

Problem Set Seven Hints
Math 499, Spring 2005

Problem 2: If $(a * b) = c$, can you calculate $(a * b) * (a * b)$ in two different ways? Note that the binary operations in Problems 1 and 2 are different; they are distinct problems.

Problem 3: Yet another typo here: the z^{p^2} in the third row, first column should be a x^{p^2} .

What does congruent modulo p mean? Consider an example: $p(x) = x^{17} + 5x^8 + 7x^2 + 3x + 6$. What is this function mod 3 (for example)? We can first reduce all the coefficients mod 3:

$$p(x) \equiv x^{17} + 2x^8 + x^2$$

and then reduce the powers using Fermat's little theorem: $x^p \equiv x, \text{ mod } p$. And so

$$\begin{aligned} p(x) &\equiv x^{3 \cdot 5 + 2} + 2x^{3 \cdot 2 + 2} + x^2 \\ &\equiv (x^3)^5 x^2 + 2(x^3)^2 x^2 + x^2 \\ &\equiv x^5 x^2 + 2x^2 x^2 + x^2 \\ &\equiv x^{3 \cdot 2 + 1} + 2x^3 x + x^2 \\ &\equiv (x^3)^2 x + 2xx + x^2 \\ &\equiv x^2 x + 3x^2 \\ &\equiv x^3 \\ &\equiv x \end{aligned}$$

And so, mod 3, we expect that $p(x) \equiv x$. We can check this:

$$\begin{aligned} p(0) &= 6 \equiv 0 \text{ mod } 3 \\ p(1) &= 1 + 5 + 7 + 3 + 6 = 22 \equiv 1 \text{ mod } 3 \\ p(2) &= 132392 = 44130 \cdot 3 + 2 \equiv 2 \text{ mod } 3 \end{aligned}$$

For the given determinant, can you reduce it (like the above) to a product of linear terms of the form $ax + by + cz$? In other words, if D is the determinant, can you find integers $a_1, b_1, c_1, a_2, b_2, c_2, \dots$ so that

$$D \equiv (a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z) \cdots \text{ mod } p$$

with a finite number of factors?