Homework 5: English proofs

Due date: Wednesday May 5 at 11:00 PM (Seattle time, i.e. GMT-7)
If you work with others (and you should!), remember to follow the collaboration policy.
In general, you are graded on both the clarity and accuracy of your work. Your solution should be clear enough that someone in the class who had not seen the problem before would understand it.
We sometimes describe approximately how long our explanations are. These are intended to help you understand approximately how much detail we are expecting.

Be sure to read the grading guidelines for more information on what we're looking for.

While working on the assignment, please (roughly) keep track of the time you spent on each problem. This is so that you have an idea of how to answer the feedback questions!

1. Collaborators

List any collaborators (i.e., other students) you worked with and which problems you worked on together, or state that you worked alone.

2. Euclid's algorithm [10 points]

Compute each of the following using Euclid's Algorithm. Show your intermediate results both as a sequence of gcd() calls. For your own understanding (and potentially for grading partial credit), we recommend writing out the tableau of intermediate values.

(a) $\text{gcd}(225, 65)$ [4 points]

(b) $\text{gcd}(354, 123)$ [5 points]

(c) $\text{gcd}(3^{30} + 1, 3)$ [1 point]

3. Inverses [20 points]

(a) Compute a multiplicative inverse of 15 $\pmod{103}$. Use the Extended Euclidean algorithm, showing the tableau and the sequence of substitutions. [5 points]

(b) Find **all** integer solutions to

$$15x \equiv 11 \pmod{103}$$

You must show **all** your work for this part. See lecture 15 for an example of the work needed. [8 points]

(c) Prove there are no integer solutions to

$$10x \equiv 3 \pmod{15}$$

Note: it's not enough to say that 10 does not have a multiplicative inverse $\pmod{15}$. If that were enough, then you could say the same for $10x \equiv 10 \pmod{15}$, but $x = 1$ is a solution to that equivalence.

You'll want to use proof by contradiction (suppose that there is an integer solution and go from there). [7 points]

4. GCD proof [6 points]

Show that if $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$ then $b \equiv c \pmod{d}$ where $d = \gcd(m, n)$.

5. A Proof By Contradiction [7 points]

Let p be a prime number, show that $\sqrt{p}$ is irrational. You may want to adapt the proof that $\sqrt{2}$ is irrational (see the section of week 4, problem 3.(c)). You can use the following fact without proof: For integers a, b and a prime number p: if $p|(ab)$ then $p|a$ or $p|b$.

6. Unique in Division [7 points]

Recall that the division theorem states that for any integers a and m with $m \geq 1$, there exist unique integers q and r such that $0 \leq r < m$ and $a = qm + r$. In this problem, you will show one part of this theorem — that the pair (q, r) is unique. More concretely, prove that the following holds: Suppose there exists integers q_1, r_1, q_2, r_2 satisfying $a = q_1 m + r_1$ and $a = q_2 m + r_2$ with $0 \leq r_1 < m$ and $0 \leq r_2 < m$, then $q_1 = q_2$ and $r_1 = r_2$.

7. Find The Bug [16 points]

7.1. I'm not FIBbing

Your friend is doing a proof with the Fibonacci numbers. The function f is defined by $f(0) = f(1) = 1$ and for all $n \geq 2$, and $f(n) = f(n-1) + f(n-2)$.

They are trying to show that $f(4) = 5$ – here is the proof they show you:

$$\begin{aligned}
f(4) &= 5 \\
f(3) + f(2) &= 5 \\
[f(2) + f(1)] + f(2) &= 5 \\
2f(2) + 1 &= 5 \\
2f(2) &= 4 \\
2(f(1) + f(0)) &= 4 \\
2(1 + 1) &= 4 \\
4 &= 4
\end{aligned}$$

(a) Clearly explain why the proof is incorrect. Your explanation must deal with the proof directly, not just the statement they are showing (e.g. just providing a counter-example is not sufficient for this part). [3 points]

(b) If the statement is correct, then write a correct proof. If it is incorrect, provide a counter example. [5 points]

7.2. Well...maybe I'm fibbing

Another friend wishes to show $(x-3)(-x+4) = x^2 - 7x + 12$ is true for all x. They show you their proof:

$$\begin{aligned}
&(x-3)(-x+4) = x^2 - 7x + 12 \\
&[(x-3)(-x+4)]^2 = (x^2 - 7x + 12)^2 \\
&(x^2 - 6x + 9)(x^2 - 8x + 16) = (x^4 - 7x^3 + 12x^2) + (-7x^3 + 49x^2 - 84x) + (12x^2 - 84x + 144) \\
&(x^4 - 8x^3 + 16x^2) + (-6x^3 + 48x^2 - 96x) + (9x^2 - 72x + 144) = x^4 - 14x^3 + 73x^2 - 168x + 144 \\
&x^4 - 14x^3 + 73x^2 - 168x + 144 = x^4 - 14x^3 + 73x^2 - 168x + 144
\end{aligned}$$

(a) Clearly explain why the proof is incorrect. Your explanation must deal with the proof directly, not just the statement they are showing (e.g. just providing a counter-example is not sufficient for this part). [3 points]

(b) If the statement is correct, then write a correct proof. If it is incorrect, provide a counter example. [5 points]

Extra Credit: Exponentially increasing fun [0 points]

Since $a\%n \equiv a \pmod{n}$, we know that we can reduce the base of an exponent in $\pmod{n}$ arithmetic. That is: $a^k \equiv (a\%n)^k \pmod{n}$. But the same is **not** true of the exponent! That is, we cannot say that $a^k \equiv a^{k\%n} \pmod{n}$. Consider, for instance, that $2^{10} \,\%\, 3 = 1$ but $2^{10\%3} \,\%\, 3 = 2^1 \,\%\, 3 = 2$. The correct way to simplify exponents is quite a bit more subtle. In this problem you'll prove it in steps.

(a) Let $R = \{t \in \mathbb{Z} : 1 \leq t \leq n-1 \land \text{gcd}(t,n) = 1\}$. Define the set $aR = \{ax\%n : x \in R\}$. Prove that $aR = R$ for every integer $a > 0$ with $\text{gcd}(a,n) = 1$.

(b) Consider the product of all elements in R (taken $\%n$) and consider the product of all the elements in aR (again, taken $\%n$). By comparing these two expressions, conclude that for all $a \in R$ we have $a^{\varphi(n)} \equiv 1 \pmod{n}$ where $\varphi(n) = |R|$.

(c) Use the previous part to show that for any $b \geq 0$ and $a \in R$ we have $a^b \equiv a^{b\%\varphi(n)} \pmod{n}$.

(d) Now suppose that $y = x^e \pmod{n}$ for some x with $\text{gcd}(x,n) = 1$ and e some integer ≥ 0 such that $\text{gcd}(e, \varphi(n)) = 1$. Let $d = e^{-1} \pmod{\varphi(n)}$. Prove that $y^d \equiv x \pmod{n}$.

(e) Prove the following two facts about φ: First, if p is prime then $\varphi(p) = p - 1$. Second, for any positive integers a and b with $\text{gcd}(a,b) = 1$, we have $\varphi(ab) = \varphi(a)\varphi(b)$.

These facts together are the basis for the most-widely used "public key encryption system." One chooses $n = pq$ for large primes p and q, and a value of e. The numbers n and e are made public to anyone who wants to send a message securely. To send a message x, the sender computes $y = x^e \,\%\, n$ and sends y (the "encrypted text"). To decrypt, one computes $y^d \,\%\, n$ (note that the recipient must be the one who chose p, q so they can calculate d). The security of the system relies on it being hard to compute d from just e and m.

8. Feedback

Please keep track of how much time you spend on this homework and answer the following questions. This can help us calibrate future assignments and future iterations of the course, and can help you identify which areas are most challenging for you.

- How many hours did you spend working on this assignment?
- Which problem did you spend the most time on?
- Which problem did you find to be the most confusing?
- Any other feedback for us?