Mathematics 115 Professor K. A. Ribet

Homework due Friday, November 9, 2012

I. *What follows is an interesting proposed proof by Paul Pollack that there are infinitely many primes:*

> Consider the power series $\sum_{n=1}^{\infty} a_n x^n$ where $a_n = \sum_{d|n} \mu(d)$. By Theorem 4.7, this apparently infinite series contains only one non-zero term, namely x. Assume that there are only finitely many prime numbers, and let D be the product of the primes. Then $\mu(d) \neq 0$ precisely when d divides D. When x is a real number in $(-1, 1)$, we can rewrite $\sum a_n x^n$ as
>
> $$\sum_d \mu(d) \left(x^d + x^{2d} + x^{3d} + \cdots\right) = \sum_d \frac{\mu(d)x^d}{1-x^d},$$
>
> where the equality comes from the geometric series formula. The sum on d extends over all positive integers d in principle, but in fact is a finite sum over the diviors d of D. Hence we have simply
>
> $$x = \sum_{d|D} \frac{\mu(d)x^d}{1-x^d}.$$
>
> All of the denominators $1 - x^d$ are divisors of the single polynomial $1 - x^D$. Multiply all terms by this common denominator to get
>
> $$x(1-x^D) = \sum_{d|D} \mu(d)x^d f_d(x)$$
>
> where $f_d(x) = \dfrac{1-x^D}{1-x^d} = 1 + x^d + x^{2d} + \cdots + x^{D-d}$. Our reasoning shows that this identity is valid for real numbers of absolute value less than 1. However, both sides are polynomials in x with integer coefficients. The polynomials on the two sides of the equality must be equal as polynomials because they coincide for an infinite number of values of x. The degree of $f_d(x)$ is $D - d$, so the degree of $x^d f_d(x)$ is D. Thus we have written $x(1 - x^D)$ as a sum of polynomials of degree D. This is a contradiction because $x(1 - x^D)$ has degree $D + 1$.

Decide whether or not this skeletal proof is correct. If it is correct, rewrite it so that it includes adequate justifications of all subtle points. If it is flawed, explain carefully why the proposed proof is meritricious.

II. (Reference: `en.wikipedia.org/wiki/LucasLehmer_primality_test`.) As in the lecture on November 1, p is an odd prime number and M is the Mersenne number $2^p - 1$. Let $\sqrt{3} \approx 1.73$ be the positive real square root of 3 and write $\mathbf{Z}[\sqrt{3}]$ for $\{\, a + b\sqrt{3} \mid a, b \in \mathbf{Z}\,\}$. Let s_i be the Lucas–Lehmer sequence 4, 14, 194, 37634,.... First off, *write a proof* that one has

$$s_i = (2+\sqrt{3})^{2^i} + (2+\sqrt{3})^{-2^i}$$

for $i = 0, 1, \ldots$.

We suppose now that $s_{p-2} \equiv 0 \bmod M$ and wish to show that M is prime. What follows is a skeletal proof. *Your job is to rewrite the proof in your own words, giving detailed justification for your arguments.*

> Suppose that M is *not* prime and let q be the smallest positive divisor of M other than 1 and M. Then $2 < q \leq \sqrt{M}$. Declare two elements $a + b\sqrt{3}$ and $c + d\sqrt{3}$ of $\mathbf{Z}[\sqrt{3}]$ equivalent if $a \equiv c \bmod q$ and $b \equiv d \bmod q$. Let R be the set of equivalence classes for this relation and note that we can add, subtract and multiply elements of R just as we do for elements of $\mathbf{Z}/q\mathbf{Z}$. In fact, $\mathbf{Z}/q\mathbf{Z}$ is a subset of R because we can identify a mod q with the equivalence class of $a + 0\sqrt{3}$. The inclusion $\mathbf{Z}/q\mathbf{Z} \hookrightarrow R$ is compatible with the arithemtic operations $+$, $-$, $\times$ on the two sets (which would be called rings in Math 113).
>
> Let ω be the equivalence class of $2 + \sqrt{3}$. Then we have $0 = s_{p-2} = \omega^{2^{p-2}} + \omega^{-2^{p-2}}$ in R, so that $\omega^{2^{p-1}} = -1$ in R. We may deduce from this equation that $\omega^{2^p} = 1$ and that $\omega^j \neq 1$ for positive integers j less than 2^p. It follows that ω has precisely 2^p distinct powers in R. Since all of these powers are non-zero, we have $2^p < q^2 - 1$, i.e., $M < q^2$. This is a contradiction.