TEN. The Baby-Step-Giant-Step algorithm.

Let G be a cyclic group with n elements, and let $a \in G$ be a generator of the group. It means that $G = \{a,\ a^2,\ \ldots,\ a^n = e\}$. In particular, every $x \in G$ can be written as $x = a^s$, for some $s \in \mathbb{Z}$. The exponent s, which by Lagrange's theorem it is only well defined modulo n, is *by definition* the discrete logarithm of x in base a

$$s := \log_a(x) \bmod n.$$

The Baby-Step-Giant-Step algorithm is a deterministic algorithm for computing the discrete logarithm in an arbitrary finite cyclic group. It exploits the fact that every element $x \in G$ can be written as

$$x = a^{j+mi}, \tag{1}$$

for integers $m,\ i,\ j$ satisfying $m \sim \sqrt{n}$, and $0 \leq i,\ j \leq m$. Equation (1) can be rewritten as $a^i = xa^{-mj}$. Then the logarithm $\log(x)_a$ is obtained by comparing two lists: the baby steps a^i and the giant steps xa^{-mj}, for $0 \leq i, j \leq m$. When a coincidence is found between the two lists, namely one has $a^{i_0} = xa^{-mj_0}$, for some i_0 and j_0, then the desired logarithm is given by $i_0 + mj_0 = \log(x)_a$.
Computing at most $2m \sim 2\sqrt{p}$ powers modulo p and comparing the two lists, one surely obtains the desired logarithm. Note that with the naif method one could possibly have to compute up to p powers modulo p, before obtaining the desired result.

Example. Fix $p = 433$ and let $a = 7$ be a primitive root in $\mathbb{Z}_p^*$. We want to calculate the discrete logarithm of $x = 166$ in base a. In this case, $m = 21 \sim \sqrt{433}$.
We first produce the list of the **Baby-Steps** $a^i \bmod p$, for $0 \leq i \leq m-1$:
$a^0 = 1$
$a^1 = 7$
$a^2 = 49$
$a^3 = 343$
$a^4 = 236$
$a^5 = 353$
$a^6 = 306$
$a^7 = 410$
$a^8 = 272$
$a^9 = 172$
$a^{10} = 338$
$a^{11} = 201$
$a^{12} = 108$
$a^{13} = 323$
$a^{14} = 96$
$a^{15} = 239$
$a^{16} = 374$
$a^{17} = 20$
$a^{18} = 140$
$a^{19} = 114$
$a^{20} = 365$

$a^{-m} = a^{-21} = 292$

Next we produce the list of the **Giant-Steps** $xa^{-mj} \bmod p$, for $0 \leq j \leq m-1$, and each time we check whether the value the new Giant-Step already appears in the list of the Baby-Steps. When that is the case, we are done.

$x \cdot a^0 = 166$
$x \cdot a^{-21} = 409$

$x \cdot a^{-42} = 353$!!!

We have found a coincidence between the two lists: $a^5 = x \cdot a^{-42}$. This means that

$$x = a^{5+42} = a^{47} \quad \text{and} \quad \log_7(166) = 47.$$

Indeed one can check that $7^{47} = 166 \bmod 433$.