Rational Solutions of Polynomial Equations

In general, there is no explicit way to solve polynomial equations. However, if we have a polynomial with integral (integer) coefficients, which has the highest coefficient equal to 1 (example: \( P(x) = 2 + 3x - 7x^3 + x^5 \)), then we can find all the rational solutions of the equation \( P(x) = 0 \) in a very explicit way.

So let

\[
P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + x^n
\]

be such a polynomial (of degree \( n \geq 0 \))
Theorem: Let $x$ be a rational solution of the equation $P(x) = 0$ with $P(x)$ as above. Then $x$ is an integer, and $x$ divides $a_0$.

Proof: Let $x = \frac{k}{l}$, where $k, l$ are relatively prime integers, with $l > 0$. We want to show that $l$ must be 1, and that $k$ must divide $a_0$.

So we have

$$a_0 + a_1 \frac{k}{l} + \cdots + a_{n-1} \frac{k^{n-1}}{l^{n-1}} + \frac{k^n}{l^n} = 0 \quad (\star)$$

Multiply $(\star)$ by $l^n$

$$a_0 l^n + a_1 k l^{n-1} + \cdots + a_{n-1} k^{n-1} l + k^n = 0 \quad (\star \star)$$

or, after bringing $k^n$ to right hand side, and factoring $l$ out

$$l(a_0 l^{n-1} + a_1 k l^{n-2} + \cdots + a_{n-1} k^{n-1}) = -k^n \quad (\star \star \star)$$

$l$ divides LHS, so $l$ divides RHS, i.e., $-k^n$.
By Fund. Theorem of Arithmetics, \( l \) must divide \( k \), so \( l \) must be \( = 1 \). Thus

\[ x = k \]

So now (i) becomes

\[ a_0 + a_1k + \cdots + a_{n-1}k^{n-1} + k^n = 0 \]  (***)

or

\[ a_0 = -k(a_1 + a_2k + \cdots + k^{n-1}) \]

But this implies that \( k \) divides \( a_0 \), i.e.

\[ x \mid a_0 \]