MA 453
Homework A Week 1

---

1. Suppose that $p_1, ..., p_k$ is a finite list of primes

   let $c = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$

   so, pick any p_i, where $1 \leq i \leq k$

   so, $gcd(c, p_i) = gcd(p_i, (p_1 \cdot p_2 \cdot ... \cdot p_k + 1) \text{ mod } p_i)$

   so, $p_1, ..., p_k$ are all primes so for any p_i, we get remainder of 1

   so, $gcd(p_i, (p_1 \cdot p_2 \cdot ... \cdot p_k + 1) \text{ mod } p_i) = gcd(p_i, 1) = 1$

   For every p_i we get that $gcd(p_i, c) = 1$

   so, c is a coprime of every p_i by definition. $(\star)$

   Next suppose that there are finitely many primes $p_1, ..., p_k$ and suppose that $N = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$

   by $(\star)$ $gcd(N, p_i) = 1$ for every $1 \leq i \leq k$

   so, none of $p_1, ..., p_k$ divides N

   so, every integer $N > 1$ has a prime divisor

   so, N must have a prime divisor q, s.t $q \notin p_1, ..., p_k$

   q is a new prime! Ouch!

2. Suppose that S is the set of $\mathbb{N}$ s.t every $s \in S$ has two different prime factorizations and $S \neq \emptyset$ and let $n = p_1 \cdot ... \cdot p_k = q_1 \cdot ... \cdot q_l$ be the min in S, that is $n \leq s$ for all $s \in S$

so, $p_1 = \min\{p_i\}$ and $q_1 = \min\{q_j\}$

by Euclid's lemma $\Rightarrow p_1 | q_1 \cdot ... \cdot q_l$

so, $p_1 = q_j$ for some $1 \leq j \leq l$

similarly, Euclid's lemma $\Rightarrow q_1 | p_1 \cdot ... \cdot p_k$

so, $q_1 = p_i$ for some $1 \leq i \leq k$

since $q_1 \leq q_2 \leq ... \leq q_l \Rightarrow q_1 \leq q_j = p_1 \Rightarrow q_1 \leq p_1$

and similarly, $p_1 \leq p_2 \leq ... \leq p_k \Rightarrow p_1 \leq p_k = q_1 \Rightarrow p_1 \leq q_1$

Aha! $p_1 = q_1$

so, $\frac{n}{p_1} = p_2 \cdot ... p_k = q_2 \cdot ... q_l$

so, if $p_i \neq q_j$ for all $i = j$

then there is an $m \in S$ s.t $m = \frac{n}{p_1} < n$

but this contradicts that n is the min. element of S

so the factorizations must be identical

so, $k - 1 = l - 1$ and $p_i = q_j$ for all $i = j$, where $i, j \geq 2$ and we showed earlier that $p_1 = q_1$

which contradicts that $n \in S$

so $S = \emptyset$

3. $c = a + 4$

   $b + 2 = a + 4 \Rightarrow b = a + 2$

   $(a, a + 2, a + 4) \leftarrow$ prime tuple must have form

   so case $a = 2$

   $a = 2, b = 4, c = 6$ can't happen because b and c are not primes. Ouch!

   Since all primes > 2 are odd then $(a, a + 2, a + 4)$ must all be odd and also they must be consecutive prime numbers.

   So, among three consecutive odd numbers one must be divisible by 3

   So, the only prime triple that works must be $(3, 5, 7)$

4. Base case: $n = 1 \Rightarrow 11^1 - 4^1 = 7 \bmod 7 \equiv 0$

   Now suppose we've checked up to the $n = k$ case, then we know
   $(11^k - 4^k) \bmod 7 \equiv 0 \quad (\star)$

   so, $11^{k+1} - 4^{k+1} = 11^k \cdot 11 - 4^k \cdot 4 = (11 \cdot 11^k - 11 \cdot 4^k) + (11 \cdot 4^k - 4^k \cdot 4)$

   $11 \cdot (11^k - 4^k) + 4^k(11 - 4) = 11 \cdot (11^k - 4^k) + 4^k(7)$

   so, $4^k \cdot 7 \bmod 7 \equiv 0$ trivial, and $11 \cdot (11^k - 4^k) \bmod 7 \equiv 0$ by $(\star)$

   So, $11 \cdot (11^k - 4^k) + 4^k(7) \bmod 7 \equiv 0$

   Hence true for the $n = k + 1$ case.