Solving discrete problems — Math 2020, Spring 2005

Solutions to homework 2

To fit on the paper better, I'll start with 4 first:

4. find a proof by contradiction for the statement "$x = \log_{10}(5)$ is irrational", using the following steps:
   o. Aiming for a contradiction, assume x is rational. (The opposite (or **negation**) of what we want to prove.)
   i. Use the **definition**: What does it mean for x to be rational?
   ii. Use the **definition**: What does it mean for $x = \log_{10}(5)$?
   iii. Put i and ii together, and use some **properties** of logatithms, e.g., $(a^{b/c})^c = a^b$, so that from the equality $x = \log_{10}(5)$ you get another equality, involving only integers, and using notation introduced in steps i and ii.
   iv. Use a **previous result**, in this case, apply unique prime factorisation.
   v. Derive a contradiction. This means that step o was wrong, so x is irrational. QED

Proof that $\log_{10}(5)$ is irrational:
Suppose that x was rational. Then for some integers a, b, we have $x = a/b$.
By definition, if $x = \log_{10}(5)$, then $10^x = 5$.
Note that since 5 is greater than 1, this means x must be positive, so a and b can also be taken to be positive.
Substituting $x = a/b$ into $10^x = 5$ gives $10^{a/b} = 5$, now take b powers of both sides, to get $(10^{a/b})^b = 5^b$ so $10^a = 5^b$, where a and b are positive integers.
But $10^b = (2 \times 5)^b = 2^b \times 5^b$ is even, and 5^b is odd, so we have an odd number equal to an even number, which is impossible.
So the original assumption that x is irrational must have been wrong.
So x must be irrational. QED

As discussed in the class before the homework is due, it's useful to do question 3 before question 1:

3. For any positive integer m, the polynomial $(x - 1)$ divides $x^m - 1$. What is the quotient?

First, note that $(x - 1)$ *does* divide the polynomial $f(x) = x^m - 1$.
This follows from the result that says that

$$(x - a) \text{ is a factor of } f(x) \iff f(a) = 0.$$

So, this means we can make the division, with no remainder. What we get is:

$$\frac{(x^m - 1)}{(x - 1)} = x^{m-1} + x^{m-2} + \cdots + x + 1,$$

or in other words,

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1).$$

There are several ways to show this; we can use long division of polynomials (which you should be able to do), or proof by induction (which we've not discussed), or else you can just prove that $(x-1)(x^{m-1}+x^{m-2}+\cdots+x+1) = x^m - 1$ by a direct computation:

$$\begin{aligned}
(x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1) &= x \times (x^{m-1} + x^{m-2} + \cdots + x + 1) - 1 \times (x^{m-1} + x^{m-2} + \cdots + x + 1) \\
&= x \times (x^{m-1} + x^{m-2} + \cdots + x + 1) \\
&\quad -1 \times (x^{m-1} + x^{m-2} + \cdots + x + 1) \\
&= x^m + x^{m-1} + x^{m-2} + \cdots + x^2 + x \\
&\qquad - x^{m-1} - x^{m-2} - \cdots - x^2 - x - 1 \\
&= x^m - 1 \quad \text{(since all the terms apart from these cancel)}
\end{aligned}$$

As discussed in class, there is another useful factorisation to know, closely related to the above:

If m is odd, then

$$\frac{(x^m + 1)}{(x + 1)} = x^{m-1} - x^{m-2} + \cdots - x + 1,$$

or in other words,

$$x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + \cdots - x + 1).$$

This can be proved by a similar direct caclulation as above, or else by substituting $x = -t$ in the previous formula, and then changing t to x.

1. Find the prime factorisations of

$$2^{15}+1,\ 2^{36}-1,\ 3^{15}-1,\ 3^{30}-1$$

Several factors can be found by applying the formulas above:

$$\begin{aligned}
2^{15}+1 &= (2^5+1)((2^5)^2-2^5+1) && \text{apply formula with } m=3\\
&= (2+1)(2^4-2^3+2^2-2+1)((2^5)^2-2^5+1) && \text{apply formula with } m=5\\
&= 3\times 11\times 993 && \text{multiply out expressions in previous line}\\
&= 3\times 11\times 3\times 331 && \text{factor by hand}\\
&= 3^2\times 11\times 331 && \text{collect terms}
\end{aligned}$$

You now need to check that 331 is prime, e.g., by checking that it is not divisible by any prime up to $\sqrt{331}=18.19..$, i.e., check to see it is not divisible by $2,3,5,7,11,13,17$.

$$\begin{aligned}
2^{36}-1 &= (2^{18}+1)(2^{18}-1) && \text{apply formula with } m=2\\
&= (2^6+1)((2^6)^2-2^6+1)(2^9-1)(2^9+1) && \text{apply formula with } m=2 \text{ and } m=3\\
&= (2^2+1)((2^2)^2-2^2+1)((2^6)^2-2^6+1)(2^3-1)((2^3)^2+2^3+1)(2^3+1)((2^3)^2-2^3+1)\\
& && \text{apply formulas three times, with } m=3\\
&= 5\times 13\times 4033\times 7\times 73\times 9\times 57 && \text{multiply out expressions in previous line}\\
&= 5\times 13\times 37\times 109\times 7\times 73\times 3\times 3\times 3\times 19 && \text{factor by hand}\\
&= 3^3\times 5\times 17\times 13\times 19\times 37\times 73\times 109 && \text{collect terms}
\end{aligned}$$

Note, here we had to factor 4033 by hand, by trial and error — just try all the primes up to it's square root. Then we also have to check that all the factors we have now are prime, by a similar check.

Other examples work similarly; the final solutions will be:

$$3^{15}-1=2\times 11^2\times 13\times 4561$$

$$(3^{30}-1)=2^3\times 7\times 11^2\times 13\times 31\times 61\times 271\times 4561$$

You'll have to check that 4561 is prime by checking whether it's divisible by primes up to $\sqrt{4561}=67.53$.

2. Find four prime divisors of $34^{110}-1$.

Using the same formulas as above, you can show this is divisble by $34-1=33=3\times 11$ and $34+1=35=5\times 7$ — see example in lecture notes. So four factors are $3,5,7,11$.

It's actually quite hard to get much further than this. You can factor $x^{110}-1$ further; you'll get the following factors:

$$\begin{aligned}
&(x-1)\\
&(x+1)\\
&(x^4-x^3+x^2-x+1)\\
&(x^4+x^3+x^2+x+1)\\
&(x^10-x^9+x^8-x^7+x^6-x^5+x^4-x^3+x^2-x+1)\\
&(x^10+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)\\
&(x^{40}-x^{39}+x^{35}-x^{34}+x^{30}-x^{28}+x^{25}-x^{23}+x^{20}-x^{17}+x^{15}-x^{12}+x^{10}-x^6+x^5-x+1)\\
&(x^{40}+x^{39}-x^{35}-x^{34}+x^{30}-x^{28}-x^{25}+x^{23}+x^{20}+x^{17}-x^{15}-x^{12}+x^{10}-x^6-x^5+x+1)
\end{aligned}$$

These correspond to taking $m=2,5,11$ in the formulas, so this should not be too hard for you to find these factors.

Now substitute $x=34$ in each of these, to get: $34^{110}-1 = 33\times 35\times 1298155\times 1376831\times 2005395532515211\times 2126934655697951\times 1762754021281961784468986211478383142283336007888426464145555 1\times 186958751603288101691671588615473011545742554776377050715140 51$

Although these are much smaller than

$34^{110}-1=2901889523880178336291943666966124899737193689356338261769831486911088680280492287484 6999958329819924496806146599866914788861277835823321005031376912339682675492923637 75$,

these numbers are still too big for most computers to factor in a reasonable length of time.

But the question only asked for 4 factors, so at least you don't need to try and factor these huge numbers for homework.