MATH 382: Hints to Assignment 1 (due: September 26, 2019)

---

1. Use the Euclidean algorithm to find all integers x and y such that

$$42823x + 6409y = 17.$$

Solution: Using the division algorithm, first compute the gcd of 42828 and 6409 and show that it is 17. Then, using the matrix method described in class, find integers x_0, y_0 such that

$$42823x_0 + 6409y_0 = 17.$$

Then, by a theorem proved in class, **all** solutions are given by

$$x = x_0 - 6409t, \quad y_0 + 42823t, \qquad t \in \mathbb{Z}.$$

2. If $m = p_1^{a_1} \cdots p_k^{a_k}$ and $n = p_1^{b_1} \cdots p_k^{b_k}$ are the respective unique factorizations, show that

$$\text{gcd}(m,n) = p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}},$$

and

$$\text{lcm}(m,n) = p_1^{\max\{a_1,b_1\}} \cdots p_k^{\max\{a_k,b_k\}}.$$

Solution: This is an immediate consequence of the unique factorization theorem.

3. Show that for all natural numbers $n \geq 1$,

$$1 \cdot 1! + 2 \cdot 2! + \cdots n \cdot n! = (n+1)! - 1.$$

Solution: Apply induction on n.

4. Find all integers x such that

$$11111x \equiv 10 \pmod{78787}.$$

Solution: Using the method of question 1, show that the gcd of 78787 and 11111 is 1. Using the matrix method, find integers a and b such that

$$11111a + 78787b = 1.$$

Thus, $11111a \equiv 1$ (mod 78787). Multiplying the given congruence by a on both sides we get

$$(11111a)x \equiv x \equiv 10a \pmod{78787}.$$

5. Show that for all natural numbers $N \geq 1$,
$$\sum_{n=1}^{N} \frac{1}{n(n+1)} = 1 - \frac{1}{N+1}.$$
Solution: This is trivial by induction on N.

6. Let p_n denote the n-th prime. Show that for $n \geq 1$,
$$p_n < 2^{2^n}.$$
Solution: By Euclid's proof of the infinitude or primes,
$$p_n \leq p_1 p_2 \cdots p_{n-1} - 1.$$
Now apply induction on n and observe that
$$2^{2+2^2+\cdots+2^{n-1}} = 2^{2^n-2} < 2^{2^n}.$$

7. Show that if $n | 2^n - 1$, then $n = 1$. Suppose $n > 1$ and $n | 2^n - 1$. Let n_0 be the smallest among such numbers. Then,
$$2^{n_0} \equiv 1 \pmod{n_0}.$$
But by Euler's theorem
$$2^{\phi(n_0)} \equiv 1 \pmod{n_0}.$$
Let $d =$ gcd of n_0 and $\phi(n_0)$. Then $2^d \equiv 1$ (mod n_0). Since $d | n_0$, we get $2^d \equiv 1$ (mod d). By minimality of n_0, and as $d < n_0$, we see that $d_0 = 1$. But then, $2 \equiv 1$ (mod n_0), a contradiction to $n_0 > 1$.

8. Show that for any natural number $n > 1$, the number
$$S := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$
is not a natural number. [Hint: consider k such that $n/2 < 2^k \leq n$ and let d be the lcm of all the numbers 1, 2, ..., n except for 2^k and analyze dS.]
Solution: Using the hint, consider dS which is
$$d + \frac{d}{2} + \cdots + \frac{d}{2^k} + \cdots + \frac{d}{n}.$$
If S is a natural number, then dS is a natural number but this is not the case since every summand above except for $\frac{d}{2^k}$ is an integer.

9. Let $d = \gcd(m,n)$. Show that
$$\gcd(a^m - 1, a^n - 1) = a^d - 1,$$
for any natural number $a > 1$.
Solution: We will induct on $m + n$. Suppose without any loss of generality that $m \geq n$. The gcd of $a^m - 1$ and $a^n - 1$ is the gcd of $a^n - 1$ and $a^m - a^n = a^n(a^{m-n} - 1)$ (just subtract the two numbers). Thus, $\gcd(a^m - 1, a^n - 1) = \gcd(a^n - 1, a^{m-n} - 1) = a^e - 1$ where $e = \gcd(n, m-n)$ by induction. But $e = d$ as the gcd of n and $m - n$ is the same as the gcd of m and n.

10. The Fibonacci sequence is defined as follows. $F_1 = 1$, $F_2 = 1$ and for $n \geq 3$, $F_n = F_{n-1} + F_{n-2}$. Show that
   (a) the gcd of F_n and F_{n-1} is 1 for $n \geq 2$;
   Solution: By the recursion, it is clear that the gcd of F_n and F_{n-1} is the same as the gcd of F_{n-1} and F_{n-2}. Continuing this way, we get to $F_1 = 1$.
   (b) $F_{n+m} = F_{n-1}F_m + F_nF_{m+1}$ for $n \geq 2$ and $m \geq 1$; [Hint: induct on m.]
   Solution: This is clear by an easy induction on m and the recursion for F_n.

   (c) $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.
   Solution: Applying (b) with $m = n$ shows $F_n | F_{2n}$. Inductively, putting $m = (q-1)n$, in (b) gives by $F_n | F_{qn}$. Now write, $n = qm + r$ by the division algorithm, with $0 \leq r < m$ to get from (b) that
$$F_{qm+r} = F_{qm-1}F_r + F_{qm}F_{r+1}.$$
   Thus,
$$(F_n, F_m) = (F_{qm-1}F_r + F_{qm}F_{r+1}, F_m) = (F_r, F_m)$$
   because by (a), the gcd of two consecutive Fibonacci numbers is 1 and by our remark, $F_m | F_{qm}$. We see that the gcd of F_n and F_m is the same as the gcd of F_m and F_r. By induction, this is $F_{(m,r)}$ which is the same as $F_{(n,m)}$.