

A corollary of chinese remainder theorem.

**Theorem 2.** *For positive integers, if* $b > \varphi(c)$ *then*

$$a^b \equiv a^{b\%\varphi(c)+\varphi(c)} \pmod{c}$$

*where % is modulo operator.*

*Proof.* If suffices to show that

$$a^{k_1\varphi(c)} \equiv a^{\varphi(c)} \pmod{c} \quad k_1 > 0 \tag{1.1}$$

since $b$ can be rewritten as a remainder $b\%\varphi(c)$ plus a multiple of $\varphi(c)$.

Due to Euler's theorem this is trivial when $gcd(a, c) = 1$. Hence it remains $gcd(a, c) \neq 1$.

First, factorize $c$ into prime powers

$$c = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots$$

Generalization of Lemma (1) allows us to consider equation (1.1) for each $p_i^{e_i}$ individually as a modulus.

$$a^{k_1\varphi(c)} \equiv a^{\varphi(c)} \pmod{p_i^{e_i}} \tag{1.2}$$

For those primes $p_i$ that do not divide $a$, equation (1.2) is simple show due to Euler's theorem and $gcd(p_i^{e_i}, a) = 1$.

Therefore, we have to consider cases where $p_i$ divides $a$.

Let $a = p_i^w a_i$ and $gcd(a_i, p_i) = 1$, thus $a_i$ consists of all prime powers other than $p_i$.

$$(a_i p_i^w)^{k_1\varphi(c)} \equiv (a_i p_i^w)^{\varphi(c)} \pmod{p_i^{e_i}}$$

We can simplify this by considering that $a_i^{\varphi(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$.

$$p_i^{wk_1\varphi(c)} \equiv p_i^{w\varphi(c)} \pmod{p_i^{e_i}}$$

$$\left(p_i^{\varphi(p_i^{e_i})}\right)^{wk_1\varphi(c/p_i^{e_i})} \equiv \left(p_i^{\varphi(p_i^{e_i})}\right)^{w\varphi(c/p_i^{e_i})} \pmod{p_i^{e_i}}$$

Both sides are equal to zero due to Lemma 3.

□

**Lemma 3.** *For prime $p_i$ and $e_i > 0$ it follows that*

$$p_i^{\varphi(p_i^{e_i})} \equiv 0 \pmod{p_i^{e_i}}$$

*Proof.* Left side will be multiple of the modulus provided that

$$\varphi(p_i^{e_i}) = (p-1)p^{e_i-1} \geq e_i$$

We use mathematical induction to show $p^{e_i-1} \geq e_i$.

Starting from, $p = 2$ and $e_i = 1$ both sides are equal to 1.

Assuming $p^{e_i-1} \geq e_i$ it is easy to see that $(p+1)^{e_i-1} \geq e_i$ is also true.

For induction on second parameter $e_i$, we multiply both sides of $p^{e_i-1} \geq e_i$ by $p$

$$p^{e_i-1}p = p^{e_i} \geq e_i p \geq e_i + 1$$

□