CONGRUENCES

for the Perplexed

Andreas Klappenecker

September 24, 2002

Two integers a and b are called congruent modulo m, written $a \equiv b \bmod m$, if and only if m divides $a - b$. In other words, $a - b$ is an element of $m\mathbf{Z} = \{mx \mid x \in \mathbf{Z}\}$, an ideal in the ring $\mathbf{Z}$ of integers.

X1 Show that $a_0 \equiv b_0 \bmod m$ and $a_1 \equiv b_1 \bmod m$ implies $a_0 a_1 \equiv b_0 b_1 \bmod m$.

Let $\mathbf{Z}[x]$ be the ring of polynomials with integer coefficients. The congruence $a(x) \equiv b(x) \bmod \langle x^r - 1\rangle$ means that the difference $a(x) - b(x)$ is a multiple of the polynomial $x^r - 1$. A simple but important consequence is that $x^r \equiv 1 \bmod \langle x^r - 1\rangle$ holds.

Therefore, $a_3x^3 + a_0 \equiv a_3 + a_0 \bmod \langle x^3 - 1\rangle$, because a_3x^3 is congruent to a_3 modulo $x^3 - 1$. Similarly, $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \equiv (a_5 + a_3 + a_1)x + (a_4 + a_2 + a_0) \bmod \langle x^2 - 1\rangle$.

X2 Show that $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 - (a_5 + a_3 + a_1)x - (a_4 + a_2 + a_0)$ is indeed a multiple of $x^2 - 1$.

The congruence of polynomials in $\mathbf{Z}[x]$ modulo the ideal $\langle x^r - 1, n\rangle$ is crucial in the AKS primality test. Again, $a(x) \equiv b(x) \bmod \langle x^r - 1, n\rangle$ means that the difference $a(x) - b(x)$ is an element of the ideal $\langle x^r - 1, n\rangle$.

The most important consequences are that $x^r \equiv 1 \bmod \langle x^r - 1, n\rangle$ and that $n \equiv 0 \bmod \langle x^r - 1, n\rangle$.

X3 Let $m = n \bmod r$. Explain why $x^n - a \equiv x^m - a \bmod \langle x^r - 1, n\rangle$.

X4 Implement a fast algorithm to evaluate $(x - a)^n \bmod \langle x^r - 1, n\rangle$.

Solutions

S1 It follows from the hypothesis that m divides $a_0 - b_0$, hence m divides $a_0a_1 - b_0a_1$, whence $a_0a_1 \equiv b_0a_1 \bmod m$. Similarly, we get $b_0a_1 \equiv b_0b_1 \bmod m$ from $a_1 \equiv b_1 \bmod m$. Consequently, $a_0a_1 \equiv b_0a_1 \equiv b_0b_1 \bmod m$, which proves the result.

S2 $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 - (a_5 + a_3 + a_1)x - (a_4 + a_2 + a_0) = (a_5x^3 + a_4x^2 + (a_5 + a_3)x + (a_4 + a_2))(x^2 - 1)$.

S3 We have $x^n = x^{rq+m} = (x^r)^q x^m \equiv x^m \bmod \langle x^r - 1, n\rangle$, since x^r is equivalent to 1 modulo $\langle x^r - 1, n\rangle$.

S4 Use square and multiply with arithmetic modulo n. Take advantage of the fact that x^r is congruent to 1, whenever the resulting polynomial is of degree $\geq r$. For large n, it might pay off to use the binary gcd algorithm in the implementation of the modular arithmetic.