Putnam Study Group 2015-1 — ANSWERS

A8) Prove there is an integer k for which $k^3 - 36k^2 + 51k - 97$ is a multiple of 3^{2015}.

I messed this up at Monday's session so let me start over.

We have a polynomial f and we want to find an integer k that makes $f(k)$ divisible by a high power of a prime p. We will do so by successive approximations, finding integers k for which $f(k)$ is divisible by higher and higher powers of p. For example $f(1)$ is a multiple of 3^4 for the given polynomial.

The basic idea is that, if we already have an integer k making $f(k)$ divisible by p^i, then we try replacing k by $k + rp^i$ for some unknown integer r. We try to choose r so that $f(k + rp^i)$ is divisible by at least p^{i+1}. We'll see that $f(k + rp^i)$ will differ from $f(k) + f'(k)rp^i$ by a multiple of p^{2i}, so if we choose r to make $f(k)/p^i + f'(k)r$ be a multiple of p, then $f(k) + f'(k)rp^i$ is a multiple of p^{i+1}. This is essentially the idea of Newton's Method in calculus: we are replacing our approximate solution k by a better solution $k' = k - f(k)/f'(k)$. I'll give another example after solving our original problem to illustrate this idea.

OK, begin by expanding $f(k + x)$; you can do this manually or use the Taylor series around k to get four terms:

$$f(k + x) = f(k) + f'(k)x + (f''(k)/2)\,x^2 + (f'''(k)/6)\,x^3$$

If $f(k)$ is a multiple of 3^i for some $i \geq 3$, let $x = f(k)/3$. Then x is a multiple of 3^{i-1}, so x^2 and x^3 will be divisible by 3^{i+1} ($i + 1 \leq 2(i - 1)$ for these i). So we only retain the first two terms: $f(x + k) \equiv f(k) + f'(k)x = f(k)(1 + f'(k)/3)$ modulo 3^{i+1}. But $1 + f'(k)/3 = k^2 - 24k - 16$ is a multiple of 3 since $k \equiv 1 \pmod 3$, so $f(x + k)$ has at least one more factor of 3 than $f(k)$ did, i.e., it's a multiple of 3^{i+1}.

Iterating this construction gives a succession of integers $k \equiv 1 \pmod 3$ for which $f(k)$ is divisible by increasingly large powers of 3, and so we are done.

This process is very general and allows us to "solve" polynomial equations. In fact, the example of this question is more complicated than most because $f'(k)$ itself was a multiple of 3. Let me illustrate with a simpler example: I will compute the square root of 4456321 by finding a solution of the equation $x^2 - 4456321 = 0$. As above I will find values of x that make $x^2 - 4456321$ divisible by increasing powers of 3. We first need to make it divisible by 3 itself; $x = 2$ does this. The next iteration uses $x' = x - f(x)/f'(x) = 2 - (-4456317)/4$ which I compute modulo 9: $x' = 2 - (6)(7) = -40 \equiv 5$ (where $1/4 \equiv 7$ mod 9 because $4 \cdot 7 \equiv 1$); that is, $x' = 2 + 1 \cdot 3$. Then we compute our next iteration modulo 27: $x' = x - f(x)/f'(x) = 5 - (-4456296)/(10) = 5 - (0)(10) = 5 = 2 + 1 \cdot 3 + 0 \cdot 3^2$. Continuing in this way we obtain better and better approximations: $x \equiv 5 \pmod{81}; x \equiv 167 \pmod{243}; x \equiv 653 \pmod{729}; x \equiv 2111 \pmod{2187}$. At this point we have a value of x that not only makes $f(x)$ be divisible by a high power of 3; it really *is* zero! The solution we have found is $2 + 1 \cdot 3 + 0 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5 + 2 \cdot 3^6$, i.e. it's 2220012 when written in base-3.

You might want to compute the square root of 7 in this way: it turns out to be

$$1 + 1 \cdot 3^1 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + 0 \cdot 3^5 + 0 \cdot 3^6 + 2 \cdot 3^7 + \dots$$

Now, you might object that this makes no sense because the sequence will go on forever and thus not converge, but that's because you're trying to solve this equation in the real number line, which is only one of many nice fields that contain the integers. This particular series *does* converge in the ring of the 3-adic integers, which I invite you to look up!