UBC Math Circle 2018 Problem Set 4

I. Introductory Problems

1. Prove that if ab is a perfect square and $(a, b) = 1$, then both a and b must be perfect squares.

Solution: Since we know ab is a perfect square, we know that all exponents in the prime factorization must be even numbers and since we know a and b are relatively co-prime (their GCD is 1), we know that for each prime, if its exponent is non-zero in a, it must be zero in b (and vice versa). Together this shows that all exponents in the prime factorization of a must be even, and the same goes for all the exponents in the prime factorization of b. So both must be perfect squares.

2. Solve the congruence $42x \equiv 12 \pmod{90}$.

Solution: We have gcd(42, 90) = 6, so there is a solution since 6 is a factor of 12. Solving the congruence $42x \equiv 12 \pmod{90}$ is equivalent to solving the equation $42x = 12 + 90q$ for integers x and q. This reduces to $7x = 2 + 15q$, or $7x \equiv 2 \pmod{15}$. We next use trial and error to look for the multiplicative inverse of 7 modulo 15. The numbers congruent to 1 modulo 15 are 16, 31, 46, 61, etc., and 14, 29, 44, etc. Among these, we see that 7 is a factor of 14, so we multiply both sides of the congruence by 2 since $(2)(7) = 14 \equiv 1 \pmod{15}$. Thus we have $14x \equiv 4 \pmod{15}$, or $x \equiv 11 \pmod{15}$. The solution is $x \equiv 11, 26, 41, 56, 71, 86 \pmod{90}$.

3. Find all solutions to the congruence $55x \equiv 36 \pmod{75}$.

Solution: There is no solution, since $\gcd(55, 75) = 5$ is not a divisor of 36.

4. Is 4^{100} divisible by 3? Show that a number is divisible by 9 if the sum of it's digits is divisible by 9.

Solution: No, since $4^{100} \equiv 1^{100} \equiv 1 \pmod{3}$. Or you can write 2^{200} as the prime factorization, and then $\gcd(3, 2^{200}) = 1$.

Let $(abcdef \dots k)_{10}$ be a number in base ten. Then we can rewrite $abcdef \dots k$ as $a(10^{k-1}) + b(10^{k-2}) + \dots k(10^0) \equiv a(1) + b(1) + \dots k(1) \pmod{9}$ and therefore if this is equivalent to 0 (mod 9) then $9 | (abcdef \dots k)_{10}$.

5. Consider the integer $Q_n = n! + 1$, where n is a positive integer. Show that Q_n has a prime factor greater than n, use this to argue that there are infinitely many primes. (Hint: What if Q_n has a prime factor less than n?)

> **Solution:** Suppose that Q_n has a prime factor $p \leq n$. Then p divides $n!$ and since p divides Q_n also, p divides their difference, which is 1 – a contradiction (p is an integer greater than 1). Therefore Q_n must have a prime factor greater than n (every positive integer has at least one prime factor). Now for any integer n, there is a prime p greater than n. Since n is arbitrary, we conclude that there can be no largest prime number; there are infinitely many primes.

II. Intermediate Problems

6. Let $n \in \mathbb{N}$ be composite and greater than 4. Show that n divides $(n-1)!$.

> **Solution:** Since n is composite, we can write $n = ab$ where $a, b > 1$.
>
> - Case 1: $a \neq b$: Then since a and b divide n, they are both less than n. Since a and b are distinct integers which occur in the sequence $1, 2, \ldots, n-2, n-1$, we conclude that $ab = n$ divides $(n-1)!$.
> - Case 2: a=b, then $n = a^2$. Note that $a > 2$ (since $2^2 = 4 < n$), such that $n = a^2 > 2a > a$. Since a and $2a$ are distinct and occur in the sequence $1, 2, \ldots, n-2, n-1$, we deduce that $2a \cdot a = 2n$ divides $(n-1)!$. Since n divides $2n$, we conclude that n divides $(n-1)!$.

7. For this question, consider only positive integers. Let p and q be distinct primes, and let a and b be integers. Define $\tau(n)$ to be the function which returns the number of distinct divisors of n (e.g. $\tau(4) = 3$).

   (a) What are $\tau(p^a)$, $\tau(q^b)$, and $\tau(p^a q^b)$? Argue that $\tau(p^a q^b) = \tau(p^a) \cdot \tau(q^b)$.

   > **Solution:** The factors of p^a are the integers $1, p, p^2, \ldots, p^{a-1}, p^a$ – so there are $a+1$ factors of p^a. Similarly there are $b+1$ factors of q^b. Using the counting principle there are $(a+1) \cdot (b+1)$ factors of $p^a q^b$. We see that $\tau(p^a q^b) = \tau(p^a) \cdot \tau(q^b)$.

   (b) Argue that for a product of prime powers $\prod_{i=1}^{r} p_i^{a_i}$ (i.e. an r number of primes p_1 to p_r where each $a_i \geq 1$) that $\tau(\prod_{i=1}^{r} p_i^{a_i}) = \prod_{i=1}^{r} \tau(p_i^{a_i})$ (with this property τ is called a *multiplicative function*).

Solution: The factors of $\prod_{i=1}^{r} p_i^{a_i}$ are of the form $\prod_{i=1}^{r} p_i^{b_i}$, where for each i: $0 \leq b_i \leq a_i$. We use the counting principle in the same way as for (a): there are $a_1 + 1$ possibilities for powers of the first prime, $a_2 + 1$ possibilities for powers of the second prime, etc. such that there are $\prod_{i=1}^{r}(a_i + 1) = \prod_{i=1}^{r} \tau(p_i^{a_i})$ factors of $\prod_{i=1}^{r} p_i^{a_i}$.

(c) Classify all forms of integers with an odd number of distinct divisors.

Solution: Our goal is to find all integers n such that $\tau(n)$ is even. Let n have prime factorization $n = \prod_{i=1}^{r} p_i^{a_i}$ (i.e. n has r distinct prime factors p_1 to p_r with $a_i \geq 1$. Using part (b), we can expand $\tau(n) = \prod_{i=1}^{r}(a_i+1)$. It is straightforward that this product is odd if and only if every $a_i + 1$ is odd, if and only if every a_i is even. We conclude that all integers with an odd number of distinct divisors are of the form $n = \prod_{i=1}^{r} p_i^{a_i}$, where each $a_i \geq 1$ is even.

(d) Classify all forms of integers with exactly 77 distinct divisors (i.e. describe in some way or with some formula the integers with 77 divisors).

Solution: Our goal is to find all integers n such that $\tau(n) = 77$. Let n have prime factorization $n = \prod_{i=1}^{r} p_i^{a_i}$ (i.e. n has r distinct prime factors p_1 to p_r with $a_i \geq 1$. Using part 1 (and a little induction), we can expand $\tau(n) = \prod_{i=1}^{r} \tau(p_i^{a_i}) = \prod_{i=1}^{r}(a_i + 1) = 77$. We factor $77 = 7 \cdot 11$.

- Case 1: n has one prime factor p. Then $a + 1 = 77$, such that n is of the form $n = p^{76}$.

- Case 2: n has two distinct prime factors p and q. Then $(a_p+1) \cdot (a_q+1) = 7 \cdot 11$. Since $a_p, a_q \geq 1$, it is clear that (without loss of generality) $a_p = 6$ and $a_1 = 10$. So n is of the form $n = p^6 q^{10}$.

- Case 3: n has 3 or more distinct prime factors. Consider the first 3 factors p, q, and k. Then $(a_p + 1) \cdot (a_q + 1) \cdot (a_k + 1) = 7 \cdot 11$, which is a contradiction, since $7 \cdot 11$ has only two distinct factors greater than 1, while $(a_p + 1) \cdot (a_q + 1) \cdot (a_k + 1)$ has three factors greater than 1 (since each $a \geq 1$). The case where n has more than 3 distinct prime factors follows an identical contradiction.

We conclude that all integers with 77 distinct divisors are either of the form $n = p^{76}$, or of the form $n = p^6 q^{10}$ – for prime p and q. 1 is also a valid integer with this property.

III. Advanced Problems

8. For this question, consider only positive integers. Let p and q be distinct primes, and let a and b be integers. Define $\sigma(n)$ to be the function which returns the sum of the divisors of n (e.g. $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12$).

(a) What are $\sigma(p^a)$, $\sigma(q^b)$, and $\sigma(p^a q^b)$? Argue that $\sigma(p^a q^b) = \sigma(p^a) \cdot \sigma(q^b)$.

Solution: The factors of p^a are the integers $1, p, p^2, \ldots, p^{a-1}, p^a$. So $\sigma(p^a) = 1 + p + \ldots + p^a = \sum_{k=0}^{a} p^k = \frac{1-p^{a+1}}{1-p}$. Similarly $\sigma(q^b) = \frac{1-q^{b+1}}{1-q}$.
The factors of $p^a q^b$ are the integers $p^k q^l$ where $0 \le k \le a$ and $0 \le l \le b$. So $\sigma(p^a q^b) = \sum_{k=0}^{a} \sum_{l=0}^{b} p^k q^l$
Notice that $\sigma(p^a) \cdot \sigma(q^b) = (1+p+\ldots+p^a) \cdot (1+q+\ldots+q^b) = 1 \cdot (1+q+\ldots+q^b) + p \cdot (1+q+\ldots+q^b) + \ldots + p^a(1+q+\ldots+q^b) = \sum_{l=0}^{b} 1 \cdot q^l + \sum_{l=0}^{b} p \cdot q^l + \ldots + \sum_{l=0}^{b} p^a \cdot q^l = \sum_{k=0}^{a} \sum_{l=0}^{b} p^k q^l = \sigma(p^a q^b)$.

(b) Argue that for a product of prime powers $\prod_{i=1}^{r} p_i^{a_i}$ (i.e. an r number of primes p_1 to p_r where each $a_i \ge 1$) that $\sigma(\prod_{i=1}^{r} p_i^{a_i}) = \prod_{i=1}^{r} \sigma(p_i^{a_i})$

Solution: We use proof by induction. We have shown $r = 2$ as a base case ($r = 1$ is trivial). Now suppose that for $r \ge 2$ that $\sigma(\prod_{i=1}^{r} p_i^{a_i}) = \prod_{i=1}^{r} \sigma(p_i^{a_i})$. Now consider the product $\prod_{i=1}^{r+1} p_i^{a_i}$ (where we simply add another prime p_{r+1} to the product). The factors of this number are of the form $p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r} \cdot p_{r+1}^{b_{r+1}}$ (where for each i: $0 \le b_i \le a_i$), such that:

$$\sigma(\prod_{i=1}^{r+1} p_i^{a_i}) = \sum_{b_{r+1}=0}^{a_{r+1}} \sum_{b_r=0}^{a_r} \cdots \sum_{b_2=0}^{a_2} \sum_{b_1=0}^{a_1} p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r} \cdot p_{r+1}^{b_{r+1}}$$

Notice that:

$$\sigma(\prod_{i=1}^{r} p_i^{a_i}) \cdot \sigma(p_{r+1}^{a_{r+1}}) = (\sum_{b_r=0}^{a_r} \cdots \sum_{b_2=0}^{a_2} \sum_{b_1=0}^{a_1} p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r}) \cdot (1 + p_{r+1} + \ldots + p_{r+1}^{a_{r+1}})$$

$$= (\sum_{b_r=0}^{a_r} \cdots \sum_{b_2=0}^{a_2} \sum_{b_1=0}^{a_1} p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r} \cdot 1) + (\sum_{b_r=0}^{a_r} \cdots \sum_{b_2=0}^{a_2} \sum_{b_1=0}^{a_1} p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r} \cdot p_{r+1})$$

$$+ \ldots + (\sum_{b_r=0}^{a_r} \cdots \sum_{b_2=0}^{a_2} \sum_{b_1=0}^{a_1} p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r} \cdot p_{r+1}^{a_{r+1}})$$

$$= \sum_{b_{r+1}=0}^{a_{r+1}} \sum_{b_r=0}^{a_r} \cdots \sum_{b_2=0}^{a_2} \sum_{b_1=0}^{a_1} p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r} \cdot p_{r+1}^{b_{r+1}} = \sigma(\prod_{i=1}^{r+1} p_i^{a_i})$$

But by our inductive hypothesis $\sigma(\prod_{i=1}^{r} p_i^{a_i}) = \prod_{i=1}^{r} \sigma(p_i^{a_i})$, so we conclude that $\sigma(\prod_{i=1}^{r+1} p_i^{a_i}) = \prod_{i=1}^{r+1} \sigma(p_i^{a_i})$.

(c) Classify all forms of integers whose sum of their divisors is odd (e.g. 2 is such an integer: 1+2=3).

Solution: Let n be an integer with prime factorization $n = \prod_{i=1}^{r} p_i^{a_i}$. Then $\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{a_1})$. It is clear that $\sigma(n)$ will be odd if and only if each $\sigma(p_i^{a_i})$ is odd. Consider some particular prime in this factorization p_j.

- Case 1: p_j=2: Then $\sigma(p_j^{a_j}) = \sigma(2^{a_j}) = 1 + 2 + \ldots + 2^{a_j}$, where the sum from 2 to 2^{a_j} will always be even, then the addition of 1 makes $\sigma(2^{a_j})$ odd. So there is no restriction on the power of 2.

- Case 2: p_j is an odd prime: Then $\sigma(p_j^{a_j}) = 1 + p_j + \ldots + p_j^{a_j}$, where it is simple to show that a sum of odd integers is odd if and only if there are an odd number of terms in the sum, i.e. a_j is even. So we must restrict the powers of odd primes to be even.

We conclude that all integers with an odd sum of their divisors is of the form $n = 2^{a_1} \cdot \prod_{i>1} p_i^{a_i}$, where for each $i > 1$, a_i is even (a_1 may be any non-negative integer).

9. Prove that there exists a Fibonacci number whose last 2018 digits are all 9s.

Solution: Let $M = 10^{2018}$. Consider extending the Fibonacci sequence backwards so that $F_{-2} = -1 \equiv -1 \pmod{M}$. Note that since there are finitely many pairs of possible consecutive Fibonacci numbers (F_i, F_{i+1}), the Fibonacci numbers will eventually repeat, as it is an infinite sequence, and two consecutive Fibonacci numbers uniquely determines the next. Hence there will be some j such that $F_j \equiv -1 \pmod{M}$, for which $j > 0$ so $F_j > 0$.

Any positive number that is $-1 \pmod{M}$ ends in 2018 9s.

10. Each of the positive integers $a_1, a_2, \ldots, a_n$ is less than 2018. The least common multiple of any two of these is greater than 2018. Show that

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} < 2.$$

Solution: The number of integers from 1 to 2018 which are multiples of b is $\left\lfloor \frac{2018}{b} \right\rfloor$. From the problem, we know that no integer less than 2018 is divisible by two or more of the numbers $a_1, ..., a_n$. Then, the number of integers less that 2018 that is divisible by one of $a_1, ..., a_n$ is exactly

$$\left\lfloor \frac{2018}{a_1} \right\rfloor + \left\lfloor \frac{2018}{a_2} \right\rfloor + \cdots + \left\lfloor \frac{2018}{a_n} \right\rfloor.$$

Since this is at most the number of integers less than 2018, we get

$$\sum_{i=1}^{n} \left(\frac{2018}{a_i} - 1 \right) < \sum_{i=1}^{n} \left(\frac{2018}{a_i} \right) < 2018$$

$$2018 \sum_{i=1}^{n} \frac{1}{a_i} < 2018 + 2018$$

$$\sum_{i=1}^{n} \frac{1}{a_i} < 2.$$

11. Let a and b be positive integers such that $ab + 1$ divides $a^2 + b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Solution: IMO 1988 Q6.

"Nobody of the six members of the Australian problem committee could solve it. Two of the members were husband and wife George and Esther Szekeres, both famous problem solvers and problem creators. Since it was a number theoretic problem it was sent to the four most renowned Australian number theorists. They were asked to work on it for six hours. None of them could solve it in this time. The problem committee submitted it to the jury of the XXIX IMO marked with a double asterisk, which meant a superhard problem, possibly too hard to pose. After a long discussion, the jury finally had the courage to choose it as the last problem of the competition. Eleven students gave perfect solutions."

–Arthur Engel

Click for solution

12. Let $n \geq 2$ be an integer. Show that $m = 2n^2 - 1$ is the least natural number such that there exist n positive integers $a_1, a_2, \ldots, a_n$ satisfying

    1. $a_1 < a_2 < \ldots < a_n = m$
    2. All of $\frac{a_1^2+a_2^2}{2}, \frac{a_2^2+a_3^2}{2}, \ldots, \frac{a_{n-1}^2+a_n^2}{2}$ are perfect squares.

Solution: Notice that for any positive integers $b > a$, if $\frac{a^2+b^2}{2}$ is a perfect square then b must be somewhat greater than a. We shall make this precise.
Let $b = a + d$ where d is even (if not $\frac{a^2+b^2}{2}$ would not be an integer) then $\frac{b^2+a^2}{2} = \frac{a^2+(a+d)^2}{2} = a^2 + ad + \frac{d^2}{2}$.
Now $a^2 + ad + \frac{d^2}{2} > a^2 + ad + \frac{d^2}{4} = (a + \frac{d}{2})^2$, so in order for $a^2 + ad + \frac{d^2}{2}$ to be a perfect square it must be that $a^2 + ad + \frac{d^2}{2} \geq (a + \frac{d}{2} + 1)^2$. We would like to bound the difference d by a, hence solving this equation gives $d \geq \left\lfloor 2\sqrt{2a+2} \right\rfloor + 2$
Going back to the problem, essentially we want to see how small a_n can be. A natural way to do this is to choose $a_1 = 1$, and try to bound $a_2, \ldots a_n$ using the bound above. Indeed, assume that $a_i \geq 2i^2 - 1$ (this is true for a_1) then by what was proven above, $a_{i+1} \geq \left\lfloor 2\sqrt{2a_i+2} \right\rfloor + a_i + 2 = 2(i+1)^2 - 1$. Hence, by induction we have $m = a_n \geq 2n^2 - 1$, which is exactly what we want to prove. For such a value of m we can choose $a_i = 2i^2 - 1$ and the two conditions are satisfied.