Cyclotomic trinomials

Robert Israel

July 14, 2015

Theorem 1 *The cyclotomic polynomial $C_n(x)$ has exactly three terms if and only if $n = 2^a 3^b$ for integers $a \geq 0$, $b \geq 1$.*

Proof Suppose $n = 3^b$, $b \geq 1$, and let $w = \exp(2j\pi i/3^b)$ be a primitive 3^b'th root of unity. Then $w^{3^{b-1}}$ is a primitive cube root of unity, i.e. a root of $z^2 + z + 1$. Thus w is a root of $x^{2\cdot 3^{b-1}} + x^{3^{b-1}} + 1$. There are $2 \times 3^{b-1}$ primitive 3^b'th roots of unity, so these are all the roots of the polynomial $x^{2\cdot 3^{b-1}} + x^{3^{b-1}} + 1$, which is therefore $C_n(x)$.

Similarly, if $n = 2^a * 3^b$, $a, b \geq 1$, then $C_n(x) = x^{2^a 3^{b-1}} - x^{2^{a-1} 3^{b-1}} + 1$.

Conversely suppose $C_m(x) = x^r + cx^s + 1$ is cyclotomic. Since C_m is a self-reciprocal polynomial we have $r = 2s$. The s'th powers of roots of C_m are roots of $z^2 + cz + 1$, so these must have absolute value 1, which is true if and only if $-2 \leq c \leq 2$. Now the coefficients of cyclotomics are integers, and $c = \pm 2$ would produce the reducible polynomials $(x^s \pm 1)^2$, while $c = 0$ would make 2 terms instead of 3. Thus we must have $c = \pm 1$.

If s is a prime other than 2 or 3, $x^{2s} \pm x^s + 1$ is divisible by $x^2 \pm x + 1$ (because the s'th power of a primitive cube root of 1 or -1 is again a primitive cube root of 1 or -1). Similarly, if $s = kp$ for some prime p other than 2 or 3, $x^{2s} \pm x^s + 1$ is divisible by $x^{2k} \pm x^k + 1$. Thus the only prime divisors of s are 2 and 3, and these do produce the cyclotomics for $n = 2^a 3^b$ as shown above.