Problem Set 4

Due: **Friday**, April 26th by 11:00pm

Instructions

Solutions submission. You must submit your solution via Gradescope. In particular:

- Submit a *single* PDF file containing your solutions to Task 1, 3, 5, & 6 (and optionally 7). Follow the prompt on Gradescope to link tasks to your pages.
- The instructions for separately submitting Task 1(a), 2, 3(a), and 4 appear below those parts.

Task 1 – Even So Soon? [16 pts]

For any predicate for which we have a definition, we have rules that allow us to replace the predicate with its definition or vice versa. As an example, consider "Even", defined by $\text{Even}(x) := \exists y\,(x = 2 \cdot y)$. We can use this definition via these two rules:

Def of Even

$$\frac{\text{Even}(x)}{\therefore\ \exists y\,(x = 2 \cdot y)}$$

Undef Even

$$\frac{\exists y\,(x = 2 \cdot y)}{\therefore\ \text{Even}(x)}$$

For example, if we know $\text{Even}(6)$ holds, then "Def of Even" allows us to infer $\exists y\,(6 = 2 \cdot y)$. On the other hand, if we know that $\exists y\,(10 = 2 \cdot y)$, then "Undef Even" allows us to infer $\text{Even}(10)$.

In English proofs, we do not distinguish between replacing $\text{Even}(x)$ by its definition and vice versa (both are "by the definition of Even"), but in Cozy, you need to say which direction you are doing by using `defof Even` or `undef Even`.

We will also need to use Cozy's `algebra` rule, which lets you infer equations implied by others:

Algebra

$$\frac{x_1 = y_1 \quad \ldots \quad x_n = y_n}{\therefore\ x = y \text{ (if implied)}}$$

For example, if you know that $2x = 3y + 1$ and $y = 2$, then you can infer $2x = 7$ by `algebra`. Cozy will not infer, from that, that $x = 7/2$ because the latter is not an integer. More generally, Cozy will only add equations and multiply both sides by constants. It will not do division.

To gain some familiarity with these rules, let's do a proof...

Let domain of discourse be the integers. Consider the following claim:

$$\forall x \, \forall y \, ((\text{Even}(x) \wedge \text{Odd}(y)) \rightarrow \text{Odd}(2x + 3y))$$

In English, this says that, for any even integer x and odd integer y, the integer $2x + 3y$ is odd.

a) Write a **formal proof** that the claim holds.

Remember that Cozy (like Java) expects a "*" for multiplication. It will misunderstand if you write `2a + 2 = 2(a+1)`. You have to write that as `2*a + 2 = 2*(a+1)`.

Submit and check your formal proof here:
http://cozy.cs.washington.edu
You **must also** include your solution (as a screenshot, typeset LaTeX, or rewritten by hand) in the PDF you submit to **Gradescope**.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Note that Cozy will provide an English translation of your formal proof, but this translation is *purposefully bad*. It will give you something to start with, but as you will see, it is not well written.

Task 2 – Fiddler on the Proof [16 pts]

Let domain of discourse be the integers. Consider the following claim:

$$\forall a \, \forall b \, (((a \equiv_{12} 7) \wedge (b \equiv_9 5)) \rightarrow (a - b \equiv_3 5))$$

In English, this says that, for any integers a and b, if a is congruent to 7 modulo 12 and b is congruent to 5 modulo 9, then $a - b$ is congruent to 5 modulo 3.

Write a **formal proof** that the claim holds.

Note that, while Cozy has special notation for the predicate "=", it uses predicate notation for everything else. In particular, $a \mid b$ is written Divides(a, b), and $a \equiv_m b$ is written Congruent(a, b, m)

Submit and check your formal proof here:
http://cozy.cs.washington.edu
You can make as many attempts as needed to find a correct answer.

Task 3 – Weekend At Cape Mod [16 pts]

For any known theorem, we have rules that allow us to cite the fact that the theorem holds and, if the statement of the theorem is a domain-restricted $\forall$, to apply it in one step to specific values.

As an example, suppose that "Thm1" says that $\forall x\,(P(x) \to Q(x))$. We can use this theorem in a formal proof via these two rules:

Cite Thm1

$$\frac{}{\therefore\ \forall x\,(P(x) \to Q(x))}$$

Apply Thm1

$$\frac{P(3)}{\therefore\ Q(3)}$$

The first rule simply writes down the known fact that Thm1 is true. If we know that $P(3)$ holds, we could then use "Elim $\forall$" to specialize it to $x = 3$ and then Modus Ponens to establish that $Q(3)$ holds. However, the second rule allows us to do that in one step!

To gain some familiarity with these rules, let's do a proof...

Let domain of discourse be the integers, and let n and c be *nonzero* integers. Consider this claim:

$$\forall a\,\forall b\,((ca \equiv_{cn} cb) \to (a \equiv_n b))$$

In English, this says that, for any integers a and b, if ca is congruent to cb modulo cn, then a is congruent to b modulo n.

a) Write a **formal proof** that the claim holds.

Some important notes:

- In Cozy, you will want to `cite` or `apply` the theorem DivideEqn, which says:

$$\forall a\,\forall b\,\forall c\,((ca = cb) \wedge \neg(c = 0)) \to (a = b))$$

- Note that this proposition has three $\forall$s in front! You can still use Cozy's `apply` rule here. For example, if you have proven that $(z \cdot (2x + 1) = z \cdot (y - 15)) \wedge \neg(z = 0)$ on line 1.2.3, then `apply DivideEqn 1.2.3 {2*x+1, y-15, z}` gives you $2x + 1 = y - 15$ on the next line.
- Cozy can only apply DivideEqn to an equation that looks *exactly* like $c(\dots) = c(\dots)$. For example, it cannot be applied to the equation $c = ca + cb$. Instead, you would first rewrite it as $c \cdot 1 = c(a + b)$ using the `algebra` rule and then apply DivideEqn.

  In particular, note that cab means $(ca)b$ in Cozy because multiplication associates to the left (as in Java), so you would need to explicitly transform $cab = cde$ to $c(ab) = c(de)$ using `algebra` before you can divide by c.

> Submit and check your formal proof here:
>
> http://cozy.cs.washington.edu
>
> You **must also** include your solution (as a screenshot, typeset LaTeX, or rewritten by hand) in the PDF you submit to **Gradescope**.

b) Translate your formal proof to an **English proof**.

Follow the same rules as in Task 1.

Task 4 – A Good Prime Was Had By All [18 pts]

In addition to algebra, one thing we can do with equations is substitute one side for the other. Since the two sides describe the exact same number, whatever facts hold for one side, hold for the other side. That fact is formalized in the following rule:

Substitute

$$\frac{P(x) \quad x = y}{\therefore \quad P(y)}$$

For example, if we know Prime$(2x + 5)$ — i.e., that $2x + 5$ is a prime number — and we know that $x = 2y + 1$, then we can substitute $2y + 1$ for x in the first fact to get Prime$(2(2y + 1) + 5)$ — i.e., that $2(2y + 1) + 5$ is a prime number.

To gain some familiarity with these rules, let's do some proofs...

Let domain of discourse be the *positive* integers. Write formal proofs of each of the following claims:

a) $\forall a\, \forall b\, \forall m\, ((\neg(a = 1) \wedge (m = ab)) \rightarrow \neg(b = m))$

Hint: The implication inside the $\forall$s is equivalent to $((m = ab) \wedge (b = m)) \rightarrow (a = 1)$. You will want to prove that implication instead and transform it using the Equivalent rule. (That implication is easier to prove because no facts are negated!)

You will need to use the theorem called DividePosEqn:

$$\forall a\, \forall b\, \forall c\, ((ca = cb) \rightarrow (a = b))$$

Note that there is no need to require $c \neq 0$ because 0 is not in the domain of discourse.

b) Given that $\exists n\, \exists m\, ((p = nm) \wedge (n \neq 1) \wedge (m \neq 1))$, it follows that $\neg$ Prime(p).

Recall the definition of prime given in lecture:

$$\text{Prime}(p) := \neg(p = 1) \wedge \forall x\, ((x \mid p) \rightarrow (x = 1 \vee x = p))$$

By De Morgan, the negation of the right side is equivalent to

$$(p = 1) \vee \exists x\, ((x \mid p) \wedge \neg(x = 1) \wedge \neg(x = p))$$

Hint: To show that a number p is *not* prime, you need to either show that $p = 1$ or that there is some number x with $x \neq 1$, $x \neq p$, and $x \mid p$. You will want to show that the **second** of those holds for some number x. **Before** you try to do this in Cozy, find a number mentioned in the Givens that has these properties! (Once you show that such a number exists, you use Intro $\vee$ to build up the expression above and then Equivalent to turn it into $\neg$Prime(p).)

You will need the fact you proved in part (a)! It is available to you under the name "`Lemma2`".

Submit and check your formal proofs here:

http://cozy.cs.washington.edu

You can make as many attempts as needed to find a correct answer.

Task 5 – A Wink and a Mod [12 pts]

For each of the problems below, **calculate** *one solution* to the modular equation using the Extended Euclidean Algorithm. Then, **state** *all solutions* to the equation. Your decription should be of the form "$x = C + Dk$ for any $k \in \mathbb{Z}$", where C and D are integers with $0 \leqslant C < D$.

Show your work for the first part by writing out the sequence of quotients and remainders, the resulting tableau, and the sequence of substitutions needed to calculate the relevant multiplicative inverse. Then, show how multiplying the initial equation on both sides by the multiplicative inverse gives you a solution to the equation.

a) $16x \equiv_{45} 4$

b) $18x \equiv_{67} 3$

Note that both equations are in the form $Ax \equiv_n B$ for some constants A, B, and n. We will say that such an equation is in "**standard form**".

Task 6 – The Mod Couple [16 pts]

In this problem, we will solve the following modular equation, which is **not** in standard form:

$$5 \cdot (4x + 1) \equiv_{53} 6x + 8$$

a) Show that any solution to the original equation is also a solution to $14x \equiv_{53} 3$, i.e., that we can infer the fact that $14x \equiv_{53} 3$ holds from the fact that the original equation holds.

Write your solution as a formal proof, where each of your explanations is one of the following:

- "Given": the original equation is assumed to hold
- "Algebra": justifies a regular (non-modular) equation by ordinary algebra
- "To Modular": transform a regular equation into a modular one
- "Add Equations": add two modular equations
- "Transitivity": infer $a \equiv_n g$ from $a \equiv_n b$, $b \equiv_n c$, $\ldots$, $f \equiv_n g$ (with any number of equations)

Note that this proof could also be done in Cozy, with each of the steps above translated into an `apply` of the appropriate theorem from lecture.

b) Find all solutions to $14x \equiv_{53} 3$. Format your answer as in Task 5.

c) Show that any solution to $14x \equiv_{53} 3$ is also a solution to the original equation.

Format your answer as a formal proof as in part (a).

d) Explain, in your own words, why we have proven that your solutions to (b) are also all the solutions to the original modular equation.

Task 7 – Extra Credit: Walk Like an Encryption [0 pts]

We know that we can reduce the *base* of an exponent modulo m : $a^k \equiv_m (a \bmod m)^k$. But the same is not true of the exponent! That is, we cannot write $a^k \equiv_m a^{k \bmod m}$. This is easily seen to be false in general. Consider, for instance, that $2^{10} \bmod 3 = 1$ but $2^{10 \bmod 3} \bmod 3 = 2^1 \bmod 3 = 2$.

The correct law for the exponent is more subtle. We will prove it in steps....

(a) Let $R = \{n \in \mathbb{Z} : 1 \leqslant n \leqslant m-1 \wedge \gcd(n,m) = 1\}$. Define the set $aR = \{ax \bmod m : x \in R\}$. Prove that $aR = R$ for every integer $a > 0$ with $\gcd(a,m) = 1$.

(b) Consider the product of all the elements in R modulo m and the elements in aR modulo m. By comparing those two expressions, conclude that, for all $a \in R$, we have $a^{\phi(m)} \equiv_m 1$, where $\phi(m) = |R|$.

(c) Use the last result to show that, for any $b \geqslant 0$ and $a \in R$, we have $a^b \equiv_m a^{b \bmod \phi(m)}$.

(d) Finally, prove the following two facts about the function ϕ above. First, if p is prime, then $\phi(p) = p - 1$. Second, for any primes a and b with $a \neq b$, we have $\phi(ab) = \phi(a)\phi(b)$. (Or slightly more challenging: show this second claim for *all positive integers* a and b with $\gcd(a,b) = 1$.)

The second fact of part (d) implies that, if p and q are primes, then $\phi(pq) = (p-1)(q-1)$. That along with part (c) prove the final claim from lecture about RSA, completing the proof of correctness of the algorithm.