Il calcolo modulare

Di Cristiano Armellini, cristiano.armellini@alice.it

In base al piccolo teorema di Fermat

$$a^p \equiv a, mod(p), p\ primo$$

$$2b = p + q, p\ primo$$

$$a^{2b-q} \equiv a\ , mod(p)$$

$$a^{2b} \equiv a^{q+1}\ , mod(p)$$

Tuttavia se

$$2b + 1 = p + 2m, p\ primo$$

$$p = 2b + 1 - 2m = 2(b - m) + 1, m < b$$

$$a^{2b+1} \equiv a^{2m+1}, mod(p)$$

Mentre è ovvio che

$$n = pq, p, q\ primi$$

$$(a^p)^q \equiv a^p, mod(q)$$

$$(a^q)^p \equiv a^q, mod\ (p)$$