189-346/377B: Number Theory
Assignment 1: Corrections

1. Show that the cubic equation $x^3 - 3x + 1 = 0$ has three real roots. Write down an explicit formula for the roots of this equation in terms of nested square and cube roots of rational numbers, using the Cardano formula proved in class. Evaluate the resulting expression to 8 digits of decimal accuracy (in all possible ways!) and check that you indeed obtain, among the resulting expressions, real approximations to the three roots of the equation.

The fact that the polynomial has three real roots follows from a study of its local maxima and minima, using the intermediate value theorem. Cardano's formula for the roots gives the expressions

$$\left(\frac{-1+\sqrt{-3}}{2}\right)^{1/3} + \left(\frac{-1-\sqrt{-3}}{2}\right)^{1/3}. \tag{1}$$

Each of the two term in this sum has three possible complex cube roots, so evaluating the expression as a complex number by taking the cube roots arbitrarily, one is faced with 9 possible values. However, only a few of these possible evaluations lead to real numbers. For example, one can observe that

$$\frac{-1+\sqrt{-3}}{2} = \cos(2\pi/3) + i\sin(2\pi/3)$$

is a cube root of 1, and therefore its cube roots are primitive ninth roots of 1, of the form

$$\cos(2k\pi/9) + i\sin(2k\pi/9), \qquad \text{with } k \equiv 1 \pmod 3,$$

i.e., $k = 1, 4$ or 7. If one chooses the second cube root in (1) to be the complex conjugate quantity, one obtains the three real values

$$\begin{aligned} r_1 &= 2\cos(2\pi/9) = 1.5320\ldots \\ r_2 &= 2\cos(8\pi/9) = -1.8793\ldots \\ r_3 &= 2\cos(14\pi/9) = 0.3472\ldots \end{aligned}$$

which one can check (numerically, for example) agree with the roots of the original cubic.

2. Make a table of the factorisations of the integers $2^k + 1$ for $1 \leq k \leq 16$. For which values of k is this integer a prime? Formulate a conjecture about the values of k for which $2^k + 1$ is prime, based on your calculations.

The pattern that almost everyone discerned is that $2^k + 1$ seemed to be prime only when k was a power of 2. The most ambitious conjecture, that $2^k + 1$ is prime *if and only if* k is a power of 2, turns out to be false – it fails when $k = 2^5$, and what's more, appears to fail consistently from that point on!– although Fermat apparently fell into the trap. However, one could show that if k is *not* a power of 2, then $2^k + 1$ is necessarily composite, by showing that if $k = 2^e k_0$ with k_0 odd, then $2^k + 1$ is divisible by $2^{2^e} + 1$, which is necessarily a proper divisor of $2^k + 1$ when $k_0 \neq 1$.

3. Let $li(x) = \int_2^x \frac{dt}{\log(t)}$ be the function that occurs in Gauss's statement of the Prime Number Theorem. Show that

$$\lim_{x \longrightarrow \infty} \frac{li(x)}{x/\log(x)} = 1,$$

and conclude that $li(x)$ can be replaced by the simpler function $x/log(x)$ in the statement of the PNT.

Integration by parts gives

$$li(x) = \frac{x}{\log(x)} - \frac{2}{\log(2)} - \int_2^x \frac{dt}{\log^2(t)}.$$

Hence, one is done if one can show that

$$\lim_{x \to \infty} \frac{\int_2^x \frac{dt}{\log^2 t}}{\int_2^x \frac{dt}{\log(t)}} = 0.$$

This can be proved using l'Hopital's rule.

4. Show that 55 can be written as a difference of two perfect integer squares in exactly two different ways, and write down those expressions.

If

$$55 = a^2 - b^2 = (a - b)(a + b),$$

then we can assume that $a > b \geq 0$ without loss of generality, since changing the signs of a and b does not affect the squares in the expression. Since $a - b$ is smaller than $a + b$ and both are factors of 55, the only possibilities are $(a - b, a + b) = (1, 55)$ or $(5, 11)$. Solving the linear equations gives $(a, b) = (28, 27)$ or $(8, 3)$.