MATH 335 Homework 1

Chris Camano: ccamano@sfsu.edu

September 1, 2022

1. Let's start with a warm-up exercise for doing proofs where you need to use induction: Prove that for all $n \in \mathbb{N}$
$$1+2+2^2+2^3+\cdots+2^n \;=\; 2^{n+1}-1.$$

Re-expressing the problem statement:
Prove that $\forall n \in \mathbb{N}$
$$\sum_{i=0}^{n} 2^i = 2^{n+1}-1$$

Proof. Base case: n=2
$$1+2^1+2^2 = 2^3-1$$
$$7 = 7$$

Inductive Hypothesis:
$$P(k) = \sum_{i=0}^{k} 2^i = 2^{k+1}-1$$

$$P(k+1):$$

$$\sum_{i=0}^{k+1} 2^i = 2^{k+2}-1$$

$$\sum_{i=0}^{k} 2^i + 2^{k+1} = 2^{k+2}-1$$

$$2^{k+1}-1+2^{k+1} = 2^{k+2}-1$$

$$2(2^{k+1})-1 = 2^{k+2}-1$$

$$2^{k+2}-1 = 2^{k+2}-1$$

$\square$

2. And here is a second warm-up exercise: if x is a nonnegative real number show that $(1+x)^n - 1 \geq nx$ for $n = 0, 1, 2, \ldots$.

   Re-expressing the problem statment:
   let $x \in \mathbb{R}, x \geq 0$, Show that
   $$(1+x)^n - 1 \geq nx, \forall n \in \mathbb{W}$$

   Proof. Suppose $x \in \mathbb{R}, x \geq 0$
   $$(1+x)^n - 1 \geq nx$$
   $$(1+x)^n \geq nx + 1$$
   $$\sum_{k=0}^{n} \binom{n}{k} x^k \geq nx + 1$$
   $$nx + 1 + \sum_{k=2}^{n} \binom{n}{k} x^k \geq nx + 1$$
   $$\therefore (1+x)^n \geq nx + 1$$
   Which implies
   $$(1+x)^n - 1 \geq nx$$

   $\square$

3. Show that if p is a prime number, there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e. $\sqrt{p}$ is not a rational number).
   If p is a prime number then the only divisors of p are 1 and p
   Let a and be expressed in the prime factorization:
   $$a = \prod_{i=1}^{k} P_i^{\alpha_i}$$
   $$b = \prod_{i=1}^{k} P_i^{\beta_i}$$
   the original statement is then:
   $$\left[\prod_{i=1}^{k} p_i^{\alpha_i}\right]^2 = p\left[\prod_{i=1}^{k} p_i^{\beta_i}\right]^2$$
   $$\prod_{i=1}^{k} p_i^{2\alpha_i} = p\prod_{i=1}^{k} p_i^{2\beta_i}$$
   If $a^2 = b^2$ then they would have identical prime factorizations. Since the integer is raised to the second power this implies that for all prime factors, each has an even exponent.
   if p is not a prime factor of b then it would have an odd exponent. If p was a prime factor of b then it would form an odd exponent when combined with the corresponding prime factor since the each prime factor in b^2 has an even exponent. In either case p exists as a prime number with an odd exponent therefore it cannot be equal to a since a has a prime factorization that has even exponenets for each prime factor.

4. Compute the gcd of the following pairs of integers:

   i) 14 and 39;

$$\begin{aligned}
39 &= 14(2)+11 \\
14 &= 11(1)+3 \\
11 &= 3(3)+2 \\
3 &= 2(1)+1 \\
2 &= 1(2)+0
\end{aligned}$$

   gcd(39,14)=1

   ii) 234 and 165;

$$\begin{aligned}
234 &= 165(1)+69 \\
165 &= 69(2)+27 \\
69 &= 27(2)+15 \\
27 &= 15(1)+12 \\
15 &= 12(1)+3 \\
12 &= 3(4)+0
\end{aligned}$$

   gcd(234,165)=3

   iii) 471 and 562.

$$\begin{aligned}
562 &= 471(1)+91 \\
471 &= 91(5)+16 \\
91 &= 16(5)+11 \\
16 &= 11(1)+5 \\
11 &= 5(2)+1 \\
5 &= 1(5)+0
\end{aligned}$$

   gcd(562,471)=1

5. Let $a,b,c \in \mathbb{Z}$. Prove that if $\gcd(a,b)=1$ and $a \mid bc$ then $a|c$.
   Lemma: If $d = gcd(a,b)$ then there exist x,y such that:

$$d = ax+by$$

   Proof. Consider the following set:

$$S = \{ax+by \in \mathbb{Z}_{>0}, a,b \in \mathbb{Z}\}$$

   Since $S \subset \mathbb{N}$ due to the exclusion of integer values greater than zero then by the well ordering principle there exist a least value, here denoted as$S_{\min}$

   Let d be $S_{\min}$. we now prove that d is the gcd of a and b by satisfying the definition of gcd.

Proof. Suppose that d does not divide a. Then by the division algorithm a can be expressed as the following :

$$a = qd + r \quad 0 < r < d \quad q \geq 0$$

$$\begin{aligned}
a &= q(ax+by)+r \\
r &= a - q(ax+by) \\
r &= a - qax - qby \\
r &= a(1-qx) - qby \\
r &= a(1-qx) + b(-qy)
\end{aligned}$$

so r$\in S$ since $r > 0$ by construction, however $r < d$ which contradicts that $S_{\min}$ is d so $d|a$ and by a symmetric proof $d|b$ $\square$

We must show that for all other common divisiors of a and b that d is the greatest:

Proof. let e be a common divisor of a and b, therefore $a = ek, k \in \mathbb{Z}$ and $b = el, l \in \mathbb{Z}$ Then:

$$\begin{aligned}
d &= ax+by \\
d &= ekx+ely \\
d &= e(kx+ly)
\end{aligned}$$

so it is clear that if there is a common divisor e then $e|d$ $\square$

The proof above then implies that since there exist x,y such that :

$$gcd(a,b) = ax+by$$

that

$$ax+by = 1$$

$$\begin{aligned}
&ax+by = 1 \\
&cax+cby = c \\
&a|bc \mapsto bc = ak, k \in \mathbb{Z} \\
&cax+aky = c \\
&a(cx+ky) = c
\end{aligned}$$

so we have proven that $a|c$ $\square$

6. Let a and b be positive integers where

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad \text{and} \qquad a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

with $p_1, \ldots, p_k$ distinct primes and $\alpha_i, \beta_i \geq 0$ for $i = 1, \ldots, k$. Show that

$$\operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}.$$

Proof. Let a and b be expressed in a product form as follows:

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}$$

$$b = \prod_{i=1}^{k} p_i^{\beta_i}$$

Let:

$$l = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}$$

for l to be the least common multiple of a and b it must satisfy two conditions.

(a) $a|l$ and $b|l$ (common multiple)

(b) if there exists a multiple e such that $a|e$ and $b|e$ then $l|e$ (least common multiple)

a) We must prove that $l = ak, k \in \mathbb{Z}$ which can be done in the following way:

$$l = ak$$

$$\prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} = \left[\prod_{i=1}^{k} p_i^{\alpha_i}\right] k$$

$$\prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} = \left[\prod_{i=1}^{k} p_i^{\alpha_i}\right] \left[\prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)-\alpha_i}\right]$$

where $P_1, ..., P_k$ are distinct primes and:

$$\max\{\alpha_i, \beta_i\} \geq \alpha_i \quad \forall \alpha_i$$

By similar reasoning it can be shown that $b|l$.

b) We now prove that if there exists another common multiple that l must be smaller.
Suppose there exists another common multiple e, this is to say, $a|e$, and $b|e$ to prove that l is the least common multiple we must show that $l|e$.

e is a common multiple so:

$$a|e \mapsto e = am, m \in \mathbb{Z}$$

$$b|e \mapsto e = an, n \in \mathbb{Z}$$

We will first express e in its prime factorization:

$$e = \prod_{i=1}^{k} p_i^{\delta_i}$$

where $P_1, ..., P_k$ are distinct primes and: $\delta_i \geq max(\alpha_i, \beta_i)$ Due to the fact that e is composed of prime factors of a and also prime factors of b then the if :

$$l = \prod_{i=1}^{k} p_i^{max\{\alpha_i, \beta_i\}}$$

then for each prime since $\delta_i \geq max(\alpha_i, \beta_i)$ this implies that l is smaller since $l|e$ since each exponent of the prime factors is smaller than that of the exponent in the prime factorizaion of e for $l \neq e$. $\square$