The Cyclotomic Polynomials

Definition: Let $n \in \mathbb{N}$ and $\omega_1, \omega_2, ..., \omega_{\phi(n)}$ be the n'th primitive roots of unity. The n'th cyclotomic polynomial is the polynomial

$$\Phi_n(x) = \Pi_{i=1}^{\phi(n)}(x - \omega_i).$$

Here are the first few cyclotomic polynomials.

n	$x^n - 1$	$\Phi_n(x)$
1	$x - 1$	$x - 1$
2	$x^2 - 1 = (x-1)(x+1)$	$x + 1$
3	$x^3 - 1 = (x-1)(x^2+x+1)$	$x^2 + x + 1$
4	$x^4 - 1 = (x^2-1)(x^2+1)$	$x^2 + 1$
5	$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$	$x^4 + x^3 + x^2 + x + 1$
6	$x^6 - 1 = (x^3-1)(x+1)(x^2-x+1)$	$x^2 - x + 1$

One way to compute $\Phi_n(x)$ is to use of the following result.

Theorem 1: $\Phi_n(x) = (x^n - 1)/(\Pi_{d|n, d<n}\Phi_d(x))$.

E.g. $\Phi_{10}(x) = \frac{x^{10}-1}{\Phi_1(x)\Phi_2(x)\Phi_5(x)} = \frac{x^{10}-1}{(x-1)(x+1)(x^4+x^3+x^2+x+1)} = x^4 - x^3 + x^2 - x + 1.$

Theorem 1 implies that $\Phi_n(x)$ is monic with integer coefficients. It turns out that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. For $1 \leq n \leq 6$, you can see from the above table that the coefficients are all 1 or -1. This is not true for larger n.

Theorem 2: Let $H_n \in \mathbb{Z}$ be the largest coefficient in $\Phi_n(x)$. Then

n	H_n	$\log_2 H_n$
1,181,895	14102773	23.7
43,730,115	862550638890874931	59.6
1,880,394,945	64540997036010911566826446181523888971563	135.6