Math 110 HW 3 solutions

May 8, 2013

1. For any positive real number r, prove that $x^r = O(e^x)$ as functions of x.

   Suppose $r < 1$. Then $\lim_{x\to\infty} x^r = 0$. And $\lim_{x\to\infty} e^x = \infty$. Therefore

   $$\lim_{x\to\infty} \frac{x^r}{e^x} = 0,$$

   which means $x^r = O(e^x)$.

   Now suppose $r \geq 1$. Consider the ratio $\frac{x^r}{e^x}$, where both numerator and denominator approach ∞ at ∞. Using L'Hôpital's rule, this limit is the same as that of $r \cdot \frac{x^{r-1}}{e^x}$. If $r - 1 = 0$ then we mean $1/e^x$, whose limit is 0. If $0 < r < 1$ we have reduced to the previous case.

   So, for a positive integer n, suppose $n \leq r < n + 1$, then after n iterations of L'Hôpital's rule, we conclude that the limit is 0. Thus, $x^r = O(e^x)$ for all $r > 0$.

2. Compute the continued fraction expansion of the three numbers $427/67$, $\sqrt{7}$ and $\tan(1)$. (For the latter number, you don't need to prove the result you get is correct, simply do enough computations to be able to guess the pattern (and show how these computations were performed). Of course 1 is in radians).

   First, $67 \cdot 6 = 402$, so $427/67 = 6 + 25/67$. Now $25 \cdot 2 = 50$, so $67/25 = 2 + 17/25$, so far we have

   $$427/67 = 6 + \frac{1}{2 + \frac{17}{25}}.$$

   Similarly $25/17 = 1 + 8/17$, and $17/8 = 2 + 1/8$, and finally $8/1 = 8$. So altogether we have a terminating continued fraction, with $a_0 = 6, a_1 = 2, a_2 = 1, a_3 = 2, a_4 = 8$:

   $$427/67 = 6 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + 1/8}}}.$$

   For $\sqrt{7}$, let's start with the approximate decimal expansion. 2.64575131.

   Below is a list of decimals where each one is obtained from the last by removing the integer

part and taking the reciprocal.

$$\begin{aligned}
2.64575131106 &\approx 2.64575131106\\
1/.64575131106 &\approx 1.54858377037\\
1/.54858377037 &\approx 1.82287565548\\
1/.82287565548 &\approx 1.2152504371\\
1/.2152504371 &\approx 4.64575130937\\
1/.64575130937 &\approx 1.54858377442
\end{aligned}$$

and so on. In this way we obtain $a_0 = 2, a_1 = a_2 = a_3 = 1, a_4 = 4$, and based on the similarities in decimal expansions, conjecture that $a_{n+4} = a_n$ for all $n > 0$.

We can check this conjecture explicitly. The sequence of numbers above may be written, taking siginficant figures into account, as

$$\begin{aligned}
\sqrt{7} &\approx 2.64575131106\\
\frac{1}{\sqrt{7}-2} &\approx 1.5485837703\\
\frac{1}{\frac{1}{\sqrt{7}-2}-1} &\approx 1.822875655\\
\frac{1}{\frac{1}{\frac{1}{\sqrt{7}-2}-1}-1} &\approx 1.21525044\\
\frac{1}{\frac{1}{\frac{1}{\frac{1}{\sqrt{7}-2}-1}-1}-1} &= \sqrt{7}+2 \text{ (our conjecture).}
\end{aligned}$$

And rewriting this sequence once more, we get

$$\sqrt{7}, \frac{1}{\sqrt{7}-2}, \frac{\sqrt{7}-2}{3-\sqrt{7}}, \frac{3-\sqrt{7}}{2\sqrt{7}-5}, \frac{2\sqrt{7}-5}{8-3\sqrt{7}}$$

So the claim is that the last fraction in that sequence is equal to $\sqrt{7}+2$, which is to say

$$(8-3\sqrt{7})(\sqrt{7}+2) = 2\sqrt{7}-5,$$

which is true. Thus the continued fraction expansion of $\sqrt{7}$ uses the sequence $2, 1, 1, 1, 4, 1, 1, 1, 4, 1, \ldots$.

For $\tan(1)$, let us make a sequence of decimals as above. We get, reducing significant figures

due to calculator limitations:

$$\begin{aligned}
\tan 1 &\approx 1.55740772465 \\
1/.55740772465 &\approx 1.79401891251 \\
1/.79401891251 &\approx 1.2594158454 \\
1/.25941584545 &\approx 3.854814644 \\
1/.85481464428 &\approx 1.16984425 \\
1/.16984425418 &\approx 5.8877470 \\
1/.88774701168 &\approx 1.126447 \\
1/.12644704724 &\approx 7.90844 \\
1/.90844880784 &\approx 1.1007 \\
1/.10077749166 &\approx 9.922
\end{aligned}$$

So we guess that the continued fraction has coefficients $1, 1, 1, 3, 1, 5, 1, 7, 1, 9, 1, 11 \ldots$ in other words $a_{2n} = 1, a_{2n+1} = 2n + 1$. To write it out explicitly we have

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5 + \ldots}}}}}$$

3. In the continued fraction expansion of $\sqrt{7}$ calculated in the previous problem, let n be any integer such that $a_{n+1} = 2a_0$. Compute the convergent $\frac{p_n}{q_n}$ and show that $x = p_n, y = q_n$ gives a solution to Pell's equation $x^2 - 7y^2 = 1$.

   As we know that means $a_{n+1} = 4$, which happens when $n = 4k - 1$ for integer $k > 0$, and we always mean $a_n = 1$.

   Since the $a_0 = 2$ but otherwise $a_{4k} = 4$, we have the formula for $r_{n+4} = \frac{p_{n+4}}{q_{n+4}}$:

$$\begin{aligned}
\frac{p_{n+4}}{q_{n+4}} &= 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{r_n + 2}}}} \\
&= \frac{8r_n + 21}{3r_n + 8} \\
&= \frac{8p_n + 21q_n}{3p_n + 8q_n}.
\end{aligned}$$

   Calculating explicitly that $p_3/q_3 = 8/3$ and $p_7/q_7 = 127/48$ we see this does fit the formula.

   To write down a closed form for this we would write

$$\begin{bmatrix} p_{n+4} \\ q_{n+4} \end{bmatrix} = \begin{bmatrix} 8 & 21 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} p_n \\ q_n \end{bmatrix}$$

   and write more explicitly the powers of the 2×2 matrix A. But that is not much more enlightening as it involves for example calculating $(8 + 3\sqrt{7})^n$.

Suppose (p_n, q_n) is a solution to Pell's equation as given, i.e. $p_n^2 - 7q_n^2 = 1$. Then multiplying out $(8p_n + 21q_n)^2 - 7 \cdot (3p_n + 8q_n)^2$, we have $64(p_n^2 - 7q_n^2) - 63(p_n^2 - 7q_n^2) = 64 - 63 = 1$. Therefore (p_{n+4}, q_{n+4}) is also a solution to the same Pell's equation. We proceed by induction: the pair $(p_3, q_3) = (8, 3)$ satisfies $8^2 - 7 \cdot 3^2 = 1$, therefore for all $n = 4k - 1$, the pair (p_n, q_n) is a solution to the Pell's equation $x^2 - 7y^2 = 1$.

4. Let $N = 8633243$. You compute that $2^{8633242} \equiv 8236849 \pmod{N}$. From this information, what can you conclude about the prime factorisation of N?

   We can conclude that N is not prime, because otherwise $2^{N-1} \equiv 1 \pmod{N}$ as N is clearly not divisible by 2.

5. Let a and n be positive integers with $\gcd(a; n) = 1$. The order of a modulo n (denoted $ord_n(a)$) is defined to be the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

   Let r be a positive integer. Prove that $a^r \equiv 1(modn)$ if and only if r is divisible by $ord_n(a)$. (This is Exercise 20 in Chapter 3 of Trappe & Washington, which gives out hints for the proof).

   For the "if" direction, suppose $d|r$ where $d = ord_n(a)$. Then $a^r = a^{kd}$ for some integer k, which means $a^r = (a^d)^k \equiv 1^k \equiv 1 \pmod{n}$.

   For the other direction, suppose $a^r \equiv 1 \pmod{n}$. We know $d \leq r$, so there are unique integers b, c such that $bd + c = r$, $b > 0$ and $0 \leq c < d$. Now, $a^{bd} \equiv 1 \pmod{n}$ as in the previous argument, and also $a^{bd+c} \equiv r \pmod{n}$. We cannot simply divide by a^{bd}. But this gives us

   $$a^{bd+c} = a^b d \cdot a^c \equiv 1 \cdot a^c \equiv 1 \pmod{n}.$$

   Since 1 is the identity under multiplication, we know $1 \cdot a^c \equiv a^c \pmod{n}$, so $a^c \equiv 1 \pmod{n}$.

   Now, we know $0 \leq c < d$. If $c \neq 0$, then c is a positive integer such that $a^c \equiv 1 \pmod{n}$, which contradicts the definition of d as $ord_n(a)$. So $c = 0$, which means $r = bd$ for some positive integer b, i.e., r is divisible by b.

   (Again, do NOT do any division mod n in this solution unless you have explained why the number being divided is a unit mod n.)

6. Show that 65 is a strong pseudoprime to base 8 and base 18 but not to base 14 (which is the product of 8 and 18 modulo 65).

   Since 64 is a power of 2, we can write $d = 1$ and $r = 6$ for the general case $n - 1 = 2^d \cdot r$. Obviously 8, 18 and 14 are not 1 mod 65. But let us look at how they exponentiate:

   $8^2 \equiv -1 \pmod{65}$, and so $8^{2^n} \equiv 1 \pmod{65}$ for all $n > 1$. That makes 8 a strong pseudoprime mod 65.

   Also, $18^2 = 324 \equiv -1 \pmod{65}$, so similarly, 18 is a strong pseudoprime mod 65.

   However, $14^2 = 196 \equiv 1 \pmod{65}$, so there is no $i \leq r$ for which $2^i \cdot d \equiv -1 \pmod{6}5$, and $14^1 \not\equiv 1 \pmod{65}$. Thus 14 is not a strong pseudoprime mod 65.

7. Let n be an odd composite integer which is either a prime power or divisible by an integer which is congruent to 3 modulo 4. Suppose that n is a strong pseudoprime to the bases b_1 and b_2. Prove that n is a strong pseudoprime to the base $b_1 b_2$.

Since n is odd, its factors are odd. If $m|n$ and $m \equiv 3 \pmod 4$, then at least one of the primes dividing m must be $3 \pmod 4$. So let us consider when a prime $p|n$ and $p \equiv 3 \pmod 4$.

In this case, writing $n - 1 = 2^s \cdot d$ for $r \geq 0$ and d odd, if $b_i^{2^r \cdot d} \equiv -1 \pmod n$ then it is $-1 \pmod p$, which is impossible for $r > 0$ as -1 is not a square mod p. Thus, $b_1^d \equiv \pm 1 \pmod n$ and $b_2^d \equiv \pm 1 \pmod n$. Therefore $(b_1 b_2)^d \equiv \pm 1 \pmod n$, so n is a strong pseudoprime to the base $b_1 b_2$.

Now suppose $n = p^k$ for an odd prime p. In this case 1 only has two square roots mod n, which are ± 1.

To see this, first note that any square root of $1 \pmod p^k$ must be equal to $\pm 1 \pmod p$. Write $a = mp \pm 1$ for some integers m, a such that $a^2 = 1 \pmod p^k$.

$a^2 = (mp \pm 1)^2 = m^2 p^2 \pm 2mp + 1$ so $p^k | (m^2 p^2 \pm 2mp)$, so $p^{k-1} | m^2 p \pm 2m$. Since p divides the first term it must divide the second, and $p \nmid 2$ so $p|m$; but then a higher power of p divides the first term, and thus must also divide the second, and in the end we get $p^{k-1}|m$ so $p^{k-1}|m$.

But then $p^k | mp$, so $a = \pm 1 \mod p^k$.

Thus, defining d similarly to the above part we find that $b_i^d = \pm 1 \pmod n$, and again, n is a strong pseudoprime to the base $b_1 b_2$.