Problem Set for Unit 5

Here are some problems about **GCDs and inverses**. Before working on this problem set, you will need to have read the corresponding lecture notes posted on the course website. Some of these problems ask you to write out proofs for things mentioned without proof in the lecture notes. In such cases, you can't just cite the lecture notes to say that the result has been proved in class (since it hasn't).

By now you are familiar with what needs to be submitted towards graded homework and when.

The symbols $\mathbb{N}, \mathbb{N}^+, \mathbb{Z}, \mathbb{Z}_d, \mathbb{Q}$, and $\mathbb{R}$ have their usual meanings.

PS5-1 ^{HW}

The lecture notes contain an example gcd computation, using the numbers 1147 and 899.

a. In a similar way, compute the gcd of 13631 and 8213, showing your work at each step.

b. Let the gcd be g. Then, according to the GCD Linear Combination Theorem (LCT), there exists a pair of integers (k, ℓ), such that $13631k + 8213\ell = g$. Find one such pair.

c. Find another such pair.

PS5-2

An "integer linear combination (IntLC) of a and b" is defined to be an expression of the form $ka + \ell b$, where k and ℓ are integers.

For each of the following statements, indicate "true" or "false." If true, provide a concise proof. If false, provide a specific counterexample.

For all $a, b, c, n \in \mathbb{N}^+$,

a. $\gcd(a, b) \neq 1 \wedge \gcd(b, c) \neq 1 \implies \gcd(a, c) \neq 1$.

b. $\gcd(a^n, b^n) = \gcd(a, b)^n$.

c. $\gcd(ab, ac) = a \cdot \gcd(b, c)$.

d. $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$.

e. if an IntLC of a and b equals 1, then so does some IntLC of a and b^2.

f. if no IntLC of a and b equals 2, then neither does any IntLC of a^2 and b^2.

PS5-3 ^{HW}

The Python code for the function "egcd" given in the lecture notes does not correctly handle *all* possible inputs $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0, 0)\}$.

a. Find a pair of integers (a, b) for which the answer returned by egcd(a, b) is incorrect, according to the definition of gcd given in class and the lecture notes.

b. Fix the code for egcd to handle all cases correctly. You should add a small bit of logic to the existing code; don't write a completely new egcd function.

PS5-4

The proof of LCT given in the lecture notes has a subtle flaw: it assumes that the recursion will terminate. Thankfully, we can *prove* that it will indeed terminate.

Consider a function call egcd(a, b). We'll say that it is a "good" call if $0 \neq a \geq b \geq 0$ and that the "size" of the call is $a + b$.

a. Prove that if we make a good call to egcd whose size is s and this results in an immediate recursive call to egcd, then this new call is also good and it has size $< s$.

b. Using the above result, prove that every good call to egcd eventually terminates (i.e., recursive calls don't keep happening forever).

You'll find that your proof depends on the following crucial property of $\mathbb{N}$: every nonempty subset of $\mathbb{N}$ has a minimal element. This is called the *Well-Ordering Principle*.

Problem Set for Unit 5

Prof. Amit Chakrabarti
Computer Science Dept
Dartmouth College

PS5-5

Study the Fundamental Theorem of Arithmetic (a.k.a. Unique Factorization Theorem) and its proof, as presented in the [LLM] textbook. It's Lemma 9.4.3 in the June 2018 edition of the book (linked from the course website).

PS5-6 ^{HW}

For $a, b \in \mathbb{N}^+$, the *least common multiple* $\operatorname{lcm}(a,b)$ is defined to be the minimum positive integer that is a multiple of both a and b, i.e.,

$$\operatorname{lcm}(a,b) = \min\{m \in \mathbb{N}^+ : a \mid m \text{ and } b \mid m\}.$$

The result is well-defined because there is always at least one common multiple—namely, ab—and we're taking the minimum of a subset of $\mathbb{N}$ (recall the Well-Ordering Principle).

a. Prove that $\exists\, x, y \in \mathbb{N}^+$ such that $\operatorname{lcm}(a,b) = ax = by$ and $\gcd(x,y) = 1$.

b. Using LCT, express a/y as an integer linear combination of a and b.

c. Using the above, show that $\gcd(a,b) \mid a/y$.

d. On the other hand, show that a/y is a divisor of both a and b.

e. Conclude that $\gcd(a,b) = a/y$.

f. Based on all of the above, prove the following very pretty theorem:

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab.$$

PS5-7

Using the Inverse Existence Theorem (see the lecture notes), prove the following. If p is a prime, $b \in \mathbb{Z}_p$, and $b \neq 0$, then

a. b has an inverse modulo p;

b. the function $f_b : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f_b(x) = bx \bmod p$ is a bijection.

PS5-8

Establish the fact that "n^2 is even $\Rightarrow n$ is even."

a. Using the above fact, give a detailed proof that $\sqrt{2}$ is irrational. Do a proof by contradiction, starting with the assumption that $\sqrt{2} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$.

b. A generalization of the above fact is that if p is a prime, then n^2 is divisible by p only if n is. Prove this generalization using Euclid's Lemma.

c. Give a detailed proof that $\sqrt{p}$ is irrational for every prime p.

d. Generalize further to show that $p^{1/n}$ is irrational for every prime p and every integer $n \geq 2$.

PS5-9 ^{HW}

Let $m \in \mathbb{N}^+$ and $a \in \mathbb{Z}_m$. We say that a is a self-inverse modulo m if $a = a^{-1}$. Equivalently, $a^2 \equiv 1 \pmod{m}$.

a. Prove that if $p \geq 3$ is a prime, there are exactly two self-inverses modulo p.

b. Find all numbers is $\mathbb{Z}_{15}$ that are self-inverses modulo 15.

Hint: Use Euclid's Lemma.

PS5-10 ^{EC}

Generalize your work in ***PS5-8*** to show that for all $a, n \in \mathbb{N}^+$, $a^{1/n}$ is either an integer or an irrational number.