Cyprian's Last Theorem

Martin Kochanski

9 May 2007

Cyprian's Last Theorem states that the equation

$$\sum_{1}^{n}(N-i)^n = N^n$$

(henceforth "CLE") has no integer solutions $< n, N >$ other than the obvious $<2,1>$, $<2,5>$, and $<3,6>$: that is, $(-1)^2 + 0^2 = 1^2$, $3^2 + 4^2 = 5^2$, and $3^3 + 4^3 + 5^3 = 6^3$.

The interesting thing about this theorem is that it is so very specific (not only must the nth powers be consecutive but they must add up to the next nth power) that it ought to be easy to prove by elementary methods. It is, after all, so **obviously** true.

Either it is unexpectedly difficult to prove or I am being dim. In either case, here is the story so far.

Some notation

$$CLF_n(N) = \sum_{1}^{n}(1 - \frac{i}{N})^n$$

so that an equivalent statement of the theorem is "$CLF_n(N) = 1$ has no integer solutions other than those stated".

We will also use $N(n)$ to denote "the largest value of N that satisfies $CLF_n(N) = 1$", so that the theorem is "$N(n)$ is not an integer if $n > 3$", and, for convenience, we will define $k(n) = N(n)/n$.

Even values of n

Lemma:

For all integers i,

$$i^{2^m} \equiv 0 \, or \, 1 \, (mod \, 2^{m+1})$$

(the proof is by induction).

Now let us write $n = 2^m l$, where l is odd, and let us consider residues modulo 2^{m+1}. Then

$$\sum_{1}^{n}(N-i)^n \equiv \frac{1}{2}n = 2^{m-1}l$$

since there are an even number of terms and their nth powers will be 1 for odd terms and 0 for even ones. From the lemma it follows that N^n must be either 0 or 1 modulo 2^{m+1}. So if CLE is satisfied, either $2^{m-1}l$ must be divisible by 2^{m+1}, which is impossible, or $2^{m-1}l - 1$ must be divisible by 2^{m+1}, which can only happen if $m = 1$.

So for CLE to be satisfied for even n, we must have

$$n \equiv 2\,(mod\,4)$$

Next, consider residues modulo 8. If $n \equiv 2\,(mod\,4)$, the consecutive nth powers modulo 8 are 0, 1, 0, 1, 0, 1,... so that (as before) the sum of n nth powers modulo 8 is $\frac{1}{2}n$. Thus we have either $\frac{1}{2}n \equiv 0$, which is impossible, or $\frac{1}{2}n \equiv 1$. In other words, for CLE to be satisfied for even n we must have

$$n \equiv 2\,(mod\,16)$$

Odd values of n

If n is odd then

$$\sum_{1}^{n}(N-i)^n \equiv 0\,(mod\,n)$$

(Proof: the series is equivalent to $\sum_{-(n-1)/2}^{(n-1)/2} i^n$, but since n is odd, $(-i)^n + i^n = 0$).

This implies $n \mid N^n$. If n is square-free (ie. has no repeated factors) then it further implies $n \mid N$, which implies that $k = N/n$ is an integer. Since we shall show later in this paper that $1 < k(n) < 2$ for $n > 3$, this is a contradiction and so CLE cannot be satisfied. (For an example of $n \mid N^n \not\Rightarrow n \mid N$, consider $n = 9$ and $N = 12$. 12^9 is divisible by 9, but 12 is not).

Next, consider residues modulo 8. If n is odd then the consecutive nth powers modulo 8 are 0, 1, 0, 3, 0, 5, 0, 7,... To get a perfect nth power as the sum of the previous n nth powers, consider the different possible values of $n\,mod\,8$:

1: there is no way of getting the sum of 1 term in the series to equal the next term (ie. there are no identical consecutive numbers in the series).

3: the only ways of getting the sum of 3 consecutive terms in the series to equal the next term are $3 + 0 + 5 = 0$ and $7 + 0 + 1 = 0$.

5: there is no way of getting the sum of 5 terms in the series to equal the next term.

7: any series of 7 terms beginning with a non-zero value will add up to 0 and consequently equal the next term in the series.

Thus for CLE to be satisfied for odd n we must have

$$n \equiv 3 \, (mod \, 4)$$

and n must have at least one repeated factor.

[Note also that if we denote by $sq(n)$ the factor by which n fails to be square-free (so that $sq(n)$ equals n divided by all the primes that divide n: for example, $sq(6) = 1$, $sq(18) = 3$, $sq(54) = 9$) then $k(n)$ must be an integer multiple of $1/sq(n)$. This may come in useful in further research, since it will be seen that $k(n) \to 1/ln2$ very rapidly as $n \to \infty$.]

Evaluating $N(n)$

We have $CLF_n(N) = \sum_1^n (1 - i/N)^n$.

But $(1 - i/N)^N < e^{-i}$ and $(1 - i/N)^N \to e^{-i}$ as $n \to \infty$,

whence $(1 - i/N)^N < e^{-in/N} = e^{-i/k}$.

Thus

$$CLF_n(N) < e^{-1/k} + e^{-2/k} + e^{-3/k} + ... = \frac{e^{-1/k} - e^{-(n+1)/k}}{1 - e^{-1/k}}$$

which gives us the simpler inequality

$$CLF_n(N) < \frac{e^{-1/k}}{1 - e^{-1/k}}$$

Since $CLF_n(N)$ is an increasing function of N and hence of k, and so is the right-hand side of this inequality, it follows that if k_0 is the value of k that makes the RHS equal to 1, the value of k that makes $CLF_n(N) = 1$ will be greater than k_0.

But RHS=1 means $e^{-1/k} = 1 - e^{-1/k}$, which means $k_0 = 1/ln2$. Thus we have

$$k(n) > 1/ln2$$

Numerical observations

Solving $CLF_n(N) = 1$ numerically, the following facts emerge:

$k(n)$ is a decreasing function of n. Not only is it bounded below by $1/ln2$ but it actually converges to it.

$N(n) = 1.5 + \frac{n}{ln2} + O(1/n)$. **This formula is remarkably accurate:** for $n > 10$ the value of the $O(1/n)$ term is about $\frac{1}{400n}$.

Equivalently, we can say $k(n) = \frac{1}{ln2} + \frac{1.5}{n} + O(1/n^2)$.

Here is a table of some calculated values:

n	$1.5+n/ln2$	$N(n)$
2	4.385390	5.000000
4	7.270780	7.329472
8	13.041560	13.042709
16	24.583121	24.583271
32	47.666241	47.666320
64	93.832483	93.832523
128	186.164965	186.164986
256	370.829930	370.829940

Summary

For odd n the theorem is proved unless n has a repeated prime factor and $n \equiv 3\,(mod\,4)$.

For even n the theorem is proved unless $n \equiv 2\,(mod\,16)$.

Calculations show that for the theorem to be false, $N(n) = 1.5 + \frac{n}{ln2} + \varepsilon(n)$ must be an integer, where $\varepsilon(n) \sim \frac{1}{400n}$.

Future directions

It would be delightful to have a proof of the formula $N(n) = 1.5 + \frac{n}{ln2} + O(1/n)$ rather than having to deduce it from the observed results of computations.

On the modular arithmetic side, the case of non-square-free n needs to be looked into in more detail.

On the numerical side, we can rephrase the theorem in terms of rational approximations to $1/ln2$: the theorem holds for large n as long as $\frac{n}{ln2}$ is never too close to a half-integer. There is a whole section of Hardy and Wright on approximation of irrationals by rationals that I have never read thoroughly enough.

Another line of attack is the observation that when n is not square-free then $k(n)$ must be a multiple of $1/sq(n)$. Can we combine this with the observed numerical formula for $k(n)$ and thus obtain a contradiction? It may be that $k(n)$ always manages to squeeze so close to $1/ln2$ that there is no room for it to be a multiple of $1/sq(n)$.

A different line of approach: Bernoulli polynomials

Bernoulli polynomials are an extension of Bernoulli numbers. They obey this recurrence relation:

$$B_n(x) = (B + x)^n$$

where "B^n" is replaced by "B_n" after the right-hand side has been expanded symbolically. They can also be derived as coefficients in the following power series expansion:

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!}$$

The hopeful fact about Bernoulli polynomials in our case is that

$$\sum_{i=a}^{b} i^n = \frac{1}{n+1}\{B_{n+1}(b+1) - B_{n+1}(a)\}$$

which means that the equation whose solutions we are investigating,

$$\sum_{1}^{n}(x-i)^n = x^n$$

boils down to

$$\frac{1}{n+1}\{B_{n+1}(x) - B_{n+1}(x-n)\} = x^n$$

or even

$$B_{n+1}(x) - B_{n+1}(x-n) = (n+1)x^n$$

Now $B_{n+1}(x)$ is a polynomial of degree $n+1$ in x, so that in the area we're looking in, with $x \approx n/ln2$, $x - n \approx 0.3x$, which means that $B_{n+1}(x-n)$ will be infinitesimal in comparison with $B_{n+1}(x)$, so that the simplified equation

$$B_{n+1}(x) = (n+1)x^n$$

will probably end up having the same asymptotic behaviour as the original.

Another hopeful line of inquiry is that $B_{n+1}(x)$ is the coefficient of $t^{n+1}/(n+1)!$in the expansion of $te^{tx}/(e^t-1)$, and x^n is the coefficient of $t^n/n!$ in the expansion of e^{tx}, so that $(n+1)x^n$ is the coefficient of $t^{n+1}/(n+1)!$ in the expansion of te^{tx}. As it stands, the only way to make use of this correspondence is to differentiate both $e^{tx}/(e^t-1)$ and e^{tx} n times with respect to t - but it is still good to find some sort of an occurrence of an exponential function, given that we are trying to get a reason for $\ln 2$ appearing in the result.

ADDITIONAL MATERIAL

Sketch of an extension for even n

(This has been copied from the manuscript and has not yet been checked in detail: don't read it until it has been checked and corrected).

We have the standard number-theoretic function $\phi(n)$, which is defined by $\phi(p) = p - 1$ and $\phi(pq) = \phi(p)\phi(q)$. Let us define an alternative, $\hat{\phi}(n)$, which is defined by $\hat{\phi}(p) = p - 1$ and $\hat{\phi}(pq) = LCM(\hat{\phi}(p)\hat{\phi}(q))$.

Lemma:

$\sum_0^{n-1} i^n \neq 0\,(mod\, M)$ only if $\hat{\phi}(M) \mid n$.

Unchecked proof:

If $\hat{\phi}(M) \nmid n$ then $\exists j$ such that $j^n \neq 1\,(mod\, M)$ and j is relatively prime to M. (this assertion needs checking as well).

Then, still working modulo M:

By relative primality, $0, j, 2j, \dots\dots, (n-1)j$ is a permutation of $0, 1, 2, \dots\dots n-1$,

so that $\sum (ij)^n = \sum i^n$,

or $j^n \sum i^n = \sum i^n$, or $(j^n - 1) \sum i^n = 0$,

which implies $(j^n - 1) \sum i^n = 0$, since $j^n \neq 1\,(mod\, M)$.

(this needs correcting, since what we actually need is not only $j^n - 1 \neq 0\,(mod\, M)$ but also that $j^n - 1$ should be relatively prime to M).

Anyway, if the lemma can be shown to hold to the extent to which it is needed, we can put $M = n$ and deduce that if $\hat{\phi}(M) \nmid n$ then $N^n \equiv 0\,(mod\, n)$, which means that we once more get "for CLE to be satisfied, n must have at least one square factor", just as in the case of odd n. But even assuming that the proof can be made to work, this is still a weaker result than in the odd case, since $\hat{\phi}(n) \mid n$ for $n = 6$ and $n = 42$, to give just two examples.

There is a further obscure note in the manuscript: "If $\hat{\phi}(n) \mid n$ then all powers are 1 mod n, and a fortiori $1 \mid p\,(\mid n)$. This makes it harder to constrain N, but not impossible".