Midterm 1 review problems, part 1

(try to solve before coming to the review session, 03/02 5-7pm, 306 Soda)

1. (Based on Rosen, *Disc Math*, 5th ed.) Consider the universe of people, with predicates $F(a, b)$, "a is b's friend", and $P(x)$, "x is perfect".
   (a) Translate into first-order logic expressions (that is, expressions with propositional operators $\wedge$, *lor*, and *lnot* and quantifiers $\forall$ and $\exists$):
      i. No one is perfect.
      ii. Not everyone is perfect.
      iii. All your friends are perfect.
      iv. One of your friends is perfect.
      v. Everyone is your friend and is perfect.
      vi. Not everybody is your friend or someone is not perfect.
   (b) Use DeMorgan's law to negate the logical expression you got in 1(a)v above. Translate the result back into English.
   (c) Use DeMorgan's law to negate the logical expression you got in 1(a)vi above. Translate the result back into English.
2. The "Lucas numbers" are a sequence of integers defined by setting $L_0 = 2$ and $L_1 = 1$, and then, for integers $n \geq 2$, $L_n = L_{n-1} + L_{n-2}$: $L_2 = 2 + 1 = 3$, $L_3 = 1 + 3 = 4$, $L_4 = 4 + 3 = 7$, etc.
   (a) Let ϕ be the golden ratio, $\frac{1+\sqrt{5}}{2}$. The golden ratio is so called because it's a root of $\phi^2 - \phi - 1$, an polynomial that arises naturally surprisingly often. Prove that $L_n = \phi^n + (1 - \phi)^n$. *Hint*: that polynomial will come in useful here, too.
   (b) Prove or disprove: there exists an n such that $L_n > n^5$.
   (c) Compute L_7 and L_8 and run Euclid's algorithm to find $\gcd(L_7, L_8)$.
   (d) Based on the results above, take a guess at (i) exactly how many steps Euclid's algorithm takes when you run it on (L_n, L_{n+1}), and (ii) the value of $\gcd(L_n, L_{n+1})$. Prove that your guesses are correct by strong induction.

      Remember that, by convention, we have Euclid's algorithm terminate at a step that looks like $a = bk + 0$ (some sources will use the convention that it terminates one step before that, $a = bk + c$ where $c|b$).
3. Evaluate:
   (a) $4^{-1} \pmod{17}$
   (b) $306^{-1} \pmod{679}$
   (c) $679^{-1} \pmod{306}$
4. Let n be an odd integer. Find $2^{-1} \pmod{n}$.
5. Given a prime p, prove that $(ab)^{-1} \equiv a^{-1}b^{-1} \pmod{p}$, that is, that in $\mathbb{Z}_p$, the inverse of ab is congruent to the product of the inverses of a and b.

6. Many of you have asked whether it's reasonable to take expressions like $\frac{6}{2} \pmod 7$ or $\frac{15}{12} \pmod{17}$ and reduce them the way you normally would when dealing with normal (rational) fractions, to $3 \pmod 7$ and $\frac{5}{4} \pmod{17}$. Remember, we *defined* division in $\mathbb{Z}_p$ by saying that $\frac{a}{b} \pmod p$ is defined as $a \cdot b^{-1} \pmod p$, that is, the product of a and the inverse of b modulo p.

   Prove, without assuming any properties of modular division other than its definition, that this definition of division still allows "simplifying fractions" modulo a prime. That is, if p is *prime* and you're given some a, b, c, d, such that $a \equiv kc \pmod p$ and $b \equiv kd \pmod p$ for some k, then $\frac{a}{b} \equiv \frac{c}{d} \pmod p$.